WebSphere® Premises Server

IBM

Version 6.1.0.1

WebSphere Premises Server Information Center

Contents

Chapter 1. Welcome to the documentation

This section introduces features of the product documentation and of the information center in which you view the product documentation.

Intended audience

This information center is intended for people who are installing, administering, and maintaining the IBM® WebSphere® Premises Server solution.

This information center assumes that users have prior knowledge of or proficiency with WebSphere Application Server, WebSphere MQ, and DB2® for Linux®, UNIX®, and Windows® support. Training for these base 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.

Refer to each base product for details about administration and maintenance. You can find links to the base product documentation in the "Additional information" on page 413 section.

Using the documentation offline

Use these instructions to download and install the information center for WebSphere Premises Server on your local system.

Before you begin

These instructions require Internet access and a machine running on a Windows operating system to which you can download content. If you find a difference between these instructions and the instructions that accompany the IBM User Interface Help System Built on Eclipse that you download, follow the latter instructions.

1. Download the ZIP file that contains the IBM User Interface Help System Built on Eclipse to a machine running on the Windows operating system. The help system is a download available from the following IBM Web site: http://www.alphaworks.ibm.com/tech/iehs

   Note: The Requirements tab on IBM alphaWorks® Web page lists the platform requirements for the IBM User Interface Help System Built on Eclipse.

2. Extract the ZIP file content to a directory on your local system.

3. Read the installation instructions located in the installation_directory/ IBM_Help_301_Win/getting_started.html file, where installation_directory is the directory into which you extracted the ZIP file content. This file describes how to set up a local information center.

4. Run the installation_directory/IBM_Help_301_Win/ibm_help/help_start.bat file. If a browser window opens with an empty information center, then you are successful. If not, troubleshoot the issue beginning with the documentation that is provided in the getting_started.html file.

5. Run the installation_directory/IBM_Help_301_Win/ibm_help/help_end.bat file to stop the help system.

6. Download the documentation plug-in ZIP files from the product Library page: http://www.ibm.com/software/integration/premises_server/library/index.html

7. Extract the plug-in contents to the installation_directory/IBM_Help_301_Win/ibm_help/eclipse/plugins directory. See the getting_started.html document for more information on installing the plug-ins.

8. Start the help system using the installation_directory/IBM_Help_301_Win/ibm_help/help_start.bat file.

Results

Your documentation plug-in is available in your local help system. You can also download and use additional documentation plug-ins from other IBM or third-party vendors that use an Eclipse-based help system like the IBM User Interface Help System.

Conventions

The information center uses several typeface conventions for special terms and actions.

These conventions have the following meanings.

Type	Description of convention
Bold	**Boldface type** indicates commands or graphical user interface (GUI) controls such as names of fields, buttons, or menu choices.
Italic	*Italic type* indicates new terms, book titles, CD labels, or variable information that must be replaced by an actual value.
`Monospace`	Commands, command options, and flags that appear on a separate line, code examples, output, and message text appear like this, in `monospace type`. Names of files and directories, text strings you must type, when they appear within text, names of Java™ methods and classes, and HTML and XML tags also appear like this, in `monospace type`.

Note: The terms *edge controller*, *Data Capture and Delivery*, *remote Data Capture and Delivery*, and *local Data Capture and Delivery* all refer to the same functional concept, and can be used interchangeably most of the time. These terms refer to the portion of the RFID system that interfaces directly with the physical readers, collecting the raw data and performing some basic processing. Starting with the WebSphere RFID Premises Server 6.0 release, this functionality can run as part of the WebSphere Premises Server (local Data Capture and Delivery), or on a separate processor (remote Data Capture and Delivery) to distribute load. In previous versions of WebSphere RFID Premises Server, this functionality running on a remote processor was referred to as an edge controller. For simplicity and compatibility with previous versions of the product, the term edge controller is still used in the product documentation.

The following variables are used in this documentation:

- *IBM_RFID_HOME* is a variable for Windows and Linux that is defined during the installation of WebSphere Premises Server. On Windows, typing `echo %IBM_RFID_HOME%` at a command prompt shows you the path where WebSphere Premises Server is installed, such as C:\Program Files\IBM\RFID. On Linux,

typing `echo $IBM_RFID_HOME` at a command prompt shows you the path where WebSphere Premises Server is installed, such as /opt/IBM/RFID.

- *IHS_HOME* is a variable representing the installation path of IBM HTTP Server.
- *WAS_HOME* is a variable representing the installation path of WebSphere Application Server.

For reference, the WebSphere Premises Server default installation paths are:

Windows C:\Program Files\IBM\RFID

Linux /opt/IBM/RFID

Publications terms of use

Permissions for the use publications is granted subject to the following terms and conditions.

Personal Use: You may reproduce these publications for your personal, non commercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial Use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Chapter 2. System overview

System integrators use WebSphere Premises Server and its related products to implement sensor solutions for business problems. To learn more about this technology, refer to "What are sensors and actuators?"

One type of sensor solution uses RFID devices, such as tag readers, edge controllers, and WebSphere Premises Server. For more descriptions of supported scenarios in which these devices and servers are used, refer to "Example usage scenarios" on page 14.

WebSphere Premises Server also integrates with WebSphere RFID Information Center to enable solutions to manage and integrate RFID information with enterprise applications, as well as to securely share RFID information and events with selected trading partners in an EPCglobal standards-based repository.

The WebSphere Premises Server solution employs various agents and adapters to control I/O devices, filter tag information, and perform other tasks in the Data Capture and Delivery domain.

For more information on devices, Data Capture and Delivery controllers, and WebSphere Premises Server, refer to the topics under "Components" on page 9.

What are sensors and actuators?

A *sensor* is any device, such as a thermometer, that detects a physical condition in the world. *Actuators* are devices, such as valves and switches, that perform actions such as turning things on or off or making adjustments in an operational system. Companies can integrate sensors and actuators to create a closed-loop operational system between remote locations such as retail stores, distribution centers, or manufacturing sites and the enterprise applications used to run the business.

One form of sensor technology is radio frequency identification (RFID), a method of identifying distinct items using radio waves. RFID is based on tags that contain microscopic chips used to store information about the item to which it is attached. The tag also contains a small, flat antenna. If the tag contains a power source, it is an active tag. If it depends on the reader for power, then it is a passive tag.

A passive tag read is activated by the radio waves emitted by a tag reader. When the antenna in the RFID tag encounters these radio waves, it forms a magnetic field that allows the tag to draw power and send information back to the reader. An active tag read occurs when the RFID tag has its own power source for the antenna and emits a signal that can be tracked.

For more information on the possible business solutions with this technology, refer to IBM Sensors and actuators.

What is new in this release?

This topic describes new enhancements and features that are provided with WebSphere Premises Server 6.1.x.

Version 6.1 Fix Pack 1

Updated prerequisite software levels and support

This release includes updated levels of some of the prerequisite software, as well as support for new levels of software. See "Hardware and software requirements" on page 17 for details.

High availability

This fix pack release of WebSphere Premises Server supports a high availability topology. See "Planning your high availability topology" on page 16 to get started.

Migration

You can migrate WebSphere Premises Server from version 6.1 to version 6.1.0.1. See "Migrating the product" on page 66 to get started.

Flexible timer values for the PortalControllerAgent

In releases prior to WebSphere Premises Server 6.1 Fix Pack 1, each timer was associated with one timeout value. In Fix Pack 1, you can make a timeout value flexible, meaning you can apply one timer to different timeout values. See "Configuring the PortalControllerAgent to use flexible timer values" on page 108 for more details.

Changes in the WebSphere Premises Server Administrative Console

A Find and Install link has been added to the WebSphere Premises Server Administrative Console to allow you to download Data Capture and Delivery bundles. See "Downloading bundles" on page 177 for more information.

The Configuration Variables link in the console has been removed. You can see the system configuration by viewing the properties in the SystemAgent.

The **About** link was removed from the console. To find out how to retrieve version information, refer to "Checking the server version" on page 99.

SystemAgent

In previous releases of WebSphere Premises Server, you used the premises.properties file to make configuration changes to the system. In this fix pack release, the premises.properties file has been replaced by an agent called the SystemAgent. The SystemAgent is configurable through the WebSphere Premises Server Administrative Console like other agents. When you add or modify a property for this agent, there is a 60 second delay before it is available to the system.

Task agents

Event flows into and out of WebSphere Premises Server are now controlled by agents that are TaskAgentType, and which are configurable through the WebSphere Premises Server Administrative Console like other agents.

Importing XML

In this release, in addition to being able to import XML through the WebSphere Premises Server Administrative Console, you can also do it using a command line.

Print profile inbound servlet

A new servlet is available to update the status of inbound print profile topics. See "Print profile support" on page 199 for details.

ALE Administrative Console

This release of WebSphere Premises Server supports the Application Level Events (ALE) 1.1 specification. As part of this support, the product provides an ALE Administrative Console, which enables you to easily administer the ALE server. See "Managing ALE" on page 206 for details on this new console.

ALE 1.1 ECReports servlet

This new servlet builds on the event gateway servlet by accepting XML as input and then converting the XML into an IBM Sensor Event that is placed on the SIBus. You can use this servlet to get ALE events from Data Capture and Delivery to WebSphere Premises Server ALE. See "ALE 1.1 ECReports servlet" on page 222 for details.

Reusable Event Monitor

The Reusable Event Monitor component enables WebSphere Premises Server applications to include dynamic event information. See "Reusable Event Monitor component and sample user interface" on page 375 for details.

Updates in Data Capture and Delivery

A Write to Tag Profile has been added to Device Kit. For more information, see the Device Kit documentation available at: http://www.eclipse.org/ohf/components/soda/.

New Data Capture and Delivery agents have been added to the configuration:
- "Test Tag agent" on page 148
- "ID Transformation agent" on page 126
- "Log File agent" on page 129

See "Agent details" on page 111 for a complete list of agents.

Version 6.1

Product name

The WebSphere RFID Premises Server product is now called WebSphere Premises Server.

Installer

WebSphere Premises Server now uses an installation wizard that installs all of the prerequisite software for you. For details on using this installer, see "Installing the product" on page 26.

WebSphere RFID Device Infrastructure support

Support for WebSphere RFID Device Infrastructure 1.1.1 has been removed from this release.

Device Manager server support

WebSphere Premises Server 6.1.x no longer packages Device Manager server. If you have Device Manager server from WebSphere Premises Server 6.0, you can still use it with this version of WebSphere Premises Server.

Bundle loader

Instead of using Device Manager server, this release uses a bundle loader, which is an OSGi bundle that locates a list of bundles and performs the action specified on each bundle in the list once it is started. For more information on using this bundle, see "Installing a remote Data Capture and Delivery controller" on page 72.

Event flow

WebSphere Premises Server uses a new event format, called the "IBM Sensor Event" on page 217, and has a new event flow which leverages the WebSphere Application Server service integration bus (SIBus). For more information on this new event flow, refer to "Managing event processing" on page 178.

Location Awareness Services for WebSphere Premises Server

The Location Awareness Services for WebSphere Premises Server component is included in this release of WebSphere Premises Server. Location Awareness Services for WebSphere Premises Server provides a visual console that automatically locates the active tags that are monitored in real time. Personnel or assets can be monitored in virtual danger zones and Location Awareness Services for WebSphere Premises Server will send safety and security breach alerts if assets or personnel are not qualified for entry or exit. For more information, see Chapter 7, "Location Awareness Services for WebSphere Premises Server," on page 235.

Print profiles

This release introduces a new way of printing using profiles to send and receive messages through the WebSphere Application Server service integration bus. For more information, refer to "Managing printing" on page 198.

EPCIS Connector sample application

This release provides an EPCIS Connector sample application to convert tag reads and aggregated tag read generic events into EPCIS XML events, messages that adhere to a standard EPCIS schema, that then are augmented with information either from the database or from the generic event. For more information, refer to "EPCIS Connector sample application" on page 375.

Changes in the WebSphere Premises Server Administrative Console

The WebSphere Premises Server Administrative Console now supports Mozilla Firefox and Internet Explorer 7.0 Web browsers.

WebSphere Premises Server uses Business Intelligence and Reporting Tools (BIRT), an Eclipse-based open source reporting system, to run and display the tag read reports within the WebSphere Premises Server Administrative Console. For more information, see "Reporting" on page 207.

Tivoli® Provisioning Manager for Software

WebSphere Premises Server provides Tivoli Provisioning Manager for Software SPD files for WebSphere Application Server, DB2 for Linux, UNIX, and Windows and WebSphere MQ running on Windows platforms only. For more information, see "Installing using Tivoli Provisioning Manager for Software" on page 53.

Components

WebSphere Premises Server

WebSphere Premises Server is an application platform for sensor solutions, such as RFID, at the local premises. For example, the premises might be a retail store, distribution center, or manufacturing facility.

WebSphere Premises Server contains an administrative console that an operator uses to configure and manage the system. WebSphere Premises Server can also be set up to perform additional tag processing.

WebSphere Premises Server consists of WebSphere Application Server, DB2 for Linux, UNIX, and Windows systems (or Oracle), WebSphere MQ, MicroBroker, Data Transformation, Data Capture and Delivery, and a Web application for the administrative console.

Data Transformation is the bridge between MicroBroker and WebSphere MQ. Data Capture and Delivery interfaces directly with logical and physical devices, collecting raw data and performing some basic processing, and the IBM Data Capture and Delivery Toolkit for WebSphere Premises Server allows you to customize the sample agents shipped with the product.

In addition to the IBM Data Capture and Delivery Toolkit for WebSphere Premises Server, WebSphere Premises Server includes the WebSphere Premises Server Toolkit, which provides an environment for you to create and test custom applications.

WebSphere Premises Server includes several example applications: the Warehouse Management sample, Print, Verify, and Ship, Standard Dock Door Receiving, and Enhanced Dock Door Receiving example applications.

WebSphere Premises Server also includes Tivoli Resource Models for WebSphere Application Server and WebSphere MQ that monitor WebSphere Premises Server. Software Package Definition (SPD) files are also provided for the WebSphere Premises Server components, for optional installation using Tivoli Provisioning Manager for Software.

Data Capture and Delivery

Data Capture and Delivery communicates with RFID devices and then communicates that information to WebSphere Premises Server.

Data Capture and Delivery is organized as a system of agents that use the publish/subscribe model to communicate with each other. Agent to agent communication is done through the notification service built upon the OSGi's Event Admin Service, which is an open standard communication mechanism. Data Capture and Delivery communicates with WebSphere Premises Server through the MicroBroker, which connects to the remote servers and acts as an embedded gateway that provides quality of service, persistent messaging, and seamless bridging. A notification service to MicroBroker enables the flow of messages between the agents on the Data Capture and Delivery controller and the MicroBroker using the topic names.

When WebSphere Premises Server receives events from Data Capture and Delivery, it processes them using various J2EE components that use application specific interfaces to communicate with the enterprise and business domain.

Data Capture and Delivery controller

A Data Capture and Delivery controller is a computer located near the edge of the RFID system. It is the network node that controls a set of I/O devices on the edge of the system, for example the motion sensors, antennae, and light tree of a dock door in a distribution center.

Note: The terms *edge controller*, *Data Capture and Delivery*, *remote Data Capture and Delivery*, and *local Data Capture and Delivery* all refer to the same functional concept, and can be used interchangeably most of the time. These terms refer to the portion of the RFID system that interfaces directly with the physical readers, collecting the raw data and performing some basic processing. Starting with the WebSphere RFID Premises Server 6.0 release, this functionality can run as part of the WebSphere Premises Server (local Data Capture and Delivery), or on a separate processor (remote Data Capture and Delivery) to distribute load. In previous versions of WebSphere RFID Premises Server, this functionality running on a remote processor was referred to as an edge controller. For simplicity and compatibility with previous versions of the product, the term edge controller is still used in the product documentation.

Data Capture and Delivery controllers control I/O devices, filter tag information, and send tag information to the WebSphere Premises Server for additional processing. The Data Capture and Delivery software consists of various agents that are delivered as OSGi bundles and activated on the Data Capture and Delivery controller. These agents facilitate the delivery of tag information that is captured by the Data Capture and Delivery controller from the I/O devices and delivered to the WebSphere Premises Server through the MicroBroker.

WebSphere Premises Server supports several Data Capture and Delivery controllers. For information on the IBM device validation program and supported devices, refer to the IBM Ready for WebSphere Premises Server solutions page at: http://www-304.ibm.com/jct09002c/gsdod/weblistfilter.do?prog=RFWSRFID &tab=1

The components include:
- Device agents - Interface to RFID device functions.
- Location agents - Interface to I/O device functions and filter and aggregate tag data before passing the data to the MicroBroker and up to the WebSphere Premises Server.

- Controller agents - Coordinate actions on the edge controller. For example, a controller agent can implement a state machine that subscribes to topics published by motion sensors, and trigger tag reads for specified time periods.

There are also additional agents to transform data formats, manage configuration, handle alerts, and manage general health notification.

For more information on OSGi and bundles, go to the OSGi Alliance web site at www.osgi.org. Refer to the OSGi Techology page for an overview of how OSGi works.
- OSGi Alliance home page
- OSGi Technology overview

Devices

RFID devices provide an I/O interface for processing RFID data.

RFID devices can send the tag information to the Data Capture and Delivery controller and receive information from the controller. Each device has its own protocol. The device adapters hide the protocol differences from the application software on the Data Capture and Delivery controller.

Tag readers are one kind of device that uses radio frequency antennas to scan for tags and read information from the tags and then sends the data to the Data Capture and Delivery controller.

For information on the IBM device validation program and supported devices, refer to the IBM Ready for WebSphere Premises Server solutions page at: http://www-304.ibm.com/jct09002c/gsdod/weblistfilter.do?prog=RFWSRFID &tab=1

Agents

Agents perform several functions. They connect adapters to the publish and subscribe applications. For example, the reader agent connects the reader adapter to the messaging service. They also act as controllers for the I/O environment and filters for tag information.

Agents for RFID are distributed as example code.

Reader Agents
> Agents for each reader adapter, connecting the adapter to the messaging service. Reader agents are available as open source. As part of the open-sourcing, the reader API was subdivided into *reader profiles*, each representing a specific subset of the API to support a type of use case. Vendors are responsible to update and maintain their implementation of the API specific to their reader. See "Device Kit" on page 12 for more information about these profiles.

I/O Agents
> Agents for each I/O Adapter, connecting the adapter to the messaging service.

Portal Controller Agents
> An agent that defines the possible states, transition triggers, and state/transition actions as a result of sensor inputs (timers are also supported). The product ships with the following options:
> - Basic Dock Door Receiving: Once the portal is activated, this matrix will cycle the reader on and off.

- Standard Dock Door Receiving: This option uses only a motion sensor (and optional switch), and is described in "Standard dock door receiving example usage scenario" on page 351.
- Enhanced Dock Door Receiving: This option uses a motion sensor and a light barrier, and is described in "Enhanced dock door receiving example usage scenario" on page 352.

Filter Agents

Agents that filter and aggregate tag data before passing the data to the WebSphere Premises Server.

For information on the IBM device validation program and supported devices, refer to the IBM Ready for WebSphere Premises Server solutions page at: http://www-304.ibm.com/jct09002c/gsdod/weblistfilter.do?prog=RFWSRFID &tab=1

Adapters

Adapters interface with hardware components, for example, tag reader devices and I/O devices such as light trees and motion sensors.

Adapters are written using Device Kit which is a framework for quickly creating Java API-level interfaces to attached devices, for example tag readers, tag printers, motion sensors, light trees, and I/O boards. It allows a common development model for interfacing with varying devices.

Reader Adapters

Interface with the readers. This module is the API-level interface to a specific make and model of a tag reader. It enables complete access to the capabilities of the tag reader. There is a reader adapter for each tag reader model. Reader adapter are only available as open source.

I/O Adapters

Interface with the I/O devices such as light trees and motion sensors. This module is the API-level interface to the particular device, and it is device-specific. It enables complete access to the capabilities of the device.

For information on the IBM device validation program and supported devices, refer to the IBM Ready for WebSphere Premises Server solutions page at: http://www-304.ibm.com/jct09002c/gsdod/weblistfilter.do?prog=RFWSRFID &tab=1

MicroBroker

The OSGI high-speed publication/subscription engine, Event Admin, is used for internal communications within Data Capture and Delivery; however, Event Admin only supports communication within the same JVM. Therefore, MicroBroker is used to interface externally with WebSphere Premises Server. MicroBroker is a publication/subscription engine that supports remote communication using TCP/IP.

Device Kit

The Device Kit is a core component of IBM Data Capture and Delivery Toolkit for WebSphere Premises Server. It provides a common interface for the application code to interact with RFID readers and other device sensors and actuators.

The Device Kit is an OSGi enabled technology that provides support for interfacing with hardware devices from Java code. The Device Kit can be used to split the serialized dependency that software development has on hardware platform

development. Application code and business logic interface with the Device Kit to get information from the hardware device. It provides a layer of abstraction against which applications can be developed for devices even when hardware-specific information is unknown.

The Device Kit environment consists of the following components: an application, a runtime, and a hardware device. The runtime is divided into the adapter and profile layer, device layer, transport layer, and the connection layer.

Connection layer

The connection layer supports the reading and writing of byte streams to the hardware device. The connection does not understand the meaning of the bytes but supports the delivery of the output bytes and receiving of the input bytes.

Transport layer

The transport layer supports the sending and receiving of messages. While the transport layer understands the format of a message, it does not understand the meaning of the message. When a device requests that a message to sent, the transport formats the message into a correct bytes to be written to the connection. The transport reads input bytes from the connection and parses the bytes into received messages. The interested devices are notified of the received messages.

Device layer

The device layer provides the application with an interface to the hardware device. The device layer should shield the application from the low level details of the hardware device. The device layer understands the meaning of the messages and any parameters within a message. When an application executes a command, the command requests that the transport send the command message. Any signals listeners are notified if any received messages from the transport match the signal messages.

Adapter and profile layer

The adapter and profile layer provides the application with common interface to a set of common hardware devices. For example, the adapter and profile layer for RFID readers will provide a common interface for the application to a set of common functions provided by all RFID readers. This layer uses a publish/subscribe Service Oriented Architecture (SOA) interface. The adapter and profile should shield the application from the knowing which of the common hardware device is being used.

Data Capture and Delivery profiles

The following profiles are used in the scenarios provided in Data Capture and Delivery:
- GPIO Profile – specifies the interface to general purpose I/O. It provides measurement values for the current states of input and output pins. It supports the ability to set the value of output pins through a command interface as well as triggering the state of an output pin with an LDAP expression.
- RFID Inventory Profile – controls RFID tag reading, tag filtering, and aggregation reporting. This profile supports starting and stopping the reading mode, providing tag data in a common format, filtering tags as duplicates or by

interest masks, collecting tags into an aggregation report, and marking tag reports with metadata called data extensions. The RFID Inventory Profile can be configured to trigger reading, filtering, and aggregating behavior based on events published by the GPIO Profile and Control Profile.

- Control Profile – provides a set of control values, represented by bit or long values, which can be manipulated by software. In addition to bit and long values being set by a direct command, the value of the bit controls can be determined by an LDAP expression.

Resources

The Device Kit is available in the open source domain provided under the Eclipse Public License. Runtime, tooling, documentation, and source code are available at the following URL: http://www.eclipse.org/ohf/components/soda/

Location Awareness Services for WebSphere Premises Server

Location Awareness Services for WebSphere Premises Server allows companies to continuously track active tags in real time in predefined areas of refineries, plants, and office buildings. Third-party asset location systems provide the tags, which may be carried by employees or visitors, or fixed to assets. Third-party systems also include reader infrastructure and a location engine, which is software that calculates tag positions based on the tag signals received by different readers. The Location Awareness Services for WebSphere Premises Server solution works with these systems to visualize locations that are being monitored and to display the current position of personnel or assets carrying the tags.

For more information, see "What is Location Awareness Services for WebSphere Premises Server?" on page 235.

Example usage scenarios

WebSphere Premises Server provides several product usage scenarios and samples. Usage scenarios provide an outline of the events that occur when a user or the application performs a particular action.

- "Standard dock door receiving example usage scenario" on page 351
- "Enhanced dock door receiving example usage scenario" on page 352
- "Print, Verify, and Ship example usage scenario" on page 356

For more details about these usage scenarios and for information on the samples shipped with WebSphere Premises Server, such as the "EPCIS Connector sample application" on page 375 and the "Reusable Event Monitor component and sample user interface" on page 375, see Chapter 8, "Use cases and samples," on page 351.

Chapter 3. Installing and configuring

These topics describe how to install WebSphere Premises Server and its components.

Preparing for installation

Use these topics to plan and prepare for your WebSphere Premises Server installation.

Planning your single server topology

Use the scenarios described in this section to plan for your installation of WebSphere Premises Server.

Possible topologies

WebSphere Premises Server supports the following topology options:
- A locally installed or remote database server, which can be either Oracle or DB2
- A locally installed or remote Bundle Repository Server
- Optional Location Awareness Services for WebSphere Premises Server component on Windows using a DB2 database

Installation scenarios

During the product installation, you are prompted for the available tasks the installer performs.

The first task is to choose your database server. If you decide to use an existing installation of either DB2 or Oracle, you will need to provide the server information for the installer. If you decide to use the installer to install DB2 (either remotely or locally), then the installer can do that. The installer cannot install an Oracle database.

The second task is to install WebSphere Premises Server, and optionally Location Awareness Services for WebSphere Premises Server.

Restriction: Location Awareness Services for WebSphere Premises Server must be installed on a Windows operating system on the same server as WebSphere Premises Server.

With this second installation task, you also have the option of installing both the WebSphere Premises Server and the Bundle Repository Server on the same server in your environment, or you can install the Bundle Repository Server on a separate server.

For example, if you install WebSphere Premises Server and the Bundle Repository Server on Server A, and then install an additional WebSphere Premises Server on Server B, both premises servers can use the Bundle Repository Server on Server A. You can also install the Bundle Repository Server on Server C and install only WebSphere Premises Server on Servers A and B. Again, both premises servers can use the Bundle Repository Server on Server C.

> **Restriction:** Your database server and WebSphere Premises Server must be installed on servers with the same operating system.

Planning your high availability topology

This topic helps you plan the topology of high availability for your WebSphere Premises Server.

Requirements

- Setting up a high availability system requires a WebSphere Premises Server Central Site Server license.
- All servers in the high availability system must run the same operating system.
- All cluster members must have the prerequisite software installed in the same path as the central server.

See "Prerequisite steps for a high availability system" on page 20 for more information on prerequisites.

Topology

A WebSphere Premises Server high availability topology consists of the following:

- WebSphere Premises Server deployed in a WebSphere clustered configuration
- A centralized database
- A centralized WebSphere MQ server
- WebSphere Application Server Network Deployment components, which are installed on a machine called the *cluster controller*.

> **Note:** WebSphere Application Server Network Deployment does not support local operating system security. If you need to enable security in your environment, use LDAP or the custom user registry.

The following points apply to the sample configuration diagram pictured below:

- Only two nodes are pictured in this sample, but there can be *n* number of nodes in your configuration.
- The two servers with WebSphere Application Server that are not part of the cluster contain some WebSphere Premises Server components as well, such as the messaging gateway. The WebSphere Application Server pictured in the background is in passive standby, while the one in the foreground is active.
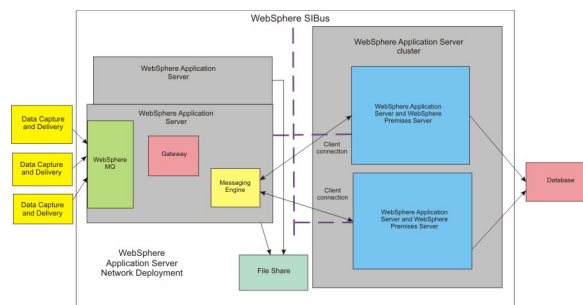
Packaging

The packaging for WebSphere Premises Server includes the following software products.

- Disk 1 - Quick Start, including product documentation
- Disk 2 (DVD format)
  - WebSphere Premises Server for Windows and its prerequisite middleware
  - WebSphere Premises Server SPDs for installing with Tivoli Provisioning Manager for Software on Windows
  - WebSphere Application Server 6.1 Supplements for Windows
  - WebSphere Application Server 6.0 Edge Components for Windows (optional)
- Disk 3 (DVD format)
  - WebSphere Premises Server for Linux and its prerequisite middleware
  - WebSphere Application Server 6.1 Supplements for Linux
  - WebSphere Application Server 6.0 Edge Components for Linux (optional)
- Disk 4
  - WebSphere Premises Server Toolkit
- Disk 5 - IBM Data Capture and Delivery Toolkit for WebSphere Premises Server, including Eclipse and Equinox
- Disk 6 - High Availability for WebSphere Premises Server Central Site Server on Windows (available only with a Central Site Server license)
- Disk 7 - High Availability for WebSphere Premises Server Central Site Server on Linux (available only with a Central Site Server license)

Additional software

Additional software and components are available for purchase:

- Location Awareness Services for WebSphere Premises Server for Windows

  Location Awareness Services for WebSphere Premises Server is an optional component that allows you to continuously track active tags in real time in predefined areas.
- Sensor Data Services for WebSphere Premises Server for Windows or Linux

  Sensor Data Services for WebSphere Premises Server installs WebSphere Premises Server on an existing WebSphere Remote Server installation.

Prerequisites

Use these topics to prepare for your WebSphere Premises Server installation.

Hardware and software requirements
Hardware requirements

Supported hardware for WebSphere Premises Server includes servers that meet the minimum hardware criteria defined below.

Table 1. Minimum supported hardware for WebSphere Premises Server

Processor	Memory (RAM)	Free Disk Space	Temporary disk space during installation
3 GHz Pentium® 4	3 GB	10 GB	1 GB

A two-processor configuration is recommended.

The following hardware is required for Location Awareness Services for WebSphere Premises Server *in addition* to what is listed in Table 1:

Table 2. Additional hardware required for Location Awareness Services for WebSphere Premises Server

Processor	Memory (RAM)	Free Disk Space	Temporary disk space during installation
3 GHz or more	1 GB recommended	500 MB	100 MB

The system for the Location Awareness Services for WebSphere Premises Server Spatial Management Client must meet the following minimum requirements:

- Memory (RAM): 512 MB or more
- CPU: 1 GHz or more
- Monitor resolution: 1024 by 768 pixels, 1280 by 1024 pixels, or higher
- A LAN connection (100 M-bit or more)

Software requirements

Operating systems

WebSphere Premises Server supports the following operating systems:

- > Windows Windows Server 2003 Standard or Enterprise editions with Service Pack 2, or Windows Server 2003 R2 Standard or Enterprise editions with Service Pack 2
- > Linux SUSE Linux Enterprise Server V9.3 (Kernel 2.6), or SUSE Linux Enterprise Server V10.1

Notes:

- See the WebSphere Premises Server system requirements page for the latest information about supported operating platforms.
- A high availability WebSphere Premises Server topology is not supported on SUSE Linux Enterprise Server V9.3.
- Location Awareness Services for WebSphere Premises Server only supports the Windows platforms listed. It does not support Linux platforms.
- A high availability WebSphere Premises Server topology is not supported with Location Awareness Services for WebSphere Premises Server.

Browsers and other GUI software

In order to use the WebSphere Premises Server Administrative Console, you must have Mozilla Firefox or Internet Explorer 6.0 or later installed on your operating system and JavaScript™ enabled.

The following software is required on the systems where you install the Location Awareness Services for WebSphere Premises Server Spatial Management Client:

- Internet Explorer 6.0
- Adobe® Scalable Vector Graphics (SVG) Viewer

Middleware

The following software is required for WebSphere Premises Server. These software packages are installed with WebSphere Premises Server, with the exception of Oracle. See "Packaging" on page 16 for more details on how the software is delivered.

- WebSphere Application Server 6.1.0.17
- IBM HTTP Server 6.1.0.17
- WebSphere MQ 6.0.2.3
- DB2 for Linux, UNIX, and Windows 9.1.4 Enterprise Server Edition, or Oracle 10.2.0.2 (10g driver) or Oracle 11g with the patched ojdbc5.jar file. See http://www.oracle.com/technology/software/tech/java/sqlj_jdbc/htdocs/jdbc_111060.html to download the patched file.

    Installation tip: If you use an Oracle database on a remote server, you must have the Oracle client on your server with WebSphere Premises Server.

Notes:

- DB2 for Linux, UNIX, and Windows 9.1.4 Workgroup Server Edition and DB2 for Linux, UNIX, and Windows 9.5.2 are also supported, but not packaged with WebSphere Premises Server.
- If you are using Oracle with a Linux operating system, the Oracle 10g driver can be installed on SUSE Linux Enterprise Server 9 or later versions, but Oracle 11g can only be installed on SUSE Linux Enterprise Server 10 and later versions.
- Location Awareness Services for WebSphere Premises Server only supports the DB2 database versions listed. It does not support Oracle.

You can optionally use the following Tivoli products to install and manage your network:

- Tivoli Omegamon XE for Messaging for Distributed Platforms 6.0.1 (optional)
- Tivoli Composite Application Manager for WebSphere 6.1 (optional)
- Tivoli Enterprise Console® 3.9 Fix Pack 6 (optional)
- Tivoli Provisioning Manager for Software 5.1.0.2 (optional)
- IBM Tivoli Monitoring 6.2 (optional)
- IBM Tivoli Monitoring for Databases 6.2 (optional)

Tivoli Provisioning Manager for Software Software Package Definition (SPD) files: WebSphere Premises Server provides Tivoli Provisioning Manager for Software SPD files for WebSphere Application Server, DB2 for Linux, UNIX, and Windows platforms and WebSphere MQ running on Windows platforms only. You can use Tivoli Provisioning Manager for Software to install and configure these prerequisites on WebSphere Premises Server. For instructions on how to do this, refer to "Installing using Tivoli Provisioning Manager for Software" on page 53.

Prerequisite configuration

This topic contains prerequisite information for installing WebSphere Premises Server.

Before installing WebSphere Premises Server, identify the hardware and software you require, and then refer to the topics below for any additional prerequisites.

- "Configuring Linux for the prerequisite software" on page 20
- "Configuring Internet Explorer" on page 20

- "Configuring Mozilla Firefox"

Important: If you do not plan to verify the installation after installing the software, be sure to turn off the simulated reader which is turned on by default. Turning off the simulated reader helps system performance. Refer to the topic, Verifying the installation, for instructions.

Configuring Linux for the prerequisite software:
About this task

You must perform the following tasks to run the prerequisite software on Linux platforms:

1. Prepare the Linux operating system for WebSphere Application Server.
2. Prepare the SUSE Linux Enterprise Server operating system for WebSphere Application Server.
   - SUSE Linux Enterprise Server 9
   - SUSE Linux Enterprise Server 10
3. Prepare the Linux operating system for WebSphere MQ
4. Check for any entries in the /etc/hosts file that include the IP address, 127.0.0.2, and comment them out before installing WebSphere Premises Server.

Configuring Internet Explorer:
About this task

By default, Internet Explorer has scripting disabled when it is installed. You must enable scripting to use the WebSphere Premises Server Administrative Console with Internet Explorer.

1. In the browser, navigate to **Tools** → **Internet Options**.
2. Select the **Security** tab.
3. Click **Custom Level**.
4. Scroll down to **Scripting** → **Active Scripting**, and click **Enable**.
5. Click **Ok**, and then click **Ok** again.

Configuring Mozilla Firefox:
About this task

By default, Mozilla Firefox has scripting enabled when it is installed. If you have disabled it, make sure to re-enable it so that you can use the WebSphere Premises Server Administrative Console with Mozilla Firefox.

1. In the browser, navigate to **Tools** → **Options**.
2. Select **Content**.
3. Mark the check box next to **Enable JavaScript**, and click **Ok**.

Prerequisite steps for a high availability system

Follow the steps in this topic to prepare for your high availability system installation with WebSphere Premises Server.

Before you begin

Remember: Setting up a high availability system requires a WebSphere Premises Server Central Site Server license.

1. Install WebSphere Premises Server on a central server.

Be sure to verify that your installation is successful, and that your environment is set up for remote Data Capture and Delivery controllers. See "Planning your high availability topology" on page 16 and "Installing a remote Data Capture and Delivery controller" on page 72 for more information.

You can install WebSphere Premises Server with Location Awareness Services for WebSphere Premises Server on your central server, but the Location Awareness Services for WebSphere Premises Server applications will not run in a cluster.

2. Create a deployment manager profile on your WebSphere Premises Server central server. For details on how to do this, see Creating a deployment manager profile.

   Note: Do not federate your WebSphere Premises Server into the network deployment environment.

3. On a cluster node server, install the following prerequisite software:
   - WebSphere Application Server 6.1.0.17
   - a database client, either DB2 for Linux, UNIX, and Windows or Oracle. See the WebSphere Premises Server software requirements for more information.
   - a WebSphere MQ 6.0.2.3 client. To install this, copy the contents of the *MQ_INSTALL_ROOT*\java\lib\ directory from your central server to same path on your node server. *MQ_INSTALL_ROOT* is the installation path for WebSphere MQ.

   Important:
   - All servers in the high availability system must run the same operating system.
   - A high availability WebSphere Premises Server topology is not supported on SUSE Linux Enterprise Server V9.3.
   - All cluster members must have the prerequisite software installed in the same path as the central server.
   - You cannot have duplicate node names in the same cell. For example, the central server is called PremisesNode, so none of the cluster members can have that same node name. If you have two servers with the same node name, then you will need to drop the WebSphere Application Server profile and recreate it with a new name to continue with the high availability topology.

   For more detailed information on clustering, see Creating clusters.

4. On the cluster node server, federate the WebSphere Application Server nodes to WebSphere Application Server Network Deployment (deployment manager) running on the central server. To do this, run the addNode command:

   ```
   addNode WASND_host WASND_SOAP_port
   ```

   Tip: Make sure the deployment manager has been started on the central server before trying to federate the nodes.

5. Optional: Delete servers from WebSphere Application Server Network Deployment.
   a. Open the WebSphere Application Server Network Deployment administrative console.
   b. Navigate to **Servers** → **Application servers**. You will see all servers from each cluster node.
   c. Select all servers and delete them.
   d. Save the master configuration.

6. If you have WebSphere Application Server security enabled, disable it. The installer cannot run properly with security enabled.

7. Restart the deployment manager, all node agents, and all servers.

What to do next

Follow the instructions for "Installing a high availability system" on page 46.

Toolkit prerequisites

This topic contains prerequisite information for installing the toolkits available with WebSphere Premises Server.

Prerequisites for WebSphere Premises Server Toolkit

WebSphere Premises Server Toolkit requires the following hardware and software.

Hardware
- 2 GHz Pentium 4 (3 GHz preferred)
- 2 GB RAM

Software
- ![Windows] Windows XP, or Windows Server 2003 Standard or Enterprise editions with Service Pack 2, or Windows Server 2003 R2 Standard or Enterprise editions with Service Pack 2

    Note: WebSphere Premises Server Toolkit is not supported on Linux.
- Rational® Application Developer for WebSphere Software 7.0.0.5
- DB2 for Linux, UNIX, and Windows 9.1.4 Enterprise Server Edition, or Oracle 10.2.0.2 (10g driver) or Oracle 11g with the patched ojdbc5.jar file. See http://www.oracle.com/technology/software/tech/java/sqlj_jdbc/htdocs/jdbc_111060.html to download the patched file.

    Installation tip: If you use an Oracle database on a remote server, you must have the Oracle client on your server with WebSphere Premises Server.
- IBM HTTP Server 6.1.0.17
- WebSphere MQ 6.0.2.3
- WebSphere Application Server 6.1.0 Fix Pack 17 installed on the WebSphere Application Server runtime that is installed with Rational Application Developer for WebSphere Software

Note: DB2 for Linux, UNIX, and Windows 9.1.4 Workgroup Server Edition and DB2 for Linux, UNIX, and Windows 9.5.2 are also supported, but not packaged with WebSphere Premises Server.

Prerequisites for IBM Data Capture and Delivery Toolkit for WebSphere Premises Server

This toolkit requires the following software:
- ![Windows] Windows XP

In addition, Eclipse 3.3.2 is required for the toolkit. Eclipse can be installed by extracting the eclipse-SDK-3.3.2-win32.zip file into a local directory. The .zip file is available on the disk containing the IBM Data Capture and Delivery Toolkit for WebSphere Premises Server.

If you intend to extend the IBM Data Capture and Delivery Toolkit for WebSphere Premises Server, it is recommended that you compile all code changes against the OSGi/Minimum-1.1 specification. A reference specification is contained in the ee.minimum.jar file that you can download from OSGi at http://www2.osgi.org/ Release4/Download. Specifically, for WebSphere Premises Server 6.1.x versions, you need Release 4 Version 4.1, available at http://www.osgi.org/Download/ Release4V41.

This environment is recommended for small hardware platforms that run a very minimal Java environment. If you do not need to deploy IBM Data Capture and Delivery Toolkit for WebSphere Premises Server on such a platform, then you may choose to use a larger environment, such as CDC/Foundation. If you use an OSGi/Minimum-1.1 environment, your code will be able to run on larger Java environments as well.

Configuring the installation program paths

Use the steps in this topic to modify the default paths used by the deployment wizard.

Changing the deployment package path:
About this task

The installer copies its deployment packages temporarily to a default path:

> Windows   C:\Program Files\SolutionFiles\wizard\1
> Linux   /opt/SolutionFiles/wizard/1

The installer also copies additional temporary files used for installation to a location specified by the TEMP environment variable. If you want to change the location of the temporary installer files, modify the TEMP environment variable settings.

If you do not have a large partition for the default drive, there can be problems when you try to install the product because large amounts of data are temporarily copied to that location.

Note: After installation is complete, the only files that remain in that default deployment file path are the log files for the deployment wizard.

Use these steps to define the location where the deployment package files are copied after you have already started the installation program.

1. Click **Edit → Preferences** in menu on the Welcome panel.
2. The Deployment Preferences panel appears and you can modify the deployment package path to your desired location.
3. Click **OK** when you are finished with your changes to return to the Welcome panel.

Changing the deployment wizard path: The default path for the deployment wizard is:

> Windows   C:\Program Files\SolutionFiles

> **Linux** /opt/SolutionFiles

You can modify the location of this default path by changing the setting for the `installLocation.value` variable. This setting controls the file path for the location of the deployment wizard on the server. All log files are consolidated in a logs subfolder and left behind after the deployment wizard runtime is removed. There are two ways to change this location variable:

- From a command line, issue the following command, replacing *path* with your desired location:

    > **Windows** `WindowsSetup.exe -W installLocation.value="path/SolutionFiles"`

    > **Linux** `LinuxSetup.exe -W installLocation.value="path/SolutionFiles"`

- Or, before running the installation program, open the IRU_install.iss file and change the value of `$D(install)` in this line to reflect your desired location:

    `-W installLocation.value="$D(install)/SolutionFiles`

Restriction: There is a known limitation with the installation of WebSphere MQ where you cannot install to a directory other than the default one. See APAR IC47296 for more information.

Prerequisite software files

If you do not choose to have the installation wizard install the prerequisite software for WebSphere Premises Server, you can extract the compressed files and install the products separately.

File locations

Windows

These files are located on Disk 2.
- *disk_root*\sat_installer\bin\com\ibm\jsdt\webserver\tree\db2win.xx.jar
- *disk_root*\sat_installer\bin\com\ibm\jsdt\webserver\tree\ihswin.xx.jar
- *disk_root*\sat_installer\bin\com\ibm\jsdt\webserver\tree\ihsfpwin.xx.jar
- *disk_root*\sat_installer\bin\com\ibm\jsdt\webserver\tree\waswin.xx.jar
- *disk_root*\sat_installer\bin\com\ibm\jsdt\webserver\tree\wasupdateinstallerwin.xx.jar
- *disk_root*\sat_installer\bin\com\ibm\jsdt\webserver\tree\mqwin.xx.jar
- *disk_root*\sat_installer\bin\com\ibm\jsdt\webserver\tree\mq6rp2fp3win.xx.jar

Linux

These files are located on Disk 3.
- *disk_root*/sat_installer/bin/com/ibm/jsdt/webserver/tree/db2linux.xx.jar
- *disk_root*/sat_installer/bin/com/ibm/jsdt/webserver/tree/ihslinux.xx.jar
- *disk_root*/sat_installer/bin/com/ibm/jsdt/webserver/tree/ihsfplinux.xx.jar
- *disk_root*/sat_installer/bin/com/ibm/jsdt/webserver/tree/waslinux.xx.jar
- *disk_root*/sat_installer/bin/com/ibm/jsdt/webserver/tree/wasupdateinstallerlinux.xx.jar
- *disk_root*/sat_installer/bin/com/ibm/jsdt/webserver/tree/mqlinux.xx.jar
- *disk_root*/sat_installer/bin/com/ibm/jsdt/webserver/tree/mq6rp2fp3linux.xx.jar

Creating the database, tablespace, tables, and data

Use this topic to manually create the database, tablespace, tables, and populate the data required for WebSphere Premises Server. If you are using the WebSphere Premises Server installer to install and create the database, you do not need to follow these steps.

Creating the database manually:

Use these instructions when a Database Administrator creates the database and tablespace manually, and then the tables and data are created during the installation of WebSphere Premises Server.

About this task

If you are using Oracle, you should have been prompted to create the SID when you installed the product. If not, refer to the Oracle documentation to set up a SID.

Note: These instructions use the database name, IBMRFID, but you can use a different database name.

1. Create the WebSphere Premises Server database for DB2 or Oracle.

   For a local or remote DB2 database:

   a. Open the DB2 Control Center.

   b. Right-click **All Databases** and select **Create Database → Standard**.

      1) Enter IBMRFID as the database name.

         Note: Linux commands are case-sensitive.

      2) Select the option to **Enable database for XML (Code set will be set to UTF-8)**. For more information on this option, refer to the DB2 information center.

   c. Click **Finish**. Do not fine tune the database when it is created.

   d. Exit the DB2 Control Center.

   e. (Optional) Catalog the remote database, IBMRFID, to the local machine.

   For an Oracle database, use the Database Configuration Assistant to create the new database called IBMRFID. Be sure to select the Unicode AL32UTF8 character set.

2. Create the tablespace. You can use the SQL statements provided here or you can use the sample DDL files, amit_tablespace_db2.ddl and amit_tablespace_oracle.ddl, provided in the db_script directory on the WebSphere Premises Server CD. These DDL files can be run from a DB2 command line or from an Oracle sqlplus tool. You must update the tablespace file name and database installation path and make sure the directory and file can be created before running the DDL files or SQL statements.

   For DB2:

```
-- Drop tablespaces and buffer pool
DROP TABLESPACE LONGTABLESPACE;
DROP TABLESPACE LONGTEMPTABLESPACE;
DROP BUFFERPOOL "LONGBUFFPOOL";

-- create tablespaces and buffer pool
CREATE BUFFERPOOL "LONGBUFFPOOL"  SIZE 10000 PAGESIZE 32768 NOT EXTENDED STORAGE;
CREATE REGULAR TABLESPACE LONGTABLESPACE IN DATABASE PARTITION GROUP IBMDEFAULTGROUP PAGESIZE 32768
MANAGED BY DATABASE USING (FILE 'C:\DB2\LONGTABLESPACE1' 6400)  EXTENTSIZE 8 PREFETCHSIZE AUTOMATIC
BUFFERPOOL LONGBUFFPOOL OVERHEAD 12.670000 TRANSFERRATE 0.180000 DROPPED TABLE RECOVERY ON;
CREATE SYSTEM TEMPORARY  TABLESPACE LONGTEMPTABLESPACE PAGESIZE 32 K  MANAGED BY SYSTEM  USING
('C:\DB2\LONGSYSTMP' ) EXTENTSIZE 8 OVERHEAD 12.67 PREFETCHSIZE 8 TRANSFERRATE 0.18 BUFFERPOOL
LONGBUFFPOOL ;
```

For Oracle:

```
-- Drop tablespaces
DROP TABLESPACE LONGTABLESPACE INCLUDING CONTENTS AND DATAFILES;

-- create tablespaces and buffer pool
CREATE BIGFILE TABLESPACE "LONGTABLESPACE"
 DATAFILE 'C:\oracle\product\10.2.0\ORADATA\LONGTABLESPACE.ORA' SIZE 300M REUSE LOGGING EXTENT
MANAGEMENT LOCAL SEGMENT SPACE MANAGEMENT AUTO;
```

3. When installing WebSphere Premises Server, select the option to create tables and populate the data for the database.

Creating the databases using scripts:

Run the scripts provided in the db_script directory on the WebSphere Premises Server CD to create the database, tablespace, tables and populate data.

Before you begin

Before running the scripts be aware of the following restrictions and take the appropriate action:

- You must be a database user (such as db2inst1 or oracle) to run the scripts on Linux.
- For Oracle, the sqlplus executable must be added in the PATH on Linux.
- The specified tablespace directory must exist.
- You must have the authorization to access the specified tablespace directory if you are using Linux only.
- The specified tablespace file cannot be used by another database.

Example

For DB2: **Windows**

```
createIBMRFID_db2.bat dbName longTablespaceFile longTempTablespaceFile
```

Linux

```
createIBMRFID_db2.sh dbName longTablespaceFile longTempTablespaceFile
```

For Oracle: **Windows**

```
createIBMRFID_oracle.bat dbUser dbPassword dbSpec longTablespaceFile
```

Linux

```
createIBMRFID_oracle.sh dbUser dbPassword dbSpec longTablespaceFile
```

The database, tablespace, table and data are created under dbSpec.

Installing the product

Use these topics to install WebSphere Premises Server and its components.

Installing WebSphere Premises Server

Follow the steps in this topic to install WebSphere Premises Server and its prerequisite middleware.

Before you begin

Important: When specifying installation paths, make sure the directories contains only US English ASCII characters. Also enter only US English ASCII characters in directory paths in properties files.

Important: Enter a password that meets the password rules of the target machine. A password that is not valid will cause installation to fail.

1. Check your hardware and operating system and make sure that they meet the necessary requirements.
2. Make sure that you have completed all the prerequisite steps necessary for your environment. If you would like to modify the path used by the deployment wizard, follow the steps in "Changing the deployment wizard path" on page 23 before launching the installation program.
3. Make sure your database is encoded for UTF-8.
   - If you plan to use DB2 as your database server, and you would like to use an existing database, make sure that database was created with the option to **Enable database for XML (Code set will be set to UTF-8)**. If your DB2 database was not created with that option, you will need to delete and recreate that database if you want to use it.
   - If you are using Oracle, make sure that the database was created with the Unicode AL32UTF8 character set.

   The installer will create a database for you, but you have the option to install one manually as well.
4. If you have a Windows operating system and you are running Terminal Server and Terminal Server Licensing, run the change user /install Windows command before starting the WebSphere Premises Server installation program.

   If you do not issue this command and you have those Windows components installed, the installation may fail because the installer cannot write to the vpd.properties file. To see if you have Terminal Server and Terminal Server Licensing installed, navigate to **Control Panel** → **Add or Remove Programs** → **Add or Remove Windows Components**. When you have successfully issued the command, the response is `User session is ready to install applications.` or `Install mode does not apply to a Terminal server configured for remote administration.` if the command was not needed. For more information, refer to the Windows Server 2003 Product Help.
5. Run the installation program located in the sat_installer directory of the WebSphere Premises Server disk appropriate for your operating system.

   If you have a Linux operating system, make sure you run LinuxSetup from a new shell window.

   > **Windows** WindowsSetup.exe

   > **Linux** LinuxSetup

   When you run the installation program, the deployment wizard is temporarily installed on your hard drive. It will uninstall itself when the installation is complete. When the deployment wizard installation completes, it automatically launches and guides you through the installation of the product and its prerequisite software. It may take a few minutes to begin.

   You can also run the installation program in silent mode. Refer to "Installing silently" on page 51 for further instructions.
6. Select the radio button beside the **I accept both the IBM and the non-IBM terms** statement if you agree to the license agreement and click **Next** to continue.

7. When the Welcome panel appears you can either:
   - Click **Next** to continue installing the product.
   - Or, if you would like to change the default path used for the deployment package, follow the instructions in "Changing the deployment package path" on page 23 before continuing with the next steps.
8. On the Select Tasks panel, click **Next** to install the product and to choose the database type.
9. Choose to use either DB2 or Oracle as your local or remote database.
   - If you choose DB2 and do not have it installed on your server, then the installer will install it for you if you want it installed locally. If you already have DB2 installed on your local server, then the installer will recognize that it is already there and check to make sure it meets the requirements.
   - Choose Oracle if you have an existing installation of that database that you would like to use.
10. Choose to install WebSphere Premises Server only and click **Next**. If you would like to install both WebSphere Premises Server and Location Awareness Services for WebSphere Premises Server, refer to "Installing WebSphere Premises Server and Location Awareness Services for WebSphere Premises Server" on page 34. If you would like to install Location Awareness Services for WebSphere Premises Server on top of an existing WebSphere Premises Server installation, refer to "Installing Location Awareness Services for WebSphere Premises Server" on page 42.
11. Click **Next** to install the required Bundle Repository Server.

    Note: If you do not install Bundle Repository Server on your local server, then you need to install the prerequisite middleware on the remote server before installing Bundle Repository Server. Make sure that you have purchased a separate license for the required middleware that you install on a remote server. Also, you will need to modify the WebSphere Premises Server SystemAgent to reflect the correct location of your Bundle Repository Server.
12. On the Specify Target Computers panel for your database server, specify the target computer for DB2 or your existing Oracle database and click **Next**.
    - For a local server installation for DB2 or an existing installation of Oracle, the default value is localhost. You can either keep this value or change it.
    - If you are installing the product and DB2 on separate servers, specify the fully qualified host name, operating system, user ID, and password of the server where DB2 should be installed.
    - If you are installing the product on one server and using an existing Oracle installation on another server, specify the fully qualified host name, operating system, user ID, and password of the server where Oracle is installed.
    - Optionally, use the **Test connections** button to test access to the remote target computer. Firewalls can have an adverse effect on the installation even though the connection test result is successful.
13. On the Specify Target Computers panel for WebSphere Premises Server, specify the target computer for WebSphere Premises Server and click **Next**.
    - For a local server installation, the default value is localhost. You can either keep this value or change it.

- If you are installing WebSphere Premises Server and its required middleware on a remote server, specify the fully qualified host name, operating system, user ID, and password of the server where it should be installed.
- Optionally, use the **Test connections** button to test access to the remote target computer. Firewalls can have an adverse effect on the installation even though the connection test result is successful.

14. On the Specify Target Computers panel for Bundle Repository Server, specify the target computer for Bundle Repository Server and click **Next**.
    - For a local server installation, the default value is localhost. You can either keep this value or change it.
    - If you are installing Bundle Repository Server on a remote server, specify the fully qualified host name, operating system, user ID, and password of the server where it should be installed.

      Remember: You must install the required middleware on the remote server before installing Bundle Repository Server.
    - Optionally, use the **Test connections** button to test access to the remote target computer. Firewalls can have an adverse effect on the installation even though the connection test result is successful.

15. Enter your database configuration information.
    - If you already have a database server installed, enter the correct user ID and password for that database server. If you are installing DB2, enter a user ID and password to be created.

      Remember: Enter a password that meets the password rules of the target machine. A password that is not valid will cause installation to fail.
    - If you are using Oracle, enter your correct JDBC JAR path.
    - If you would like the installation program to run database scripts to create tables and populate data on the database you have provided, check **Create and populate 6.1.0.1 tables** and click **Next**. This option is especially useful for remote databases, reinstallation on the same server, and clustered environments.
    - If you have already created your database manually with the scripts provided, select **Do not change the database**. The database creation is required for the successful installation of WebSphere Premises Server.

16. Enter the necessary information for WebSphere MQ and click **Next**.
    - **Windows** If you are installing on a Windows operating system, you are prompted to enter the installation directory for WebSphere MQ or accept the default installation directory.
    - **Linux** If you are installing on a Linux operating system, you are prompted for a password.

17. Enter your WebSphere Application Server configuration information and click **Next**.

    Important:
    - If you have an existing version of WebSphere Application Server that is 6.1.0.0 or later (but not the required version 6.1.0.17), and you want the installer to update your WebSphere

Application Server version, then you must have WebSphere Application Server stopped before deploying the WebSphere Premises Server installation.

- WebSphere Application Server security is not enabled by the installer. You must set up and configure security separately.
- If you are going to use any WebSphere Premises Server APIs or the Print, Verify, and Ship application, make sure that the profile you choose to use has the **HTTP transport port** set to 9080.
- If you do not plan to install WebSphere Premises Server and WebSphere Application Server on the default drive (such as the C drive on Windows operating systems), click the **Advanced** tab for the configuration parameters and make sure your WebSphere Application Server profile path reflects the correct drive location for your installation.

18. Enter your IBM HTTP Server configuration information and click **Next**.
19. Enter the installation directory for WebSphere Premises Server.
20. Enter the configuration information for Bundle Repository Server.
21. On the Summary Panel, confirm your choices. The summary provides a list of tasks that you selected and an estimated time for their completion.
    - To start all installation and configuration tasks, click **Deploy all**.
    - If you only want to start a specific task, click **Deploy task**, but make sure that the tasks you choose are in the correct sequence on the panel. For example, you cannot deploy WebSphere Premises Server before deploying DB2 if you do not already have a database installed.

    Click **Back** to make any changes. After you start the deployment, you have the option to click **Stop Deployment** if you need to stop the installation before it is finished. Once all deployment tasks are complete, the Deployment Status screen indicates if the deployment was successful.
22. When the installation is complete, check the log files for any errors. From the Deployment wizard, you can view detailed messages or the master log. Click **Master log** and select **Save as...** to save the log file. The logs can be found in deployment_wizard_installation_dir/logs, where *deployment_wizard_installation_dir* is the installation location of the Deployment wizard.

    > Windows   C:\Program Files\SolutionFiles\logs
    > Linux   opt/SolutionFiles/logs
23. Click the X at the top, right-hand side of the panel to exit the wizard. The wizard displays some messages:
    - A prompt for whether you want to save changes. If you plan to run the wizard again, click **Yes**. Otherwise, click **No**.
    - A prompt for whether you wish to exit. Click **Yes** to exit the wizard.

Results

When you have successfully completed the installation, your server should have the following products installed:

- WebSphere Premises Server in this default location:
    > Windows   C:\Program Files\IBM\RFID
    > Linux   /opt/IBM/RFID
- WebSphere Application Server

- WebSphere MQ
- IBM HTTP Server
- DB2 for Linux, UNIX, and Windows (if you selected to install it)
- a Bundle Repository Server (installed either locally or remotely)

The installation also creates a bundle repository in your IBM HTTP Server document root path, *IHS_HOME*\htdocs\en_US\bundles. For example, the path for a Windows operating system may be C:\Program Files\IBM HTTP Server\htdocs\en_US\bundles. This repository stores all the device application bundles for OSGi Equinox for management by the Bundle Repository Server.

Post-installation steps
Before you begin

If you see errors with the installation, refer to "Troubleshooting tips" on page 399 for possible resolutions to the problem.

1. Make sure that the WAS_HOME environment variable is set to point to the WebSphere Application Server installation directory. The default installation directories for WebSphere Application Server are:

   Windows C:\Program Files\IBM\WebSphere\AppServer

   Linux /opt/IBM/WebSphere/AppServer

   Important: If you have deployed WebSphere Premises Server remotely, you should log out from the target server and then log in again before continuing with the remaining post-installation steps in order to make sure that the WAS_HOME environment variable is applied correctly.

2. Make sure that the correct file paths are specified for the edge alerts and heartbeat log files in the SystemAgent.

   See "Log file locations and settings" on page 386 for the default installation locations of the edge alerts and heartbeat log files.

3. Make sure that the delete filter for Data Capture and Delivery is set correctly in the SystemAgent. See "Setting the delete filter for Data Capture and Delivery" on page 211.

4. Make sure that the IBM RFID and DC Queue Managers are running.

   - **Windows** Open the WebSphere MQ explorer and look for IBM.RFID.QM and IBM.DC.QM in the Queue Managers folder. If there are green arrows next to each queue manager, then they are running.

   - **Linux** Run the command dspmq in /opt/mqm/bin. This command tells you the current status of a queue manager.

   If the queue managers are not running, refer to the WebSphere MQ information center for troubleshooting topics.

5. Make sure all WebSphere Application Server applications are running. Open the WebSphere Application Server administrative console, expand **Applications**, and click **Enterprise Applications**.

   The following applications should appear with green status arrows next to them:

   - AMITJ2EE
   - IBM_ALE_Application
   - IBM_Bundles_Management

> **Note:** If you installed Bundle Repository Server remotely, you will not see this application.

- IBM_EPCIS_Adapter
- IBM_Premises_Admin_Console
- IBM_Premises_Diagnostics
- IBM_Premises_Event_Monitor
- IBM_Premises_DockDoorApp
- IBM_Premises_PVSConsole
- IBM_Premises_Server
- IBM_Premises_Server_BIRT
- IBM_SensorEvent_Engine
- IBM_SensorEvent_Gateway

6. Open the WebSphere Premises Server Administrative Console to verify that it is accessible.

7. Check for errors in the WebSphere Application Server and WebSphere Premises Server log files. Refer to "Log file locations and settings" on page 386 for information about where to find the log files.

8. Open the config.ini file in the *IBM_RFID_HOME*\dts\configuration directory and update the server IP address, port number, bundle list file, and Data Capture and Delivery controller, as necessary.

   `com.ibm.rfid.bundle.list.url=http://IP_address:port_number/bundleadmin/GetBundle?name=http://IBM_HTTP_Server_IP_address/bundles/bundlelists/dc_core4dts.txt`

   This code specifies the URL used by the bundle loader to retrieve the list of bundles to load. If the Bundle Repository Server is on a separate server from WebSphere Premises Server, then replace the *IP_address* and *IBM_HTTP_Server_IP_address* values in this property with the IP address of the server hosting the Bundle Repository Server.

   The default port number is 9080. This port number is defined when you create your WebSphere Application Server profile.

   The bundle list should be set to the dc_core4dts.txt file.

   `com.ibm.rfid.edge.config.url=http://IP_address:port_number/ibmrfidadmin/premises.sl?action=getconfig&edge=E2&version=6.1`

   This code specifies the Data Capture and Delivery controller to use. For testing purposes, the configuration uses the default E2 controller, which is shipped as a sample Data Capture and Delivery controller with WebSphere Premises Server. The E2 controller loads the Simulated Reader to help verify your configuration before testing with a real reader. For a production environment, use the E0 controller.

   > **Note:** This step and the next one help you associate WebSphere Premises Server to a local Data Capture and Delivery device that you can use to verify your installation. In a production environment you should use remote Data Capture and Delivery controllers. See "Installing a remote Data Capture and Delivery controller" on page 72 for details on how to install them.

9. Edit the dc_core4dts.txt file and provide the correct IP address of your Bundle Repository Server.

   The default is the localhost address, 127.0.0.1.

   `PREFIX http://IP_address/bundles/`

10. If Data Transformation service is started as a service, stop it and complete the following steps as they apply to your topology and desired configuration.

    a. Stop the Data Transformation service.

- > Windows < For Windows operating systems, stop the service by going to **Start** → **Control Panel** → **Administrative tools** → **Services**. Select **IBM WebSphere Premises Server DT Service** and click **Stop**.
- > Linux < For Linux operating systems, run the `ibm_dts_service stop` command in the *IBM_RFID_HOME*/dts directory.

b. Modify the startup sequence for WebSphere Application Server, IBM HTTP Server, WebSphere MQ, and Data Transformation service.

> Windows < For Windows operating systems, if you are running WebSphere Application Server, IBM HTTP Server, WebSphere MQ, and Data Transformation service on the same server, you need to ensure that the Data Transformation service starts after WebSphere Application Server and WebSphere MQ when the computer is rebooted. By default, there can be a situation where Data Transformation service starts before the other applications, resulting in errors.

1) Run this command.

> **Important:** The Sc.exe command-line utility syntax requires a space after the = (equal symbol). For more information on this tool, see the Microsoft® Web site.

```
sc config IBMWebSpherePremisesServerDTService depend=
"MQSeriesServices/IBMHTTPServer6.1/IBMWAS61Service - PremisesNode"
```

2) Go to **Start** → **Control Panel** → **Administrative tools** → **Services**.

3) Select **IBM WebSphere Premises Server DT Service**, right-click and select **Properties** → **Dependencies**.

Data Transformation service should show a dependency on the starting of the WebSphere Application Server, IBM HTTP Server, and WebSphere MQ services.

> **Note:** Setting this dependency also means that the Data Transformation service will stop if you stop any one of the WebSphere Application Server, IBM HTTP Server, or WebSphere MQ services. This dependency also assumes that all of these products are on the same server.

> Linux < In a Linux environment, WebSphere Application Server and IBM HTTP Server are not automatically started when the computer reboots, but Data Transformation service and WebSphere MQ are automatically started. If all of the products are installed on the same server, the startup sequence can result in errors.

To reduce the possibility of errors occurring, remove the `ibm_dts_service` from the automatic startup by issuing this command:

```
chkconfig --level 35 ibm_dts_service off
```

11. Restart the Data Transformation service manually.
   - > Windows < For Windows operating systems, run the dts.bat file in the *IBM_RFID_HOME*/dts directory.
   - > Linux < For Linux, run the dts.sh file in the *IBM_RFID_HOME*/dts directory.

These commands start the Data Transformation service and display a Data Transformation prompt.

12. Check the log files for any failures in loading the bundles.
13. Tune your database to improve performance.
14. If you are using the Print, Verify, and Ship example usage scenario, edit the contents of the pvsapp.properties file to point to the correct directory and host

name for your IBM HTTP Server. Specifically, modify the following properties: `premises.hostname`, `report.location.csv`, and `report.location.csv.url`. The pvsapp.properties file is located in the \installedApps*profile_cell_name*\ IBM_Premises_PVSConsole.ear\ibmrfid_premises_pvsapp.war\config\ directory.

15. If you are using the Print, Verify, and Ship example usage scenario, enable ALE.

    a. Open the WebSphere Application Server administrative console.

    b. Navigate to **Resources** → **JMS** → **Activation specifications** → **ALEWrapperAS**.

    c. Change the text in the **Message selector** field to `ibmse='RfidInventory/ TagReport' OR ibmse='RfidInventory/TagAggregationReport' OR ibmse LIKE '%/report/TagReport' OR ibmse LIKE '%/report/ TagAggregationReport'`.

16. Verify the WebSphere Premises Server installation. Choose **R2** as your simulated test reader.

What to do next

If you need to uninstall the WebSphere Premises Server software, refer to "Uninstalling WebSphere Premises Server" on page 95.

Installing WebSphere Premises Server and Location Awareness Services for WebSphere Premises Server

Follow the steps in this topic to install WebSphere Premises Server, Location Awareness Services for WebSphere Premises Server, and their prerequisite middleware.

Before you begin

Restriction: Location Awareness Services for WebSphere Premises Server must be installed on a Windows operating system on the same server as WebSphere Premises Server.

Important: When specifying installation paths, make sure the directories contains only US English ASCII characters. Also enter only US English ASCII characters in directory paths in properties files.

Important: Enter a password that meets the password rules of the target machine. A password that is not valid will cause installation to fail.

1. Check your hardware and operating system and make sure that they meet the necessary requirements.

2. Make sure that you have completed all the prerequisite steps necessary for your environment. If you would like to modify the path used by the deployment wizard, follow the steps in "Changing the deployment wizard path" on page 23 before launching the installation program.

3. If you would like to use an existing DB2 database, make sure that database was created with the option to **Enable database for XML (Code set will be set to UTF-8)**. If your DB2 database was not created with that option, you will need to delete and recreate that database if you want to use it.

   The installer will create three databases for you, but you have the option to install databases manually as well.

4. If you are running Terminal Server and Terminal Server Licensing, run the change user /install Windows command before starting the WebSphere Premises Server installation program.

   If you do not issue this command and you have those Windows components installed, the installation may fail because the installer cannot write to the vpd.properties file. To see if you have Terminal Server and Terminal Server Licensing installed, navigate to **Control Panel** → **Add or Remove Programs** → **Add or Remove Windows Components**. When you have successfully issued the command, the response is `User session is ready to install applications.` or `Install mode does not apply to a Terminal server configured for remote administration.` if the command was not needed. For more information, refer to the Windows Server 2003 Product Help.

5. Run the installation program located in the sat_installer directory of the WebSphere Premises Server disk for Windows.

   Location Awareness Services for WebSphere Premises Server is only supported on Windows.

   > WindowsSetup.exe

   When you run the installation program, the deployment wizard is temporarily installed on your hard drive. It will uninstall itself when the installation is complete. When the deployment wizard installation completes, it automatically launches and guides you through the installation of the product and its prerequisite software. It may take a few minutes to begin.

   You can also run the installation program in silent mode. Refer to "Installing silently" on page 51 for further instructions.

6. Select the radio button beside the **I accept both the IBM and the non-IBM terms** statement if you agree to the license agreement and click **Next** to continue.

7. When the Welcome panel appears you can either:
   - Click **Next** to continue installing the product.
   - Or, if you would like to change the default path used for the deployment package, follow the instructions in "Changing the deployment package path" on page 23 before continuing with the next steps.

8. On the Select Tasks panel, click **Next** to install the product and to choose the database type.

9. Choose to use DB2 as either your local or remote database. If you do not have DB2 installed on your server, then the installer will install it for you if you want it installed locally. If you already have DB2 installed on your local server, then the installer will recognize that it is already there and check to make sure it meets the requirements.

10. Choose to install WebSphere Premises Server and Location Awareness Services for WebSphere Premises Server and click **Next**. If you would like to install only WebSphere Premises Server, refer to "Installing WebSphere Premises Server" on page 26. If you would like to install Location Awareness Services for WebSphere Premises Server on top of an existing WebSphere Premises Server installation, refer to "Installing Location Awareness Services for WebSphere Premises Server" on page 42.

11. Click **Next** to install the required Bundle Repository Server.

    Note: If you do not install Bundle Repository Server on your local server, then you need to install the prerequisite middleware on the remote server before installing Bundle Repository Server. Make sure that you have purchased a separate license for the required middleware that you

install on a remote server. Also, you will need to modify the WebSphere Premises Server SystemAgent to reflect the correct location of your Bundle Repository Server.

12. On the Specify Target Computers panel for your database server, specify the target computer for DB2 database and click **Next**.
    - For a local server installation for DB2, the default value is localhost. You can either keep this value or change it.
    - If you are installing the product and DB2 on separate servers, specify the fully qualified host name, operating system, user ID, and password of the server where DB2 should be installed.
    - Optionally, use the **Test connections** button to test access to the remote target computer. Firewalls can have an adverse effect on the installation even though the connection test result is successful.

13. On the Specify Target Computers panel for WebSphere Premises Server including Location Awareness Services for WebSphere Premises Server, specify the target computer and click **Next**.
    - For a local server installation, the default value is localhost. You can either keep this value or change it.
    - If you are installing WebSphere Premises Server including Location Awareness Services for WebSphere Premises Server and their required middleware on a remote server, specify the fully qualified host name, operating system, user ID, and password of the server where it should be installed.
    - Optionally, use the **Test connections** button to test access to the remote target computer. Firewalls can have an adverse effect on the installation even though the connection test result is successful.

14. On the Specify Target Computers panel for Bundle Repository Server, specify the target computer for Bundle Repository Server and click **Next**.
    - For a local server installation, the default value is localhost. You can either keep this value or change it.
    - If you are installing Bundle Repository Server on a remote server, specify the fully qualified host name, operating system, user ID, and password of the server where it should be installed.

      Remember: You must install the required middleware on the remote server before installing Bundle Repository Server.
    - Optionally, use the **Test connections** button to test access to the remote target computer. Firewalls can have an adverse effect on the installation even though the connection test result is successful.

15. Enter your database configuration information.
    - If you already have a database server installed, enter the correct user ID and password for that database server. If you are installing DB2, enter a user ID and password to be created.

      Remember: Enter a password that meets the password rules of the target machine. A password that is not valid will cause installation to fail.
    - If you would like the installation program to run database scripts to create tables and populate data on the database you have provided, check **Create and populate 6.1.0.1 tables** and click **Next**. This option is especially useful for remote databases, reinstallation on the same server, and clustered environments.

- If you have already created your database manually with the scripts provided, select **Do not change the database**. The database creation is required for the successful installation of WebSphere Premises Server.

16. Enter the installation directory for WebSphere MQ or accept the default installation directory and click **Next**.

17. Enter your WebSphere Application Server configuration information and click **Next**.

   Restriction: Location Awareness Services for WebSphere Premises Server can only run properly when WebSphere Application Server is installed with the default paths provided by the installer. The installation directory, the name of the profile, the path of the profile, and the ports of this profile must not be modified. Otherwise, Location Awareness Services for WebSphere Premises Server fails.

   Important:
   - WebSphere Application Server security is not enabled by the installer. You must set up and configure security separately.
   - If you are going to use any WebSphere Premises Server APIs or the Print, Verify, and Ship application, make sure that the profile you choose to use has the **HTTP transport port** set to 9080.

18. Enter your IBM HTTP Server configuration information and click **Next**.

19. Enter the required information for DB2 Universal Database Enterprise Server Edition Client.

20. Enter the installation directory for WebSphere Premises Server.

21. Enter the configuration information for Location Awareness Services for WebSphere Premises Server.

   Note: If you would like to install the samples, but your language is not in the S-1 group in DB2, then you should choose **-nosamples** in the installer panel and manually install the samples instead.

22. Enter the configuration information for Bundle Repository Server.

23. On the Summary Panel, confirm your choices. The summary provides a list of tasks that you selected and an estimated time for their completion.
   - To start all installation and configuration tasks, click **Deploy all**.
   - If you only want to start a specific task, click **Deploy task**, but make sure that the tasks you choose are in the correct sequence on the panel. For example, you cannot deploy WebSphere Premises Server before deploying DB2 if you do not already have a database installed.

   Click **Back** to make any changes. After you start the deployment, you have the option to click **Stop Deployment** if you need to stop the installation before it is finished. Once all deployment tasks are complete, the Deployment Status screen indicates if the deployment was successful.

24. Insert the Location Awareness Services for WebSphere Premises Server CD when prompted.

25. When the installation is complete, check the log files for any errors. From the Deployment wizard, you can view detailed messages or the master log. Click **Master log** and select **Save as...** to save the log file. The logs can be found in deployment_wizard_installation_dir/logs, where *deployment_wizard_installation_dir* is the installation location of the Deployment wizard.

C:\Program Files\SolutionFiles\logs

26. Click the X at the top, right-hand side of the panel to exit the wizard. The wizard displays some messages:
    - A prompt for whether you want to save changes. If you plan to run the wizard again, click **Yes**. Otherwise, click **No**.
    - A prompt for whether you wish to exit. Click **Yes** to exit the wizard.

Results

When you have successfully completed the installation, your server should have the following products and components installed:

- WebSphere Premises Server in this default location:

    C:\Program Files\IBM\RFID

- Location Awareness Services for WebSphere Premises Server in this default location:

    C:\LAS

- WebSphere Application Server
- WebSphere MQ
- IBM HTTP Server
- DB2 for Linux, UNIX, and Windows (if you selected to install it)
- a Bundle Repository Server (installed either locally or remotely)

The installation also creates a bundle repository in your IBM HTTP Server document root path, *IHS_HOME*\htdocs\en_US\bundles. For example, the path for a Windows operating system may be C:\Program Files\IBM HTTP Server\htdocs\en_US\bundles. This repository stores all the device application bundles for OSGi Equinox for management by the Bundle Repository Server.

Post-installation steps
Before you begin

If you see errors with the installation, refer to "Troubleshooting tips" on page 399 and "General troubleshooting tips" on page 336 for possible resolutions to the problem.

1. Make sure that the WAS_HOME environment variable is set to point to the WebSphere Application Server installation directory.

    Important: If you have deployed WebSphere Premises Server remotely, you should log out from the target server and then log in again before continuing with the remaining post-installation steps in order to make sure that the WAS_HOME environment variable is applied correctly.

2. Make sure that the correct file paths are specified for the edge alerts and heartbeat log files in the SystemAgent.

    See "Log file locations and settings" on page 386 for the default installation locations of the edge alerts and heartbeat log files.

3. Make sure that the delete filter for Data Capture and Delivery is set correctly in the SystemAgent. See "Setting the delete filter for Data Capture and Delivery" on page 211.

4. Make sure that the IBM RFID and DC Queue Managers are running.
    a. Open the WebSphere MQ explorer.

b. Look for IBM.RFID.QM and IBM.DC.QM in the Queue Managers folder. If there are green arrows next to each queue manager, then they are running.

If the queue managers are not running, refer to the WebSphere MQ information center for troubleshooting topics.

5. Make sure all WebSphere Application Server applications are running. Open the WebSphere Application Server administrative console, expand **Applications**, and click **Enterprise Applications**.

The following applications should appear with green status arrows next to them:

- AMITJ2EE
- AtlasAlertHandlerEJBEAR
- AtlasEMailSampleServiceEAR
- AtlasEventSubscriberEAR
- AtlasImportEAR
- AtlasReportingServletEAR
- IBM_ALE_Application
- IBM_Bundles_Management

   Note: If you installed Bundle Repository Server remotely, you will not see this application.

- IBM_EPCIS_Adapter
- IBM_Premises_Admin_Console
- IBM_Premises_Diagnostics
- IBM_Premises_Event_Monitor
- IBM_Premises_DockDoorApp
- IBM_Premises_PVSConsole
- IBM_Premises_Server
- IBM_Premises_Server_BIRT
- IBM_SensorEvent_Engine
- IBM_SensorEvent_Gateway

6. Open the WebSphere Premises Server Administrative Console to verify that it is accessible.

7. Check for errors in the WebSphere Application Server and WebSphere Premises Server log files. Refer to "Log file locations and settings" on page 386 for information about where to find the log files.

8. Open the config.ini file in the *IBM_RFID_HOME*\dts\configuration directory and update the server IP address, port number, bundle list file, and Data Capture and Delivery controller, as necessary.

   `com.ibm.rfid.bundle.list.url=http://IP_address:port_number/bundleadmin/GetBundle?name=http://IBM_HTTP_Server_IP_address/bundles/bundlelists/dc_core4dts.txt`

   This code specifies the URL used by the bundle loader to retrieve the list of bundles to load. If the Bundle Repository Server is on a separate server from WebSphere Premises Server, then replace the *IP_address* and *IBM_HTTP_Server_IP_address* values in this property with the IP address of the server hosting the Bundle Repository Server.

   The default port number is 9080. This port number is defined when you create your WebSphere Application Server profile.

   The bundle list should be set to the dc_core4dts.txt file.

   `com.ibm.rfid.edge.config.url=http://IP_address:port_number/ibmrfidadmin/premises.sl?action=getconfig&edge=E2&version=6.1`

This code specifies the Data Capture and Delivery controller to use. For testing purposes, the configuration uses the default E2 controller, which is shipped as a sample Data Capture and Delivery controller with WebSphere Premises Server. The E2 controller loads the Simulated Reader to help verify your configuration before testing with a real reader. For a production environment, use the E0 controller.

> **Note:** This step and the next one help you associate WebSphere Premises Server to a local Data Capture and Delivery device that you can use to verify your installation. In a production environment you should use remote Data Capture and Delivery controllers. See "Installing a remote Data Capture and Delivery controller" on page 72 for details on how to install them.

9. Edit the dc_core4dts.txt file and provide the correct IP address of your Bundle Repository Server.

   The default is the localhost address, 127.0.0.1.

   ```
   PREFIX http://IP_address/bundles/
   ```

10. If Data Transformation service is started as a service, stop it and complete the following steps as they apply to your topology and desired configuration.

    a. Stop the Data Transformation service by going to **Start** → **Control Panel** → **Administrative tools** → **Services**.

    b. Select **IBM WebSphere Premises Server DT Service** and click **Stop**.

    c. Modify the startup sequence for WebSphere Application Server, IBM HTTP Server, WebSphere MQ, and Data Transformation service.

       If you are running WebSphere Application Server, IBM HTTP Server, WebSphere MQ, and Data Transformation service on the same server, you need to ensure that the Data Transformation service starts after WebSphere Application Server and WebSphere MQ when the computer is rebooted. By default, there can be a situation where Data Transformation service starts before the other applications, resulting in errors.

       1) Run this command.

          > **Important:** The Sc.exe command-line utility syntax requires a space after the = (equal symbol). For more information on this tool, see the Microsoft Web site.

          ```
          sc config IBMWebSpherePremisesServerDTService depend=
          "MQSeriesServices/IBMHTTPServer6.1/IBMWAS61Service - PremisesNode"
          ```

       2) Go to **Start** → **Control Panel** → **Administrative tools** → **Services**.

       3) Select **IBM WebSphere Premises Server DT Service**, right-click and select **Properties** → **Dependencies**.

          Data Transformation service should show a dependency on the starting of the WebSphere Application Server, IBM HTTP Server, and WebSphere MQ services.

          > **Note:** Setting this dependency also means that the Data Transformation service will stop if you stop any one of the WebSphere Application Server, IBM HTTP Server, or WebSphere MQ services. This dependency also assumes that all of these products are on the same server.

11. Restart the Data Transformation service manually by running the dts.bat file in the *IBM_RFID_HOME*/dts directory.

    This command starts the Data Transformation service and displays a Data Transformation prompt.

12. Check the log files for any failures in loading the bundles.
13. Tune your database to improve performance.
14. If you are using the Print, Verify, and Ship example usage scenario, edit the contents of the pvsapp.properties file to point to the correct directory and host name for your IBM HTTP Server. Specifically, modify the following properties: `premises.hostname`, `report.location.csv`, and `report.location.csv.url`. The pvsapp.properties file is located in the \installedApps*profile_cell_name*\ IBM_Premises_PVSConsole.ear\ibmrfid_premises_pvsapp.war\config\ directory.
15. If you are using the Print, Verify, and Ship example usage scenario, enable ALE.
    a. Open the WebSphere Application Server administrative console.
    b. Navigate to **Resources** → **JMS** → **Activation specifications** → **ALEWrapperAS**.
    c. Change the text in the **Message selector** field to `ibmse='RfidInventory/ TagReport' OR ibmse='RfidInventory/TagAggregationReport' OR ibmse LIKE '%/report/TagReport' OR ibmse LIKE '%/report/ TagAggregationReport'`.
16. Verify the WebSphere Premises Server installation. Choose **R2** as your simulated test reader.
17. Configure the Spatial Management Client for Location Awareness Services for WebSphere Premises Server.
    a. Change directory to the Spatial Management Client root directory in IBM HTTP Server (for example, C:\Program Files\IBM\HTTPServer\htdocs\ en_US\Tracking GUI).
    b. Go to the xml directory and edit the prefsV3.xml file.
       1) Replace `localhost` with the IP address or the fully qualified host name of your server in the `<host>` element.

          Note: The value you specify for the `<host>` element and the value you use to browse to the Spatial Management Client must be identical.
       2) Save your changes.
18. Enable security for WebSphere Application Server.
19. Synchronize the DB2 server time and WebSphere Application Server time prior to running your configuration because location events use the DB2 server time for event creation, but Common Event Infrastructure (CEI) events use the WebSphere Application Server time for event creation.
20. Configure and verify the Location Awareness Services for WebSphere Premises Server installation.
21. The default Location Awareness Services for WebSphere Premises Server installation can support small scenarios, using between 100 and 200 tags. To use Location Awareness Services for WebSphere Premises Server in a production environment or to use it with more tags, tune your ATLASDB database for additional buffer pools, and add more hard drives to avoid bottlenecks.

What to do next

If you need to uninstall the WebSphere Premises Server and Location Awareness Services for WebSphere Premises Server software, refer to "Uninstalling WebSphere Premises Server" on page 95.

Installing Location Awareness Services for WebSphere Premises Server

Follow the steps in this topic to install Location Awareness Services for WebSphere Premises Server on an existing installation of WebSphere Premises Server.

Before you begin

Restriction: Location Awareness Services for WebSphere Premises Server must be installed on a Windows operating system on the same server as WebSphere Premises Server.

Important: When specifying installation paths, make sure the directories contains only US English ASCII characters. Also enter only US English ASCII characters in directory paths in properties files.

Important: Enter a password that meets the password rules of the target machine. A password that is not valid will cause installation to fail.

1. Check your hardware and operating system and make sure that they meet the necessary requirements.
2. Make sure that you have completed all the prerequisite steps necessary for your environment. If you would like to modify the path used by the deployment wizard, follow the steps in "Changing the deployment wizard path" on page 23 before launching the installation program.
3. If you are running Terminal Server and Terminal Server Licensing, run the change user /install Windows command before starting the WebSphere Premises Server installation program.

   If you do not issue this command and you have those Windows components installed, the installation may fail because the installer cannot write to the vpd.properties file. To see if you have Terminal Server and Terminal Server Licensing installed, navigate to **Control Panel** → **Add or Remove Programs** → **Add or Remove Windows Components**. When you have successfully issued the command, the response is User session is ready to install applications. or Install mode does not apply to a Terminal server configured for remote administration. if the command was not needed. For more information, refer to the Windows Server 2003 Product Help.
4. Run the installation program located in the sat_installer directory of the WebSphere Premises Server disk for Windows.

   Location Awareness Services for WebSphere Premises Server is only supported on Windows.

   > WindowsSetup.exe

   When you run the installation program, the deployment wizard is temporarily installed on your hard drive. It will uninstall itself when the installation is complete. When the deployment wizard installation completes, it automatically launches and guides you through the installation of the product and its prerequisite software. It may take a few minutes to begin.

   You can also run the installation program in silent mode. Refer to "Installing silently" on page 51 for further instructions.
5. Select the radio button beside the **I accept both the IBM and the non-IBM terms** statement if you agree to the license agreement and click **Next** to continue.
6. When the Welcome panel appears you can either:
   - Click **Next** to continue installing the product.

- Or, if you would like to change the default path used for the deployment package, follow the instructions in "Changing the deployment package path" on page 23 before continuing with the next steps.

7. On the Select Tasks panel, click **Next** to install the product and to choose the database type.

8. Choose to use DB2 as either your local or remote database. If you do not have DB2 installed on your server, then the installer will install it for you if you want it installed locally. If you already have DB2 installed on your local server, then the installer will recognize that it is already there and check to make sure it meets the requirements.

9. Choose to install Location Awareness Services for WebSphere Premises Server and click **Next**. If you would like to install only WebSphere Premises Server, refer to "Installing WebSphere Premises Server" on page 26. If you would like to install both WebSphere Premises Server and Location Awareness Services for WebSphere Premises Server, refer to "Installing WebSphere Premises Server and Location Awareness Services for WebSphere Premises Server" on page 34.

10. Click **Next** to install the required Bundle Repository Server.

   Note: If you do not install Bundle Repository Server on your local server, then you need to install the prerequisite middleware on the remote server before installing Bundle Repository Server. Make sure that you have purchased a separate license for the required middleware that you install on a remote server. Also, you will need to modify the WebSphere Premises Server SystemAgent to reflect the correct location of your Bundle Repository Server.

11. On the Specify Target Computers panel for your database server, specify the target computer for DB2 database and click **Next**.
    - For a local server installation for DB2, the default value is localhost. You can either keep this value or change it.
    - If you are installing the product and DB2 on separate servers, specify the fully qualified host name, operating system, user ID, and password of the server where DB2 should be installed.
    - Optionally, use the **Test connections** button to test access to the remote target computer. Firewalls can have an adverse effect on the installation even though the connection test result is successful.

12. On the Specify Target Computers panel for WebSphere Premises Server including Location Awareness Services for WebSphere Premises Server, specify the target computer and click **Next**.
    - For a local server installation, the default value is localhost. You can either keep this value or change it.
    - If you are installing WebSphere Premises Server including Location Awareness Services for WebSphere Premises Server and their required middleware on a remote server, specify the fully qualified host name, operating system, user ID, and password of the server where it should be installed.
    - Optionally, use the **Test connections** button to test access to the remote target computer. Firewalls can have an adverse effect on the installation even though the connection test result is successful.

13. Enter your database configuration information.
    - If you already have a database server installed, enter the correct user ID and password for that database server. If you are installing DB2, enter a user ID and password to be created.

> **Remember:** Enter a password that meets the password rules of the target machine. A password that is not valid will cause installation to fail.

- If you would like the installation program to run database scripts to create tables and populate data on the database you have provided, check **Create and populate 6.1.0.1 tables** and click **Next**. This option is especially useful for remote databases, reinstallation on the same server, and clustered environments.
- If you have already created your database manually with the scripts provided, select **Do not change the database**. The database creation is required for the successful installation of WebSphere Premises Server.

14. Enter the installation directory for WebSphere MQ or accept the default installation directory and click **Next**.

15. Enter your WebSphere Application Server configuration information and click **Next**.

> **Restriction:** Location Awareness Services for WebSphere Premises Server can only run properly when WebSphere Application Server is installed with the default paths provided by the installer. The installation directory, the name of the profile, the path of the profile, and the ports of this profile must not be modified. Otherwise, Location Awareness Services for WebSphere Premises Server fails.

> **Important:**
> - WebSphere Application Server security is not enabled by the installer. You must set up and configure security separately.
> - If you are going to use any WebSphere Premises Server APIs or the Print, Verify, and Ship application, make sure that the profile you choose to use has the **HTTP transport port** set to 9080.

16. Enter your IBM HTTP Server configuration information and click **Next**.

17. Enter the required information for DB2 Universal Database Enterprise Server Edition Client.

18. Enter the installation directory for WebSphere Premises Server.

19. Enter the configuration information for Location Awareness Services for WebSphere Premises Server.

> **Note:** If you would like to install the samples, but your language is not in the S-1 group in DB2, then you should choose **-nosamples** in the installer panel and manually install the samples instead.

20. On the Summary Panel, confirm your choices. The summary provides a list of tasks that you selected and an estimated time for their completion.
- To start all installation and configuration tasks, click **Deploy all**.
- If you only want to start a specific task, click **Deploy task**, but make sure that the tasks you choose are in the correct sequence on the panel. For example, you cannot deploy WebSphere Premises Server before deploying DB2 if you do not already have a database installed.

Click **Back** to make any changes. After you start the deployment, you have the option to click **Stop Deployment** if you need to stop the installation before it is finished. Once all deployment tasks are complete, the Deployment Status screen indicates if the deployment was successful.

21. Insert the Location Awareness Services for WebSphere Premises Server CD when prompted.
22. When the installation is complete, check the log files for any errors. From the Deployment wizard, you can view detailed messages or the master log. Click **Master log** and select **Save as...** to save the log file. The logs can be found in deployment_wizard_installation_dir/logs, where *deployment_wizard_installation_dir* is the installation location of the Deployment wizard.

    C:\Program Files\SolutionFiles\logs
23. Click the X at the top, right-hand side of the panel to exit the wizard. The wizard displays some messages:
    - A prompt for whether you want to save changes. If you plan to run the wizard again, click **Yes**. Otherwise, click **No**.
    - A prompt for whether you wish to exit. Click **Yes** to exit the wizard.

Results

When you have successfully completed the installation, your server should have Location Awareness Services for WebSphere Premises Server installed in this default location:

    C:\LAS

Post-installation steps
Before you begin

If you see errors with the installation, refer to "General troubleshooting tips" on page 336 for possible resolutions to the problem.

1. Make sure all WebSphere Application Server applications are running. Open the WebSphere Application Server administrative console, expand **Applications**, and click **Enterprise Applications**.

    The following applications should appear with green status arrows next to them:
    - AMITJ2EE
    - AtlasAlertHandlerEJBEAR
    - AtlasEMailSampleServiceEAR
    - AtlasEventSubscriberEAR
    - AtlasImportEAR
    - AtlasReportingServletEAR
    - IBM_ALE_Application
    - IBM_Bundles_Management

        Note: If you installed Bundle Repository Server remotely, you will not see this application.
    - IBM_EPCIS_Adapter
    - IBM_Premises_Admin_Console
    - IBM_Premises_Diagnostics
    - IBM_Premises_Event_Monitor
    - IBM_Premises_DockDoorApp
    - IBM_Premises_PVSConsole
    - IBM_Premises_Server

- IBM_Premises_Server_BIRT
- IBM_SensorEvent_Engine
- IBM_SensorEvent_Gateway

2. Configure the Spatial Management Client for Location Awareness Services for WebSphere Premises Server.

   a. Change directory to the Spatial Management Client root directory in IBM HTTP Server (for example, C:\Program Files\IBM\HTTPServer\htdocs\en_US\Tracking GUI).

   b. Go to the xml directory and edit the prefsV3.xml file.

      1) Replace `localhost` with the IP address or the fully qualified host name of your server in the `<host>` element.

         Note: The value you specify for the `<host>` element and the value you use to browse to the Spatial Management Client must be identical.

      2) Save your changes.

3. Enable security for WebSphere Application Server.

4. Synchronize the DB2 server time and WebSphere Application Server time prior to running your configuration because location events use the DB2 server time for event creation, but Common Event Infrastructure (CEI) events use the WebSphere Application Server time for event creation.

5. Configure and verify the Location Awareness Services for WebSphere Premises Server installation.

6. The default Location Awareness Services for WebSphere Premises Server installation can support small scenarios, using between 100 and 200 tags. To use Location Awareness Services for WebSphere Premises Server in a production environment or to use it with more tags, tune your ATLASDB database for additional buffer pools, and add more hard drives to avoid bottlenecks.

What to do next

If you need to uninstall the WebSphere Premises Server and Location Awareness Services for WebSphere Premises Server software, refer to "Uninstalling WebSphere Premises Server" on page 95.

Installing a high availability system

High availability provides several benefits, including load balancing and failover. High availability with WebSphere Premises Server consists of setting up a server cluster and then configuring those servers for load balancing.

About this task

The installer creates the cluster topology and load balances the node servers.

1. Make sure that you have completed all the prerequisite steps necessary for high availability.

2. Launch the high availability post-installation script located at the root of the High Availability for IBM WebSphere Premises Server Central Site Server disk.

   Windows   setupwin32.exe

   Linux   setuplinux.bin

   The Welcome panel displays.

3. Click **Next**.

4. This panel shows the installation directory for the WebSphere Premises Server high availability system.

   The directory is:

   > **Windows** *IBM_RFID_HOME*\HA
   > **Linux** *IBM_RFID_HOME*/HA

   Click **Next** to continue.

5. Enter the host name and port for WebSphere Application Server Network Deployment, and click **Next**.

   Tip: Make sure that WebSphere Application Server Network Deployment is running. The installer verifies that it can connect to WebSphere Application Server Network Deployment using the port and host name you have provided before continuing. If it cannot connect, you will be asked to go **Back** and edit the values on the previous panel, or you can **Cancel** out of the installer.

6. Create the cluster members. Create at least one member on this panel in order to proceed with the installation.

   Use the **Add Member** button to add cluster members. The created member's name, node, and weight appear in the box at the bottom of the installer panel.

   To delete a cluster member, select the member name from the list of created members and click **Delete Member**.

   For more information on creating cluster members, see Adding members to a cluster.

7. Click **Next**.

8. A summary panel displays your installation selections. Click **Install** to continue the installation process.

   When the installation is complete, another summary panel displays the installation status and prompts you to check the log file for any errors.

   > **Windows** *IBM_RFID_HOME*\HA\logs\install.log
   > **Linux** *IBM_RFID_HOME*/HA/logs/install.log

   If you do see errors or exceptions in the installation log file, try uninstalling and reinstalling the high availability topology. Also check the "Troubleshooting tips" on page 399 documentation for possible resolutions to the problem. If you are unable to resolve the errors, contact IBM Support.

9. If you see exceptions in the WebSphere Application Server SystemOut.log file on the central and node servers, follow the procedure in this technote.

10. Restart the central server and the cluster.

11. If you are using WebSphere Application Server security, enable it, and then restart the deployment manager, all node agents, and all servers.

12. Enable dynamic cache replication for all servers in the cluster.

    a. In the WebSphere Application Server administrative console, go to **Servers** → **Application servers** → *server name* → **Container Services** → **Dynamic cache service** and check **Enable service at server startup** for each server in the cluster.

    b. Define a new replication domain by going to **Environment** → **Replication domains** → **New**. Choose **Entire domain** when creating the new replication domain.

    c. Navigate to **Resources** → **Cache instances** → **Object cache instances** and add the new replication to all object cache components.

       1) Check Enable cache replication.

2) Choose your cluster name for **Full group replication domain**.

3) Choose **Push only** for **Replication type**.

4) Set **Push frequency** to **1** seconds.

13. Configure the Data Capture and Delivery controllers for high availability.

   a. Make sure you are using Java 1.4.2 on your Data Capture and Delivery controllers.

   b. Set the appropriate MQ user name for your operating system in the controller's Equinox script.

   > Windows   `-Duser.name=MUSR_MQADMIN`

   > Linux   `-Duser.name=mqm`

   If you used the sample files provided with the IBM Data Capture and Delivery Toolkit for WebSphere Premises Server to set up your remote Data Capture and Delivery controllers, modify the remoteDC script with the MQ user name.

   For example: > Windows

   ```
   %JAVA_HOME%\bin\java" -Duser.name=MUSR_MQADMIN -Xmx256M -Xms256M
   ```

   > Linux

   ```
   "$JAVA_HOME/bin/java" -Duser.name=mqm -Xmx256M -Xms256M
   ```

   c. Edit the config.ini file in the controller's Equinox configuration directory make sure the configuration is set to the dc_core4dts.txt file for the bundle list and E4 for the edge controller.

   ```
   com.ibm.rfid.bundle.list.url=http://IP_address:port_number/bundleadmin/GetBundle?name=http://IBM_HTTP_Server_IP_address/bundles/bundlelists/dc_core4dts.txt
   com.ibm.rfid.edge.config.url=http://IP_address:port_number/ibmrfidadmin/premises.sl?action=getconfig&edge=E4&version=6.1
   ```

   The values for *IP_address* and *IBM_HTTP_Server_IP_address* are the name of the server that is hosting the Bundle Repository Server.

   The second line of code points to the E4 controller, which is installed with WebSphere Premises Server specifically for high availability.

14. Check to see if Data Transformation is running (started as a service) on your central server, and if so, stop it.

15. Start the Equinox runtime on the Data Capture and Delivery controllers.

16. Start the bundle loader on the Data Capture and Delivery controllers.

   a. Find the ID of the bundle loader bundle by running the OSGi `ss` command.

   b. Start the bundle loader bundle by entering `start bundle_ID` at the OSGi prompt.

17. Test the clustered configuration using the Simulated Reader in the WebSphere Premises Server Administrative Console. Choose **R4** as your simulated test reader.

   Optionally, you can test with a real reader.

18. Create a new remote Data Capture and Delivery controller based on the E4 sample to use with your real reader.

What to do next

If you need to create additional cluster members, follow the steps in "Installing additional cluster members" on page 51.

Manually configuring the clustered system for multiple messaging engines

After you have run the high availability installer for WebSphere Premises Server, you can use these instructions to add more messaging engines.

WebSphere Premises Server SIBus configuration overview

There are two SIBuses created with the WebSphere Premises Server installation, AMIT and ibmsensorevent.

The high availability cluster configuration is the default configuration created when a cluster of application servers in a cell is created. When the SIBus is created, there is only one active messaging engine on one of the cluster servers, and all service requests to cluster members are routed through this single messaging engine. Therefore, for a cluster of *n* servers, there is one local message put action for routing the service request on the server with the active messaging engine, and *(n-1)* remote message put actions for each of the servers with inactive messaging engines.

For workload management, the cluster configuration requires additional configuration from the default cluster installation. The purpose of this configuration is to remove the dependence on the messaging engine remote put calls by explicitly creating an additional messaging engine for each of the servers in the cluster and defining a CoreGroup policy to "assign" the messaging engine to an individual server in the cluster. With *n* active messaging engines in a cluster of *n* servers, each service request is processed locally on the server receiving the message rather than getting routed to an active messaging engine.

Adding multiple messaging engines:
About this task

These steps are specifically for the ibmsensorevent SIBus. You will also need to perform these steps for the AMIT SIBus.
  1. Open the WebSphere Application Server Network Deployment administrative console and navigate to **Servers** → **Core groups** → **Core group settings** → **DefaultCoreGroup** → **Policies**.
  2. Click **New** and select **One of N policy** for the policy type.
  3. Click **Next**.
  4. Define the new policy.
     a. For **Name**, enter `SIBusClusterME001Policy`.
     b. Select the checkbox for **Failback**.
     c. Select the checkbox for **Preferred servers only**.
     d. Click **Apply**.
  5. Under **Additional Properties**, click **Match criteria**.
  6. Click **New** and define the match criteria for the policy.
     a. For **Name**, enter `type`.
     b. For **Value**, enter `WSAF_SIB`.
     c. Click **OK**.

     In the next three steps, you repeat the actions in this step to define additional match criteria for the policy.
  7. Click **New** and define an additional match criteria for the policy.
     a. For **Name**, enter `WSAF_SIB_BUS`.

     b. For **Value**, enter `ibmsensorevent`.

     c. Click **OK**.

8. Click **New** and define an additional match criteria for the policy.

     a. For **Name**, enter `WSAF_SIB_MESSAGING_ENGINE`.

     b. For **Value**, enter `PremisesCluster.000-ibmsensorevent`.

     c. Click **OK**.

9. Click **New** and define an additional match criteria for the policy.

     a. For **Name**, enter `IBM_hc`.

     b. For **Value**, enter `PremisesCluster`.

     c. Click **OK**.

10. Navigate back to the **SIBusClusterME001Policy** and click **Preferred servers** under **Additional Properties**.

11. Select the server name of a cluster member from the **Core group servers** and click **Add>>**.

12. Click **OK**.

13. Repeat steps 4 on page 49 through 12 to create new policies and assign each to a cluster member. Every cluster member except the central server needs a policy.

14. Create messaging engines for each cluster member.

When you ran the high availability installer, a cluster member named PremisesCluster.000-ibmsensorevent was created on the ibmsensorevent SIBus. This steps shows you how to create the messaging engine for that cluster member. Repeat this step as necessary to create *(n-1)* messaging engines for *n* cluster members.

     a. Navigate to **Service integration** ▸ **Buses** ▸ **ibmsensorevent** ▸ **Bus members** ▸ **PremisesCluster**.

     b. Click **Add messaging engine** and select **File store**.

       Note: You can use **Data store** instead of **File store**.

     c. Click **Next**.

     d. For **Log directory path**, enter `${LOG_ROOT}/sibus-se`.

     e. For **Permanent store directory path**, enter `${LOG_ROOT}/sibus-se`.

     f. Click **Next**.

     g. Click **Finish**.

15. Synchronize all cluster members and server configurations by navigating to **System administrator** ▸ **Nodes** and clicking **Full Resynchronize**.

16. Restart the PremisesCluster cluster and the central server.

     a. Navigate to **Server** ▸ **Clusters**.

     b. Select **PremisesCluster** and click **Stop**.

     c. Once it all cluster members are stopped, click **Start**.

     d. Navigate to **Server** ▸ **Application servers**.

     e. Select the central server (such as PremisesNode, server1).

     f. Click **Stop**.

     g. Once the central server has stopped, click **Start**.

17. Repeat all of the previous steps for the AMIT SIBus. To do this, replace every instance of "ibmsensorevent" with "AMIT" in the instructions, specifically in the console paths, SIBus name, and messaging engine names.

Installing additional cluster members

If you have already run the installer for high availability for WebSphere Premises Server, and you need to add more cluster members, use these instructions to add cluster members manually.

Before you begin

Before adding a new node, make sure to complete the prerequisite steps for the new node. Refer to steps 3 on page 21 and 4 on page 21 in "Prerequisite steps for a high availability system" on page 20.

1. Open the WebSphere Application Server Network Deployment administrative console.
2. Navigate to **Servers** → **Clusters** → **PremisesCluster** → **Cluster members**.
3. Click **New** to a new cluster member.
4. In the **Step 2: Create additional cluster members** panel, complete the following steps.
   a. Type a new member name.
   b. Select the node you wish to add as a new cluster member.
   c. Click **Add Member**.
   d. Click **Next**.
5. Click **Finish** to complete creating the new cluster member.
6. Save your master configuration, synchronize all nodes, and restart the cluster for your changes to take effect.

Installing silently

This topic describes how to perform a silent installation of the product.

About this task

Note: Silent uninstallation is not supported.

You must customize the sample response file for your environment before installing silently. Instructions on how to customize the file are also included in the sample file. After customizing the file, you can issue the command to silently install. Silent installation is particularly useful if you install the product often or if you are installing from a remote command prompt.

To run the installer in silent mode, follow these directions.

1. Choose the sample response file for your desired installation. The sample response files are located in the sat_installer\tasks directory of the WebSphere Premises Server CD appropriate for your operating system.

   Windows There are three sample response files for Windows operating systems:
   - PremisesSolutionForWindowsDB2_LAS_Task.xml for WebSphere Premises Server and Location Awareness Services for WebSphere Premises Server using DB2
   - PremisesSolutionForWindowsDB2_Task.xml for WebSphere Premises Server only using DB2
   - PremisesSolutionForWindowsOracle_Task.xml for WebSphere Premises Server only using Oracle

   Linux There are two sample response file for Linux operating systems:

- PremisesSolutionForLinuxDB2_Task.xml for WebSphere Premises Server only using DB2
- PremisesSolutionForLinuxOracle_Task.xml for WebSphere Premises Server only using Oracle

2. Accept the WebSphere Premises Server license.
   a. Open the IRU_install.iss file located in the sat_installer directory of the WebSphere Premises Server CD appropriate for your operating system.
   b. Replace `-G licenseAccepted=false` with `-G licenseAccepted=true`.

3. Open and update the sample response file.
   a. Specify the target computer for the deployment tasks.
      - Search for the `<targetHostname>` tag and specify the target computer name within that element for each deployment task.
      - If the target computer is not localhost, search for and uncomment the `<credentialsSat>` element. Then, update this line with the target computer's host name, user ID, and password.

        ```
        <addCredentials hostname="localhost" userId="Administrator" password="*******"/>
        ```

        Note: If you have more than one target computer for different deployment tasks, add this line for each of the target computers.
   b. Modify the required variable element ID attributes for the different applications to the correct values for your desired installation.

      Tip: Search for `<variable id=` to find all of the variable element ID attributes in the response file.

4. Clean the log files. If you ran the installer previously, be sure to remove any old log files.

   > **Windows** C:\Program Files\SolutionFiles\logs

   > **Linux** \opt\SolutionFiles\logs

5. Launch the installer in silent mode.

   > **Windows** For Windows operating systems:
   a. Open a command line prompt.
   b. Change directory to the location of the sat_installer directory.
   c. Run this command.

      ```
      WindowsSetup.exe -silent -W solutionLauncher.taskFileName="silent_response_filename"
      -options IRU_install.iss
      ```

   > **Linux** For Linux operating systems:
   a. Open a shell window.
   b. Change directory to the location of the sat_installer directory.
   c. Run this command.

      ```
      LinuxSetup -silent -W solutionLauncher.taskFileName="silent_response_filename"
      -options IRU_install.iss
      ```

   Note: The variable, *silent_response_filename*, means the name of the sample response file. Do not include the path of the file.

6. Verify the success of the installation by checking the logs. If there are log files in these directories, then the silent installation completed.

   > **Windows** C:\Program Files\SolutionFiles\logs

   > **Linux** \opt\SolutionFiles\logs

   If you see errors in the log files, refer to "Troubleshooting tips" on page 399 for possible resolutions to the problem.

Installing using Tivoli Provisioning Manager for Software

This topic describes how to install WebSphere Premises Server and its prerequisite software using Tivoli Provisioning Manager for Software.

Before you begin

Important: These instructions apply only if you are using Tivoli Provisioning Manager for Software to install the WebSphere Premises Server software on Windows operating systems.

Tivoli Provisioning Manager for Software is recommended for deploying multiple premises servers. It helps to automate the installation of the prerequisite software across multiple servers. Some steps must be performed manually on each server.

1. Check your hardware and operating system and make sure that they meet the necessary requirements.
2. Install Tivoli Provisioning Manager for Software using the instructions in the Tivoli Provisioning Manager for Software documentation.
3. Discover your endpoints (one for each WebSphere Premises Server) for Tivoli Provisioning Manager for Software.
4. Install the common agent on each endpoint server. If you are installing DB2, make sure to set the common agent as `LOCAL_SYSTEM` on the client server.
5. Set up Tivoli Provisioning Manager for Software to install the prerequisite software for WebSphere Premises Server.
   a. Copy the contents of WebSphere Premises Server for Windows operating systems (disk 2) to the Tivoli Provisioning Manager for Software server's C: drive.
   b. Copy WASEC61 directory on WebSphere Premises Server disk 2 to C:\IBM\SIF\isp\windows\cdimages\WASEC61.
   c. Extract *disk_root*\sat_installer\bin\com\ibm\jsdt\webserver\tree\ ihswin.xx.jar to C:\IBM\SIF\isp\windows\cdimages\WASND61.
   d. Extract *disk_root*\sat_installer\bin\com\ibm\jsdt\webserver\tree\ waswin.xx.jar to C:\IBM\SIF\isp\windows\cdimages\WASND61.
   e. Extract *disk_root*\sat_installer\bin\com\ibm\jsdt\webserver\tree\ db2win.xx.jar to C:\IBM\SIF\isp\windows\cdimages\DB2ESE91FP4.

      Note: If you are installing DB2, the provided response file uses the DB2 user name, `db2admin`, and the password, `Passw8rd`. The response file is located at *disk_root*\TPM\IBM\SIF\isp\windows\bin\ DB2ESE91FP4\SifInstall_DB2ESE91FP4.rsp

   f. Extract *disk_root*\sat_installer\bin\com\ibm\jsdt\webserver\tree\ mqwin.xx.jar to C:\IBM\SIF\isp\windows\cdimages\MQ6.
   g. Extract *disk_root*\sat_installer\bin\com\ibm\jsdt\webserver\tree\ mq6rp2fp3win.xx.jar to C:\IBM\SIF\isp\windows\cdimages\MQ602FP3.
6. Open the software packages in the Software Package Editor. You can launch Software Package Editor through Java Web Start or in an Eclipse environment.
7. Create the software package block by selecting **File** → **Save** → **Save to repository** and choosing **LocalFileRepository**.

   If you navigate to **Software Management** → **Manage Software Catalog** or if you open a software package block using the Software Package Editor, you should see the list of packages in the repository (LocalFileRepository).

Table 3. Data packages for Windows

Package name	Package description
Base61WinD	This package contains the directory structure and utilities that must be installed before the following packages.
Mq6WinD	Contains the installable image of WebSphere MQ 6.0
Mq602Fp3WinD	Contains WebSphere MQ 6.0.2 Fix Pack 3, which brings the product level to 6.0.2.3
Db2Ese91Fp4WinD	Contains the installable image of DB2 for Linux, UNIX, and Windows 9.1 Fix Pack 4 Enterprise Server Edition
WasNd61WinD	Contains the installable image of WebSphere Application Server 6.1.0.17 (includes IBM HTTP Server 6.1 and the Web Services plug-in for 6.1)
WasEc61WinD	Contains the installable image of WebSphere Application Server 6.1 Edge Components

Table 4. Installation packages for Windows

Package name	Package description
Mq6WinI	Installs WebSphere MQ 6.0
Mq602Fp3WinI	Installs WebSphere MQ 6.0.2 Fix Pack 3, which brings the product level to 6.0.2.3
Db2Ese91Fp4WinI	Installs DB2 for Linux, UNIX, and Windows 9.1 Fix Pack 4 Enterprise Server Edition
WasNd61WinI	Installs WebSphere Application Server 6.1.0.17 (includes IBM HTTP Server 6.1 and the Web Services plug-in for 6.1)
WasEc61WinI	Installs WebSphere Application Server 6.1 Edge Components

8. Select the target servers for the software package blocks, and install the "D" packages first. Distribute all "D" packages to the endpoints before distributing the "I" packages.

   For example, if you want to install DB2 for Linux, UNIX, and Windows 9.1 Fix Pack 4 remotely, distribute and install the packages in the following sequence.

   a. Base61WinD

   b. Db2Ese91Fp4WinD

   c. Db2Ese91Fp4WinI

   To install WebSphere MQ 6.0.2.3 remotely, distribute and install the packages in the following sequence.

   a. Base61WinD

   b. Mq6WinD

   c. Mq602Fp3WinD

   d. Mq6WinI

   e. Mq602Fp3WinI

To install WebSphere Application Server 6.1.0.17, IBM HTTP Server 6.1, and the Web Services plug-in for 6.1 remotely, distribute and install the packages in the following sequence:

a. Base61WinD

b. WasNd61WinD

c. WasNd61WinI

9. If you would like to change your DB2 password from the defaults used in the DB2 installation, follow these steps:

a. Navigate to **Start** → **Administrative Tools** → **Computer Management** → **Local Users and Groups** → **Users** on your Windows server.

b. Right-click **db2admin** and choose **Set Password**.

10. Follow the steps provided in "Installing WebSphere Premises Server" on page 26.

What to do next

If you need to uninstall the WebSphere Premises Server software, refer to "Uninstalling WebSphere Premises Server" on page 95.

Installing the Sensor Data Services for WebSphere Premises Server

Follow the steps in this topic to install the Sensor Data Services for WebSphere Premises Server.

About this task

The Sensor Data Services for WebSphere Premises Server installs WebSphere Premises Server on top of an existing WebSphere Remote Server 6.1 installation.

Note: The installer panels refer to Sensor Data Services for WebSphere Premises Server as WebSphere Premises Server.

1. Check your hardware and operating system and make sure that they meet the necessary requirements.

2. Make sure that you have completed all the prerequisite steps necessary for your environment and that you have already have an existing installation of WebSphere Remote Server.

3. Install the prerequisite software fix packs for WebSphere MQ, DB2 for Linux, UNIX, and Windows, and WebSphere Application Server.

   • WebSphere MQ 6.0.2.3 - available for download at: http://www.ibm.com/support/docview.wss?rs=171&uid=swg27007069

   • DB2 for Linux, UNIX, and Windows 9.1.4 - available for download at: http://www.ibm.com/support/docview.wss?rs=71&uid=swg21255572

   • WebSphere Application Server 6.1.0.17 - available for download at: http://www.ibm.com/support/docview.wss?rs=180&uid=swg27007951

4. Verify that you have properly installed WebSphere Application Server before installing the Sensor Data Services for WebSphere Premises Server.

5. Create the database.

6. Run the installation program located in the root directory of the Sensor Data Services for WebSphere Premises Server CD appropriate for your operating system.

    ▶ Windows setupwin32.exe

> **Linux** setupLinux.bin

> **Note:** Make sure you run setupLinux.bin from a shell window.

7. Choose the language for your installation.

8. In the installation wizard Welcome panel, click **Next** to continue.

9. Click the radio button beside the **I accept both the IBM and the non-IBM terms** statement if you agree to the license agreement and click **Next** to continue. After you accept the licensing terms, the installation wizard checks for the product prerequisites.

10. Select the installation directory for WebSphere Premises Server.

11. The installation wizard prompts you to select either a **Typical** or **Custom** installation.

    - Select the **Typical** radio button if you are installing both WebSphere Premises Server and the Bundle Repository Server. Click **Next** to continue.

        Important: If you are installing both WebSphere Premises Server and Bundle Repository Server on the same server, choose to install both (**Typical**) when prompted. If you choose to install one and later want to install the other, then you will need to uninstall and reinstall the product.

    - Select the **Custom** radio button if you are installing either WebSphere Premises Server or the Bundle Repository Server. Click **Next** to continue.

        Important: If you want to install Bundle Repository Server on a server separate from WebSphere Premises Server, install Bundle Repository Server before installing WebSphere Premises Server.

12. Choose a database type, either DB2 or Oracle, and click **Next**.

13. Enter your database information. If you would like the installation program to run database scripts to create tables and populate data on the database you have provided, check **Create and populate tables**. This option is especially useful for remote databases, reinstallation on the same server, and clustered environments. Click **Next**.

14. Choose your WebSphere Application Server installation location and profile and click **Next**.

    - Choose to install on an existing WebSphere Application Server profile by selecting one of the profiles available on the screen.

    - Choose to create a new profile for installation by selecting the box beside **Create new WebSphere profile**. This action brings up a WebSphere Application Server profile creation wizard.

        Note: If you are going to use any WebSphere Premises Server APIs or the Print, Verify, and Ship application, set the **HTTP transport port** to 9080 when you create the profile.

15. Enter your WebSphere Application Server profile information and click **Next**.

    - If you have WebSphere Application Server security enabled, you are prompted for the administrator ID and password, which will be validated in order to continue with the WebSphere Premises Server installation.

    - If you do not have WebSphere Application Server security enabled, then you may proceed without filling in an administrator ID and password.

16. Enter your Web server information or accept the defaults provided and click **Next**.

> **Note:** You are prompted for this information only if you chose to install the
> Bundle Repository Server.

17. Browse to your WebSphere MQ installation directory and click **Next**.
18. If you did not choose to install the Bundle Repository Server with WebSphere
    Premises Server, a panel prompts you to enter your Bundle Repository Server
    information.
19. A summary panel displays your installation selections. Click **Install** to
    continue the installation process.
20. When the installation is complete, another summary panel displays the
    installation status and prompts you to check the log files for any errors.

    install.log

    > Windows *IBM_RFID_HOME*\logs\install.log
    > Linux   *IBM_RFID_HOME*/logs/install.log

    If you do see errors or exceptions in the installation log files, try reinstalling
    the product after changing the installer's input values by according to the
    install.log file. If you are still seeing errors after reinstalling WebSphere
    Premises Server, contact IBM Support.

Results

When you have successfully completed the installation, your server should have
the following products installed:

- WebSphere Premises Server in this default location:

    > Windows C:\Program Files\IBM\RFID
    > Linux   /opt/IBM/RFID

- a Bundle Repository Server (installed either locally or remotely, if you chose to
  install it)

The installation also creates a bundle repository in your IBM HTTP Server
document root path, *IHS_HOME*\htdocs*system_locale*\bundles. For example, the
path for a Windows operating system may be C:\Program Files\IBM HTTP
Server\htdocs\en_US\bundles. This repository stores all the device application
bundles for OSGi Equinox for management by the Bundle Repository Server.

Post-installation steps
Before you begin

If you see errors with the installation, refer to "Troubleshooting tips" on page 399
for possible resolutions to the problem.

1. Make sure that the WAS_HOME environment variable is set to point to the
   WebSphere Application Server installation directory. The default installation
   directories for WebSphere Application Server are:

   > Windows C:\Program Files\IBM\WebSphere\AppServer
   > Linux   /opt/IBM/WebSphere/AppServer

   Important: If you have deployed WebSphere Premises Server remotely, you
   should log out from the target server and then log in again before
   continuing with the remaining post-installation steps in order to
   make sure that the WAS_HOME environment variable is applied
   correctly.

2. Make sure that the correct file paths are specified for the edge alerts and
   heartbeat log files in the SystemAgent.

See "Log file locations and settings" on page 386 for the default installation locations of the edge alerts and heartbeat log files.

3. Make sure that the delete filter for Data Capture and Delivery is set correctly in the SystemAgent. See "Setting the delete filter for Data Capture and Delivery" on page 211.

4. Make sure that the IBM RFID and DC Queue Managers are running.
   - **Windows** Open the WebSphere MQ explorer and look for IBM.RFID.QM and IBM.DC.QM in the Queue Managers folder. If there are green arrows next to each queue manager, then they are running.
   - **Linux** Run the command dspmq in /opt/mqm/bin. This command tells you the current status of a queue manager.

   If the queue managers are not running, refer to the WebSphere MQ information center for troubleshooting topics.

5. Make sure all WebSphere Application Server applications are running. Open the WebSphere Application Server administrative console, expand **Applications**, and click **Enterprise Applications**.

   The following applications should appear with green status arrows next to them:
   - AMITJ2EE
   - IBM_ALE_Application
   - IBM_Bundles_Management

     Note: If you installed Bundle Repository Server remotely, you will not see this application.
   - IBM_EPCIS_Adapter
   - IBM_Premises_Admin_Console
   - IBM_Premises_Diagnostics
   - IBM_Premises_Event_Monitor
   - IBM_Premises_DockDoorApp
   - IBM_Premises_PVSConsole
   - IBM_Premises_Server
   - IBM_Premises_Server_BIRT
   - IBM_SensorEvent_Engine
   - IBM_SensorEvent_Gateway

6. Open the WebSphere Premises Server Administrative Console to verify that it is accessible.

7. Check for errors in the WebSphere Application Server and WebSphere Premises Server log files. Refer to "Log file locations and settings" on page 386 for information about where to find the log files.

8. Open the config.ini file in the *IBM_RFID_HOME*\dts\configuration directory and update the server IP address, port number, bundle list file, and Data Capture and Delivery controller, as necessary.

   com.ibm.rfid.bundle.list.url=http://*IP_address:port_number*/bundleadmin/GetBundle?name=http://*IBM_HTTP_Server_IP_address*/bundles/bundlelists/**dc_core4dts.txt**

   This code specifies the URL used by the bundle loader to retrieve the list of bundles to load. If the Bundle Repository Server is on a separate server from WebSphere Premises Server, then replace the *IP_address* and *IBM_HTTP_Server_IP_address* values in this property with the IP address of the server hosting the Bundle Repository Server.

   The default port number is 9080. This port number is defined when you create your WebSphere Application Server profile.

The bundle list should be set to the dc_core4dts.txt file.

`com.ibm.rfid.edge.config.url=http://`*`IP_address:port_number`*`/ibmrfidadmin/premises.sl?action=getconfig&edge=`**`E2`**`&version=6.1`

This code specifies the Data Capture and Delivery controller to use. For testing purposes, the configuration uses the default E2 controller, which is shipped as a sample Data Capture and Delivery controller with WebSphere Premises Server. The E2 controller loads the Simulated Reader to help verify your configuration before testing with a real reader. For a production environment, use the E0 controller.

Note: This step and the next one help you associate WebSphere Premises Server to a local Data Capture and Delivery device that you can use to verify your installation. In a production environment you should use remote Data Capture and Delivery controllers. See "Installing a remote Data Capture and Delivery controller" on page 72 for details on how to install them.

9. Edit the dc_core4dts.txt file and provide the correct IP address of your Bundle Repository Server.

   The default is the localhost address, 127.0.0.1.

   `PREFIX http://`*`IP_address`*`/bundles/`

10. If Data Transformation service is started as a service, stop it and complete the following steps as they apply to your topology and desired configuration.

    a. Stop the Data Transformation service.

       - **Windows** For Windows operating systems, stop the service by going to **Start** ⇒ **Control Panel** ⇒ **Administrative tools** ⇒ **Services**. Select **IBM WebSphere Premises Server DT Service** and click **Stop**.

       - **Linux** For Linux operating systems, run the `ibm_dts_service stop` command in the *IBM_RFID_HOME*/dts directory.

    b. Modify the startup sequence for WebSphere Application Server, IBM HTTP Server, WebSphere MQ, and Data Transformation service.

       Windows For Windows operating systems, if you are running WebSphere Application Server, IBM HTTP Server, WebSphere MQ, and Data Transformation service on the same server, you need to ensure that the Data Transformation service starts after WebSphere Application Server and WebSphere MQ when the computer is rebooted. By default, there can be a situation where Data Transformation service starts before the other applications, resulting in errors.

       1) Run this command.

          Important: The Sc.exe command-line utility syntax requires a space after the = (equal symbol). For more information on this tool, see the Microsoft Web site.

          `sc config IBMWebSpherePremisesServerDTService depend= "MQSeriesServices/IBMHTTPServer6.1/IBMWAS61Service - PremisesNode"`

       2) Go to **Start** ⇒ **Control Panel** ⇒ **Administrative tools** ⇒ **Services**.

       3) Select **IBM WebSphere Premises Server DT Service**, right-click and select **Properties** ⇒ **Dependencies**.

          Data Transformation service should show a dependency on the starting of the WebSphere Application Server, IBM HTTP Server, and WebSphere MQ services.

       Note: Setting this dependency also means that the Data Transformation service will stop if you stop any one of the WebSphere Application

Server, IBM HTTP Server, or WebSphere MQ services. This dependency also assumes that all of these products are on the same server.

> **Linux** In a Linux environment, WebSphere Application Server and IBM HTTP Server are not automatically started when the computer reboots, but Data Transformation service and WebSphere MQ are automatically started. If all of the products are installed on the same server, the startup sequence can result in errors.

To reduce the possibility of errors occurring, remove the `ibm_dts_service` from the automatic startup by issuing this command:

```
chkconfig --level 35 ibm_dts_service off
```

11. Restart the Data Transformation service manually.
    - **Windows** For Windows operating systems, run the dts.bat file in the *IBM_RFID_HOME*/dts directory.
    - **Linux** For Linux, run the dts.sh file in the *IBM_RFID_HOME*/dts directory.

    These commands start the Data Transformation service and display a Data Transformation prompt.
12. Check the log files for any failures in loading the bundles.
13. Tune your database to improve performance.
14. If you are using the Print, Verify, and Ship example usage scenario, edit the contents of the pvsapp.properties file to point to the correct directory and host name for your IBM HTTP Server. Specifically, modify the following properties: `premises.hostname`, `report.location.csv`, and `report.location.csv.url`. The pvsapp.properties file is located in the \installedApps*profile_cell_name*\ IBM_Premises_PVSConsole.ear\ibmrfid_premises_pvsapp.war\config\ directory.
15. If you are using the Print, Verify, and Ship example usage scenario, enable ALE.
    a. Open the WebSphere Application Server administrative console.
    b. Navigate to **Resources** → **JMS** → **Activation specifications** → **ALEWrapperAS**.
    c. Change the text in the **Message selector** field to `ibmse='RfidInventory/TagReport' OR ibmse='RfidInventory/TagAggregationReport' OR ibmse LIKE '%/report/TagReport' OR ibmse LIKE '%/report/TagAggregationReport'`.
16. Verify the WebSphere Premises Server installation. Choose **R2** as your simulated test reader.

What to do next

If you need to uninstall the WebSphere Premises Server software, refer to "Uninstalling WebSphere Premises Server" on page 95.

Installing and enabling IBM Tivoli License Compliance Manager

Tivoli License Compliance Manager monitors license compliance. Basically, it recognizes and monitors what product offerings and their versions, releases, and fix packs are installed and used on the system.

WebSphere Premises Server supports the use of Tivoli License Compliance Manager server to collect and monitor usage information.

To install and enable Tivoli License Compliance Manager, you must download the Tivoli License Compliance Manager agent and install it on each WebSphere Premises Server. Instructions for downloading the Tivoli License Compliance Manager are documented in the Tivoli License Compliance Manager information center.

The required WebSphere Premises Server signature file for the Tivoli License Compliance Manager agent is deployed to WebSphere Application Server during the WebSphere Premises Server installation. A backup version of the file is located at:

> **Windows** `IBM_RFID_HOME\premises\itlm\WRPSRV_6_1_0_00601.SYS2`

> **Linux** `IBM_RFID_HOME/premises/itlm/WRPSRV_6_1_0_00601.SYS2`

Installing the toolkits

Use the topics below to install the toolkits shipped with WebSphere Premises Server.

Installing WebSphere Premises Server Toolkit

Use these steps to install the WebSphere Premises Server Toolkit.

1. Check your hardware and operating system and make sure that they meet the necessary requirements.
2. Start Rational Application Developer for WebSphere Software using a new workspace directory.
3. From the menu select **Help** → **Software Updates** → **Find and Install**.
4. Select **Search for new features to install** and click **Next**.
5. Click **New Local Site** and navigate to your local directory or network location containing the toolkit update site for WebSphere Premises Server Toolkit. The update site is located on disk 4 of the WebSphere Premises Server media package in the PremisesServerToolkit directory.
6. Expand the PremisesServerToolkit directory and select **ibmrfid_toolkit_update_site** and click **OK**.
7. Click **OK** to close the Edit Local Site window.
8. In the sites list, select only **PremisesServerToolkit/ ibmrfid_toolkit_update_site** and click **Finish**.
9. In the Search Results window, expand **PremisesServerToolkit/ ibmrfid_toolkit_update_site** → **IBM WebSphere Premises Server Toolkit** and select **IBM WebSphere Premises Server Toolkit Feature** *version*, where *version* is the number of the toolkit release you wish to install.
10. Click **Next**.
11. Accept the license agreement and click **Next**.
12. In the Installation window, click **Finish** to install the plug-in into the default location.

Note: If you choose to create a new WebSphere Application Server profile and you are going to use any WebSphere Premises Server APIs or the Print, Verify, and Ship application, make sure to set the **HTTP transport port** to 9080 when you create the profile.

13. In the Feature Verification window, click **Install All**.

14. When the installation completes, click **Yes** when prompted to restart the workbench.

15. If you see any errors after installation, refer to the troubleshooting tips in the WebSphere Premises Server Toolkit help.

What to do next

From within Rational Application Developer for WebSphere Software, click **Help** → **Help Contents** → **IBM WebSphere Premises Server Toolkit** and follow the steps to configure the toolkit.

If you need to uninstall the WebSphere Premises Server Toolkit software, refer to "Uninstalling the WebSphere Premises Server Toolkit" on page 97.

Installing IBM Data Capture and Delivery Toolkit for WebSphere Premises Server

Use these steps to install the IBM Data Capture and Delivery Toolkit for WebSphere Premises Server.

1. Check your hardware and operating system and make sure that they meet the necessary requirements.

2. Start Eclipse.

3. From the menu select **Help** → **Software Updates** → **Find and Install**.

4. Select **Search for new features to install** and click **Next**.

5. Click **New Local Site** and navigate to your local directory containing the toolkit update site for IBM Data Capture and Delivery Toolkit for WebSphere Premises Server. Then click **OK**. The update site is located on the CD containing the toolkits in the update directory.

6. If desired, enter a more descriptive name for the local site and click **OK**.

7. Click **Finish**.

8. Expand the new local site and select **IBM Data Capture and Delivery Toolkit** *version*.

9. Click **Next**.

10. Accept the license agreement and click **Next**.

11. Select an installation location and click **Finish**.

12. On the Feature Verification panel, review your choices and click **Install All**.

13. Click **Yes** when prompted to restart the Eclipse SDK.

14. When Eclipse has restarted, you can import the sample agents and launch configurations for IBM Data Capture and Delivery Toolkit for WebSphere Premises Server by selecting **File** → **New** → **Project** → **IBM WebSphere Premises Server Toolkits** → **Data Capture and Delivery Toolkit** and click **Next**.

15. Select **Data Capture**.

16. Click **Finish** to install the toolkit project in the current workspace.

What to do next

If you need to uninstall the IBM Data Capture and Delivery Toolkit for WebSphere Premises Server software, refer to "Uninstalling the IBM Data Capture and Delivery Toolkit for WebSphere Premises Server" on page 97.

Configuring the IBM Data Capture and Delivery Toolkit for WebSphere Premises Server

This task describes how to configure the IBM Data Capture and Delivery Toolkit for WebSphere Premises Server.

When using the IBM Data Capture and Delivery Toolkit for WebSphere Premises Server, make sure the Java compiler is set to compliance level 1.4. To verify and set the compliance level, start Eclipse and click **Window** → **Preferences** → **Java** → **Compiler**.

The following launch configurations are included in the toolkit:

DataCapture-FullSim
> Launches both the Simulated Reader and the simulated WebSphere Premises Server on one machine. This configuration launches the I/O Simulator, the Premises Simulator, and the Premises Simulator Status Window interfaces.

> The *I/O Simulator interface* allows you to simulate input and output pins.

> The *Premises Simulator interface* allows you to set the portal ID and the Data Capture and Delivery device ID, to start and stop the reader simulator on the Data Capture and Delivery device, to restart the OSGi framework for the Data Capture and Delivery device, and to reload the XML configuration for the Data Capture and Delivery device.

> The *Premises Simulator Status Window interface* allows you to set the Data Capture and Delivery device ID. It also displays the last heartbeat, the last alert, and the total batch processing time that was received from the Data Capture and Delivery device.

> This launch configuration works immediately after installation and no other machine or WebSphere Premises Server is required. You can use this launch configuration to verify the installation.

DataCapture-RdrSim
> Launches a remote Data Capture and Delivery device, the Simulated Reader, and the I/O Simulator interface. This configuration simulates a remote Data Capture and Delivery device that has a Simulated Reader and is connected to a WebSphere Premises Server (real or simulated) that is running on a separate machine. The I/O Simulator interface is also launched.

> This launch configuration requires another machine and also requires additional configuration.

DataCapture-LLRP
> Launches the LLRP reader agent and the I/O Simulator interface.

> Low Level Reader Protocol (LLRP) is a standard specification for the network interface between an RFID reader and its controlling software or hardware. For more information on LLRP, see http://www.epcglobalinc.org/standards/llrp/.

This launch configuration requires that WebSphere Premises Server (real or simulated) is running on another machine.

DataCapture-PremSim

Launches a simulated WebSphere Premises Server. The Premises Simulator interface and Premises Simulator Status Window interface are also launched.

The simulated server must be run on a separate machine from the Simulated Reader.

Launching the Simulated Reader and simulated WebSphere Premises Server on the local system

This section describes how to configure the Simulated Reader and WebSphere Premises Server simulator on a local system. This launch configuration allows you to run the simulators on one machine.

1. From within Eclipse, click **Run** → **Open Run Dialog...**.
2. Browse to and select **DataCapture-FullSim**. It is located under **OSGi Framework**.
3. Click **Run**.

Launching the Simulated Reader and I/O Simulator interface while connecting to a remote WebSphere Premises Server or Premises Simulator

This section describes how to configure the Simulated Reader and I/O Simulator interface when you are connecting it to a WebSphere Premises Server (real or simulated), which is located on another machine.

1. Ensure the configuration file that is sent to the Data Capture and Delivery controller contains the correct value for the `server.ip` property in the MicroBroker configuration agent. To do this, add the following line to the HOSTS file on the machine that hosts the Simulated Reader:

   `premises_server_ip_address put_premises_hostname_here`

   For *premises_server_ip_address*, enter the WebSphere Premises Server IP address. All instances of "put_premises_hostname_here" in the configuration file will be replaced with this IP address.

2. In the edge-rdrsim-llrp.xml file, which is located in the com.ibm.rfid.resource.toolkit project in the Configurations folder, modify the matrix.properties property of the PortalControllerAgent as follows:

   a. Make sure the following properties are commented as follows:

   ```
   <property key="matrix.properties" value="file:BDDR.properties"/>
   <!--<property key="matrix.properties"
   value="http://put_premises_hostname_here/bundles/BDDR.properties"/>-->
   ```

   b. Copy com.ibm.rfid.resource.toolkit/Matrices/BDDR.properties from the workspace to the root runtime directory. By default the root runtime directory is the Eclipse installation root, which is the directory location for the eclipse.exe file.

3. From within Eclipse, click **Run** → **Open Run Dialog...**.
4. Browse to and select **DataCapture-RdrSim**. It is located under **OSGi Framework**.
5. Click **Run**.

What to do next

The MicroBroker console view can be used to interact with the publish and subscribe engine and trigger events. Do not start the application ping bundle, which is stopped by default.

Note: On a remote system, Data Capture and Delivery cannot log messages unless you install the console log manually. For example, run the following command from the remote Data Capture and Delivery console:

```
install http://fully_qualified_host_name/bundles/com.ibm.rfid.console.log_version.jar start
```

The log level of the remote Data Capture and Delivery console is determined by the Alert Agent edge.log.threshold property in the Data Capture and Delivery XML configuration file. The default value of this property is error. If you change the value of this property, restart the remote Data Capture and Delivery environment or reload the configuration.

Launching the LLRP Reader while connecting to a remote WebSphere Premises Server or Premises Simulator

This section describes how to configure the LLRP Reader when you are connecting it to a WebSphere Premises Server (real or simulated), which is located on another machine.

1. Ensure the configuration file that is sent to the Data Capture and Delivery controller contains the correct value for the server.ip property in the MicroBroker configuration agent. To do this, add the following line to the HOSTS file on the machine that hosts the Simulated Reader:

   ```
   premises_server_ip_address put_premises_hostname_here
   ```

   For *premises_server_ip_address*, enter the WebSphere Premises Server IP address. All instances of "put_premises_hostname_here" in the configuration file will be replaced with this IP address.

2. In the edge-rdrsim-llrp.xml file, which is located in the com.ibm.rfid.resource.toolkit project in the Configurations folder, modify the matrix.properties property of the PortalControllerAgent as follows:

   a. Make sure the following properties are commented as follows:

   ```
   <property key="matrix.properties" value="file:BDDR.properties"/>
   <!--<property key="matrix.properties"
   value="http://put_premises_hostname_here/bundles/BDDR.properties"/>-->
   ```

   b. Copy com.ibm.rfid.resource.toolkit/Matrices/BDDR.properties from the workspace to the root runtime directory. By default the root runtime directory is the Eclipse installation root, which is the directory location for the eclipse.exe file.

3. From within Eclipse, click **Run** → **Open Run Dialog...**.

4. Browse to and select **DataCapture-LLRP**. It is located under **OSGi Framework**.

5. Click **Run**.

What to do next

The MicroBroker console view can be used to interact with the publish and subscribe engine and trigger events. Do not start the application ping bundle, which is stopped by default.

Note: On a remote system, Data Capture and Delivery cannot log messages unless you install the console log manually. For example, run the following command from the remote Data Capture and Delivery console:

```
install http://fully_qualified_host_name/bundles/com.ibm.rfid.console.log_version.jar start
```

The log level of the remote Data Capture and Delivery console is determined by the Alert Agent edge.log.threshold property in the Data Capture and Delivery XML configuration file. The default value of this property is error. If you change the value of this property, restart the remote Data Capture and Delivery environment or reload the configuration.

Launching the Premises Simulator

This section describes how to configure the Premises Simulator for use with the IBM Data Capture and Delivery Toolkit for WebSphere Premises Server.

1. From within Eclipse, click **Run** → **Open Run Dialog...**.
2. Browse to and select **DataCapture-PremSim**. It is located under **OSGi Framework**.
3. Click **Run**.

Adding additional XML configuration files to the Premises Simulator

This section describes how to add additional configuration files to the Premises Simulator for use with the IBM Data Capture and Delivery Toolkit for WebSphere Premises Server.

1. Copy the new configuration file to the Configurations directory within the com.ibm.rfid.resource.toolkit project. For example, com.ibm.rfid.resource.toolkit/Configurations/edge-samsys.xml.
2. Add a new, unique property to the com.ibm.rfid.premises.simulator.servlet.properties file within the com.ibm.rfid.premises.simulator.servlet.bundle package of the com.ibm.rfid.premises.simulator.servlet project, which maps the new configuration file to a Data Capture and Delivery controller ID. For example, E2=edge-samsys.xml.
3. Restart the Premises Simulator.

Migrating the product

Use these topics to migrate from WebSphere Premises Server 6.1 to WebSphere Premises Server 6.1.0.1.

Migrating WebSphere Premises Server

Use these instructions to migrate from WebSphere Premises Server 6.1 to WebSphere Premises Server 6.1.0.1.

Before you begin

1. Close the Data Transformation service console.
2. Stop all WebSphere Application Server processes.
3. If you are using a remote Bundle Repository Server, update WebSphere Application Server and IBM HTTP Server on the Bundle Repository Server to the level required by the fix pack. See "Hardware and software requirements" on page 17 for details.
4. If you are using Oracle, update to the level required by the fix pack. See "Hardware and software requirements" on page 17 for details.
5. Back up your database.
   1. Run the installation program located in the sat_installer directory of the WebSphere Premises Server disk appropriate for your operating system.

      If you have a Linux operating system, make sure you run LinuxSetup from a new shell window.

      > **Windows**   WindowsSetup.exe
      > **Linux**   LinuxSetup

      When you run the installation program, the deployment wizard is temporarily installed on your hard drive. It will uninstall itself when the installation is

complete. When the deployment wizard installation completes, it automatically launches and guides you through the installation of the product and its prerequisite software. It may take a few minutes to begin.

You can also run the installation program in silent mode. Refer to "Installing silently" on page 51 for further instructions.

2. Select the radio button beside the **I accept both the IBM and the non-IBM terms** statement if you agree to the license agreement and click **Next** to continue.

3. When the Welcome panel appears you can either:
   - Click **Next** to continue installing the product.
   - Or, if you would like to change the default path used for the deployment package, follow the instructions in "Changing the deployment package path" on page 23 before continuing with the next steps.

4. On the Select Tasks panel, click **Next** to install the product and to choose the database type.

5. Choose to use either DB2 or Oracle as your local or remote database.

6. Choose to install WebSphere Premises Server only and click **Next**.

   Important: Migration of Location Awareness Services for WebSphere Premises Server is not supported. You can update your Location Awareness Services for WebSphere Premises Server version from 6.1 to 6.1.0.1 using the installer, but any customization, such as defined areas and classes, will not be retained.

7. Click **Next** to install the required Bundle Repository Server.

   Note: If you do not install Bundle Repository Server on your local server, then you need to install the prerequisite middleware on the remote server before installing Bundle Repository Server. Make sure that you have purchased a separate license for the required middleware that you install on a remote server. Also, you will need to modify the WebSphere Premises Server SystemAgent to reflect the correct location of your Bundle Repository Server.

8. On the Specify Target Computers panel for your database server, specify the target computer for DB2 or your existing Oracle database and click **Next**.
   - For a local server installation for DB2 or an existing installation of Oracle, the default value is localhost. You can either keep this value or change it.
   - If you are installing the product and DB2 on separate servers, specify the fully qualified host name, operating system, user ID, and password of the server where DB2 should be installed.
   - If you are installing the product on one server and using an existing Oracle installation on another server, specify the fully qualified host name, operating system, user ID, and password of the server where Oracle is installed.
   - Optionally, use the **Test connections** button to test access to the remote target computer. Firewalls can have an adverse effect on the installation even though the connection test result is successful.

9. On the Specify Target Computers panel for WebSphere Premises Server, specify the target computer for WebSphere Premises Server and click **Next**.
   - For a local server installation, the default value is localhost. You can either keep this value or change it.

- If you are installing WebSphere Premises Server and its required middleware on a remote server, specify the fully qualified host name, operating system, user ID, and password of the server where it should be installed.
- Optionally, use the **Test connections** button to test access to the remote target computer. Firewalls can have an adverse effect on the installation even though the connection test result is successful.

10. On the Specify Target Computers panel for Bundle Repository Server, specify the target computer for Bundle Repository Server and click **Next**.
    - For a local server installation, the default value is localhost. You can either keep this value or change it.
    - If you are installing Bundle Repository Server on a remote server, specify the fully qualified host name, operating system, user ID, and password of the server where it should be installed.

        Remember: You must install the required middleware on the remote server before installing Bundle Repository Server.
    - Optionally, use the **Test connections** button to test access to the remote target computer. Firewalls can have an adverse effect on the installation even though the connection test result is successful.

11. Enter your database configuration information.
    - If you would like the installation program to run database scripts to migrate your existing tables and data on the database, check **Migrate existing 6.1 tables** and click **Next**.
    - If you would like the installation program to run database scripts to create new tables and populate new data on the database, check **Create and populate 6.1.0.1 tables** and click **Next**.
    - If you have already migrated your database manually with the scripts provided, select **Do not change the database**.

12. Enter the necessary information for WebSphere MQ and click **Next**.
    - ▶ Windows If you are installing on a Windows operating system, you are prompted to enter the installation directory for WebSphere MQ or accept the default installation directory.
    - ▶ Linux If you are installing on a Linux operating system, you are prompted for a password.

13. Enter your WebSphere Application Server configuration information and click **Next**.

    Important:
    - If you have an existing version of WebSphere Application Server that is 6.1.0.0 or later (but not the required version 6.1.0.17), and you want the installer to update your WebSphere Application Server version, then you must have WebSphere Application Server stopped before deploying the WebSphere Premises Server installation.
    - WebSphere Application Server security is not enabled by the installer. You must set up and configure security separately.
    - If you are going to use any WebSphere Premises Server APIs or the Print, Verify, and Ship application, make sure that the profile you choose to use has the **HTTP transport port** set to 9080.
    - If you do not plan to install WebSphere Premises Server and WebSphere Application Server on the default drive (such as the

C drive on Windows operating systems), click the **Advanced** tab for the configuration parameters and make sure your WebSphere Application Server profile path reflects the correct drive location for your installation.

14. Enter your IBM HTTP Server configuration information and click **Next**.

15. Enter the installation directory for WebSphere Premises Server.

16. Enter the configuration information for Bundle Repository Server.

17. On the Summary Panel, confirm your choices. The summary provides a list of tasks that you selected and an estimated time for their completion.
    - To start all installation and configuration tasks, click **Deploy all**.
    - If you only want to start a specific task, click **Deploy task**, but make sure that the tasks you choose are in the correct sequence on the panel. For example, you cannot deploy WebSphere Premises Server before deploying DB2 if you do not already have a database installed.

    Click **Back** to make any changes. After you start the deployment, you have the option to click **Stop Deployment** if you need to stop the installation before it is finished. Once all deployment tasks are complete, the Deployment Status screen indicates if the deployment was successful.

18. When the installation is complete, check the log files for any errors. From the Deployment wizard, you can view detailed messages or the master log. Click **Master log** and select **Save as...** to save the log file. The logs can be found in deployment_wizard_installation_dir/logs, where *deployment_wizard_installation_dir* is the installation location of the Deployment wizard.

    > **Windows** C:\Program Files\SolutionFiles\logs

    > **Linux** opt/SolutionFiles/logs

19. Click the X at the top, right-hand side of the panel to exit the wizard. The wizard displays some messages:
    - A prompt for whether you want to save changes. If you plan to run the wizard again, click **Yes**. Otherwise, click **No**.
    - A prompt for whether you wish to exit. Click **Yes** to exit the wizard.

20. If you want to use the simulated reader to verify your migration, run these SQL scripts for your database, either from a DB2 command line or from the Oracle sqlplus tool.

```
INSERT INTO SAGE.DCDEVICELOCATIONAGENT VALUES ('IBMSimulatedReaderAgent',
'com.ibm.rfid.reader.simulator.bundle.ReaderSimulatorManagedServiceFactoryActivator',
'TagReadingExpression', '(b1=true)', 'String', 'Tag Reading Expression',
'IBM Simulated Reader' ,'0','true', 'true' );

INSERT INTO SAGE.DCDEVICELOCATIONAGENT VALUES ('IBMSimulatedReaderAgent',
'com.ibm.rfid.reader.simulator.bundle.ReaderSimulatorManagedServiceFactoryActivator',
'log.level', '', 'String', 'log level','IBM Simulated Reader', '0','true', 'true' );
```

Results

When you have successfully completed the migration, the following software has been updated:
- WebSphere Premises Server version 6.1 to version 6.1.0.1
- WebSphere Application Server version 6.1.0.11 to version 6.1.0.17
- WebSphere MQ version 6.0.2.1 to version 6.0.2.3
- IBM HTTP Server version 6.1.0.0 to version 6.1.0.17
- DB2 for Linux, UNIX, and Windows version 9.1.2 Enterprise Standard Edition to version 9.1.4 Enterprise Standard Edition (if you are using this database)

What to do next

Follow the post-installation steps to verify your installation.

Migrating Sensor Data Services for WebSphere Premises Server

Follow these steps to migrate Sensor Data Services for WebSphere Premises Server from version 6.1 to version 6.1.0.1.

1. Upgrade the prerequisite software.

   Refer to "Hardware and software requirements" on page 17 for details. The prerequisite software fix packs for WebSphere MQ, DB2 for Linux, UNIX, and Windows, and WebSphere Application Server are available online:

   - WebSphere MQ 6.0.2.3 - available for download at: http://www.ibm.com/support/docview.wss?rs=171&uid=swg27007069
   - DB2 for Linux, UNIX, and Windows 9.1.4 - available for download at: http://www.ibm.com/support/docview.wss?rs=71&uid=swg21255572
   - WebSphere Application Server 6.1.0.17 - available for download at: http://www.ibm.com/support/docview.wss?rs=180&uid=swg27007951

2. Uninstall Sensor Data Services for WebSphere Premises Server.
3. Run the database migration scripts.
4. Install Sensor Data Services for WebSphere Premises Server 6.1.0.1.
5. If you want to use the simulated reader to verify your migration, run these SQL scripts for your database, either from a DB2 command line or from the Oracle sqlplus tool.

   ```
   INSERT INTO SAGE.DCDEVICELOCATIONAGENT VALUES ('IBMSimulatedReaderAgent',
   'com.ibm.rfid.reader.simulator.bundle.ReaderSimulatorManagedServiceFactoryActivator',
   'TagReadingExpression', '(b1=true)', 'String', 'Tag Reading Expression',
   'IBM Simulated Reader','0','true', 'true' );

   INSERT INTO SAGE.DCDEVICELOCATIONAGENT VALUES ('IBMSimulatedReaderAgent',
   'com.ibm.rfid.reader.simulator.bundle.ReaderSimulatorManagedServiceFactoryActivator',
   'log.level', '', 'String', 'log level','IBM Simulated Reader', '0','true', 'true' );
   ```

6. Verify your installation.

Migrating the database, tablespace, tables, and data

Use this topic to manually migrate the database, tablespace, tables, and populate the data required for WebSphere Premises Server. If you are using the WebSphere Premises Server installer to migrate the database, you do not need to follow these steps.

Migrating the databases using scripts

Run the scripts provided in the db_script directory on the WebSphere Premises Server disk to migrate the database, tablespace, tables and populate data.

Before you begin

Before running the scripts be aware of the following restrictions and take the appropriate action:

- You must be a database user (such as db2inst1 or oracle) to run the scripts on Linux.
- For Oracle, the sqlplus executable must be added in the PATH on Linux.
- The specified tablespace directory must exist.
- You must have the authorization to access the specified tablespace directory if you are using Linux only.
- The specified tablespace file cannot be used by another database.

Example

For DB2: `Windows`

```
migrateFrom6.1GA_db2.bat dbName longTablespaceFile longTempTablespaceFile
```

`Linux`

```
migrateFrom6.1GA_db2.sh dbName longTablespaceFile longTempTablespaceFile
```

For Oracle: `Windows`

```
migrateFrom6.1GA_oracle.bat dbUser dbPassword dbSpec longTablespaceFile
```

`Linux`

```
migrateFrom6.1GA_oracle.sh dbUser dbPassword dbSpec longTablespaceFile
```

The database, tablespace, table and data are created under dbSpec.

Verifying the installation

This topic provides instructions for how to verify that WebSphere Premises Server was installed successfully.

About this task

You can verify that WebSphere Premises Server has been correctly installed using a simulator instead installing of configuring additional hardware and software, such as readers and edge controllers.

The Simulated Reader is accessible through the WebSphere Premises Server Administrative Console. It uses an edge bundle, `com.ibm.rfid.reader.simulator`, to simulate tag reads at approximately 1 second intervals, which are shown on the console page in real time.

System administrators can also set the format of the output displayed in the Simulated Reader console page by modifying the `com.ibm.rfid.simulated.reader.display.complete.message` property in the SystemAgent. If the property is set to `false`, the Simulated Reader displays tag IDs. If the property is set to true, the Simulated Reader displays the complete XML tag read. The default value is `false`.

Note: The Simulated Reader is only intended to work with the default installation, using the BDDR.properties file (the Basic Dock Door configuration). The Simulated Reader is a very simple approximation of a real reader, and therefore does not behave completely like a real reader. It will stop and start like a real reader, send tags, and will *always* send an aggregation of tag data when turned off.

To verify your installation with the Simulated Reader, complete the following steps:

1. Complete the "Post-installation steps" on page 31.
2. Restart WebSphere Application Server.
3. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
4. Select **Simulated Reader** from the left navigation pane.
5. On the Simulated Reader console page, select a reader from the menu.

Note: The choices are limited to readers that are classified as
`IBMSimulatedReaderType`.

6. Click **Start Reader** to begin simulating tag reads.

   The following icons represent the status of the reader:

   - - The reader is off, but available.

   - - The reader status is unavailable.

   - - The reader is on and ready to read tags.

   You should see tag information appear in the output box.

7. Click **Stop Reader** to end simulating tag reads.

8. (Optional) Click **Reset Reader** to cancel the current start or stop request and reset the reader to its original state.

9. Click **Clear Output** to clear the displayed tag data.

Installing a remote Data Capture and Delivery controller

The bundle loader is an HTTP servlet that can be used to deploy Data Capture and Delivery on a remote server. To install bundles on your Data Capture and Delivery environment, the bundle loader uses a URL to receive a text file with a set of instructions for installing the bundle list. The bundle list is a file containing a list of bundles appropriate for your reader topology.

Use these topics to install a remote Data Capture and Delivery controller:

Installing the bundle loader and a bundle list

The bundle loader is an OSGi bundle that, when started, locates a list of bundles and performs the action specified on each bundle in the list.

The bundle list file format

The bundle list is a script in which each line is a command to the bundle loader to perform an action on a specified bundle. The actions that can be performed include START and INSTALL. The START action installs and starts a bundle, while the INSTALL action only installs a bundle. After the action command is the path to the bundle on which to perform the action.

The bundle list can contain the PREFIX command as well. When this is used, the string that follows PREFIX will be prepended to the name of each bundle in the bundle list.

The bundle list also supports the INCLUDE command. The INCLUDE command points to another bundle list that will also be read by the bundle loader.

This is an example of the file format:

```
// The line below will look for this exact file name
START org.eclipse.osgi.services_3.1.200.v20070605.jar
// The line below will look for a file beginning with this
// (assuming wildcarding is enabled on WebSphere Premises Server)
START org.eclipse.osgi.services_
```

The bundle list location

When the bundle loader starts, it looks in three locations for the bundle list URL:

- At startup it checks for the Configuration Admin (ConfigAdmin) service, which is an OSGi Managed Service. If the ConfigAdmin service is available and the bundle loader receives a configuration object it will look for the URL there.
- If either the ConfigAdmin is not available or the configuration object is empty, the bundle loader looks for a system property which is either set in the config.ini file or through a Java command line argument.
- If the bundle loader cannot find the list in the system property, then it looks at a default location in the file system for the ibm-rfid-bundle-list.txt bundle list.

After successfully receiving the bundle list, the bundle loader runs the commands in the list to install the bundles. This process is stored in the ConfigAdmin object as a result property (for example, `value="working"`). After this task is completed, the bundle loader saves the final result (as a success or a failure) in the result property. Then, when the bundle loader is restarted or when the configuration changes, the bundle loader looks in the result value to determine if it should download additional bundles.

Installing the bundle loader and bundle list
About this task

Use these steps to install the bundle loader and a bundle list. For reference, see the tools/remoteDC.zip sample packaged with the IBM Data Capture and Delivery Toolkit for WebSphere Premises Server.

Note: The sample config.ini uses 127.0.0.1 for the IP address of the WebSphere Premises Server. Change the value to the actual IP address if using the sample config.ini for a remote Data Capture and Delivery install.

1. Install Equinox on the server that will run the bundle loader.

   Equinox is packaged in the equinox folder of the IBM Data Capture and Delivery Toolkit for WebSphere Premises Server disk.

   Note: Other OSGi implementations are also supported, but this document only covers the Equinox implementation.

2. Create a configuration directory in the eclipse path in Equinox. For example, C:\equinox\eclipse\configuration.

3. Create a config.ini file in the configuration directory and add these lines to it:

   ```
   com.ibm.rfid.bundle.list.url=http://IP_address:port_number/bundleadmin/GetBundle?name=http://IBM_HTTP_Server_name/bundles/bundlelists/dc_core.txt

   com.ibm.rfid.edge.config.url=http://IP_address:port_number/ibmrfidadmin/premises.sl?action=getconfig&edge=E3&version=6.1
   ```

   The values for *IP_address* and *IBM_HTTP_Server_IP_address* are the name of the server that is hosting the Bundle Repository Server.

   The second line of code configures Data Capture and Delivery to use the E3 controller, which is shipped as a sample remote controller with WebSphere Premises Server. The E3 controller loads the Simulated Reader to help verify your configuration before testing with a real reader.

4. Start the Equinox runtime.

   Note:
   - Be sure the Data Transformation service is running on the server (dts.bat).

- In the case of Data Transformation, the bundle loader bundle is loaded, but not started. It must be started manually.
- The bundle lists are slightly different for Data Transformation (for example, dc_core.txt and dc_core4dts.txt). Be sure that you reference the correct bundle list version based on whether you are loading the list into a remote Data Capture and Delivery controller (dc_core.txt, dc_rdrsim.txt) or into Data Transformation (dc_core4dts.txt, dc_rdrsim4dts.txt).

5. Start the bundle loader.

   a. Find the ID of the bundle loader bundle by running the OSGi `ss` command.

   b. Start the bundle loader bundle by entering `start bundle_ID` at the OSGi prompt.

      Once the core Data Capture and Delivery bundles are loaded, Data Capture and Delivery pulls its configuration from WebSphere Premises Server (using the `com.ibm.rfid.edge.config.url=` property). If this configuration includes an update to the bundle list URL, then the bundle loader attempts to load that additional list of bundles.

      This is one method of installing multiple bundle lists into a Data Capture and Delivery controller. Data Transformation is set up with E2 to run the reader simulator. The Data Transformation config.ini file points to dc_core4dts.txt file to load the core bundles, and the Data Capture and Delivery configuration then points to the dc_rdrsim4dts.txt file to then load the reader simulator. For additional methods for installing bundle lists, refer to "Installing additional bundle lists."

6. Test the configuration using the Simulated Reader in the WebSphere Premises Server Administrative Console. Choose **R3** as your simulated test reader.

7. Create a new remote Data Capture and Delivery controller based on the E3 sample and use it with your real reader.

Installing additional bundle lists

Once the bundle loader is running, you can use it to load additional bundles. There are several methods you can use to load the bundles.

One way to load additional bundles is to change the bundle list URL in the config.ini file of Equinox, and then restart Equinox. When the bundle loader is restarted, it reads the updated configuration and loads the bundles in the new bundle list specified in the config.ini file.

To do this in a production system with a remote Data Capture and Delivery controller, use the WebSphere Premises Server Administrative Console to update the `com.ibm.rfid.bundle.list.url` property in the bundle loader agent. Then navigate to **Controllers** in the left navigation pane of the console and click the controller you are using. Click the **Reload Configuration** button to reload your controller's configuration. This triggers the Data Capture and Delivery controller to reload its configuration, including the new bundle list URL, which causes the Bundle Loader to download the new bundle list.

To install additional bundle lists within the IBM Data Capture and Delivery Toolkit for WebSphere Premises Server, modify the edge XML used to configure the Data Capture and Delivery bundles by adding a block to the XML that configures the bundle loader. Then you can force a reload of the edge configuration (possibly by

restarting the edge configuration bundle) so that the bundle loader picks up the new configuration. The following is an example of the XML used to modify the bundle loader URL property:

```
<configuration pid="com.ibm.rfid.bundle.loader">
<properties>
 <property key="bundleListURL" value="file:///bundlelist2.txt"/>
 <property key="clearCache" value="false"/>
</properties>
</configuration>
```

For more information on configuring Data Capture and Delivery, see "Managing your configuration" on page 101.

Using wildcards with the bundle loader

If the bundle loader uses the Bundle Repository Server on WebSphere Premises Server to read the bundle list, then you can use a form of wildcarding for the bundle names in the bundle list.

By default, wildcarding is turned off, so the bundle names in the bundle list must be an exact match to the bundles you want to load. To turn on wildcarding, follow these steps:

1. Set the com.ibm.rfid.bundle.server.fullname property in the bundleserver.properties file to true.

   The bundleserver.properties file is located in the *IBM_RFID_HOME*/dms/ properties directory.
2. Restart WebSphere Application Server, if it has already been started, in order for the change to take effect.

If wildcarding is turned on, then the Bundle Repository Server matches the name of each bundle in the bundle list to the bundles in its bundles directory. If it finds an exact match, then it uses the bundle that matches. If there is no match, then the Bundle Repository Server places a wildcard character on the end of the bundle name and returns the first bundle in alphabetic order that matches that pattern.

Defining the network topology

After the required software is installed on WebSphere Premises Server, the next step in installing your solution is to define the RFID network topology.

Before you begin

Before beginning this process, ensure that you:
- Obtain the IP addresses and port numbers of the tag readers and tag printers in the network.
- Obtain the MAC addresses of the Data Capture and Delivery controllers in the network.

About this task

The RFID network topology contains important information about the devices in your network. This information is stored in a configuration database on WebSphere Premises Server. The Data Capture and Delivery controller retrieves the configuration and uses it to set all of the bundle parameters including the Controller Manager and Digital I/O Manager. The following information is stored in the network topology:

- Agents and configuration properties
- Device IDs and configuration information for devices, such as tag readers and tag printers
- Location IDs for each store location, including dock door IDs
- Data Capture and Delivery controller IDs and configuration information

Use the WebSphere Premises Server Administrative Console to create and edit the topology definition.

1. Open the WebSphere Premises Server Administrative Console.. The Welcome page displays.
2. Create or download agents and configure their properties.
3. Define each device in the network.
4. Define location information (stores and dock doors) in this network.
5. Enter the Data Capture and Delivery controller IDs for the Data Capture and Delivery devices in the network.

Results

The network topology is created.

Using Data Capture and Delivery with Device Manager server

Use the instructions in these topics if you have an existing installation of Device Manager server, such as the one provided with WebSphere RFID Premises Server 6.0.x, and you would like to use it with Data Capture and Delivery.

Note: WebSphere Premises Server 6.1.x does not package or use Device Manager server with Data Capture and Delivery. This information is only for existing infrastructure with Device Manager server.

Preparing for remote deployment of the Device Manager client on a remote Data Capture and Delivery controller
Before you begin

Note: WebSphere Premises Server 6.1.x does not package or use Device Manager server with Data Capture and Delivery. This information is only for existing infrastructure with Device Manager server.

About this task

As described in "Installing the Device Manager client on a remote Data Capture and Delivery controller" on page 77, the deployment of a remote Data Capture and Delivery controller may include installing the Device Manager client code remotely from the Device Manager server. To allow remote deployment of the Device Manager client on a remote Data Capture and Delivery controller, perform the following steps:

1. Ensure the latest version of the rfid_dms_osgiclient.zip file is located in the *http_root*/htdocs/*locale*/bundles/DMS directory.
2. Extract the files directly into the Device Manager server directory.
3. Edit the file bundlefiles\dms18load.txt:
   - Comment out the "PREFIX" stanza pointing to the file system.

- Uncomment the stanza that points by means of HTTP to the bundlefiles directory.
- Fill in the correct host name.

For example:

```
//     Typically the bundles are in a local directory
//PREFIX file:./bundlefiles/

//     In case the bundles are on an HTTP server - here is an example
PREFIX http://host_name/bundles/DMS/bundlefiles/
```

Installing the Device Manager client on a remote Data Capture and Delivery controller

If you have an existing installation of Device Manager server, you can install the Device Manager client on the Data Capture and Delivery controller.

Note: WebSphere Premises Server 6.1.x does not package or use Device Manager server with Data Capture and Delivery. This information is only for existing infrastructure with Device Manager server.

In order for a remote Data Capture and Delivery controller to be deployed by the Device Manager server, it needs to run an OSGi runtime with the Device Manager client on it. The following steps install the Device Manager client on the OSGi runtime on the remote Data Capture and Delivery controller.

The files you need are contained in the rfid_dms_osgiclient.zip file. This file contains JAR files and a sample bundle loader configuration file for the Device Manager client in a directory named bundlefiles. In the root directory, the file contains a sample configuration file (sample_config.ini), a template for the Device Manager client configuration (OSGiAgent.properties.template), and two empty files (empty.txt and empty.xml) that the bundle loader and Data Capture and Delivery configuration bundle point to in their configuration settings.

You can install the Device Manager client by copying the necessary files to the Data Capture and Delivery controller or by connecting to the Device Manager server.

Installing the Device Manager client from the local machine

In this scenario, you copy necessary files to the Data Capture and Delivery controller. When the OSGi framework starts, the bundle loader installs the Device Manager client bundles with their necessary prerequisites and the Data Capture and Delivery bundles from the bundlefiles directory. The bundle loader is referenced by the osgi.bundles property in the configuration file.

About this task

Note: WebSphere Premises Server 6.1.x does not package or use Device Manager server with Data Capture and Delivery. This information is only for existing infrastructure with Device Manager server.

1. Copy the rfid_dms_osgiclient.zip file to the Data Capture and Delivery controller and extract the contents to the OSGi framework root directory.
2. Copy the applicable contents from the sample_config.ini file into your existing config.ini file.

   For example, copy the initial bundle list and the basic settings. The initial bundle list looks like:

```
osgi.bundles=bundlefiles/com.ibm.rfid.bundle.loader_version.jar@start
```
Also, the device manufacturer might provide additional settings in the config.ini file. If this is the case, these settings need to be merged with the contents of the sample_config.ini file.

The following settings are important for a Device Manager server deployment:

Note: Optionally, you can adapt the property com.ibm.rfid.dms.agentext.config.manufacturer to a meaningful value. The device manufacturer field on the Device Manager server contains the correct value.

```
com.ibm.rfid.bundle.list.url= file:./bundlefiles/dms18load.txt
com.ibm.rfid.edge.config.url=file:./empty.xml
com.ibm.rfid.edge.config.autostart=false
com.ibm.rfid.edge.config.interval= 30000
com.ibm.rfid.edge.config.bootstrap=true
com.ibm.rfid.edge.config.bootstrap.overrides=false
#
com.ibm.rfid.dms.agentext.config.manufacturer=Unknown
com.ibm.rfid.dms.agentext.config.modelextension=Edge
#the following line should remain commented out unless
#you want to define the DMS device name here
#com.ibm.rfid.dms.agentext.config.deviceidextension="staticExtension"
#For DMS notification you need to set the OSGi HTTP server port
#If you change this value you need to adapt the notification port
#on the DMS server
org.osgi.service.http.port=8777
```

3. Modify the OSGiAgent.properties.template based on your configuration and save the file as OSGiAgent.properties.bak. Set the Device Manager server address and device owner (dmsuser) user ID and password correctly.

   Note: DevId and Mod parameters are currently not supported.

4. Make sure that all OSGiAgentTree.bin files are deleted, including any backup files, such as OSGIAgentTree.bin.bak.

5. Make a copy and then rename the OSGiAgent.properties.bak to OSGiAgent.properties.

6. Start the OSGi framework.

7. Start the com.ibm.rfid.console.log bundle in order to see debug log messages.

8. Verify that the Data Capture and Delivery controller can connect to the Device Manager server. Check the HTTP server access log on the Device Manager server.

Results

The Device Manager client should now connect to the Device Manager server.

Installing the Device Manager client from the Device Manager server

In this scenario, you open an HTTP connection to the Device Manager server from the Data Capture and Delivery controller. When the OSGi framework starts, the bundle loader is retrieved from the Device Manager server and installs the Device Manager client bundles with their necessary prerequisites and the Data Capture and Delivery bundles to the Data Capture and Delivery controller using the HTTP connection. The bundle loader is referenced by the osgi.bundles property in the configuration file.

About this task

Note: WebSphere Premises Server 6.1.x does not package or use Device Manager server with Data Capture and Delivery. This information is only for existing infrastructure with Device Manager server.

1. Optional: Copy the applicable contents from the sample_config.ini file into your existing config.ini file.

   Tip: This task facilitates a large scale deployment. If you just want to do a quick test on one controller, you can skip this step and use the instructions in step 6 for loading your configuration.

   For example, copy the initial bundle list and the basic settings. The initial bundle list looks like:

   ```
   osgi.bundles=bundlefiles/com.ibm.rfid.bundle.loader_version.jar@start
   ```

   Also, the device manufacturer might provide additional settings in the config.ini file. If this is the case, these settings need to be merged with the contents of the sample_config.ini file.

   The following settings are important for a Device Manager server deployment:

   ```
   com.ibm.rfid.bundle.list.url= http://host_name/http_path/dms18load.txt
   com.ibm.rfid.edge.config.url=file:./empty.xml
   com.ibm.rfid.edge.config.autostart=false
   com.ibm.rfid.edge.config.interval= 30000
   com.ibm.rfid.edge.config.bootstrap=true
   com.ibm.rfid.edge.config.bootstrap.overrides=false
   #
   com.ibm.rfid.dms.agentext.config.manufacturer=Unknown
   com.ibm.rfid.dms.agentext.config.modelextension=Edge
   #the following line should remain commented out unless you want
   #to define the DMS device name here
   #com.ibm.rfid.dms.agentext.config.deviceidextension="staticExtension"
   #For DMS notification need to set the OSGi HTTP server port
   #If you change this value you need to adapt the notification port
   #on the DMSserver
   org.osgi.service.http.port=8777
   ```

2. Modify the OSGiAgent.properties.template based on your configuration and save the file as OSGiAgent.properties.bak. Set the Device Manager server address and device owner user ID (dmsuser) and password correctly.

   Note: DevId and Mod parameters are currently not supported.

3. Make sure that all OSGiAgentTree.bin files are deleted, including any backup files, such as OSGIAgentTree.bin.bak.

4. Make a copy and then rename the OSGiAgent.properties.bak to OSGiAgent.properties.

5. Start the OSGi framework.

6. From an osgi prompt, install the bundle loader.

   Tip: This task facilitates testing on one controller. If you followed the instructions for a large scale deployment in step 1, then you can skip this step.

   For example:

   ```
   osgi> install http://host_name/bundles/com.ibm.rfid.bundle.loader_6.0.0.v200703221650.jar
   ```

7. Start the bundle loader bundle and verify that the Device Manager client bundles are loaded and started correctly.

8. Start the com.ibm.rfid.console.log bundle in order to see debug log messages.

Results

The Device Manager client should now connect to the Device Manager server.

Using Device Manager server to change the bundle list URL

Note: WebSphere Premises Server 6.1.x does not package or use Device Manager
server with Data Capture and Delivery. This information is only for existing
infrastructure with Device Manager server.

If you are using Device Manager server to change the bundle list URL, make sure
the following is in your config.ini file:

```
com.ibm.rfid.bundle.loader.bootstrap=true
```

When this property is set to `true`, the bundle loader copies its relevant system
properties into ConfigAdmin so that a Device Manager server job can be submitted
later to update the values, including the value for the bundle list URL. When this
property is set to `false`, there is no configuration in ConfigAdmin and Device
Manager server is unable to update or create properties. By default the property is
set to `true`.

Creating Data Capture and Delivery configuration jobs

Use the XMLConfig tool to create Data Capture and Delivery configuration jobs.

Note: WebSphere Premises Server 6.1.x does not package or use Device Manager
server with Data Capture and Delivery. This information is only for existing
infrastructure with Device Manager server.

The XMLConfig tool was installed with WebSphere RFID Premises Server 6.0.x and
can be found in the *IBM_RFID_HOME*\premises\tools\dms path. There is an XML
directory that contains samples. Replace the values in these samples, as well as in
the samples included in this document, with your Device Manager server host
name, user ID (for example, dmsuser), and password in order to access the Device
Manager server Web Service. Also, specify the device name under which the Data
Capture and Delivery controller registers on the Device Manager server.

Use Device Manager commands to interact with the Device Manager server to
check job status or create jobs to retrieve the Edge Configuration Node Tree. You
can also perform these actions with the Device Manager Application. Run the
commands from the following directory:

```
IBM_RFID_HOME\DeviceManager\dmadmcli\bin
```

Refer to the following sample commands (see the Device Manager Help for more
details):
* Check jobs and their status for the OSGi device type:
  ```
  dmlsjob -dc OSGi
  ```
* Check job progress for an individual device:
  ```
  dmlsprogress -n device_ID -out PAIR
  ```
* Retrieve the Edge Configuration (Node Discovery):
  ```
  dmaddjob -dc OSGi -n device_ID -no T -jt SYNCMLDM_WTREE -jp
  TREE_WALKER_TARGET_URI=./OSGi/BundleConfiguration STORE_NODES=yes SEARCH_DEPTH=2
  ```

After running this command, you can access the Edge Config Admin settings on the Device Manager server using the Device Management Console. Right click on the device and select **View Inventory...** → **Management Tree**.

The initial deployment works with a Data Capture and Delivery controller that has been set up correctly using Device Manager server. After the initial OSGi framework startup, the device registers at the Device Manager server and waits for a Device Manager job to run.

To start the initial deployment of the Data Capture and Delivery software, verify that the Data Capture and Delivery controller registered successfully by listing all devices in the Device Management Console. Then create a Node Discovery job using the command described above and verify the Inventory Management Tree.

Use the XMLConfig tool to create a multistep configuration job. You can use the following XML as a template. Replace *device_ID* with the ID that the Data Capture and Delivery controller enrolls at the Device Manager server.

```
<?xml version="1.0" encoding="UTF-8"?>

<dms-task>
 <server uid="user_ID" passwd="password">
  <url value="http://dms_host_name/dmserver/servlet/rpcrouter"/>
 </server>

 <job action="replace" type="SYNCMLDM_CMD" deviceClass="OSGi" notification="True"
     deviceName="device_name">   <!--MUST BE EXISTING DEVICE-->
  <param name="1#REPLACE_ITEM_1_TARGET_URI"
value="./OSGi/BundleConfiguration/com.ibm.rfid.bundle.loader/bundleListURL"/>
  <param name="1#REPLACE_ITEM_1_DATA"
value="http://dms_host_name/bundleadmin/GetBundle?name=
http://host_name/bundles/bundlelists/file_name.txt"/>
  <param name="1#REPLACE_CMD_NUMBER" value="1"/>
  <param name="2#REPLACE_ITEM_1_TARGET_URI" value=
"./OSGi/BundleConfiguration/com.ibm.rfid.edge.config/com.ibm.rfid.edge.config.url"/>
  <param name="2#REPLACE_ITEM_1_DATA" value=
"http://rfid_host_name:port/ibmrfidadmin/premises.sl?action=
getconfig&amp;edge=device_ID"/>
  <param name="2#REPLACE_CMD_NUMBER" value="2"/>
  <param name="3#REPLACE_ITEM_1_TARGET_URI"
value="./OSGi/BundleConfiguration/com.ibm.rfid.edge.config/
com.ibm.rfid.edge.config.autostart"/>
  <param name="3#REPLACE_ITEM_1_DATA" value="true"/>
  <param name="3#REPLACE_CMD_NUMBER" value="3"/>
 </job>
</dms-task>
```

This sample job configures the bundle loader to retrieve a bundle list file from the Device Manager server using the bundleadmin servlet. It also configures the EdgeConfig bundle to retrieve the EdgeConfig XML file from WebSphere Premises Server. After this job runs successfully, start another node discovery job to verify the deployment results.

Note: If you copy and paste this sample XML into a file, the line breaks are replaced by blanks. Make sure you remove these blanks from your XML file.

Installing the WebSphere Application Server log file adapters

Follow the instructions below to install the WebSphere Application Server log file adapters on WebSphere Premises Server using the Tivoli Enterprise Console.

About this task

The WebSphere Application Server log file adapters enable you to view exceptions that occur on WebSphere Premises Server from the Tivoli Enterprise Console. You must first load the adapters into the Tivoli Enterprise Console, and then distribute them to your premises servers. The adapters then run as services on WebSphere Premises Server, allowing you to view the exceptions from the console.

Note: You must have Tivoli Enterprise Console installed on your Tivoli server and Tivoli endpoints installed on each premises server. For instructions on how to install these products, refer to the product documentation for Tivoli Enterprise Console. Refer to the online help in the Tivoli Enterprise Console for additional information about performing the tasks below.

1. Ensure that the following files exist in the *IBM_RFID_HOME*\monitoring directory:
   - wasjava.cds
   - wasjava.conf
   - wasjava.fmt
   - wasjava.baroc
2. Edit the following properties in wasjava.conf:
   a. Set the path to the WebSphere Application Server log file that you want to monitor.
   b. Set the Event Server name.
   c. Modify the value of the `BufEvtPath` attribute if the file named is already in use by another adapter.
   d. Adjust the `PollInterval` attribute to a suitable value.
3. Open the Tivoli Desktop.
4. Select an existing policy region or create a policy region to contain the profile manager for log file monitoring.
5. Add **ACP** to the selected policy region as a managed resource type.
6. Add **Profile Manager** to the selected region as a managed resource type.
7. Open the policy region and create a new Profile Manager.
8. Open the new Profile Manager and create a new ACP profile
9. Open the new profile for editing and add a **tecad_win** entry.
10. Click the **General** tab of the new entry and select **Identifer**. Then enter a descriptive name in the **Identifier Name** field.
11. Click the **Distribution** tab of the entry and double-click the **C/tecad_win.fmt** entry. You can now edit the entry.
12. Edit the value to reflect the location of the supplied wasjava.fmt file. Click the check mark button to save the changes.
13. Enter `tecad_win.cds` as the property name, and enter the path to the supplied wasjava.cds file as the property.
14. Click the check mark button to add the property.
15. Add the tecad_win.conf file using the supplied wasjava.conf file.
16. Click **Save & Close** to save the entry.
17. Set the subscribers for the profile manager to include the WebSphere Premises Server from which you want to monitor the WebSphere Application Server.
18. Import the supplied wasjava.baroc file.

19. After importing the new classes, compile the Rule Base and load it into the Event Server.
20. Distribute the profile to WebSphere Premises Server. After distribution, a new service should be listed in the Windows Services Manager, with an ID equal to the Identifier Name given to the ACP entry.

What to do next

Now, the log file adapter should be monitoring the log file entered into the wasjava.conf file. Exceptions logged to the WebSphere Application Server log file are changed to an instance of the `Was_Java_Exception` class and sent to the Tivoli Enterprise Console Event Server.

Installing the edge controller heartbeat log file adapters

Follow these instructions to install the edge controller heartbeat log file adapters on one or more WebSphere Premises Server using the Tivoli Enterprise Console.

About this task

The edge controller heartbeat log file adapters enable you to view the status of edge controllers and tag readers from the Tivoli Enterprise Console. You must first load the adapters into the Tivoli Enterprise Console, and then distribute them to your Premises servers. The adapters then run as services on WebSphere Premises Server, allowing you to view the exceptions from the console.

Note: You must have Tivoli Enterprise Console installed on your Tivoli server and Tivoli endpoints installed on each premises machine. For instructions on how to install these products, refer to the product documentation for Tivoli Enterprise Console. Refer to the online help in the Tivoli Enterprise Console for additional information about performing the tasks below.

1. Ensure that the following files exist in the *IBM_RFID_HOME*\monitoring directory:
   - tecad_win.cds
   - tecad_win.conf
   - tecad_win.fmt
   - premises.baroc
2. Edit the following properties in tecad_win.conf:
   a. Set the path to the edge-hearbeats.log file that you want to monitor.
   b. Set the Event Server name.
   c. Modify the value of the `BufEvtPath` attribute if the file named is already in use by another adapter.
   d. Adjust the `PollInterval` attribute to a suitable value.
3. Open the Tivoli Desktop.
4. Select an existing policy region or create a policy region to contain the profile manager for log file monitoring.
5. Add **ACP** to the selected policy region as a managed resource type.
6. Add **Profile Manager** to the selected region as a managed resource type.
7. Open the policy region and create a new Profile Manager.
8. Open the new Profile Manager and create a new ACP profile
9. Open the new profile for editing and add a **tecad_win** entry.

10. Click the **General** tab of the new entry and select **Identifer**. Then enter a descriptive name in the **Identifier Name** field.
11. Click the **Distribution** tab of the entry and double-click the **C/tecad_win.fmt** entry. You can now edit the entry.
12. Edit the value to reflect the location of the supplied tecad_win.fmt file. Click the check mark button to save the changes.
13. Enter `tecad_win.cds` as the property name, and enter the path to the supplied tecad_win.cds file as the property.
14. Click the check mark button to add the property.
15. Add the tecad_win.conf file using the supplied tecad_win.conf file.
16. Click **Save & Close** to save the entry.
17. Set the subscribers for the profile manager to include the WebSphere Premises Server from which you want to monitor the edge-heartbeats.log file.
18. Import the supplied premises.baroc file to load the necessary classes into the Tivoli Enterprise Console Event Server.
19. After importing the new classes, compile the Rule Base and load it into the Event Server.
20. Distribute the profile to WebSphere Premises Server. After distribution, a new service should be listed in the Windows Services Manager, with an ID equal to the Identifier Name given to the ACP entry.

What to do next

At this point, the log file adapter should be monitoring the log file entered into the tecad_win.conf file. Exceptions logged to the WebSphere Application Server log file will change to an instance of the `Was_Java_Exception` class and be sent to the Tivoli Enterprise Console Event Server.

Configuring security for WebSphere Application Server

Use scripts provided to enable or disable security for WebSphere Application Server with WebSphere Premises Server or Location Awareness Services for WebSphere Premises Server.

Enabling security

Scripts are provided to enable WebSphere Application Server security for WebSphere Premises Server and for Location Awareness Services for WebSphere Premises Server. You can also use these scripts to disable security at a later time.

The following are a few key concepts that you should understand about WebSphere Application Server security for WebSphere Premises Server and for Location Awareness Services for WebSphere Premises Server:

- A WebSphere Application Server administrative user has administrative access to the WebSphere Application Server administrative console. There can be more than one user who is a WebSphere Application Server administrative user. See Authorizing access to administrative roles in the WebSphere Application Server Information Center for more information.
- You must create an administrative operating system user for WebSphere Premises Server. The WebSphere Premises Server administrative user either has the user name, ibmrfidadmin, or is another user name in the ibmrfid group. The WebSphere Premises Server administrative user has administrative rights to the

WebSphere Premises Server Administrative Console. This user can also be a WebSphere Application Server administrative user, if you decide to set up your users and authorization in that way.

- Location Awareness Services for WebSphere Premises Server needs a WebSphere Application Server administrative user when you enable security, but this user does not have to be the same WebSphere Application Server administrative user that WebSphere Premises Server uses.
- "Enabling security for WebSphere Premises Server"
- "Enabling security for Location Awareness Services for WebSphere Premises Server" on page 86

Enabling security for WebSphere Premises Server
Before you begin

The ws_security script enables WebSphere Application Server security. Before running the ws_security script, ensure the following:

- A local user exists
- Or a local user group exists and has users in it

You will set a local user as the WebSphere Application Server administrative user so that after WebSphere Application Server security is enabled, you can sign on to the WebSphere Application Server administrative console as an administrator. If you want your WebSphere Application Server administrative user to have administrator access to the WebSphere Premises Server Administrative Console as well, then that user must be in the ibmrfid group.

1. Navigate to the security directory:

   Windows *IBM_RFID_HOME*\premises\install\security\

   Linux *IBM_RFID_HOME*/premises/install/security/

2. Run the following command:

   ws_security enable *userid password*

   - *userid* = Local OS user ID

     This is the user ID of the WebSphere Application Server administrator. This user must be ibmrfidadmin or must belong to the group called ibmrfid if you want the user to have administrative access to the WebSphere Premises Server Administrative Console. The WebSphere Application Server administrator ID cannot be the same as the name of your server because the repository sometimes returns server-specific information when querying a user of the same name. For more information, refer to the Local operating system settings topic in the WebSphere Application Server Information Center.

     If you have installed Location Awareness Services for WebSphere Premises Server, a WebSphere Application Server administrative user ID also has to be set in atlas.config.bat file under WASADMIN.

   - *password* = Local OS password.

     This is the password of the WebSphere Application Server administrator.

     If you have installed Location Awareness Services for WebSphere Premises Server, a WebSphere Application Server administrative password also has to be set in atlas.config.bat file under WASPSWD.

Enabling security for Location Awareness Services for WebSphere Premises Server

Complete the following steps to configure security for WebSphere Application Server when you have Location Awareness Services for WebSphere Premises Server installed. Enabling security in WebSphere Application Server provides security for the Spatial Management Client and portlets.

About this task

Note: You should not perform the steps if Location Awareness Services for WebSphere Premises Server is not installed.

1. If you have not already done so, follow the steps to run the `ws_security` script and enable security for WebSphere Application Server.

2. Navigate to the root installation directory of Location Awareness Services for WebSphere Premises Server (such as, C:\LAS).

3. Edit the `atlas.config.bat` file and define the values for WASADMIN and WASPSWD.

   The script expects that WebSphere Application Server security is already enabled. The values for WASADMIN and WASPSWD should reflect the WebSphere Application Server administrative user ID and password, respectively. These values can match the user ID and password that you used previously with the ws_security script, or they can match the ID and password for another WebSphere Application Server administrative user that you have set.

4. Open a command prompt and change to the *LAS_HOME*\WAS\scripts directory.

5. Run the ATLASWAS_SecurityConfig.bat file by typing `ATLASWAS_SecurityConfig` at the command-line prompt.

   The script completes the following actions:

   - Creates the following groups on the operating system: lassmcadministergrp, lasmonitorgrp, lasoperategrp, lasadministergrp, laslocategrp, lasregistrategrp, lasconfiguregrp, and lascustomizegrp.
   - Creates the user lasoveradmin with password lasoveradmin. This superuser can run Location Awareness Services for WebSphere Premises Server functions in the WebSphere Application Server administrative console. Use the lasoveradmin superuser for testing or proof-of-concept environments only. The lasoveradmin user should not be used in production environments.
   - Applies security settings.

6. Configure security for AtlasBus. Complete these steps to ensure that you can import data into Location Awareness Services for WebSphere Premises Server.

   a. Open the WebSphere Application Server administrative console and log in with your WebSphere Application Server administrative user ID and password.

   b. Select **Security** → **Secure administration, applications and infrastructure** → **Java Authentication and Authorization Service** → **J2C Authentication Data**.

   c. From the list select **AtlasMEAuthentication** and specify your WebSphere Application Server administrative user ID and password.

   d. Click **OK** and save your change.

   e. Navigate to **Security** → **Bus Security** → **AtlasBus**.

   f. Select **Security** under **Additional Properties**.

g. Check **Enable bus security** and select **AtlasMEAuthentication** as the inter-engine authentication alias.

h. For **Permitted transports**, choose the radio button to **Restrict the use of defined transport channel chains to those protected by SSL**.

i. Click **Apply**.

j. Under **Additional Properties**, click **Users and groups in the bus connector role**.

k. If there is no entry for the user, click **New → User name**, enter your WebSphere Application Server administrative user ID for AtlasMEAuthentication in the text field and click **OK**.

l. Navigate to **Resources → JMS → Queue connection factories → AtlasImportQueueConnectionFactory**.

m. Under **Advanced Administrative**, select **AtlasMEAuthentication** as the **Component-managed authentication alias**.

n. Save your changes.

o. Navigate to **Applications → Enterprise Applications → AtlasImportEAR**.

p. Under **References**, click **Resource References** and perform the following steps:

- Under **Specify authentication method**, select **Use default method (many-to-one mapping)** and then select **AtlasMEAuthentication** as the authentication data entry.

- In the table at the bottom of the page, select **jms/ AtlasImportConnectionFactory** as the **Target Resource JNDI Name**.

- Also in the table, check **AtlasImportEJB** and then click **Apply**.

In the right hand column of the table for AtlasImportEJB, AtlasMEAuthentication should be listed as the authentication method.

q. Click **OK**.

r. Navigate to **Resources → JMS → Activation specifications → AtlasCeiSubscribeAS** and select **AtlasMEAuthentication** as the authentication alias.

s. Click **OK**.

t. Save the configuration.

7. Navigate to **Users and Groups → Administrative Group Roles**.

8. Assign the following roles to the following groups:

Role	Group
lasadminister	lasadministergrp
laslocate	laslocategrp
lasregistrate	lasregistrategrp
lasmonitor	lasmonitorgrp
lasoperate	lasoperategrp
lasconfigure	lasconfiguregrp
lascustomize	lascustomizegrp

For each group, complete the following steps:

a. If the group is listed on the Administrative Group Roles page, click the group name and then assign one or multiple roles.

b. Click **Apply** to save your changes.

    c. If the group is not listed on the Administrative Group Roles page, click **Add** to add the group. Then assign one or multiple roles to the group.

    d. Click **Apply** to save your changes.

    e. Verify the correct roles are now assigned on the Administrative Group Roles page.

9. Navigate to **Security** → **Secure administration, applications, and infrastructure**.

10. Make sure that the following parameters are set:

- **Enable administrative security** is selected.
- **Enable application security** is selected.
- **Use Java 2 security to restrict application access to local resources** is *not* selected.
- **Current realm definition** is set to **Local operating system**.
- **Available realm definitions** is set to **Local operating system**. Then click **Configure** and set **Primary administrative user name** to the WebSphere Application Server administrative user name and click **Automatically generated server identity**.

11. Save your settings and restart WebSphere Application Server. You might need to enter the WebSphere Application Server user ID and password.

12. Edit the *LAS_HOME*\AtlasIntegrator\Data_Export.properties file to specify the real host name of your server instead of `localhost`.

13. Verify that security is running by logging into the WebSphere Application Server administrative console. If security is enabled, you are prompted for your WebSphere Application Server user ID and password. A random user ID is no longer accepted.

What to do next

Follow the steps in "Configuring security for the Control Processing portlet" on page 92.

Disabling security

Use the instructions in this topic if you have enabled WebSphere Application Server security for WebSphere Premises Server or for Location Awareness Services for WebSphere Premises Server and would like to disable it.

Since WebSphere Premises Server and Location Awareness Services for WebSphere Premises Server share the same WebSphere Application Server administrative console, if you disable security for WebSphere Premises Server, then security is also disabled for Location Awareness Services for WebSphere Premises Server. Be sure to follow the instructions in "Disabling security for WebSphere Premises Server and Location Awareness Services for WebSphere Premises Server" on page 89 to properly disable security when you have both software packages installed.

- "Disabling security when only WebSphere Premises Server is installed" on page 89
- "Disabling security for WebSphere Premises Server and Location Awareness Services for WebSphere Premises Server" on page 89

Disabling security when only WebSphere Premises Server is installed
Before you begin

These instructions are for disabling WebSphere Application Server security when you have only WebSphere Premises Server installed. If you have both WebSphere Premises Server and Location Awareness Services for WebSphere Premises Server installed, follow the instructions in "Disabling security for WebSphere Premises Server and Location Awareness Services for WebSphere Premises Server."

1. Navigate to the security directory for WebSphere Premises Server:

   Windows *IBM_RFID_HOME*\premises\install\security\

   Linux *IBM_RFID_HOME*/premises/install/security/

2. Run the following command:

   `ws_security disable *userid password*`

   - *userid* = Local OS user ID. This is the user ID of the WebSphere Application Server administrator.
   - *password* = Local OS password. This is the password of the WebSphere Application Server administrator.

Disabling security for WebSphere Premises Server and Location Awareness Services for WebSphere Premises Server

If you have installed Location Awareness Services for WebSphere Premises Server, complete the following steps to disable security for AtlasBus. Completing these steps ensures that you can import data into Location Awareness Services for WebSphere Premises Server after turning off security.

1. Open the WebSphere Application Server administrative console and log in with your WebSphere Application Server administrative user ID and password.
2. Select **Security** → **Bus Security** → **AtlasBus**.
3. Under **Additional Properties** select **Security**.
4. Clear the check box beside **Enable bus security**.
5. Choose to enable all transport chains. This step enables AtlasIntegrator to connect to the AtlasBus on a non-secure port.
6. Click **OK**.
7. Save the configuration.
8. Navigate to the security directory for WebSphere Premises Server:

   Windows *IBM_RFID_HOME*\premises\install\security\

   Linux *IBM_RFID_HOME*/premises/install/security/

9. Run the following command:

   `ws_security disable *userid password*`

   - *userid* = Local OS user ID. This is the user ID of the WebSphere Application Server administrator.
   - *password* = Local OS password. This is the password of the WebSphere Application Server administrator.

Configuring Location Awareness Services for WebSphere Premises Server

These topics describe how to configure Location Awareness Services for WebSphere Premises Server.

Configuring the database

Use this topic to modify the database for Location Awareness Services for WebSphere Premises Server.

Manually importing the sample data

This topic describes how to manually import the sample data if you did not choose to import it during installation.

Importing sample data for S-1 group languages:
About this task

If your language is in the S-1 group, complete the following steps to predefine sample values.

1. Change directory to the *LAS_HOME*\DB2\sampleData directory.

   If your DB2 server is remote, copy the DB2 directory to the database server and complete these instructions on that server.

2. Run this command, where %DB2ADMIN% is your DB2 administrative user ID and %DB2PSWD% is the corresponding password:

   ```
   db2cmd /c /w /i ATLASDB_SampleDataImport.bat %DB2ADMIN% %DB2PSWD%
   ```

Importing sample data for languages not in the S-1 group:
About this task

If your language is not in the S-1 group, complete the following steps to predefine sample values.

1. Navigate to the *LAS_HOME*\DB2 directory.
2. Verify that your DB2 user ID and password settings are correct in the SetUser.bat file.
3. Change directory to the *LAS_HOME*\DB2\sampleData directory.

   If your DB2 server is remote, copy the DB2 directory to the database server and complete these instructions on that server.

4. Run this command:

   ```
   db2cmd /c /w /i ATLASDB_IMPORT_S2D.bat
   ```

Installing the Spatial Management Client

This topic contains the steps for installing the Spatial Management Client.

Before you begin

Make sure that you installed the prerequisites for the Spatial Management Client. See "Hardware and software requirements" on page 17.

1. Make sure you installed Adobe SVG viewer on the system where you will run the user interface. You can download the Adobe SVG viewer from http://www.adobe.com/svg/viewer/install/main.html.
2. Make sure your browser is configured to run Active X plug-ins:
   a. Open your browser.
   b. Select **Tools** → **Internet Options**.
   c. On the **Security** tab, select **Internet** and click **Custom Level**.
   d. Select the zone where WebSphere Application Server and IBM HTTP Server are running. Make sure that both domains match the same zone.
   e. Make sure the following settings are correct and click **OK**:

- **ActiveX controls and plug-ins:**
  - Click **Enable** for **Automatic prompting for ActiveX controls**.
  - Click **Enable** for **Binary and script behaviors**.
  - Click **Prompt** for **Download signed ActiveX controls**.
  - Click **Disable** for **Download unsigned ActiveX controls**.
  - Click **Disable** for **Initialize and script ActiveX controls not marked as safe**.
  - Click **Enable** for **Run ActiveX controls and plug-ins**.
  - Click **Enable** for **Script ActiveX controls marked safe for scripting**.
- **Downloads:**
  - Click **Enable** for **Automatic prompting for file downloads**.
  - Click **Enable** for **File download**.
  - Click **Enable** for **Font download**.
- **Miscellaneous:**
  - Click **Enable** for **Access data sources across domains**.
  - Click **Enable** for **Allow META REFRESH**.
  - Click **Disable** for **Allow scripting of Internet Explorer Web browser control**.
  - Click **Disable** for **Allow script-initiated windows without size or position constraints**.
  - Click **Prompt** for **Allow Web pages to use restricted protocols for active**.
  - Click **Prompt** for **Display mixed content**.
  - Click **Disable** for **Don't prompt for client certificate selection when no certificates or only one certificate exists**.
  - Click **Enable** for **Drag and drop or copy and paste files**.
  - Click **Prompt** for **Installation of desktop items**.
  - Click **Prompt** for **Launching applications and unsafe files**.
  - Click **Prompt** for **Launching programs and files in an IFRAME**.
  - Click **Enable** for **Navigate sub-frames across different domains**.
  - Click **Enable** for **Open files based on content, not file extension**.
  - Click **Medium safety** for **Software channel permissions**.
  - Click **Enable** for **Submit nonencrypted form data**.
  - Click **Disable** for **Use Pop-up Blocker**.
  - Click **Enable** for **Userdata persistence**.
  - Click **Enable** for **Web sites in less privileged web content zone can navigate into this zone**.
- **Scripting:**
  - Click **Enable** for **Active scripting**.
  - Click **Enable** for **Allow past operations via script**.
  - Click **Enable** for **Scripting of Java applets**.
- **User Authentication:**
  - Click **Automatic logon only in Intranet zone** for **Logon**.
3. Open the *IHS_HOME*\htdocs\en_us\Tracking GUI\xml\prefsV3.xml file and make sure that you have replaced `localhost` with the IP address or fully qualified host name of your server in the `<host>` element.

Remember: The value you specify for the `<host>` element and the value you use to browse to the Spatial Management Client must be identical.

4. Open http://*host_name_or_IP_address*/Tracking GUI/AtlasPrefsAdmin.html and verify that your preferences are set correctly:
   - **Host** - Enter the IP address or fully qualified host name of your Location Awareness Services for WebSphere Premises Server server.
   - **Port** - Enter the port number that WebSphere Application Server listens on.
   - **remoteLogPath** - The full path name to the logs directory on the IBM HTTP Server. The Spatial Management Client logs to this directory. For example, C:\IBMHTTPServer\htdocs\en_US\Tracking GUI.
   - **Poll interval:** Enter a value to indicate the rate in milliseconds that tag data is requested from the server.

     Note: Changing this value does not affect the frequency at which a tracked item's position is reported to the system. It only affects the frequency with which the GUI is updated.

   - Click **Save Installation Changes** to save your changes to the preferences.

     These preference settings will apply each time the user logs in to the Spatial Management Client.

5. Open the Spatial Management Client using one of the following URLs:
   - http://*host_name_or_IP_address*/Tracking GUI/AtlasAdmin.html (administration version)
   - http://*host_name_or_IP_address*/Tracking GUI/AtlasMonitor.html

   Note: The variable *host_name_or_IP_address* indicates the fully qualified host name or IP address of the machine on which IBM HTTP Server is installed, which is also the Location Awareness Services for WebSphere Premises Server server. The default port number is 80; however, if a different port number is used, you must specify the new port number (*host_name_or_IP_address:port_number*).

   For more information about the Spatial Management Client, see the topics on starting the Spatial Management Client.

6. Ensure that application db2AssetMgmtEAR has been installed and is started in your WebSphere Application Server.

Configuring security for the Control Processing portlet

Complete these steps to enable security for the Control Processing portlet.

Before you begin

Important: You must enable security for WebSphere Application Server before completing these steps.

About this task

Each time a new user logs into the WebSphere Application Server administrative console to use Location Awareness Services for WebSphere Premises Server, they must perform the following step in the Control Processing portlet.

The user must be a member of the lasoperategrp or an equivalent group for these steps to work.

1. Open the WebSphere Application Server administrative console and navigate to **Topology** › **Event Provider**.
2. Select your event provider and click **Edit**.
3. Set the **Related App Server ID** to your IP address.
4. Navigate to **Control Processing**.
5. Click **Refresh List**.
6. Click **Edit** (the wrench icon) in the upper right corner.
7. Enter the user name and password of the current user.
8. Click **Save**.

Using the sample subscriber and notification programs

This topic describes how to use the two sample subscriber programs that are shipped with Location Awareness Services for WebSphere Premises Server: sample mail service program and sample alert events subscriber program.

About this task

The sample subscriber and notification programs are referenced in the sample data and can be used to verify your installation. If you do not want to use them, you can deactivate them.

1. In the *http_root*\htdocs\en_us\wsdl\EmailHandler.wsdl file, make sure that the *host_name: portnumber* key value pair reflects the real WC_defaulthost port. The sample includes 9080 as the port number.
2. In the Mail Server portlet, configure your mail server:
   a. Open the WebSphere Application Server administrative console and click **Rules/Alerts** › **Mail Server**.
   b. On the Mail Host Configuration page, click **Add**.
   c. In **Host Address**, enter the IP address or fully qualified host name of your mail server.
   d. In **Port**, enter the port number.
   e. In **Default Sender**, enter your e-mail address.
   f. In **Default Subject**, enter a default subject line to send with the notification.
   g. Click **Save** to save your settings.
3. In the Mail Receiver portlet, specify receiver information for users who should receive notification of specific events:

   Note: Times are relative to times on the database server. The machines that host the database server and WebSphere Application Server must be set to the same time zone.

   a. Open the WebSphere Application Server administrative console and click **Rules/Alerts** › **Mail Receiver**.
   b. Click **Add New Mail Receiver**.
   c. In **Receiver Name**, enter the name of a receiver.
   d. In **Receiver Address**, enter the e-mail address of a receiver.
   e. In **Week Days**, select the days of the week when the receiver should be notified of events.
   f. In **Start Time**, enter the time when the receiver should start receiving notification each day.

g. In **End Time**, enter the time when the receiver should stop receiving notification each day.

h. In **Alert Types**, select the type of alerts that the receiver should be notified about.

i. In **Mail Host**, select the mail server to associate with the receiver.

j. Click **Save** to save your settings.

Deactivate the sample programs
About this task

If you do not want to use the sample programs, perform the following steps:

1. In the Notification Channels portlet, remove the channels related to the programs that you want to deactivate:

   a. Open the WebSphere Application Server administrative console and click **Rules/Alerts** → **Notification Channels**.

   b. Select the check box next to the sample programs to remove and then click **Delete Selected**.

2. In the Notification Program Manager portlet, remove the entries for the programs that you want to deactivate:

   a. Open the WebSphere Application Server administrative console and click **Rules/Alerts** → **Notification Programs**.

   b. Select the check box next to the sample programs to remove and then click **Delete Selected**.

Verifying your installation

This topic explains how to verify your installation by verifying the Spatial Management Client and the subscriber programs.

Verifying the Spatial Management Client
This topic provides steps for verifying the Spatial Management Client installation.

Before you begin

Before verifying the Spatial Management Client installation, make sure you have performed the following tasks:

- Installed the Spatial Management Client and set your preferences in the Preferences Administration GUI. See step 3 on page 91 in "Installing the Spatial Management Client" on page 90.
- Adapted the hub data to the needs of the application and pointed to the correct server IP address and event provider hubs or controllers.

1. Follow the steps in "Configuring security for the Control Processing portlet" on page 92.

2. In the Control Processing portlet, start the tag processing servlet:

   a. Open the WebSphere Application Server administrative console and click **Control Processing**.

   b. Select the WebSphere Application Server that is related to your installation and click **Start Selected**.

3. Start the Spatial Management Client by opening the following URL: http://*fully_qualified_host_name*/Tracking GUI/AtlasMonitor.html, where *fully_qualified_host_name* is the fully qualified host name of the system where you installed IBM HTTP Server and the Spatial Management Client.

4. Define your preferences in the Location Awareness Services for WebSphere Premises Server Preferences Administration GUI. Start the GUI by opening the following URL: http://*fully_qualified_host_name*/Tracking GUI/ AtlasPrefsAdmin.html. See "Preferences Administration GUI" on page 261 for more information.

   Note: It is only necessary to define your preferences once per installation and user.

5. Under **ZONES**, select **All** from the **Visible** drop-down menu to see all defined zones. The location entitled **Matrix** has been predefined in the database and you should see three sample zones for this location.

6. Under **ALERTS**, select **Yes** from the **Hide** drop-down menu to hide all alerts or select **No** to view all alerts.

7. Start the hub simulator:

   `location_of_hub_simulator\HubSim.bat`

   The variable *location_of_hub_simulator* indicates the directory where the hub simulator is located. It must be a subdirectory of the directory in which atlas.config.bat file is located. For example, C:\LAS\HubSimulator.

8. View the simulated resources and events.

   Tip: If a tag icon is red, click the icon to see tag and alert details. Click **Acknowledge** to acknowledge the alert and the icon is no longer red. If you click the tag a second time to see details, the alert information for the tag is no longer visible.

Verifying the subscriber programs

This topic describes how to verify the subscriber programs.

Before you begin

Before verifying the subscriber programs, make sure you have performed the following tasks:

- Verified the Spatial Management Client successfully. See "Verifying the Spatial Management Client" on page 94.
- Installed the subscriber and sample notification programs and configured the mail server and receivers. See "Using the sample subscriber and notification programs" on page 93.
- When tag 00000007 enters the `myAlarm` zone in the `Matrix` area, an alarm is generated.

About this task

Verify the following:

- An e-mail is sent to the receiver you defined.
- A line is written in the sampleArchive.txt and sampleProtocol.txt files.

Uninstalling the product

Use the following topics to uninstall the product.

Uninstalling WebSphere Premises Server

This task describes how to uninstall WebSphere Premises Server and its related products and components.

About this task

The uninstaller file for WebSphere Premises Server removes the WebSphere Application Server code relative to WebSphere Premises Server, such as Enterprise Java Beans (EJBs), servlets, and Java Server Pages (JSPs). It also removes the WebSphere MQ code relative to WebSphere Premises Server, including queues and queue managers. It does not remove the WebSphere Premises Server database, but it does change the WebSphere Application Server configuration and settings for the WebSphere Premises Server applications.

Remember: To perform this task using a Linux operating system, log in as a root user.

You need to uninstall the products in the reverse order of their installation:
1. WebSphere Premises Server
2. IBM HTTP Server
3. WebSphere Application Server Network Deployment
4. WebSphere MQ
5. DB2 for Linux, UNIX, and Windows systems, if you chose to install the database
6. Location Awareness Services for WebSphere Premises Server, if you chose to install this component

If you are uninstalling Sensor Data Services for WebSphere Premises Server, follow the steps to uninstall WebSphere Premises Server (steps 1 through 4).
1. Ensure that WebSphere Application Server and WebSphere MQ are running, and that the Data Transformation service is not running.
2. Start the uninstallation wizard, and follow the instructions on the panels.
   - **Windows** `IBM_RFID_HOME\_uninst\uninstaller.exe`
     You can also use one of the following options:
     – Click **Start** ⊳ **All Programs** ⊳ **IBM WebSphere Premises Server** ⊳ **Premises Server** *version* and click the **Uninstall** icon.
     – Use the **Add or Remove Programs** application on Windows by clicking **Start** ⊳ **Control Panel** ⊳ **Add or Remove Programs**.
   - **Linux** `IBM_RFID_HOME/_uninst/uninstaller.bin`
3. A summary panel displays your uninstallation selections. Click **Uninstall** to continue the uninstallation process.
4. When the uninstallation is complete, another summary panel displays the uninstallation status. Click **Finish** to exit the uninstaller wizard.
5. Uninstall IBM HTTP Server.
6. Uninstall WebSphere Application Server Network Deployment.
7. Uninstall WebSphere MQ for Windows or Linux systems.
8. Uninstall DB2 for Linux, UNIX, and Windows for Windows or Linux systems.
9. If you installed Location Awareness Services for WebSphere Premises Server, remove its installation directory and the IBM HTTP Server htdocs\en_us\Tracking GUI directory.

Uninstalling a high availability system

This task describes how to uninstall your high availability WebSphere Premises Server system.

About this task

The high availability uninstaller restores your topology to a single WebSphere Premises Server.

Note: The information in this topic only applies to the version of WebSphere Premises Server that is available with a Central Site Server license.

1. If you have WebSphere Application Server security enabled, disable it. The uninstaller cannot run properly with security enabled.
2. Restart the deployment manager, all node agents, and all servers.
3. Start the uninstallation wizard, and follow the instructions on the panels.
    *   ▶ **Windows** *IBM_RFID_HOME*\HA_uninst\uninstaller.exe
    *   ▶ **Linux** `IBM_RFID_HOME`/HA/_uninst/uninstaller.bin
4. A summary panel displays your uninstallation selections. Click **Uninstall** to continue the uninstallation process.
5. When the uninstallation is complete, another summary panel displays the uninstallation status. Click **Finish** to exit the uninstaller wizard.
6. To remove your single WebSphere Premises Server, following the instructions in "Uninstalling WebSphere Premises Server" on page 95.

Uninstalling the toolkits

Use the topics below to uninstall the toolkits.

Uninstalling the WebSphere Premises Server Toolkit

This task describes how to uninstall the WebSphere Premises Server Toolkit.

1. Start Rational Application Developer for WebSphere Software.
2. Navigate to **Help** ▸ **Software Updates** ▸ **Manage Configuration**.
3. Expand **Rational Application Developer** in the left navigation pane.
4. Select **IBM WebSphere Premises Server Toolkit Feature** and then click **Uninstall** from the menu.
5. When prompted, click **OK** to restart Rational Application Developer for WebSphere Software.

What to do next

To uninstall any of the Rational Application Developer for WebSphere Software features, follow the instructions in the product documentation:

*   Rational Application Developer for WebSphere Software v7.0.0.3 Information Center

Uninstalling the IBM Data Capture and Delivery Toolkit for WebSphere Premises Server

This task describes how to uninstall IBM Data Capture and Delivery Toolkit for WebSphere Premises Server.

1. Start Eclipse.
2. Navigate to **Help** ▸ **Software Updates** ▸ **Manage Configuration**.
3. Expand the tree in the left navigation pane. Right click **IBM Data Capture and Delivery Toolkit** *version* and click **Uninstall**.
4. Restart Eclipse.

Chapter 4. Administering

The topics in this section describe how to perform administrative tasks for WebSphere Premises Server.

Checking the server version

Follow these steps to find out what version of WebSphere Premises Server you are running.

1. Locate the WebSphere Application Server SystemOut.log file. For the default location of the log files, see "Log file locations and settings" on page 386.
2. Open the SystemOut.log file and look for the application level of WebSphere Application Server.

   The application level line looks similar to this example:

   ```
   [8/27/08 8:28:27:767 PDT] 00000023 ApplicationMg A
   WSVR0203I: Application: IBM_Premises_Admin_Console  Application build level: 20080814_1530
   ```

WebSphere Premises Server Administrative Console overview

The WebSphere Premises Server Administrative Console is a Web-based application for defining the critical resources comprising your network, as well as the relationships among these various components.

This information is stored in a network topology database on the WebSphere Premises Server, where it is retrieved by the edge controller during device enrollment.

After the initial network topology is defined, you can modify any existing resources and perform other tasks such as modifying agent properties, creating new custom tasks, and viewing tag information. You can also restart edge controllers from the WebSphere Premises Server Administrative Console to immediately implement the changes.

Note: Use Mozilla Firefox or Internet Explorer 6.0 or later to open the WebSphere Premises Server Administrative Console. Ensure that JavaScript is enabled.

Attention: To prevent someone from overwriting your changes, be sure that when using the WebSphere Premises Server Administrative Console to modify configuration data for your RFID topology, that you make the changes from one Web browser window only.

Below is a list of the functions in the WebSphere Premises Server Administrative Console with links to corresponding topics:

- Data Capture Configuration - for information about this topic, refer to "Managing your configuration" on page 101.
  - Agent Configuration - see "Working with agents" on page 102
  - Devices - see "Working with devices" on page 150
  - Locations - see "Working with locations" on page 154
  - Controllers - see "Working with controllers" on page 162
  - Import Configurations - see "Importing the configuration file" on page 167
  - Print Templates - see "Working with print templates" on page 204

- – Update Sites - see "Working with update sites" on page 176
- – Find and Install - see "Downloading bundles" on page 177
- Event Processing - for information about this topic, refer to "Managing event processing" on page 178.
  - – Event Templates - see "Working with event templates" on page 179
  - – Output Channels - see "Working with output channels" on page 181
- EPC Configuration - for information about this topic, refer to "Managing the EPC configuration" on page 185.
  - – Profile Configuration - see "Working with profiles" on page 191
  - – Serial Number Configuration - see "Working with serial numbers" on page 193
  - – Company Prefix Index Translation - see "Working with the EPCglobal company prefix index" on page 196
- Reporting - for information about this topic, refer to "Reporting" on page 207.
  - – Tags - see "Viewing tag read reports" on page 207
- Verification - for information about this topic, refer to "Using the simulated reader" on page 212.
  - – Simulated Reader - see "Starting a simulated reader" on page 212, "Stopping a simulated reader" on page 213, and "Resetting a simulated reader" on page 213

See "Opening the WebSphere Premises Server Administrative Console" to get started.

Opening the WebSphere Premises Server Administrative Console

Use the WebSphere Premises Server Administrative Console to define and edit the components, and the relationships between these components, in your network topology.

About this task

These steps describe how to access the console from a remote server. If WebSphere Premises Server is installed on your local server, you can access the console by clicking **Start** → **All Programs** → **IBM WebSphere Premises Server** → **Premises Server** *version* → **Administrative Console**.

1. Open a new Web browser.

   Note: Use Mozilla Firefox or Internet Explorer 6.0 or later to open the WebSphere Premises Server Administrative Console. Ensure that JavaScript is enabled.

2. In the **Address** field of your Web browser, type `http:// premises_server_host_name:9080/ibmrfidadmin`, where *premises_server_host_name* is the host name of your WebSphere Premises Server.

   If WebSphere Application Server security is enabled, a login page displays. If WebSphere Application Server security is disabled, the administrative console displays without a login page. For instructions on how to enable WebSphere Application Server security, refer to "Configuring security for WebSphere Application Server" on page 84.

Managing your configuration

This section describes how to create and manage configuration groups for controllers, locations, and devices within your WebSphere Premises Server infrastructure using the WebSphere Premises Server Administrative Console and Data Capture and Delivery.

Use the WebSphere Premises Server Administrative Console to define and manage configuration groups that define the infrastructure components of the product. Configuration groups help you manage controllers, locations, agents, and devices (Bartender and Loftware logical printers, readers, and simulated reader) as part of a group instead of individually.

Configuration groups

WebSphere Premises Server offers three *configuration group types*: location type, controller type, and device type. Each configuration group type in the product defines a set of one or more agents with their configurations and a set of zero or more configuration group metadata properties. After you define a configuration group type, you assign agents and their configurations to it and then define the metadata to store with that configuration group. Configuration group and category metadata display on the WebSphere Premises Server Administrative Console; however, you define and manage the metadata through the XML configuration file that you import.

Note: The WebSphere Premises Server imports metadata files based on the Metatype Service Specification as defined within the OSGi Service Platform - Service Compendium, Release 4, August 2005 that is distributed by the OSGi Foundation. For additional information, go to www.osgi.org.

The product, by default, comes with several preset location configuration groups. One location configuration group is called *Enhanced Dock Door Receiving*. This location configuration group type contains all the agents that are part of the enhanced dock door receiving usage scenario along with the correct agent configurations. What this means is that an agent can exist in the system with different configurations for different configuration groups. In addition, you can associate each configuration group with a category. For example, you can create a device configuration group called *Sirit*. You then assign this configuration group, Sirit, to the category *reader*. Each category also has its own set of metadata properties.

You use the WebSphere Premises Server Administrative Console to implement and manage configuration groups. You can also import an XML document into the WebSphere Premises Server. The XML document enables you to create, update, and delete various product configuration groups and configuration group types.

For additional information about device, location, and controller configuration groups, refer to the topics below:
- "Device configuration group details" on page 154
- "Location configuration group details" on page 160
- "Controller configuration group details" on page 165

Configuring using the console or an XML file

You can perform the following functions using either the WebSphere Premises Server Administrative Console or the XML configuration file:

- Create, edit, and delete new location, controller, and device configuration groups.
- Create, edit, and delete locations, controllers, and devices (for readers, logical printers, and simulated readers).
- Assign locations to location configuration groups.
- Assign devices to device configuration groups.
- Assign controllers to controller configuration groups.
- Create, edit, and delete agents and agent properties for Data Capture and Delivery.
- Assign agents and their configurations to a configuration group.

You can perform the following functions only using the imported configuration XML file:

- Create new categories, and update and delete categories and category metadata.
- Create, update, and delete configuration group metadata.

Working with agents

This section explains Data Capture and Delivery agents and how to view and manage them using the Agent Configuration panel in the WebSphere Premises Server Administrative Console.

Agents are executable code modules that operate on events flowing through the system. WebSphere Premises Server comes with the following agent types: ControllerType, DeviceType, LocationType, TaskAgentType, and SystemType.

ControllerType
> An agent that creates or operates on events related to a Data Capture and Delivery controller.

DeviceType
> An agent that creates or operates on events related to a device, such as a printer or a reader.

LocationType
> An agent that creates or operates on events related to a location, such as a dock door.

TaskAgentType
> An agent that creates or operates on events that flow into and out of WebSphere Premises Server.

SystemType
> There is only one agent that is SystemType. This agent is the SystemAgent for WebSphere Premises Server. This agent controls the configuration settings for WebSphere Premises Server components.

This section contains the following topics:

Viewing existing agents
About this task

The Agent Configuration panel on the WebSphere Premises Server Administrative Console shows all of the agents defined for a particular agent type.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Navigate to **Data Capture Configuration** → **Agent Configuration** from the left navigation pane. The Agent Configuration panel displays.
3. In the **Agent Type** field, select the type of agent from the list. The table changes to display all agents defined for the type you indicated.
4. You can delete an agent from the list, add a new agent, or click **Cancel** to exit.

Understanding PIDs and factory PIDs

This topic explains Data Capture and Delivery persistent identities (PIDs) and factory PIDs.

A PID uniquely identifies a service or object within the OSGi stack that requires a configuration dictionary to be provided by the Configuration Admin service. All agents within the Data Capture and Delivery system have a PID which is used during creation, modification, or deletion. A factory PID is used to group a set of services or objects sharing a common type but having different configuration parameters. Agents having only a PID are also known as Managed Services and have only one instance per controller. Agents having both a PID and factory PID are configured through a Managed Service Factory and may have multiple instances per controller, but only one per portal.

For TaskAgents, the PID should match the Java package name of the agent, and you are not allowed to define Factory PIDs or multiple PIDs as part of the agent. For SystemAgent, you are not allowed to define additional PIDs.

For more information on PIDs and factory PIDs, see Section 104 of the OSGi Service Compendium, Release 4, Version 4.1, April 2007.

Adding and configuring a new agent and PIDs

This topic describes how to add a new agent and configure a persistent ID (PID) using the WebSphere Premises Server Administrative Console.

About this task

To define an agent, enter the agent name, a description of the agent, and indicate the agent type. A new agent can the following agent types: ControllerType, DeviceType, LocationType, or TaskAgentType. After adding an agent, you define properties for PIDs associated with the agent. For information about PIDs, refer to "Understanding PIDs and factory PIDs."

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. In the left navigation panel, navigate to **Data Capture Configuration** → **Agent Configuration**. The Agent Configuration panel displays.
3. Click **Create Agent**. The New Agent panel displays.
4. Enter a descriptive name for this agent.
5. In the **Agent Type** field, select the type of agent from the list.
6. Enter a unique description of the agent.

7. Click **Add PIDs to the Agent**.

   Note: For TaskAgents, the PID should match the Java package name of the agent, and you are not allowed to define Factory PIDs or multiple PIDs as part of the agent. For SystemAgent, you are not allowed to define additional PIDs.

   The Add Agent Properties panel is displayed with the new agent name and description. Use this panel to add properties to PIDs and PIDs to bundles.

8. In the **PID** field, enter the PID to which you are adding properties. If this PID is a factory PID, click the check box to select it. For an explanation of PIDs and factory PIDs, refer to "Understanding PIDs and factory PIDs" on page 103.

9. Enter the bundle name and bundle version to which you are associating the PID. This field is optional.

10. Enter the property information as follows:

    a. Enter the property name.

    b. Enter a value for this property.

    c. Enter a brief description of this property.

    d. Select the type of property from the list.

    e. Select the cardinality value from the list.

    f. Indicate whether the property is required. Select **true** to indicate that the property is required and **false** to indicate that it is not required.

    g. Indicate whether to include the property in the XML configuration file. Select **true** to include the property, even if it is not required, and **false** to not include it. This property is used by the Data Capture and Delivery configuration servlet that generates the XML configuration file that is sent to the Data Capture and Delivery component.

    h. To display a new line to add another property, click **Add Property**.

11. When you finish adding properties to a PID, click **Save**. The New Agent panel displays with the PID and properties that you entered.

12. To add another PID to this agent, repeat steps 7 through 11 above or click **Cancel**.

13. On the New Agent panel, when you finish adding PIDs to the agent, click **Done**.

Adding and configuring a PID for an existing agent

This topic describes how to add a PID and configuration properties to an existing agent using the WebSphere Premises Server Administrative Console.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.

2. In the left navigation panel, click **Data Capture Configuration** → **Agent Configuration**. The Agent Configuration panel displays.

3. Click on the agent that you are modifying. The Edit Agent panel displays.

4. Click **Add PIDs to the Agent**. The Add Bundle Properties panel displays.

5. In the **PID** field, enter the PID that you are adding to the agent. If this PID is a factory PID, click the **Factory PID** check box to select it. For an explanation of PIDs and factory PIDs, refer to "Understanding PIDs and factory PIDs" on page 103.

6. Enter the bundle name and bundle version to which you are associating the PID. This field is optional.

7. Enter the property information as follows:

a. Enter the property name.

   b. Enter a value for this property.

   c. Enter a brief description of this property.

   d. Select the type of property from the list.

   e. Select the cardinality value from the list.

   f. Indicate whether the property is required. Select **true** to indicate that the property is required and **false** to indicate that it is not required.

   g. Indicate whether to include the property in the XML configuration file. Select **true** to include the property, even if it is not required, and **false** to not include it. This property is used by the Data Capture and Delivery configuration servlet that generates the XML configuration file that is sent to the Data Capture and Delivery component.

   h. To display a new line to add another property, click **Add Property**.

8. When you finish adding properties to the PID, click **Save**. The Edit Agent panel displays with the PID and properties that you added.

9. Click **Update**.

Adding a new agent by downloading agent properties

This topic describes how to create a new agent by downloading agent details from an update site using the WebSphere Premises Server Administrative Console.

Before you begin

Before downloading agent details from an update site, make sure that WebSphere Application Server is running.

About this task

You can define an agent by downloading agent properties from an update site. For information about update sites, refer to "Working with update sites" on page 176.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.

2. In the left navigation panel, navigate to **Data Capture Configuration** → **Agent Configuration**. The Agent Configuration panel displays.

3. Click **Download Agent**. The Download Agent Properties panel displays.

4. Select **Create a new agent**.

5. In the **Agent Type** field, select the type of agent from the list. An agent can be ControllerType, DeviceType, or LocationType. Then click **Next**.

6. Select the update site to use for the new agent. Click **Next**.

7. Select a feature for the agent. The list of features is retrieved from the update site. Click **Next**.

    Note: The name and description of the new agent are taken from the feature you select.

8. Accept the license agreement and click **Next**.

9. Confirm your selections and then click **Finish** to begin the download process.

Results

During the download process, the status will be displayed in the Agent Configuration panel. If errors occur, you can delete the agent and then recreate it.

Note: During the download process, an XSL style sheet is used to transform the agent configuration supplied by the agent's vendor to the format that is required by WebSphere Premises Server. The default XSL file, IBMRFIDPremisesDefaultMapping.xsl, is stored in the *IHS_HOME*\bundles\ import_mappings directory. You can override the default XSL transformation by creating a new XSL file and storing it in the *IHS_HOME*\bundles\ import_mappings directory. The XSL file must have the same name as the update site's feature with an .xsl extension. The XSL file is only applied to device agents.

The input to and output from the XSL file follows the same schema used in the import XML file. See "Sample XML schema and configuration files" on page 167.

Modifying agent properties for a PID

This topic describes how to add or modify agent properties for a PID using the WebSphere Premises Server Administrative Console.

About this task

For an explanation of PIDs and factory PIDs, refer to "Understanding PIDs and factory PIDs" on page 103.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. In the left navigation panel, navigate to **Data Capture Configuration → Agent Configuration**. The Agent Configuration panel displays.
3. Click the agent that you are modifying. The Edit Agent panel displays.
4. Click the PID that you are modifying. The Edit Agent Properties panel displays.
5. Use one of the following functions to edit the properties:
   - To modify existing PID property information, modify the property settings in the **Agent Property List** and click **Update PID**.
   - To clear the settings of a property in this PID, select the checkbox next to the property and click **Clear Property**.
   - To delete a property from this PID, select the checkbox next to the property and click **Delete Property**.
   - To add a new property to this PID, click **Add Property**. A new entry line is displayed so that you can enter the property information.
     a. Complete the fields with the property information.
     b. At the top of the page, click **Update PID**. The Edit Agent panel redisplays.
     c. To update this agent in all configuration groups, click to select the **Update agent in all configuration groups** checkbox.
     d. Click **Update** to save your changes.

What to do next

Tip: You can add and modify agent properties using the **Data Capture Configuration → Agent Configuration** option on the WebSphere Premises Server Administrative Console. You can also modify an agent property in a particular device, location, or controller configuration group by accessing the configuration group. Refer to the following topics for instructions on modifying a configuration group:
  - "Modifying a device configuration group" on page 152

- "Modifying a location configuration group" on page 157
- "Modifying a controller configuration group" on page 163

Modifying agents by downloading agent properties

This topic describes how to modify an existing agent by downloading agent details from an update site using the WebSphere Premises Server Administrative Console.

Before you begin

Before downloading agent details from an update site, make sure that WebSphere Application Server is running.

About this task

You can modify an existing agent by downloading agent properties from an update site. For information about update sites, refer to "Working with update sites" on page 176.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. In the left navigation panel, navigate to **Data Capture Configuration** → **Agent Configuration**. The Agent Configuration panel displays.
3. Click **Download Agent**. The Download Agent Properties panel displays.
4. Select **Update an existing agent**.
5. In the **Agent Name** field, click the drop-down arrow and select an existing agent from the list. Then click **Next**.
6. Select the update site to use for the agent. Click **Next**.
7. Select a feature for the agent. The list of features is retrieved from the update site. Click **Next**.
8. Accept the license agreement and click **Next**.
9. Confirm your selections and then click **Finish** to begin the download process.

Results

During the download process, the status will be displayed in the Agent Configuration panel. If errors occur, you can delete the agent and then recreate it.

Note: During the download process, an XSL style sheet is used to transform the agent configuration supplied by the agent's vendor to the format that is required by WebSphere Premises Server. The default XSL file, IBMRFIDPremisesDefaultMapping.xsl, is stored in the *ihs_root*\bundles\ import_mappings directory. You can override the default XSL transformation by creating a new XSL file and storing it in the *ihs_root*\bundles\ import_mappings directory. The XSL file must have the same name as the update site's feature with an .xsl extension. For example, if you install the Intermec BRI Runtime Feature, the XSL file must be named "Intermec BRI Runtime Feature.xsl". The XSL file is only applied to device agents.

The input to and output from the XSL file follows the same schema used in the import XML file. See "Sample XML schema and configuration files" on page 167.

Deleting agent properties from a PID

Use the WebSphere Premises Server Administrative Console to delete Data Capture and Delivery agent properties from a PID.

About this task

Complete the following steps to delete agent properties from a PID.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. In the left navigation panel, navigate to **Data Capture Configuration** ⇒ **Data Capture Agent Configuration**. The Agent Configuration panel displays.
3. Click the agent that you are modifying. The Edit Agent panel displays.
4. Click the PID that you are modifying. The Edit Agent Properties panel displays.
5. Click the check boxes to select the properties that you want to delete and click **Delete Property**. The properties are removed from the properties list.

Deleting a PID from an agent

This topic describes how to delete a PID from an agent using the WebSphere Premises Server Administrative Console.

About this task

Note: Do not delete all PIDs associated with an agent before adding a new one. An error will occur. To avoid the error, add a new PID before deleting existing PIDs.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. In the left navigation panel, navigate to **Data Capture Configuration** ⇒ **Agent Configuration**. The Agent Configuration panel displays.
3. Double-click on the agent that you are modifying. The Edit Agent panel displays.
4. Click to select the check box beside the PID you are deleting.
5. Click **Delete Selected**. A message displays asking you to confirm the deletions.
6. Click **OK**.

Configuring the PortalControllerAgent to use flexible timer values

Use these instructions to make the timer values more flexible for the PortalControllerAgent.

The PortalControllerAgent can support two timer settings in the matrix.properties file. In releases prior to WebSphere Premises Server 6.1 Fix Pack 1, each timer was associated with one timeout value. In Fix Pack 1, you can make a timeout value flexible, meaning you can apply one timer to different timeout values. In order to do this, the `timer1.delay` and `timer2.delay` properties have been replaced by one `timer.delay` property.

In a default installation of WebSphere Premises Server, the PortalControllerAgent is set to use the Basic Dock Door Receiving matrix file (BDDR.properties). This properties file needs to be modified in order to use the flexible timer setting.

Modifying the PortalControllerAgent using the WebSphere Premises Server Administrative Console:

1. Follow the instructions in the "Modifying agent properties for a PID" on page 106 section, choosing the PortalControllerAgent as the agent you modify.
2. Add string integers to the **Value** setting for the `timer.delay` property.
3. Save your configuration changes.

Example

This is a sample of the XML configuration of the PortalControllerAgent with
multiple values set:

```
<configuration
factoryPid="com.ibm.rfid.agent.portalcontroller.bundle.
PortalControllerAgentManagedServiceFactoryActivator"
name="PortalControllerAgent" description="Portal Controller Agent">
 <property key="timer.delay" value="60000,20000,1000" type="String" cardinality="0"
name="Timer Delay" description="timer delay" />
```

Modifying the properties file:

1. Open the matrix properties file used by the PortalControllerAgent, such as
   BDDR.properties, in a text editor.

2. Add an index statement to one of your timers in this format, where
   index_of_configuration_value is the number of values you have set for the
   PortalControllerAgent:

   state1.4.out.timer2=ON.*index_of_configuration_value* | OFF

   The *index_of_configuration_value* starts at 0. If you do not set a value in the
   matrix properties file for the *index_of_configuration_value*, then it will be 0 by
   default.

3. Save and close your matrix properties file.

Example

This is a sample of what the properties file would look like for a flexible timer
value configuration. The index value is highlighted in bold type:

```
# state1.4:reader did not start in time
state1.4.in=OFF,DONT_CARE,DONT_CARE,DONT_CARE,DONT_CARE,OFF,NOT_EXPIRED,EXPIRED
state1.4.out.reader=OFF
state1.4.out.error=1
state1.4.out.timer2=ON.3
```

Using the Filter and Test Tag agents

The Filter agent allows you to set criteria to determine how tags are passed
through other configured agents. In order to use the Test Tag agent, you need to
set criteria in the Filter Agent.

The Filter agent is included in the bundle list by default, but must be configured in
order to work. For more information on configuring the Filter agent, see the "Filter
agent" on page 121 topic.

The Test Tag agent must be manually added to the bundle list before it can be
configured. For more information on configuring the Test Tag agent, see the "Test
Tag agent" on page 148 topic.

For more information on bundle lists, see "Installing the bundle loader and a
bundle list" on page 72.

Once the Filter agent is configured, tag reads can be passed through the filter agent
to the test tag agent if the criteria matches. The Filter agent takes in the tag reads,
and then republishes them on the FilterAgent topics.publish if they pass the filter,
or topics.publish.rejected if it fails the filter. For example, you can configure a filter
that passes the tag to the Test Tag agent if the header of the tag matches the
criteria set up in the Filter agent.

Once the tag reaches the Test Tag agent, the tag data is checked to see if it matches any of the prefixes defined in the testTagIds. If there is a match, the agent enters test mode.

In the example below, an exclude rule is configured for FF, so that it is excluded and is not passed through the filter. The FilterAgent then publishes it out of topics.publish.rejected. However, the TestTagAgent is listening to topics.publish.rejected, so the TestTagAgent takes a look at the FF to see if it is an FFF. If FFF is found, the agent enters test mode.
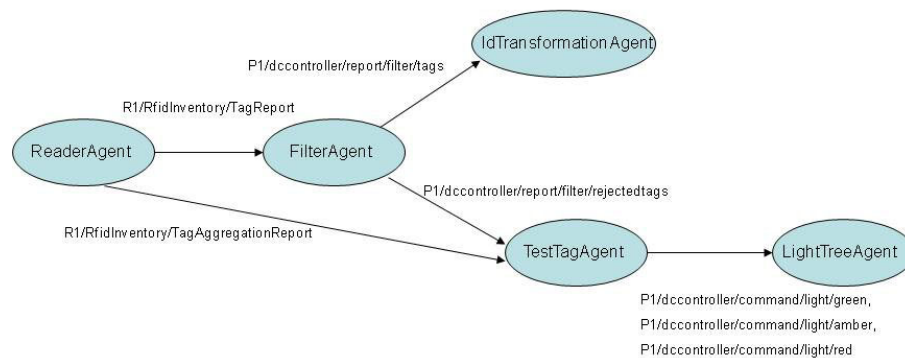
Example

The following is an example of a Test Tag agent configuration. In this example, TestTags begin with FFF. Note that the tag topic of the `rejectedtags` matches the topic coming out of the Filter agent, and the `outputTopics` matches the topics in the Light Tree agent.

```
<configuration factoryPid="com.ibm.rfid.agent.testtags.bundle.TestTagsActivator">
    <properties>
     <property key="source.id" value="P1"/>
     <property key="tracing" value="true"/>
     <property key="log.level" value="DEBUG" />
     <property key="portal.id" value="P1"/>
     <property key="portal.name" value="PortalName1"/>
     <property key="qos" value="0"/>
     <property key="lightDelay" value="2000"/>
     <property key="testModeTimeout" value="120000"/>
     <property key="tagTopic" value="P1/dccontroller/report/filter/rejectedtags"/>
     <property key="testTagIds" value="FFF"/>
     <property key="outputTopics" value="P1/dccontroller/command/light/green,P1/dccontroller/command/light/amber,P1/dccontroller/command/light/red"/>
     <property key="tagAggregationTopic" value="R1/RfidInventory/TagAggregationReport"/>
     <property key="aggregationOutputTopics" value="P1/dccontroller/command/light/red,P1/dccontroller/command/light/amber,P1/dccontroller/command/light/green"/>
    </properties>
   </configuration>

   <configuration factoryPid="com.ibm.rfid.agent.filter.bundle.FilterAgentActivator">
    <properties>
     <property key="source.id" value="P1"/>
     <property key="tracing" value="false"/>
     <property key="log.level" value="" />
     <property key="portal.id" value="P1"/>
     <property key="portal.name" value="PortalName1"/>
     <property key="filters" value="Interest"/>
```

```
    <property key="interest.include.masks.care" value=""/>
    <property key="interest.include.masks.pattern" value=""/>
    <property key="interest.exclude.masks.care" value="FF"/>
    <property key="interest.exclude.masks.pattern" value="FF"/>
    <property key="topics.publish" value="P1/dccontroller/report/filter/tags"/>
    <property key="topics.subscribe" value="R1/RfidInventory/TagReport"/>
    <property key="duplicates.decay.limit.sec" value="5"/>
    <property key="duplicates.decay.cleanup.sec" value="2"/>
    <property key="trigger.reset.topic" value=""/>
    <property key="trigger.reset.value" value=""/>
    <property key="epc.filter.strategy" value="KeepOnly"/>
    <property key="epc.filter.value" value="0"/>
    <property key="selftestmode" value="false" type="boolean"/>
    <property key="profile.id" value="BDDR"/>
    <property key="topics.publish.rejected" value="P1/dccontroller/report/filter/rejectedtags"/>
  </properties>
</configuration>

<configuration factoryPid="com.ibm.rfid.agent.lighttree.bundle.LightTreeAgentActivator">
  <properties>
    <property key="source.id" value="P1"/>
    <property key="agent.name" value="LightTreeAgent"/>
    <property key="tracing" value="false"/>
    <property key="log.level" value="" />
    <property key="portal.id" value="P1"/>
    <property key="portal.name" value="PortalName1"/>
    <property key="gpio.adapter.prefix" value="R1"/>
    <property key="refresh.topic" value="E1/dccontroller/report/diagnostic/heartbeat"/>
    <property key="control.all.topic" value="P1/dccontroller/command/light/all"/>
    <property key="pins.logical.names" value="green,amber,red,aux"/>
    <property key="control.green.topic" value="P1/dccontroller/command/light/accepted,P1/dccontroller/command/light/green"/>
    <property key="duration.green.ms" value="2000"/>
    <property key="invert.green" value="false"/>
    <property key="io.green.pin" value="3"/>
    <property key="active.green.overwrites" value=""/>
    <property key="control.amber.topic" value="P1/dccontroller/command/light/operational,P1/dccontroller/command/light/amber"/>
    <property key="duration.amber.ms" value="-1"/>
    <property key="invert.amber" value="false"/>
    <property key="io.amber.pin" value="2"/>
    <property key="active.amber.overwrites" value=""/>
    <property key="control.red.topic" value="P1/dccontroller/command/light/rejected,P1/dccontroller/command/light/red"/>
    <property key="duration.red.ms" value="2000"/>
    <property key="invert.red" value="false"/>
    <property key="io.red.pin" value="1"/>
    <property key="active.red.overwrites" value="green"/>
    <property key="control.aux.topic" value="P1/dccontroller/command/light/portalerror"/>
    <property key="duration.aux.ms" value="2000"/>
    <property key="invert.aux" value="false"/>
    <property key="io.aux.pin" value="4"/>
    <property key="active.aux.overwrites" value=""/>
  </properties>
</configuration>
<configuration factoryPid="com.ibm.rfid.agent.idtransform.bundle.IdTransformationAgentActivator">
  <properties>
    <property key="source.id" value="R1"/>
    <property key="portal.id" value="P1"/>
    <property key="portal.name" value="PortalName1"/>
    <property key="transform.from" value="P1/dccontroller/report/filter/tags,R1/RfidInventory/TagAggregationReport"/>
    <property key="transform.to" value="P1/BDDR/report/TagReport,P1/BDDR/report/TagAggregationReport"/>
    <property key="transform.eventType" value="BDDR/report/TagReport,BDDR/report/TagAggregationReport"/>
    <property key="transform.sourceId" value="P1,P1"/>
    <property key="qos" value="1" />
    <property value="false" key="tracing"/>
    <property key="log.level" value="" />
  </properties>
</configuration>
```

Agent details

Agents are OSGi bundles that perform a specific functionality and often communicate with each other through a messaging service. These agents are installed during the initial Data Capture and Delivery device controller installation and configuration process.

The agents that are installed in your network are determined by the bundle parameters you set during the initial installation of WebSphere Premises Server or by the bundle parameters set during any subsequent agent deployments.

The following topics define the available properties of the agents in the WebSphere Premises Server Administrative Console.

Alert agent:

The Alert agent forwards local log messages and alerts to a remote server.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 5. Alert agent properties

Property	Description
edge.id	The Data Capture and Delivery device ID associated with this agent
edge.log.threshold	Messages of this severity or higher are logged to the Data Capture and Delivery device console **Note:** This property is not used in WebSphere Premises Server Version 6.1.0.1
edge.name	The Data Capture and Delivery device name associated with this agent
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
org.eclipse.soda.sat.core.util.logLevel	Indicates which level of logging to enable for the Service Activation Toolkit. This level should be the same level as specified for the `edge.log.threshold` property.
org.eclipse.soda.sat.core.util.trace	Displays system level trace output. Values can be true or false.
qos	Messaging Quality of Service. A value of 0 means at most once. A value of 1 means at least once. A value of 2 means exactly once.
qos.cutoff	This value sets the lowest alert level that will be published for QoS. Any level that is below the value specified for qos.cutoff is set to publish at `qos=0`. This and higher thresholds are published at the agent-defined QoS level.
source.id	The source ID for generic events in this agent
threshold	Messages of this severity or higher are forwarded to the remote server
tracing	Displays trace output. The Alert agent must be running in order to set this property.

Alert Task agent:

The Alert Task agent is a WebSphere Premises Server task agent that formats incoming alert messages and the files used to log those messages.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration

file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 6. Alert Task agent properties

Property	Description
flag	Turns alert logging on or off. The valid values are true or false. If true, the default Alert log level will be INFO. If false, the default Alert log level will be SEVERE. The default value is true.
formatter.delimiter.close	The closing delimiter to use when making an entry in the log. The default value is a close bracket ( ]).
formatter.delimiter.open	The opening delimiter to use when making an entry in the log. The default value is an open bracket ([ ).
formatter.format	The alert log columns format sequence. The default value is: dts,type,controller,msg, where dts is the date, type is alert type, controller is the controller id, and msg is the alert message
formatter.timestamp	The format of the time stamp in the log. The default is MMM d HH:mm:ss yyyy
handler.append	Specifies whether the FileHandler should append onto any existing files. The default value is True
handler.count	Specifies how many output files to cycle through. The default value is 10.
handler.limit	Specifies an approximate maximum amount to write in bytes to any one file. If the value is set to zero, then there is no limit . The default value is 2MB.
handler.pattern	Specifies a pattern for generating the output file name. The default value is %t/edge-alerts.log.

Application Ping agent:

The Application Ping agent monitors remote server status and responds to remote server status requests.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 7. Application ping agent properties

Property	Description
edge.id	The Data Capture and Delivery device ID associated with this agent

Table 7. Application ping agent properties (continued)

Property	Description
edge.name	The Data Capture and Delivery device name associated with this agent
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
response.timeout	The threshold in milliseconds to wait for the response
source.id	The source ID for generic events in this agent
timeinterval.error	After an error, this value is the check interval in milliseconds
timeinterval.regular	The normal health check interval in milliseconds
tracing	Displays trace output. The Alert agent must be running in order to set this property.

Barrier Sensor agent:

The Barrier Sensor agent is the agent for the barrier sensor.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 8. Barrier Sensor agent properties

Property	Description
agent.name	The name of the agent
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
portal.id	The portal ID associated with this agent
portal.name	The portal name associated with this agent
selftestmode	Indicates if self-test mode is active
sensor.activelevel	Indicates a positive (HIGH) or inverse (LOW) logic of this sensor
sensor.aliasname	The alias of this sensor
sensor.blockedtimeout	If this sensor is active longer than this time in microseconds (ms) it will issue an error
sensor.inactivitydelay	Delay in microseconds if the sensor transitions from active to inactive
sensor.listen.topic	Input topic relevant for this sensor
sensor.pin	The pin number of output where this sensor is assigned to

Table 8. Barrier Sensor agent properties (continued)

Property	Description
sensor.publish.topic	Output topic used by this sensor
sensor.statelogging	Indicates whether state changes were logged with INFO, WARNING or ERROR level
source.id	The source ID for generic events in this agent
tracing	Displays trace output. The Alert agent must be running in order to set this property.

Bundle Loader agent:

The Bundle Loader agent writes log messages to stdout and stderr.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 9. Bunlde Loader agent properties

Property	Description
bundleListURL	The URL of the list of bundles to load
clearCache	Clears the cache of bundle lists that are already processed
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.

Console Log agent:

The Console Log agent writes log messages to stdout and stderr.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 10. Console log agent properties and descriptions

Property	Description
errorLogThreshold	Minimum level of messages that are written to stderr. Valid values are none, error, warning, info, or debug.
logThreshold	Minimum level of messages that are written to stdout. Valid values are none, error, warning, info, or debug. If the value is empty then the system log level is used.

DTMSQ Bridge Inbound Flow agent:

The DTMSQ Bridge Inbound Flow agent configures the MicroBroker Bridge for a 6.1 edge connector.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Note: This agent is not used in WebSphere Premises Server Version 6.1.0.1.

Table 11. DTMSQ Bridge Inbound Flow agent properties

Property	Description
direction	The direction of the flow of messages. This value can be set to either inbound or outbound.
edge.id	The Data Capture and Delivery device ID associated with this agent
edge.name	The Data Capture and Delivery device name associated with this agent
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
name	The unique name for the configuration object
qos	Messaging Quality of Service. A value of 0 means at most once. A value of 1 means at least once. A value of 2 means exactly once.
source.id	The source ID for generic events in this agent
sources	The source of messages for this flow
target	The target of messages for this flow
tracing	Displays trace output. The Alert agent must be running in order to set this property.
transformations	The comma separated list of flows that are used on messages in this flow
type	The type of configuration object that is being represented. This value can be set to pipe, flow, or transformation.

DTMSQ Bridge Pipe agent:

The DTMSQ Bridge Pipe agent configures the MicroBroker bridge on Data Transformation for a 6.1 edge controller.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Note: This agent is not used in WebSphere Premises Server Version 6.1.0.1.

Table 12. DTMSQ Bridge Pipe agent properties

Property	Description
broker.name	The name of the remote MicroBroker broker to connect to this bridge
channel	The name of the channel used to connect to the Queue Manager
edge.id	The Data Capture and Delivery device ID associated with this agent
edge.name	The Data Capture and Delivery device name associated with this agent
flows	The comma separated list of flows that are used to configure the MicroBroker Bridge
host	The host address of the MQTT Server. This property is not needed if local is set to true.
letter.queue	The queue used to place unsupported messages
local	Set to true if you are using the local binding to connect to a local MQ Server. Otherwise, set to false and provide the host and port of the MQ Server.
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
name	The unique name for the configuration object
port	The port on which the MQTT Server is listening. This property is not needed if local is set to true.
protocol	The protocol to use in connecting to a remote broker. This value can be set to MQJMS or MQTT.
queue.manager	The name of the Queue Manager on the MQ Server
source.id	The source ID for generic events in this agent
sync.queue	The queue name used to sync the message queues
tracing	Displays trace output. The Alert agent must be running in order to set this property.
type	The type of configuration object that is being represented. This value can be set to pipe, flow, or transformation.

Edge MQ Bridge Inbound Flow agent:

The Edge MQ Bridge Inbound Flow agent configures the MicroBroker bridge for a version 6.1 edge connector. This agent is only visible if you have a high availability topology.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Note: This agent is not used in WebSphere Premises Server Version 6.1.0.1.

Table 13. Edge MQ Bridge Inbound Flow agent properties

Property	Description
direction	The direction of the flow of messages. This value can be set to either inbound or outbound.
edge.id	The Data Capture and Delivery device ID associated with this agent
edge.name	The Data Capture and Delivery device name associated with this agent
jmsselector	Used to select JMS messages to process on the MicroBroker bridge By default, the jmsselector value is empty. If this value is not empty, then it overrides the value of the correlationid.
correlationid	Used to select JMS messages to process on the MicroBroker bridge By default, the correlationid is set to a macro of the controller ID. Use this value if the jmsselector property is empty.
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
name	The unique name for the configuration object
qos	Messaging Quality of Service. A value of 0 means at most once. A value of 1 means at least once. A value of 2 means exactly once.
source.id	The source ID for generic events in this agent
sources	The source of messages for this flow
target	The target of messages for this flow
tracing	Displays trace output. The Alert agent must be running in order to set this property.

Table 13. Edge MQ Bridge Inbound Flow agent properties (continued)

Property	Description
transformations	The comma separated list of flows that are used on messages in this flow
type	The type of configuration object that is being represented. This value can be set to pipe, flow, or transformation.

Edge MQ Bridge Pipe agent:

The Edge MQ Bridge Pipe agent configures the MicroBroker Bridge on Data Transformation for a version 6.1 edge connector. This agent is only visible if you have a high availability topology.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Note: This agent is not used in WebSphere Premises Server Version 6.1.0.1.

Table 14. Edge MQ Bridge Pipe agent properties

Property	Description
channel	The name of the channel used to connect to the Queue Manager
edge.id	The Data Capture and Delivery device ID associated with this agent
edge.name	The Data Capture and Delivery device name associated with this agent
flows	The comma separated list of flows that are used to configure the MicroBroker Bridge
host	The host address of the MQTT Server. This property is not needed if local is set to true.
letter.queue	The queue used to place unsupported messages
local	Set to true if you are using the local binding to connect to a local MQ Server. Otherwise, set to false and provide the host and port of the MQ Server.
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
name	The unique name for the configuration object
port	The port on which the MQTT Server is listening. This property is not needed if local is set to true.

Table 14. Edge MQ Bridge Pipe agent properties (continued)

Property	Description
protocol	The protocol to use in connecting to a remote broker. This value can be set to MQJMS or MQTT.
queue.manager	The name of the Queue Manager on the MQ Server
source.id	The source ID for generic events in this agent
sync.queue	The queue name used to sync the message queues
tracing	Displays trace output. The Alert agent must be running in order to set this property.
type	The type of configuration object that is being represented. This value can be set to pipe, flow, or transformation.

Equinox Log agent:

The Equinox Log agent configures the Eclipse log service.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 15. Equinox Log agent properties

Property	Description
log.size	The size of the internal log queue

Event Transformation agent:

The Event Transformation agent transforms the Data Capture and Delivery internal messages into the external message format.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 16. Event Transformation agent properties

Property	Description
edge.id	The Data Capture and Delivery device ID associated with this agent
edge.name	The Data Capture and Delivery device name associated with this agent

Table 16. Event Transformation agent properties (continued)

Property	Description
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
serializing	Flags whether the messages to and from the premises server are seralized or sent by XML.
source.id	The source ID for generic events in this agent
topics.transform.to.external	Defines the Payload class for a particular Notification Service topic to use in converting the Data Capture and Delivery message to an IBM Sensor Event.
tracing	Displays trace output. The Alert agent must be running in order to set this property.
xml.log.all	Determines whether the entire XML or the XML header is logged

Filter agent:

The Filter agent applies all configured filters to incoming data.

To make it through this agent, a tag must pass the test of every configured filter. The types of filters to apply are configured through the filters property. Legal types include: CaseTags, Duplicates, DecayingDuplicates, EpcFilter, and Interest.

Properties

The Case Tags filter checks the first byte of the tag ID. If the value is equal to 0x30 (i.e. SGTIN-96), the tag passes the test; otherwise, the test fails. This value is not configurable, although the source may be changed if the Data Capture superfeature is installed. There are no properties specific to the Case Tags filter.

The Duplicates filter prevents tags with the same ID from being reported more than once until the filter is reset. There are no properties specific to this filter.

The Decaying Duplicates filter prevents tags with the same ID from being reported more than once within a configurable period of time or until the filter is reset, whichever comes first. Properties specific to this filter are duplicates.decay.limit.sec and duplicates.decay.cleanup.sec.

The EpcFilter filter follows one of two configurable strategies: KeepOnly or RemoveAll. If the strategy is KeepOnly, the filter allows only those tags having the configured EPC filter value through. If the strategy is RemoveAll, the filter allows only those tags not having the configured EPC filter value through. Properties specific to this filter are epc.filter.strategy and epc.filter.value.

The Interest filter filters tags based on an include and exclude bit mask and pattern expressed in hexadecimal that is applied to each tag ID. If the tag passes both tests, it is allowed through. Properties specific to this filter are interest.include.masks.care, interest.include.masks.pattern, interest.exclude.masks.care, and interest.exclude.masks.pattern.

All other properties are in common with each filter type.

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 17. Filter agent properties

Property	Description
duplicates.decay.cleanup.sec	How often, in seconds, decayed duplicates should be deleted
duplicates.decay.limit.sec	How often, in seconds, stored duplicates should remain
epc.filter.strategy	The strategy that the EpcFilter should employ. One of KeepOnly or RemoveAll
epc.filter.value	Only tags with this as the EPC filter value will make it through this agent
filters	A comma-delimited list of filters to be configured. Filter names are: Case Tags, Duplicates, DecayingDuplicates, EPCFilter, and Interest.
interest.include.masks.care	A mask representing the bits you are interested in matching. The filter includes the tags that match.
interest.include.masks.pattern	A value with which the bits from the care bits must match. The filter includes the tags that match.
interest.exclude.masks.care	A mask representing the bits you are interested in matching. The filter exclude the tags that match.
interest.exclude.masks.pattern	A value with which the bits from the care bits must match. The filter excludes the tags that match.
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
portal.id	The portal ID associated with this agent
portal.name	The portal name associated with this agent
profile.id	Identifies the use case to which this agent is attached
qos	Messaging Quality of Service. A value of 0 means at most once. A value of 1 means at least once. A value of 2 means exactly once.
selftestmode	Indicates if self-test mode is active
source.id	The source ID for generic events in this agent
topics.publish	A comma-delimited list of topics for publishing filtered data
topics.publish.rejected	A comma-delimited list of topics for publishing data that is filtered out

Table 17. Filter agent properties (continued)

Property	Description
topics.subscribe	A comma-delimited list of topics for receiving data to be filtered
tracing	Displays trace output. The Alert agent must be running in order to set this property.
trigger.reset.topic	Publishes to this topic result in a filter reset
trigger.reset.value	Value of the message to reset the filters and clear the filter cache

Health Check agent:

The Health Check agent monitors the health of the Data Capture and Delivery device.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 18. Health Check agent properties

Property	Description
device.names	A comma-separated list of the observed sensors
edge.id	The Data Capture and Delivery device ID associated with this agent
edge.name	The Data Capture and Delivery device name associated with this agent
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
portal.id	The portal ID associated with this agent
portal.initial	Defines the initial portal state When the value is set to OFF, the agent does nothing until the Portal Controller agent is activated and the Health Check Agent assumes the location is DOWN. If the value is set to ON, the Portal Controller agent sends a signal when the portal is ready and the Data Capture and Delivery device is operational and the HealthCheckAgent assumes the location is UP.
portal.name	The portal name associated with this agent
profile.id	Identifies the use case to which this agent is attached
reader.id	The ID of the corresponding reader.
selftestmode	Indicates if self-test mode is active

Table 18. Health Check agent properties (continued)

Property	Description
source.id	The source ID for generic events in this agent
tracing	Displays trace output. The Alert agent must be running in order to set this property.

Heartbeat agent:

The Heartbeat agent monitors the reader heartbeats.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 19. Heartbeat agent properties

Property	Description
edge.id	The Data Capture and Delivery device ID associated with this agent
edge.name	The Data Capture and Delivery device name associated with this agent
heartbeat.period.ms	How often, in milliseconds, heartbeats are reported
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
portal.ids	A comma-delimited list of portals to be monitored
reader.ids	A comma-delimited list of readers to be monitored
source.id	The source ID for generic events in this agent
tracing	Displays trace output. The Alert agent must be running in order to set this property.

Heartbeat Task agent:

The Heartbeat Task agent is a WebSphere Premises Server agent that listens for heartbeat events that are sent from Data Capture and Delivery Controllers.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 20. Heartbeat Task agent properties

Property	Description
device.name	Specifies what name will be shown in heartbeat log
device.placeholder	If there is no device username defined, this placeholder is shown in the heartbeat log for the device
formatter.message.down	The string to use for the down controller, device, or location. The default value is DOWN.
formatter.message.up	The string to use for the up controller, device, or location. The default value is UP.
formatter.placeholder	If there is no location or reader defined for the controller, this placeholder will be shown in the heartbeat log for the location and reader column.
formatter.timestamp	The format of the time stamp in the log file. The default value is MMM d HH:mm:ss yyyy
handler.append	Specifies whether the FileHandler should append onto any existing files. The default value is True.
handler.count	Specifies how many output files to cycle through. The default value is 1.
handler.limit	Specifies an approximate maximum amount to write in bytes to any one file. If the value is set to zero, then there is no limit. The default value is 500KB.
handler.pattern	Specifies a pattern for generating the output file name. The default is edge-heartbeats.%g.log.

IBM Simulated Reader agent:

The Simulated Reader agent simulates an RFID reader.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 21. IBM Simulated Reader agent properties

Property	Description
RfidInventory	Tag reading will be turned on or off according to control profile bits matching the given LDAP expression (such as (b1=true))filter, ignoring the normal Set tag reading method. **Note:** This tag is not used in version 6.1.0.1. It is replaced by TagReadingExpression

Table 21. IBM Simulated Reader agent properties (continued)

Property	Description
TagReadingExpression	If defined, tag reading is turned on and off according to control profile bits matching the given LDAP expression (such as (b1=true)) filter, ignoring the normal Set tag reading method.
activateReaderOnStart	Start publishing tags without being specifically turned on over the service bus
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
passthruDelay	Optional topic to pass data object through after a delay of passthruDelay milliseconds. ReaderSimulator listens for passthreInputTopic and publishes the same data given back on passthruOutputTopic
passthruInputTopic	Optional topic to pass data object through after a delay of passthruDelay milliseconds. ReaderSimulator listens for passthreInputTopic and publishes the same data given back on passthruOutputTopic.
passthruOutputTopic	Optional topic to pass data object through after a delay of passthruDelay milliseconds. ReaderSimulator listens for passthreInputTopic and publishes the same data given back on passthruOutputTopic.
reader	The name of the reader
source.id	The source ID for generic events in this agent

ID Transformation agent:

The ID Transformation agent transforms Data Capture and Delivery messages from individual readers to messages from portals and initially populates source ID and event type fields.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 22. ID Transformation agent properties

Property	Description
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
portal.id	The portal ID associated with this agent
portal.name	The portal name associated with this agent

Table 22. ID Transformation agent properties (continued)

Property	Description
qos	Messaging Quality of Service. A value of 0 means at most once. A value of 1 means at least once. A value of 2 means exactly once.
source.id	The source ID for generic events in this agent
suffixes.transform.from	A comma-delimited list of topic suffixes to transform from. The list must be parallel order-wise to the list in the suffixes.transform.to property. This parameter is not applicable in WebSphere Premises Server 6.1.0.1. It has been replaced by the transform.from property.
suffixes.transform.to	A comma-delimited list of topic suffixes to transform to. The list must be parallel order-wise to the list in the suffixes.transform.from property. This parameter is not applicable in WebSphere Premises Server 6.1.0.1. It has been replaced by the transform.to property.
transform.eventType	A comma-delimited list of event types to assign to a transform topic. The list must be parallel order-wise to the list in the transform.from property.
transform.from	A comma-delimited list of topic suffixes to transform from. The list must be parallel order-wise to the list in the transform.to property.
transform.sourceId	A comma-delimited list of source IDs to assign to a transform topic. The list must be parallel order-wise to the list in the transform.from property.
transform.to	A comma-delimited list of topic suffixes to transform to. The list must be parallel order-wise to the list in the transform.from property.

Light Tree agent:

The Light Tree agent controls a lightstack.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 23. Light Tree agent properties

Property	Description
active.red.overwrites	The logical names list of actors that are overwritten if the corresponding actor is active

Table 23. Light Tree agent properties (continued)

Property	Description
agent.name	The name of the agent
control.all.topic	The topic that turns all actors into the given state
control.amber.topic	When received, the corresponding pin is updated. Multiple topics are allowed.
control.aux.topic	When received, the corresponding pin is updated
control.green.topic	When received, the corresponding pin is updated. Multiple topics are allowed.
control.red.topic	When received, the corresponding pin is updated. Multiple topics are allowed.
duration.amber.ms	The length of time in milliseconds that the corresponding pin is on before it goes off
duration.aux.ms	The length of time in milliseconds that the corresponding pin is on before it goes off
duration.green.ms	The length of time in milliseconds that the corresponding pin is on before it goes off
duration.red.ms	The length of time in milliseconds that the corresponding pin is on before it goes off
gpio.adapter.prefix	The prefix used to communicate with the IO-Profile
invert.amber	If set to true, the actor's pin is driven inversely
invert.aux	If set to true, the actor's pin is driven inversely
invert.green	If set to true, the actor's pin is driven inversely
invert.red	If true, the actor's pin is driven inversely
io.amber.pin	The pin associated with the corresponding logical actor name
io.aux.pin	The pin associated with the corresponding logical actor name
io.green.pin	The pin associated with the corresponding logical actor name
io.red.pin	The pin associated with the corresponding logical actor name
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
pins.logical.names	The logical names list of the actors associated to the pins
portal.id	The portal ID associated with this agent
portal.name	The portal name associated with this agent
refresh.topic	The topic that leads to a republish of the actor's state
selftestmode	Indicates if self-test mode is active

Table 23. Light Tree agent properties (continued)

Property	Description
source.id	The source ID for generic events in this agent
tracing	Displays trace output. The Alert agent must be running in order to set this property.

Log File agent:

The Log File agent controls writing log entries to the local file system.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 24. Log File agent properties

Property	Description
buffer.size	The size of the internal buffer for writing log entries to a file
edge.id	The Data Capture and Delivery device ID associated with this agent
edge.name	The Data Capture and Delivery device name associated with this agent
log.dir	The directory where the log files should be placed. If this directory does not exist it will be created.
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
log.threshold	The lowest level of messages that will be written to the log file. This depends on the system log level to be set at least to this level of logging. If the value is empty then the system log level will be used.
max.file.size	The maximum size that the log files should become. Once this size is reached, the current file is closed and a new file is created.
max.number.files	The maximum number of log files that can be kept at one time. Once the maximum number is reached, the oldest log file will be deleted.
source.id	The source ID for generic events in this agent
tracing	Displays trace output. The Alert agent must be running in order to set this property.

MQ Bridge Outbound Flow Agent:

The MQ Bridge Outbound Flow agent configures the MicroBroker Bridge on Data Transformation for a 6.1 edge controller.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 25. MQ Bridge Outbound Flow agent properties

Property	Description
direction	The direction of the flow of messages. This value can be set to either inbound or outbound.
edge.id	The Data Capture and Delivery device ID associated with this agent
edge.name	The Data Capture and Delivery device name associated with this agent
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
name	The unique name for the configuration object
qos	Messaging Quality of Service. A value of 0 means at most once. A value of 1 means at least once. A value of 2 means exactly once.
source.id	The source ID for generic events in this agent
sources	The source of messages for this flow
target	The target of messages for this flow
tracing	Displays trace output. The Alert agent must be running in order to set this property.
transformations	The comma separated list of flows that are used on messages in this flow
type	The type of configuration object that is being represented. This value can be set to pipe, flow, or transformation.

MQTT Bridge Inbound Flow agent:

The MQTT Bridge Inbound Flow agent configures the MicroBroker bridge on the edge controller to forward messages to Data Transformation.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 26. MQ Bridge Inbound Flow agent properties

Property	Description
direction	The direction of the flow of messages. This value can be set to either inbound or outbound.
edge.id	The Data Capture and Delivery device ID associated with this agent
edge.name	The Data Capture and Delivery device name associated with this agent
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
name	The unique name for the configuration object
qos	Messaging Quality of Service. A value of 0 means at most once. A value of 1 means at least once. A value of 2 means exactly once.
source.id	The source ID for generic events in this agent
sources	The source of messages for this flow
tracing	Displays trace output. The Alert agent must be running in order to set this property.
type	The type of configuration object that is being represented. This value can be set to pipe, flow, or transformation.

MQTT Bridge Outbound Flow Agent:

The MQTT Bridge Outbound Flow Agent configures the MicroBroker Bridge on the edge controller to forward messages to Data Transformation.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 27. MQTT Bridge Outbound Flow agent properties

Property	Description
direction	The direction of the flow of messages. This value can be set to either inbound or outbound.
edge.id	The Data Capture and Delivery device ID associated with this agent
edge.name	The Data Capture and Delivery device name associated with this agent
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.

Table 27. MQTT Bridge Outbound Flow agent properties (continued)

Property	Description
name	The unique name for the configuration object
qos	Messaging Quality of Service. A value of 0 means at most once. A value of 1 means at least once. A value of 2 means exactly once.
source.id	The source ID for generic events in this agent
sources	The source of messages for this flow
tracing	Displays trace output. The Alert agent must be running in order to set this property.
type	The type of configuration object that is being represented. This value can be set to pipe, flow, or transformation.

MQTT Bridge Pipe agent:

The MQTT Bridge Pipe agent configures the MicroBroker Bridge on the edge controller to forward messages to Data Transformation.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 28. MQTT Bridge Pipe agent properties

Property	Description
broker	The name of the remote MicroBroker broker to connect to this bridge
edge.id	The Data Capture and Delivery device ID associated with this agent
edge.name	The Data Capture and Delivery device name associated with this agent
flows	The comma separated list of flows that are used to configure the MicroBroker Bridge
host	The host address of the MQTT Server. This property is not needed if local is set to true.
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
name	The unique name for the configuration object
port	The port on which the MQTT Server is listening. This property is not needed if local is set to true.

Table 28. MQTT Bridge Pipe agent properties (continued)

Property	Description
protocol	The protocol to use in connecting to a remote broker. This value can be set to MQJMS or MQTT.
source.id	The source ID for generic events in this agent
tracing	Displays trace output. The Alert agent must be running in order to set this property.
type	The type of configuration object that is being represented. This value can be set to pipe, flow, or transformation.

MicroBroker Configuration agent:

The MicroBroker Configuration agent configures the MicroBroker bridge.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 29. MicroBroker Configuration agent properties

Property	Description
bridge.clean.session	If set to true, the MicroBroker bridge does not retain pending messages from a previous session
bridge.topics.down	A list of topics with messages that should be propagated from the WebSphere Premises Server
bridge.topics.up	A list of topics with messages that should be propagated to the WebSphere Premises Server
edge.id	The Data Capture and Delivery device ID associated with this agent
edge.name	The Data Capture and Delivery device name associated with this agent
edge.on.premises	A flag that indicates if the Data Capture and Delivery application is running on Data Transformation or in standalone mode
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
portal.ids	A list of portal IDs recognized by the Data Capture and Delivery device
server.ip	The IP address or host name of the WebSphere Premises Server
server.port	The remote port number on the WebSphere Premises Server

Table 29. MicroBroker Configuration agent properties (continued)

Property	Description
source.id	The source ID for generic events in this agent
tracing	Displays trace output. The Alert agent must be running in order to set this property.

MicroBroker Serialization Service:

The MicroBroker Serialization Service agent serializes and deserializes messages sent through MicroBroker.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 30. MicroBroker Serialization Service agent properties

Property	Description
edge.id	The Data Capture and Delivery device ID associated with this agent
edge.name	The Data Capture and Delivery device name associated with this agent
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
source.id	The source ID for generic events in this agent
tracing	Displays trace output. The Alert agent must be running in order to set this property.

MicroBroker agent:

The MicroBroker agent configures the broker service provided by MicroBroker messaging framework.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 31. MicroBroker agent properties

Property	Description
dir	Root directory for the MicroBroker files.
edge.id	The Data Capture and Delivery device ID associated with this agent

Table 31. MicroBroker agent properties (continued)

Property	Description
edge.name	The Data Capture and Delivery device name associated with this agent
forceCleanBroker	Force clean broker reinitialization on the configuation reload
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
maxMessageSize	The maximum size of the MicroBroker message
maxNumberOfClients	The maximum number of client instances allowed for the MicroBroker
name	The unique name for the configuration object
persistence	Messaging persistence in case of shutdown. Values can be 0, 1, or 2.
port	The port on which the MQTT Server is listening. This property is not needed if local is set to true.
queueSize	The size of internal MicroBroker messaging queue
source.id	The source ID for generic events in this agent
trace.level	Internal MicroBroker trace level byte value. Possible values for this property are min, 1, 2, 3, 4, 5, or max.
tracing	Displays trace output. The Alert agent must be running in order to set this property.
waitTimeout	Wait timeout in milliseconds

Motion Sensor agent:

The Motion Sensor agent is the name for the motion sensor.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 32. Motion Sensor agent properties

Property	Description
agent.name	The name of the agent
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
portal.id	The portal ID associated with this agent

Table 32. Motion Sensor agent properties (continued)

Property	Description
portal.name	The portal name associated with this agent
selftestmode	Indicates if self-test mode is active
sensor.activelevel	Indicates a positive (HIGH) or inverse (LOW) logic of this sensor
sensor.aliasname	The alias of this sensor
sensor.blockedtimeout	If this sensor is active longer than this time in microseconds (ms) it will issue an error
sensor.inactivitydelay	Delay in microseconds if the sensor transitions from active to inactive
sensor.listen.topic	Input topic relevant for this sensor
sensor.pin	The pin number of output where this sensor is assigned to
sensor.publish.topic	Output topic used by this sensor
sensor.statelogging	Indicates whether state changes were logged with INFO, WARNING or ERROR level
source.id	The source ID for generic events in this agent
tracing	Displays trace output. The Alert agent must be running in order to set this property.

Notification Service Bridge agent:

The Notification Service Bridge agent bridges messages between Notification Service and MicroBroker.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 33. Notification Service Bridge agent properties

Property	Description
bridge.to.mb.topics	A comma separated list of topics for which messages should be propagated from Notification Service to MicroBroker
bridge.to.ns.topics	A comma separated list of topics for which messages should be propagated from MicroBroker to Notification Service
broker.name	The name of the remote MicroBroker broker to connect to this bridge
edge.id	The Data Capture and Delivery device ID associated with this agent
edge.name	The Data Capture and Delivery device name associated with this agent

Table 33. Notification Service Bridge agent properties (continued)

Property	Description
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
qos	Messaging Quality of Service. A value of 0 means at most once. A value of 1 means at least once. A value of 2 means exactly once.
source.id	The source ID for generic events in this agent
tracing	Displays trace output. The Alert agent must be running in order to set this property.

Object Decoder Transformation agent:

The Object Decoder Transformation agent configures the MicroBroker Bridge on Data Transformation for a version 6.1 edge controller.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Note: This agent is not used in WebSphere Premises Server Version 6.1.0.1.

Table 34. Object Decoder Transformation agent properties

Property	Description
classname	The name of the transformation class to use on messages in this flow
edge.id	The Data Capture and Delivery device ID associated with this agent
edge.name	The Data Capture and Delivery device name associated with this agent
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
name	The unique name for the configuration object
source.id	The source ID for generic events in this agent
tracing	Displays trace output. The Alert agent must be running in order to set this property.
type	The type of configuration object that is being represented. This value can be set to pipe, flow, or transformation.

Object Encoder Transformation agent:

The Object Encoder Transformation agent configures the MicroBroker bridge on Data Transformation for a version 6.1 edge controller.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Note: This agent is not used in WebSphere Premises Server Version 6.1.0.1.

Table 35. Object Encoder Transformation agent properties

Property	Description
classname	The name of the transformation class to use on messages in this flow
edge.id	The Data Capture and Delivery device ID associated with this agent
edge.name	The Data Capture and Delivery device name associated with this agent
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
name	The unique name for the configuration object
source.id	The source ID for generic events in this agent
tracing	Displays trace output. The Alert agent must be running in order to set this property.
type	The type of configuration object that is being represented. This value can be set to pipe, flow, or transformation.

Portal Controller agent:

The Portal Controller agent controls and facilitates portal activity.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 36. Portal Controller agent properties

Property	Description
feedback.topic.prefix	The topic prefix that is used to republish the tag-read feedback
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.

Table 36. Portal Controller agent properties (continued)

Property	Description
matrix.properties	The file with the state transitions descriptions These matrix files are available by default with the product: • BDDR.properties - Basic Dock Door Receiving usage scenario • SDDR.properties - Standard Dock Door Receiving usage scenario • EDDR.properties - Enhanced Dock Door Receiving usage scenario
matrix.queue.processing.all	Specifies if matrix processing happens per each event (false) or for all available events (true)
operationalmode	The value can be either READER or PORTAL. If the value is **reader**, the amber light is activated when the reader starts scanning. If the value is **portal**, the amber light is activated when the portal is activated.
out.error.msg.1	The value of error message 1
out.error.msg.2	The value of error message 2
out.error.msg.3	The value of error message 3
out.error.msg.4	The value of error message 4
out.error.topic.1	Matrix action 'stateX.Y.out.error=1' publishes this topic with the corresponding value
out.error.topic.2	Matrix action 'stateX.Y.out.error=2' publishes this topic with the corresponding value
out.error.topic.3	Matrix action 'stateX.Y.out.error=3' publishes this topic with the corresponding value
out.error.topic.4	Matrix action 'stateX.Y.out.error=4' publishes this topic with the corresponding value
out.reader.onparm.1	Matrix action 'stateX.Y.out.reader=ON.1' sets this metadata before turning the reader on
out.reader.onparm.2	Matrix action 'stateX.Y.out.reader=ON.2' sets this metadata before turning the reader on
portal.id	The portal ID associated with this agent
portal.initial	Defines the initial portal state
portal.initial.delay	Time in milliseconds to delay before setting the portal to on
portal.name	The portal name associated with this agent
portal.on.execute.matrix	Execute matrix processing when a portal on command is received
profile.id	Identifies the use case to which this agent is attached
reader.activation.command.topic	The topic (without prefix) that is sent to turn on the reader

Table 36. Portal Controller agent properties (continued)

Property	Description
reader.activation.command.value	The value that is sent with the message to turn on the reader
reader.activation.signal.topic	The topic (without prefix) that is sent from the reader adapter to confirm that the reader is on
reader.adapter.prefix	The prefix used in all messages to the reader adapter
reader.adapter.reply.timeout	Specifies how long to wait (in milliseconds) for a reply from the reader adapter before timing out
reader.deactivation.command.value	The value that is sent with the message to turn the reader off
selftestmode	Indicates if self-test mode is active
sensor1.initial	The initial value of sensor 1
sensor1.topic	The topic of the first sensor in the matrix input vector
sensor2.initial	The initial value of sensor 2
sensor2.topic	The topic of the second sensor in the matrix input vector
sensor3.initial	The initial value of sensor 3
sensor3.topic	The topic of the third sensor in the matrix input vector
sensor4.initial	The initial value of sensor 4
sensor4.topic	The topic of the fourth sensor in the matrix input vector
sensor5.initial	The initial value of sensor 5
sensor5.topic	The topic of the fifth sensor in the matrix input vector
source.id	The source ID for generic events in this agent
strongchecking	Logs potential problem situations with matrix processing
timer.delay	Duration in milliseconds of timer 1 and timer 2 in the matrix input vector. See "Configuring the PortalControllerAgent to use flexible timer values" on page 108 for details on how to use this property for flexible timeout values.
timer1.delay	Duration in milliseconds of timer 1 in the matrix input vector **Note:** This property is only applicable for releases prior to WebSphere Premises Server 6.1.0.1
timer2.delay	Duration in milliseconds of timer 2 in the matrix input vector **Note:** This property is only applicable for releases prior to WebSphere Premises Server 6.1.0.1

Table 36. Portal Controller agent properties (continued)

Property	Description
tracing	Displays trace output. The Alert agent must be running in order to set this property.

Portal Metadata agent:

The Portal Metadata agent processes MetaData update messages for a portal, allowing for the MetaData associated with the portal to be modified dynamically.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 37. Portal Metadata agent properties

Property	Description
listen.topics	The topics subscribed to for incoming messages
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
portal.id	The portal ID associated with this agent
portal.name	The portal name associated with this agent
qos	Messaging Quality of Service. A value of 0 means at most once. A value of 1 means at least once. A value of 2 means exactly once.
source.id	The source ID for generic events in this agent
tracing	Displays trace output. The Alert agent must be running in order to set this property.

Reload agent:

The Reload agent reloads the Data Capture and Delivery device configuration.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 38. Reload agent properties

Property	Description
edge.id	The Data Capture and Delivery device ID associated with this agent

Table 38. Reload agent properties (continued)

Property	Description
edge.name	The Data Capture and Delivery device name associated with this agent
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
reload.topic	Reloads the configuration when data of any value is published across this topic
source.id	The source ID for generic events in this agent
tracing	Displays trace output. The Alert agent must be running in order to set this property.

Reset Sensor agent:

The Reset Sensor agent is the agent for the reset sensor.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 39. Reset Sensor agent properties

Property	Description
agent.name	The name of the agent
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
portal.id	The portal ID associated with this agent
portal.name	The portal name associated with this agent
selftestmode	Indicates if self-test mode is active
sensor.activelevel	Indicates a positive (HIGH) or inverse (LOW) logic of this sensor
sensor.aliasname	The alias of this sensor
sensor.blockedtimeout	If this sensor is active longer than this time in microseconds (ms) it will issue an error
sensor.inactivitydelay	Delay in microseconds if the sensor transitions from active to inactive
sensor.listen.topic	Input topic relevant for this sensor
sensor.pin	The pin number of output where this sensor is assigned to
sensor.publish.topic	Output topic used by this sensor
sensor.statelogging	Indicates whether state changes were logged with INFO, WARNING or ERROR level

Table 39. Reset Sensor agent properties (continued)

Property	Description
source.id	The source ID for generic events in this agent
tracing	Displays trace output. The Alert agent must be running in order to set this property.

Restart agent:

The Restart agent restarts the OSGi framework.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 40. Restart agent properties

Property	Description
edge.id	The Data Capture and Delivery device ID associated with this agent
edge.name	The Data Capture and Delivery device name associated with this agent
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
restart.topic	Restarts the OSGi framework when data is published across this topic
source.id	The source ID for generic events in this agent
tracing	Displays trace output. The Alert agent must be running in order to set this property.

Self Test agent:

The Self Test agent performs reader self-tests.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 41. Self Test agent properties

Property	Description
initial.delay	Duration in milliseconds to wait after startup of the agent until the selftest begins

Table 41. Self Test agent properties (continued)

Property	Description
inputtest.length	Duration in milliseconds of one input test phase
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
output.count	Number of outputs available to cycle through in the output test
output.length	Length in milliseconds of an output to stay activated
portal.id	The portal ID associated with this agent
portal.name	The portal name associated with this agent
reader.activation.command.topic	Topic to activate and deactivate the reader
reader.activation.command.value	Value for the Reader Activation Command Topic to activate the reader
reader.adapter.prefix	Name of the reader this instance of this agent is currently running on
reader.deactivation.command.value	Value for the Reader Activation Command Topic to deactivate the reader
readertest.length	Duration in milliseconds of one reader test phase
readertest.outputs	Comma-separated list of output indices to cycle through in the reader test
selftestmode	Indicates if self-test mode is active
source.id	The source ID for generic events in this agent

Sensor Event Transformation agent:

The Sensor Event Transformation agent configures the MicroBroker Bridge on Data Transformation for a version 6.1 edge connector.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Note: This agent is not used in WebSphere Premises Server Version 6.1.0.1.

Table 42. Sensor Event transformation agent properties

Property	Description
classname	The name of the transformation class to use on messages in this flow
edge.id	The Data Capture and Delivery device ID associated with this agent

Table 42. Sensor Event transformation agent properties (continued)

Property	Description
edge.name	The Data Capture and Delivery device name associated with this agent
input.key.topic	The data to use in performing the transformation.
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
name	The unique name for the configuration object
source.id	The source ID for generic events in this agent
tracing	Displays trace output. The Alert agent must be running in order to set this property.
type	The type of configuration object that is being represented. This value can be set to pipe, flow, or transformation.

Switch Sensor agent:

The Switch Sensor agent is the agent for the switch sensor.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 43. Switch Sensor agent properties

Property	Description
agent.name	The name of the agent
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
portal.id	The portal ID associated with this agent
portal.name	The portal name associated with this agent
selftestmode	Indicates if self-test mode is active
sensor.activelevel	Indicates a positive (HIGH) or inverse (LOW) logic of this sensor
sensor.aliasname	The alias of this sensor
sensor.blockedtimeout	If this sensor is active longer than this time in microseconds (ms) it will issue an error
sensor.inactivitydelay	Delay in microseconds if the sensor transitions from active to inactive
sensor.listen.topic	Input topic relevant for this sensor

Table 43. Switch Sensor agent properties (continued)

Property	Description
sensor.pin	The pin number of output where this sensor is assigned to
sensor.publish.topic	Output topic used by this sensor
sensor.statelogging	Indicates whether state changes were logged with INFO, WARNING or ERROR level
source.id	The source ID for generic events in this agent
tracing	Displays trace output. The Alert agent must be running in order to set this property.

System agent:

The System agent controls the configuration settings for WebSphere Premises Server components.

When you add or modify a property for this agent, there is a 60 second delay before it is available to the system.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 44. System agent properties

Property	Description
autoid.core.savantid	The EPCGlobal, Inc Savant ID
cache.refresh.interval	The interval used by WebSphere Premises Server to refresh the internal cache
com.ibm.premises.report.location	Defines the location where the WebSphere Premises Server BIRT reports are stored
com.ibm.rfid.applping.shortcut	Defines whether the application ping message is returned by EBO or WebSphere Premises Server
com.ibm.rfid.dms.server.bundlerepository	The DMS bundle repository directory
com.ibm.rfid.dms.server.hostname	The hostname of the DMS bundle repository
com.ibm.rfid.location.external.format	Indicates how locations are reported to enterprise systems
com.ibm.rfid.location.external.format.delimiter	The delimiter to use between nodes in a fully qualified name. Used in conjunction with com.ibm.rfid.location.external.format.
com.ibm.rfid.premises.edgeconfig.delete.filter	Indicates the filter value to use in the WebSphere Premises Server Edge configuration xml in <request type="delete"> <configuration filter="<property value>"/> </request>
com.ibm.rfid.premises.event.startstop.filter	This property is deprecated in versions 6.1 and later.
com.ibm.rfid.premises.externalvalidation.response.accept	This property is deprecated in versions 6.1 and later.
com.ibm.rfid.premises.externalvalidation.response.acknowledge	This property is deprecated in versions 6.1 and later.
com.ibm.rfid.premises.externalvalidation.response.name	This property is deprecated in versions 6.1 and later.
com.ibm.rfid.premises.externalvalidation.response.reject	This property is deprecated in versions 6.1 and later.
com.ibm.rfid.premises.sysman.logging.resources	Specifies the name of the ResourceBundle to use for internationalizing messages going to the WebSphere Premises Server custom log files. These files consist of the alert and heartbeat logs.
com.ibm.sensorevent.converter	Defines the class used to convert between XML and events

Table 44. System agent properties (continued)

Property	Description
com.ibm.sensorevent.persistence.db	Directs the WebSphere Premises Server to persist all events to the database; if this property is set to true, all events are saved to the database; if this property is set to any value other than true, all events are not saved to the database
com.ibm.sensorevent.persistence.epcis	Directs the WebSphere Premises Server to persist all events to EPCIS; if this property is set to true, all events are sent to EPCIS; if this property is set to any value other than true, all events are not sent to EPCIS
com.ibm.sensorevent.persistence.epcis.queue	Defines the queue through which EPCIS events will be delivered for persistence by EPCIS
com.ibm.sensorevent.persistence.epcis.queue.manager	Defines the queue manager that contains the queue specified for persistence of EPCIS events

Tag Aggregator agent:

The Tag Aggregator agent aggregates tags.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 45. Tag Aggregator agent properties

Property	Description
aggregator.incoming.tag.topic	Receive tags from this topic
aggregator.publish.topic	Publish aggregated tags to this topic
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
portal.id	The portal ID associated with this agent
portal.name	The portal name associated with this agent
selftestmode	Indicates if self-test mode is active
source.id	The source ID for generic events in this agent
tracing	Displays trace output. The Alert agent must be running in order to set this property.
trigger.dump.topic	Dump all currently aggregated tags when this topic is received
trigger.dump.value	Dump all currently aggregated tags when this data is received
trigger.start.topic	Start aggregating tags when this topic is received
trigger.start.value	Start aggregating tags when this data is received
trigger.stop.topic	Stop aggregating tags when this topic is received
trigger.stop.value	Stop aggregating tags when this data is received

Test Tag agent:

The Test Tag agent is a location type agent that provides self-test functionality for store operators to verify that sensors and light trees are working correctly.

When this agent is notified of a topic matching the value of the tagTopic property, the data is checked to see if it matches one of any of the testTagIds property values. If there is a match, the agent enters test mode.

The agent then begins to play the sequence of topics defined in the outputTopics property. A delay defined in the lightDelay property occurs between each of the topics defined in the outputTopics property.

The agent remains in test mode until it receives the topic configured in the tagAggregationTopic property or until the number of milliseconds defined in the testModeTimeout property has been reached, whichever occurs first. If the tag aggregation topic occurs before the timeout value, the agent exits test mode and begins to play the sequence of topics defined in the aggregationOutputTopics. The same delay defined in the lightDelay property occurs between each of those topics. If the timeout value is reached but no tag aggregation topic is received, then agent exits test mode but does not continue to wait for the topic.

Note: In order to properly use this agent, you need to set the Filter Agent so that it subscribes to the TagReports topic and publishes to the tagTopic defined in the Test Tag agent.

Properties

For the properties below, you can enter either strings or variables. If you enter a variable, the value is substituted from the database when the XML configuration file is generated. Refer to "Using variables for property values" on page 149 for details on what variables can be substituted.

Table 46. Test Tag agent properties

Property	Description
aggregationOutputTopics	The sequence of topics that TestTagAgent will output when exiting test mode
lightDelay	Delay in milliseconds that occurs between each of the topics listed in the aggregationOutputTopics property. This property must be greater than or equal to the duration delays defined in the Light Tree agent for each of the lights, or the behavior is undefined.
log.level	The level of logging to use with this agent. If the value is empty then the system log level will be used. The Alert agent must be running in order to set this property.
outputTopics	The sequence of topics that TestTagAgent will output when entering test mode
portal.id	The portal ID associated with this agent
portal.name	The portal name associated with this agent

Table 46. Test Tag agent properties (continued)

Property	Description
qos	Messaging Quality of Service. A value of 0 means at most once. A value of 1 means at least once. A value of 2 means exactly once.
source.id	The source ID for generic events in this agent
tagAggregationTopic	The topic that signals the end of the test mode
tagTopic	The topic that TestTagAgent listens for entering test mode
testModeTimeout	A number in milliseconds that signals the end of the test mode
testTagIds	Any prefix up to and including the full tag id. The agent will enter test mode if any tagId starts with this string.
tracing	Displays trace output. The Alert agent must be running in order to set this property.

Using variables for property values:

For agent properties, you can specify either strings or variables. If you specify a variable, the string value is retrieved from the configuration database and substituted when the XML configuration files are created.

You can make simple or iterative substitutions. Simple substitutions directly substitute the value in the database that corresponds to the parameter specified.

For example, if the value in the database is `edge.name = "%CONTROLLER_ID%"`, then the value in the Data Capture and Delivery device XML is `edge.name = "E1"` (for the edge controller named E1).

Iterative substitutions enable values to be enumerated with each value for that substitution.

For example, if the value in the database is `topics = "[LOCATIONS]%LOCATIONS%,[/LOCATIONS]"`, then the value in the Data Capture and Delivery device XML is `topics = "P1, P2, P3,"` (for the locations P1, P2, and P3).

Substitutions for location-based agents

%LOCATION_ID%
> The location ID for the agent on the Data Capture and Delivery device

%SELFTEST_MODE%
> Whether the location is set to be in self test mode

%READER_ID%
> The ID for the tag reader at the location

%READER_COM_PORT%
> The com.port for the tag reader at the location

%READER_IP%
> The IP address of the tag reader at the location

%READER_REMOTE_PORT%
>The port number of the tag reader at the location

Substitutions for controller-based agents

%PREMISES_IP%
>The IP address of the WebSphere Premises Server

%CONTROLLER_ID%
>The Data Capture and Delivery device ID of the controller

%LOGGING_THRESHOLD%
>The logging threshold of the Data Capture and Delivery device

%LOCATIONS_STR%
>The locations associated with the controller

[LOCATIONS]%LOCATION_ID%[/LOCATIONS]
>Iterative substitution with all of the values of locations configured on the controller

[READERS]%READER_ID%[/READERS]
>Iterative substitution with all of the values of the tag readers configured on the controller

Working with devices

This section explains Data Capture and Delivery devices and how to manage them using the WebSphere Premises Server Administrative Console.

Data Capture and Delivery devices include Bartender and Loftware logical printers, readers, and simulated readers. Data Capture and Delivery device agents can exist in the system with different configurations for every different device configuration group. When creating a new device configuration group, you assign it a category such as reader or printer. For example, the device configuration group, Sirit, is assigned the category, reader. Each category has its own set of metadata properties. After creating a new device configuration group, you can assign agents along with their configurations, and define metadata to store with that configuration group. This section contains the following topics:

Adding a device

This topic describes how to add a new device to your network topology definition. Supported devices are readers, simulated readers, and logical printers.

About this task

Devices are readers, simulated readers, and Loftware and Bartender logical printers. After you create a device, you can associate it with a location and controllers as part of the network topology definition.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Under **Data Capture Configuration**, click **Devices** in the left navigation pane. The Devices panel displays.
3. Click **New**. The Create a New Device panel displays.
4. In the **Device ID** field, enter a unique identifier for the new device.
5. In the **Device Name** field, enter a unique description of the device.

6. In the **Configuration Group** field, click the drop-down arrow and select the type of device you are creating. For more information about configuration groups and configuration group types, refer to "Managing your configuration" on page 101.

7. If you selected a simulated reader as the configuration group, continue now with step 8. If you selected a reader or a logical printer as the configuration group, complete the remaining fields. For an explanation of the information required for these fields, refer to "Device details" on page 153.

8. Click **Create**. The Devices panel is displayed with the device you added.

Adding device configuration groups

Use the WebSphere Premises Server Administrative Console to add new Data Capture and Delivery device configuration groups to your network topology definition. You also associate each device configuration group with a category to further distinguish devices. Categories include printers, logical printers, readers, and simulated readers.

About this task

Devices in the WebSphere Premises Server Administrative Console are logical representations of the physical devices installed in your network. First you define the device configuration group and indicate the category. Then, you select the agent to associate with that device configuration group. Only one agent is associated with a device configuration group, and you can associate multiple PIDs with an agent.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.

2. Click **Data Capture Configuration** → **Devices** from the left navigation pane. The Devices panel displays.

3. Under Configuration Groups, click **Create**. The New Device Configuration Group panel displays.

4. In the **Name** field, enter a unique, logical name for this device configuration group.

5. In the **Description** field, enter a unique description of the device configuration group.

6. In the **Device Manufacturer** field, enter the manufacturer of the device.

7. In the **Device Model** field, enter the model of this device configuration group.

8. In the **Category** field, select the category for this device configuration group from the list.

9. In the list of agents, click the radio button next to the agent that you are associating with the new device configuration group. If the agent is not listed, click **Add New Agent** to add it.

10. Click **Create**. The Devices panel displays.

Modifying a device

This topic describes how to modify information about a device in your network topology using the WebSphere Premises Server Administrative Console.

About this task

Use the following steps to change information about a simulated reader, a reader, or a logical printer.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Click **Data Capture Configuration** → **Devices** from the left navigation pane. The Devices panel displays.
3. Click on the device for which you are modifying information. The Edit Device Details panel displays.
4. Make all necessary changes and click **Update**. The Devices panel displays.

Modifying a device configuration group

This topic describes how to modify the Data Capture and Delivery configuration group for a particular device using the WebSphere Premises Server Administrative Console.

About this task

Use the following steps to modify the configuration group information for a device.
1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Click **Data Capture Configuration** → **Devices** from the left navigation pane. The Devices panel displays.
3. Under **Configuration Groups**, select the device configuration group that you want to modify. The Edit Device Configuration Group panel displays. You can also add a new device configuration group. For instructions on adding a new device configuration group, refer to "Adding device configuration groups" on page 151.
4. Modify the appropriate fields and click **Update**.

Deleting a device

This topic describes how to delete a device from your network topology using the WebSphere Premises Server Administrative Console.

About this task

Use the following steps to delete a simulated reader, a reader, or a logical printer from your network topology.
1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Click **Data Capture Configuration** → **Devices** from the left navigation pane. The Devices panel displays.
3. Click on the device that you want to delete. The Edit Device Details panel displays.
4. Click **Delete**. A message displays asking you to confirm the deletion.
5. Click **OK** to delete the device. The Devices panel displays.

Deleting a device configuration group

This topic describes how to delete a Data Capture and Delivery configuration group for a particular device using the WebSphere Premises Server Administrative Console.

About this task

Use the following steps to delete a configuration group for a device.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Click **Data Capture Configuration** → **Devices** from the left navigation pane. The Devices panel displays.
3. Select the device configuration groups that you want to delete and click **Delete Selected**. A message displays asking you to confirm the deletions.
4. Click **OK**.

Device details

This topic defines the fields on various device panels. Devices can be readers, simulated readers, and logical printers.

Note: If some of the fields are grayed-out in the console, then you cannot edit them.

Reader details

Table 47. Reader device details

Field	Description
Device ID	A unique identifer for this tag reader. After you create the tag reader, you cannot modify this field. **Note:** The identifier must be 10 digits (0-9) or fewer.
Device Name	A unique, textual description of the reader.
Location	The location for the reader.
Configuration Group	The configuration group for the reader.
Communication Protocol	Indicates how you want to communicate with the tag reader. Select TCPIP or SERIAL.
IP Address	The IP address for this tag reader.
IP Port Number	The IP port number for communication with this tag reader. You can find the default port number for your tag reader in the documentation provided by the manufacturer of the tag reader.
Serial Port Number	The serial port number for communication with this tag reader.

Simulated reader details

Table 48. Simulated reader device details

Field	Description
Device ID	A unique identifer for this tag reader. After you create the tag reader, you cannot modify this field. **Note:** The identifier must be 10 digits (0-9) or fewer.
Device Name	A unique, textual description of the reader.
Configuration Group	The configuration group for the reader.
Location	The location for the reader.

Logical printer details

Table 49. Logical printer device details

Field	Description
Device ID	The ID of the logical tag printer. **Note:** The identifier must be 10 digits (0-9) or fewer.
Device Name	A unique, textual description of the logical printer.
Configuration Group	The configuration group for the logical printer.
Location	The location of the logical printer.
Logical Printer Class Name	Choose either Loftware or Bartender.
Logical Printer Delimiter	If you created a Bartender printer, enter the character that you want to use to separate submitted print jobs. The default character is a comma. **Important:** Because the information sent to the Bartender printer is separated by the delimitation character you indicate, that character cannot be part of the printed label information. For example, if you enter a comma as the delimitation character and a comma is part of the company name, the print job fails. Instead use a different delimitation character, such as a star.
Logical Printer Scan Folder	Enter the following file path to indicate where the Bartender print server is installed: C:\Program Files\SCAN_FOLDER.
Number of Identical Tags to Print	Enter the number of identical tags you would like to print.

Device configuration group details

This topic provides details about the device configuration groups that come with the product for Data Capture and Delivery.

Table 50. Device configuration group details table

Configuration Group Name	Device Description	Device Category
IBM simulated reader	IBM simulated reader	Simulated reader
Bartender	Logical device to print to Bartender printing software	Logical printer
Loftware	Logical device to print to Loftware printing software	Logical printer

Working with locations

This section explains Data Capture and Delivery locations and how to manage them using the WebSphere Premises Server Administrative Console.

Data Capture and Delivery locations in the WebSphere Premises Server Administrative Console are logical entities that correspond to the physical locations at which your physical devices, such as tag readers and printers, are installed. This section describes how to create a location configuration group, assign it a category which contains a set of metadata properties, and associated the location configuration group with a location configuration group type. For more information about configuration groups and configuration group types, refer to "Managing your configuration" on page 101.

Adding a location

Use the WebSphere Premises Server Administrative Console to add new Data Capture and Delivery locations to your network topology definition.

About this task

Locations in the WebSphere Premises Server Administrative Console are logical entities that correspond to the physical locations at which your physical devices, such as tag readers, are installed.

There are two kinds of locations: contained locations and container locations. Contained locations display beneath their respective container locations in the Locations panel. For example, you might add a container location for Location 1 and a contained location for Dock Door 1 at Location 1. You need to create a location for each location and dock door in the network.

Important: When creating a location topology:

- Only locations *without* contained locations can be associated with devices.
- Locations with associated devices *cannot* have contained locations.

Note: For each location, you can associate only one reader and one other device that is not a reader.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Click **Data Capture Configuration** → **Locations** from the left navigation pane. The Locations panel displays.
3. Click the location to which you are adding a contained location. The Edit Location Details panel displays. For an explanation of the fields on this panel, refer to "Location details" on page 159.
4. Click **Create Contained Location**. The Create New Location panel displays.
5. In the **Location ID** field, enter a unique location ID to identify this location. The location ID must be 10 digits or fewer. The ID helps ensure that tag reads from a particular location are properly routed from the edge controller to the WebSphere Premises Server and accurately updated in the corresponding enterprise system.

    Note: Location IDs, including dock door IDs, must be unique. For example, you cannot create two locations with the same location ID. In addition, you cannot create two unique locations, Location 1 and Location 2 for example, that both have dock door IDs called "12340."

6. In the **Location Name** field, enter a unique name for the location.
7. In the **Location Alias** field, enter an alias. Aliases are typically used if the enterprise system to which the WebSphere Premises Server is passing data requires an identifier other than the one used in the *Location ID* field. For

example, the location in the **Location ID** field can be an easily recognized name, even if the back-end system requires a more cryptic identifier for the location.

8. In the **Description** field, enter a brief description of the location.

   Note: The field, **Is Addressable**, is not functional at this time. Continue now with the next field.

9. In the **Is In Self-Test Mode** field, to indicate that this location is in self-test mode, select **True**. If not, select **False**.

10. In the **Contact** field, click the drop-down arrow and select a contact from the list. See Adding contacts for more information.

11. Enter the address information for this location, if desired.

12. In the **Device** field, select a device from the list to associate with this location.

13. In the **Reader** field, select a reader from the list to associate with this location.

14. Click **Create**. The Locations panel displays the new location indented under the container location.

Adding a location configuration group

Use the WebSphere Premises Server Administrative Console to add a new location configuration group to your network topology definition. Then select several agents to associate with the new location configuration group.

About this task

A location configuration group consists of a name, description, and category. Locations in the WebSphere Premises Server Administrative Console are logical entities that correspond to the physical locations (indicated by the category) at which your physical devices, such as tag readers, are installed.

There are two kinds of locations: contained locations and container locations. Contained locations display underneath their respective container locations in the Locations panel. For example, you might add a container location for Store 1 and a contained location for Dock Door 1 at Store 1. You need to create a location for each store and dock door in the WebSphere Premises Server network.

Important: When creating a location topology:
- Only locations *without* contained locations can be associated with devices.
- Locations with associated devices *cannot* have contained locations.

WebSphere Premises Server comes with default location configuration groups. The Basic Dock Door location configuration group represents a dock door portal location that has only a switch and a reader. The Standard Dock Door configuration group represents a dock door portal location that has a motion sensor, switch, and a reader . The Enhanced Dock Door configuration group represents a dock door portal location that has a motion sensor, switch, barrier, and reader.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.

2. Click **Data Capture Configuration** → **Locations** from the left navigation pane. The Locations panel displays.

3. Under Configuration Groups, click **Create**. The New Location Configuration Group panel displays.

4. In the **Name** field, enter a unique name for this location configuration group.

5. In the **Description** field, enter a unique description of the location configuration group.

6. In the **Category** field, click the drop-down arrow and select the category for the location configuration group.

7. In the Configuration Group Agents list, select all of the location agents that you want to associate with this location configuration group.

8. Click **Create**.

Modifying a location

Use the WebSphere Premises Server Administrative Console to modify Data Capture and Delivery locations in your network topology.

About this task

Important: When creating a location topology:

- Only locations *without* contained locations can be associated with devices.
- Locations with associated devices *cannot* have contained locations.

Note: For each location, you can associate only one reader and one other device that is not a reader.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.

2. Navigate to **Data Capture Configuration** › **Locations** in the left navigation pane. The Locations panel displays.

3. Click on the location that you want to edit. The Edit Location Details panel displays.

4. Make the necessary changes and click **Update**.

   Note: To modify a controller associated with the location, click on the controller from the Edit Location Details panel.
   The changes are saved.

Modifying a location configuration group

This topic describes how to modify the configuration for a particular location using the WebSphere Premises Server Administrative Console.

About this task

You can modify a location configuration group by:

- Adding a contained location configuration group
- Modifying a contained location configuration group
- Adding an agent to a location configuration group

Important: When creating a location topology:

- Only locations *without* contained locations can be associated with devices.
- Locations with associated devices *cannot* have contained locations.

Adding a contained location configuration group:

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Click **Data Capture Configuration** → **Locations** from the left navigation pane. The Locations panel displays.
3. Expand the **Root Location** option to show available root locations.
4. Click on the location to which you are adding a contained location. The Edit Location Details panel displays.
5. Click **Create Contained Locations**. The Create New Location panel displays.
6. Complete the fields on this screen and click **Create**.

Modifying a contained location configuration group:
1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Click **Data Capture Configuration** → **Locations** from the left navigation pane. The Locations panel displays.
3. To modify a root location, expand the Root Location field to show contained locations.
4. Click the contained location that you want to modify. The Edit Location Details panel displays.
5. Modify the appropriate fields.
6. Click **Update**.

Adding an agent to a location configuration group:
About this task

You can add an existing agent to a location groupconfiguration group or create a new agent to add to the location configuration group.
1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Click **Data Capture Configuration** → **Locations** from the left navigation pane. The Locations panel displays.
3. Click on the location group to which you are adding an agent. The Edit Location Configuration Group panel displays.
4. Click on the agent that you want to add to the location configuration group. The agent information displays in the Selected Agent Details window.
5. Choose one of the following functions: .
   - To add a new agent, click **Add New Agent**. The New Agent panel displays. Click **Done** to add this agent to the location.
   - To add an existing agent, click the check box to select the agent from the list and click **Apply**.

Deleting a location
Use the WebSphere Premises Server Administrative Console to delete Data Capture and Delivery locations in your network topology.

Before you begin

Note: You cannot delete a location that is associated with other resources or devices, such as a controller or logical printer. Therefore, you must first delete the resources and devices associated with the location before you can delete the location.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Click **Data Capture Configuration** › **Locations** from the left navigation pane. The Locations panel displays.
3. Click the location that you want to delete. The Edit Location Details panel displays.
4. Click **Delete**. A confirmation message displays.
5. Click **OK** to delete the location.

Deleting a location configuration group

This topic describes how to delete a Data Capture and Delivery configuration group for a particular location using the WebSphere Premises Server Administrative Console.

About this task

Use the following steps to delete a configuration group for a location.
1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Click **Data Capture Configuration** › **Locations** from the left navigation pane. The Locations panel displays.
3. Select the location configuration groups that you want to delete and click **Delete Selected**. A message displays asking you to confirm the deletions.
4. Click **OK**.

Location details

The following table defines the fields on the Create New Location and Edit Location Detail panels.

Fields

Field	Description
Device (Data Capture and Delivery only)	Enter a logical identifier for the device that is associated with the location. This field is available only when you are creating a contained location.
Location ID*	Enter a logical identifier for the location you are defining. After you create the location, you cannot modify this field. **Note:** The identifier must be 10 digits (0-9) or fewer.
Location Name	Enter a unique, textual description of the location.
Location Alias*	Enter an alias for the location ID. The location alias can be different from or identical to the location ID, but it cannot be identical to another location alias.
Description	Enter a description of this location.
Is Addressable	Indicates if this location has an address entered in the system. A location is only addressable if the contact information is completed. See "Adding contacts" on page 160 for more information. This field is set to **false** by default.
Is in Self Test Mode	Indicates if self-test mode is activated for this location. This field is set to **false** by default.
Contact	Displays the contact manager at this location. See "Adding contacts" on page 160 for more information.

Field	Description
Container Location	Displays the container location for this location. This field is automatically completed with the default container location and cannot be modified. See "Adding a location" on page 155 for more information.
Controller**	Displays the controller associated with this location. See "Adding a controller" on page 162 for more information.
Address	Enter the mailing or street address for the location.
Reader	Select a reader to associate with this location.
Device	Select a device to associate with this location. **Note:** For each location, you can associate only one reader and one other device that is not a reader.
Location Type	The location configuration group associated with this location.

* Required field.

** These fields display only on the Edit Location Detail panel.

Location configuration group details

This topic lists the location configuration groups that come with the product for Data Capture and Delivery.

Table 51. Location configuration group details table

Configuration Group Name	Location Description	Location Category
Basic dock door receiving	Dock door receiving with only the switch	Receiving Portal
Standard dock door receiving	Dock door receiving with switch and motion	Receiving Portal
Enhanced dock door receiving	Dock door receiving with switch, motion, and barrier	Receiving Portal

Working with contacts

This section describes how to manage Data Capture and Delivery location contact information using the WebSphere Premises Server Administrative Console.

A location contact is the primary contact person at a location. Using the Locations panel, you can store information such as e-mail address, mobile and pager numbers, and locations managed by the contact person.

Adding contacts

Use the WebSphere Premises Server Administrative Console to add new Data Capture and Delivery location contacts to your network topology definition.

About this task

Location contacts specify important information about the primary RFID contact person at a location. You can associate a contact with multiple locations. See "Adding a location" on page 155 for more information.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.

2. Navigate to **Data Capture Configuration** → **Locations** from the left navigation pane. The Locations panel displays.
3. Under **Location Contacts**, click **Create**. The Create New Contact panel displays.
4. In the **Name** field, enter the name of the contact.
5. Complete the remaining optional fields, and click **Create**. The contact is saved.

Modifying contacts

Use the WebSphere Premises Server Administrative Console to modify existing Data Capture and Delivery location contacts in your network topology definition.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Click **Data Capture Configuration** → **Locations** from the left navigation pane. The Locations panel displays.
3. Under **Location Contacts**, click the contact that you want to modify. The Contact Details panel displays.
4. Make the necessary changes and click **Update**. The changes are saved.

Deleting contacts

Use the WebSphere Premises Server Administrative Console to delete existing location contacts from your network topology definition.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Click **Data Capture Configuration** → **Locations** from the left navigation pane. The Locations panel displays.
3. Under Location Contacts, click the contact that you want to delete. The Contact Details panel displays.
4. Click **Delete**. A confirmation message displays.
5. Click **OK** to delete the contact.

Contact details

The following table defines the fields on the Create New Contact and Contact Details panels.

Fields

Field	Description
Name*	Enter the contact person at this location. After you create the contact person, you cannot modify this field.
Email	Enter the contact person's e-mail address.
Phone	Enter the contact person's phone number.
Mobile	Enter the contact person's mobile phone number.
Pager	Enter the contact person's pager number.
Locations Managed**	Displays the locations associated with this contact person. See Adding a location for more information.

* Required field

** This field only displays on the Contact Details panel.

Working with controllers

This section explains Data Capture and Delivery controllers and how to manage them using the WebSphere Premises Server Administrative Console.

A controller is the component that interacts with and controls devices. It processes, filters, and communicates with the WebSphere Premises Server.

This section describes how to create a controller configuration group, assign it a category which contains a set of metadata properties, and associate the controller configuration group with a controller configuration group type.

Adding a controller

Use the WebSphere Premises Server Administrative Console to add new Data Capture and Delivery controllers to your network topology definition.

About this task

Controllers in the WebSphere Premises Server Administrative Console are logical representations of the physical edge devices in your WebSphere Premises Server network. You must define a controller for each edge device in the network. The information you define for each controller includes a logical identifier, MAC address, alert threshold, and the locations with which the edge devices communicate. For a Data Capture and Delivery controller, you also add the controller to a configuration group.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Navigate to **Data Capture Configuration** > **Controllers** in the left navigation pane. The Controllers panel displays.
3. Click **New**. The Create New Controller panel displays.
4. Enter a unique controller ID for this edge controller. This logical identifier is used to ensure that information is routed to and from the correct edge controller. The identifier must be 10 digits (0-9) or fewer.
5. In the **Controller Name** field, enter a unique name that describes the controller.
6. In the **Configuration Groups** field, select a configuration group for this controller. For instructions on adding a new configuration group, refer to "Adding a controller configuration group."
7. In the **MAC Address** field, enter the edge controller's MAC address.
8. Select an alert threshold to determine the level of information to be included in the edge controller log file.
9. In the **Available Locations** column, select the locations that you want to associate with this edge controller and click the right arrow. The locations display in the **Selected Locations** column.
10. Click **Create**. The new edge controller displays in the Controllers panel.

Adding a controller configuration group

Use the WebSphere Premises Server Administrative Console to add a new controller configuration group to your network topology definition. Then select one or more agents to associate with each new controller configuration group.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Click **Data Capture Configuration** > **Controllers** from the left navigation pane. The Controllers panel displays.

3. Under **Configuration Groups**, click **Create**. The New Controller Configuration Group panel displays.
4. Enter a unique, logical name for this controller configuration group.
5. Enter a unique, textual description of the controller configuration group.
6. In the **Category** field, click the drop-down arrow and select a category for this controller configuration group.
7. In the **Configuration Group Agents** list, select all the controller agents that you want to associate with the new controller configuration group.
8. Click **Create**.

Modifying a controller

Use the WebSphere Premises Server Administrative Console to modify existing Data Capture and Delivery controllers in your network topology definition.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Click **Data Capture Configuration** › **Controllers** from the left navigation pane. The Controllers panel displays.
3. Click on the controller that you want to modify. The Edit Controller Details panel displays.
4. Make the necessary changes and click **Update**. The changes are saved.

Modifying a controller configuration group

This topic describes how to modify the configuration group for a particular controller using the WebSphere Premises Server Administrative Console.

About this task

You can modify all information except the controller ID. You can also add a location to a controller configuration group.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Click **Data Capture Configuration** › **Controllers** from the left navigation pane. The Controllers panel displays.
3. To update a configuration group, continue now with step 4. To add a location to this controller:
   - Click on the controller to which you are adding a location. The Edit Controller Details panel displays.
   - Select the location in the **Available Locations** field and click the right arrow to add it to the **Selected Locations** field.
   - Click **Update**.
4. Under Configuration Groups, click the configuration group that you want to modify. The Edit Controller Configuration Group panel displays.
5. Modify the appropriate fields.
6. Click **Update**.

Deleting a controller

Use the WebSphere Premises Server Administrative Console to delete existing Data Capture and Delivery controllers from your network topology definition.

Before you begin

Note: You cannot delete a controller that is associated with locations. If the controller you are deleting shows selected locations, move them to the **Available Locations** box as indicated in step 4.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Navigate to **Data Capture Configuration** → **Controllers** in the left navigation pane. The Controllers panel displays.
3. Click on the controller that you want to delete. The Edit Controller Details panel displays.
4. Remove any items in the **Selected Locations** box by selecting them and clicking **<-** . The items move back to the **Available Locations** box.
5. If you removed locations in the previous step:
   - Click **Update**. The Controllers panel displays.
   - Click on the controller that you are deleting to return to the Edit Controller Details panel.
6. Click **Delete**. A confirmation message displays.
7. Click **OK** to delete the controller.

Deleting a controller configuration group
This topic describes how to delete a Data Capture and Delivery configuration group for a particular controller using the WebSphere Premises Server Administrative Console.

About this task

Use the following steps to delete a configuration group for a controller.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Click **Data Capture Configuration** → **Controllers** from the left navigation pane. The Controllers configuration groups display.
3. Select the controller configuration group that you want to delete and click **Delete Selected**. A message displays asking you to confirm the deletion.
4. Click **Ok**.

Controller details
The following table defines the fields on the Create New Controller and Edit Controller Detail panels. All fields are required except the **MAC Address** field.

Fields

Field	Description
Controller ID	Enter a logical identifier for the edge controller you are defining. After you create the edge controller, you cannot modify this field. **Note:** The identifier must be 10 digits (0-9) or fewer.
Controller Name	Enter a unique, textual description of the controller.
Configuration Groups - Data Capture and Delivery only	Select the configuration group that you want to use for the controller.

Field	Description
MAC Address	The MAC address assigned to the edge controller you are defining. This field is used for reference purposes only, and is not required.
IP Address	The IP address assigned to the edge controller you are defining. This field is not required.
Alert Threshold	The level of detail that you want specified in the Alert log file. The edge controller uses this value to determine which level of events are forwarded to the WebSphere Premises Server; the lower the alert level, the higher the number of events that are sent to the log file. Choose from the following alert thresholds, from highest to lowest -- for example, selecting **debug** generates the greatest number of alerts. • error (default) • warning • info • debug **Note:** Setting the alert threshold to **info** or **debug** generates a large amount of traffic, and might overload the network. Use these two settings only if necessary.
Available Locations	The list of available locations to associate with the edge controller you are defining. Select a location and click the right arrow to associate the location with this edge controller.
Selected Locations	The list of locations currently associated with the edge controller. Click the left arrow to disassociate this location with the device.

Controller configuration group details

This topic provides details about the controller configuration groups that come with the product for Data Capture and Delivery.

Table 52. Controller configuration group details table

Configuration Group Name	Controller Description	Controller Category
Distribution center	Configuration for a remote Data Capture and Delivery controller	Remote
Edge on premises	Configuration for a local Data Capture and Delivery controller	Local

Reloading Data Capture and Delivery controllers using the console

Use the **Reload Configuration** function in the Controllers panel to remotely reload a Data Capture and Delivery controller from the WebSphere Premises Server Administrative Console.

About this task

When you change a Data Capture and Delivery controller configuration, you must reload the affected controller to activate those changes. For example, if you change

a tag reader's IP address, modify an agent property, or change the alert threshold for a controller, the changes are not implemented until you reload it.

Note: The reload feature is intended for incremental updates. If you make significant changes to the controller configuration, it is possible that reloading the configuration may not be sufficient. If your configuration updates fail when you use **Reload Configuration**, restart your Data Capture and Delivery controller to update the configuration.

Follow these steps to reload a Data Capture and Delivery controller from the WebSphere Premises Server Administrative Console.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Navigate to **Data Capture Configuration** → **Controllers** from the left navigation pane. The Controllers panel displays.
3. Click the controller that you want to reload. The Edit Controller Details panel displays.
4. Click **Reload Configuration**. The Data Capture and Delivery controller reloads.

   Note: All locations associated with this controller are disabled while the device is reloading.

Installed sample controllers

WebSphere Premises Server installs sample Data Capture and Delivery controllers that are available in the WebSphere Premises Server Administrative Console.

Use this table to understand the configurations associated with the sample controllers.

Table 53. Sample controllers

Controller name(This is the controller name listed in the bundle list URL property in the config.ini file.)	Description	Bundle list file in config.ini(This is the file name listed in the bundle list URL property in the config.ini file.)	Bundle list file in XML(This is the file name listed in the bundle list URL property in the WebSphere Premises Server XML.)	Associated location	Associated device
E0	Data Transformation on WebSphere Premises Server Use in a production environment.	dc_core4dts.txt	none	none	none
E2	local Data Capture and Delivery plus Data Transformation on WebSphere Premises Server (with the reader simulator) Use for testing your installation.	dc_core4dts.txt	rdrsim.txt	P2	R2
E3	remote Data Capture and Delivery (with the reader simulator)	dc_core.txt	rdrsim.txt	P3	R3

Table 53. Sample controllers (continued)

Controller name(This is the controller name listed in the bundle list URL property in the config.ini file.)	Description	Bundle list file in config.ini(This is the file name listed in the bundle list URL property in the config.ini file.)	Bundle list file in XML(This is the file name listed in the bundle list URL property in the WebSphere Premises Server XML.)	Associated location	Associated device
E4	remote Data Capture and Delivery and Data Transformation Available if you have run the installer for high availability.	dc_core4dts.txt	rdrsim.txt	P4	R4

Importing the configuration file

This section explains the Data Capture and Delivery XML configuration file and how to import it.

This section contains the following topics:

Sample XML schema and configuration files

This topic provides XML schema definition and sample XML configuration files that you can use as a reference when configuring your WebSphere Premises Server.

You can configure the server using the **Import Configuration** link in the WebSphere Premises Server Administrative Console, by using a command line utility, or by posting a valid XML configuration file to the XMLConfigAdmin servlet. To post an XML configuration file, use the following link:

http://*premises_server_host_name*:*port*/ibmrfidadmin/XMLConfigAdmin

XML Schema

Below is the XML schema that defines the rules for headless configuration of the WebSphere Premises Server.

Note: This file is provided as a basis for understanding the XML configuration definition. The current version of this file is provided on the file system as part of the WebSphere Premises Server installation and contains the actual rules used on the server.

```
<?xml version="1.0" encoding="UTF-8"?>
<schema targetNamespace="http://www.ibm.com" version="0.1" xmlns="http://www.w3.org/2001/XMLSchema"
xmlns:ibmrfidconfigadmin="http://www.ibm.com">
<element name="configurationAdmin" type="ibmrfidconfigadmin:IBMRFIDConfigAdmin" />
<complexType name="IBMRFIDConfigAdmin">
<sequence>
<element name="requests" type="ibmrfidconfigadmin:Requests" minOccurs="1" maxOccurs="1" />
</sequence>
<attribute name="version" type="string" use="optional" />
<attribute name="orig" type="string" use="optional" />
<attribute name="dest" type="string" use="optional" />
<attribute name="dts" type="dateTime" use="optional" />
<attribute name="edgein" type="boolean" use="optional" default="false" />
</complexType>
<!-- REQUESTS DEFINITION -->
<complexType name="Requests">
<sequence>
<element maxOccurs="unbounded" minOccurs="1" name="request" type="ibmrfidconfigadmin:Request" />
</sequence>
</complexType>
```

```xml
<!-- REQUEST DEFINITION -->
<complexType name="Request">
<all>
<element maxOccurs="1" minOccurs="0" name="agentconfigurations"
type="ibmrfidconfigadmin:AgentConfigurations" />
<element maxOccurs="1" minOccurs="0" name="serverconfigurations"
type="ibmrfidconfigadmin:ServerConfigurations" />
</all>
<attribute name="type" type="ibmrfidconfigadmin:requestTypeEnum" use="required" />
<attribute name="cascade" type="boolean" use="optional" default="false"    />
</complexType>
<!-- *********AGENT CONFIGURATIONS DEFINITION ********** -->
<complexType name="AgentConfigurations">
<sequence>
<element maxOccurs="unbounded" minOccurs="1" name="configuration"
type="ibmrfidconfigadmin:Configuration" />
</sequence>
</complexType>
<!-- CONFIGURATION DEFINITION -->
<complexType name="Configuration">
<sequence>
<element maxOccurs="1" minOccurs="0" name="properties" type="ibmrfidconfigadmin:Properties" />
</sequence>
<attribute name="pid" type="string" use="optional"/>
<attribute name="factoryPid" type="string" use="optional"/>
<attribute name="filter" type="string" use="optional"/>
<attribute name="description" type="string" use="optional"/>
<attributeGroup ref="ibmrfidconfigadmin:agentattrgroup" />
</complexType>
<!-- PROPERTIES DEFINITION -->
<complexType name="Properties">
<sequence>
<element maxOccurs="unbounded" minOccurs="1" name="property" type="ibmrfidconfigadmin:Property" />
</sequence>
</complexType>
<!-- PROPERTY DEFINITION -->
<complexType name="Property">
<attribute name="key" type="ibmrfidconfigadmin:non-empty-string" use="required"/>
<attribute name="value" type="string" use="optional" />
<attribute name="name" type="string" use="optional" />
<attribute name="type"   type="ibmrfidconfigadmin:propertyTypeEnum" default="string" use="optional" />
<attribute name="default" type="string" use="optional" />
<attribute name="description" type="string" use="optional" />
<attribute name="cardinality" type="integer" default="0" use="optional" />
<attribute name="required" type="string" use="optional" />
</complexType>
<!-- *********SERVER CONFIGURATIONS DEFINITION ********** -->
<complexType name="ServerConfigurations">
<sequence>
<element maxOccurs="1" minOccurs="0" name="configurationgrouptype"
type="ibmrfidconfigadmin:ConfigurationGroupType" />
<element maxOccurs="1" minOccurs="0" name="categories"
type="ibmrfidconfigadmin:Categories" />
<element maxOccurs="1" minOccurs="0" name="configurationgroups"
type="ibmrfidconfigadmin:ConfigurationGroups" />
<element maxOccurs="1" minOccurs="0" name="devices" type="ibmrfidconfigadmin:Devices" />
<element maxOccurs="1" minOccurs="0" name="locations" type="ibmrfidconfigadmin:Locations" />
<element maxOccurs="1" minOccurs="0" name="contacts" type="ibmrfidconfigadmin:Contacts" />
<element maxOccurs="1" minOccurs="0" name="controllers" type="ibmrfidconfigadmin:Controllers" />
</sequence>
</complexType>
<!-- CATEGORIES DEFINITION  -->
<complexType name="Categories">
<sequence>
<element maxOccurs="unbounded" minOccurs="1" name="category" type="ibmrfidconfigadmin:Category" />
</sequence>
</complexType>
<!-- CONFIGURATION GROUP DEFINITION  -->
<complexType name="ConfigurationGroups">
<sequence>
<element maxOccurs="unbounded" minOccurs="1" name="configurationgroup"
type="ibmrfidconfigadmin:ConfigurationGroup" />
</sequence>
</complexType>
<!-- DEVICES DEFINITION  -->
<complexType name="Devices">
<sequence>
<element maxOccurs="unbounded" minOccurs="1" name="device" type="ibmrfidconfigadmin:Device" />
</sequence>
</complexType>
<!-- LOCATIONS DEFINITION  -->
<complexType name="Locations">
<sequence>
<element maxOccurs="unbounded" minOccurs="1" name="location" type="ibmrfidconfigadmin:Location" />
</sequence>
</complexType>
<!-- CONTROLLERS DEFINITION  -->
<complexType name="Controllers">
<sequence>
<element maxOccurs="unbounded" minOccurs="1" name="controller" type="ibmrfidconfigadmin:Controller" />
</sequence>
```

```
</complexType>
<!-- CONTACTS DEFINITION -->
<complexType name="Contacts">
<sequence>
<element maxOccurs="unbounded" minOccurs="1" name="contact" type="ibmrfidconfigadmin:Contact" />
</sequence>
</complexType>
<!-- CONFIGURATION GROUP TYPE DEFINITION -->
<complexType name="ConfigurationGroupType" >
<sequence>
<element maxOccurs="unbounded" minOccurs="1" name="config-group-type-metadata"
type="ibmrfidconfigadmin:ConfigurationGroupTypeMetaData" />
</sequence>
<attribute name="config-group-type" type="ibmrfidconfigadmin:configgrouptypeEnum" use="required"/>
</complexType>
<!-- CONFIGURATION GROUP TYPE META DATA DEFINITION -->
<complexType name="ConfigurationGroupTypeMetaData" >
<attributeGroup ref="ibmrfidconfigadmin:configgrouptypemetadata-attrgroup" />
</complexType>
<!-- CATEGORY DEFINITION -->
<complexType name="Category" >
<sequence>
<element maxOccurs="unbounded" minOccurs="0" name="category-metadata"
type="ibmrfidconfigadmin:CategoryMetaData" />
</sequence>
<attribute name="name" type="ibmrfidconfigadmin:non-empty-string" use="required"/>
<attribute name="config-group-type" type="ibmrfidconfigadmin:configgrouptypeEnum" use="required" />
</complexType>
<!-- CATEGORY META DATA DEFINITION -->
<complexType name="CategoryMetaData" >
<attributeGroup ref="ibmrfidconfigadmin:configgrouptypemetadata-attrgroup" />
</complexType>
<!-- CONFIGURATION GROUP DEFINITION -->
<complexType  name="ConfigurationGroup">
<sequence>
<element maxOccurs="unbounded" minOccurs="0" name="config-group-metadata"
type="ibmrfidconfigadmin:ConfigGroupMetadata" />
<element maxOccurs="1" minOccurs="0" name="agentconfigurations"
type="ibmrfidconfigadmin:AgentConfigurations" />
</sequence>
<attribute name="config-group-name" type="ibmrfidconfigadmin:non-empty-string" use="required"/>
<attribute name="config-group-description" type="string" use="optional"/>
<attribute name="config-group-type" type="ibmrfidconfigadmin:configgrouptypeEnum" use="required"/>
<attribute name="config-group-category" type="ibmrfidconfigadmin:non-empty-string" use="required"/>
</complexType>
<complexType name="ConfigGroupMetadata" >
<attributeGroup ref="ibmrfidconfigadmin:metadata-attrgroup"/>
</complexType>
<!-- DEVICE DEFINITION -->
<complexType name="Device">
<sequence>
<element maxOccurs="unbounded" minOccurs="0" name="device-category-metadata"
type="ibmrfidconfigadmin:DeviceCategoryMetaData" />
</sequence>
<attribute name="deviceid" type="integer" use="required" />
<attribute name="devicename" type="ibmrfidconfigadmin:non-empty-string" use="required" />
<attribute name="config-group-name" type="ibmrfidconfigadmin:non-empty-string" use="required"/>
<attribute name="deviceidprefix" type="ibmrfidconfigadmin:non-empty-string"
use="optional" default="R" />
</complexType>
<!-- DEVICE CATEGORY METADATA -->
<complexType name="DeviceCategoryMetaData" >
<attributeGroup ref="ibmrfidconfigadmin:metadata-attrgroup" />
</complexType>
<!-- LOCATION DEFINITION -->
<complexType name="Location">
<sequence>
<element maxOccurs="1" minOccurs="0" name="addressinfo" type="ibmrfidconfigadmin:LocationAddrInfo" />
<element maxOccurs="unbounded" minOccurs="0" name="location-category-metadata"
type="ibmrfidconfigadmin:LocationCategoryMetaData" />
<element maxOccurs="1" minOccurs="0" name="location-devices" type="ibmrfidconfigadmin:LocationDevices" />
</sequence>
<attribute name="locationid" type="integer" use="required" />
<attribute name="name" type="ibmrfidconfigadmin:non-empty-string" use="required" />
<attribute name="aliasname" type="ibmrfidconfigadmin:non-empty-string" use="required" />
<attribute name="description" type="string" use="optional" />
<attribute name="deviceidref" type="ibmrfidconfigadmin:non-empty-string" use="optional" />
<attribute name="controlleridref" type="ibmrfidconfigadmin:non-empty-string" use="optional" />
<attribute name="iscontainerlocation" type="boolean" use="required" />
<attribute name="isaddressable" type="boolean" use="optional" default="false"  />
<attribute name="isselftestmode" type="boolean" use="optional" default="false"  />
<attribute name="contact" type="ibmrfidconfigadmin:non-empty-string" use="optional" />
<attribute name="parentlocationref" type="ibmrfidconfigadmin:non-empty-string" use="optional"
default="Root" />
<attribute name="config-group-name" type="ibmrfidconfigadmin:non-empty-string" use="required"/>
<attribute name="locationidprefix" type="ibmrfidconfigadmin:non-empty-string" use="optional"
default="L" />
</complexType>
<complexType name="LocationAddrInfo" >
<attribute name="street1" type="string" use="optional" />
<attribute name="street2" type="string" use="optional" />
```

```xml
<attribute name="city" type="string" use="optional" />
<attribute name="state" type="string" use="optional" />
<attribute name="province" type="string" use="optional" />
<attribute name="region" type="string" use="optional" />
<attribute name="zip" type="integer" use="optional" />
</complexType>
<!-- LOCATION CATEGORY METADATA -->
<complexType name="LocationCategoryMetaData" >
<attributeGroup ref="ibmrfidconfigadmin:metadata-attrgroup" />
</complexType>
<!-- LOCATION DEVICES  -->
<complexType name="LocationDevices" >
<sequence>
<element maxOccurs="1" minOccurs="0" name="deviceid" type="ibmrfidconfigadmin:non-empty-string" />
</sequence>
</complexType>
<!-- CONTROLLER DEFINITION  -->
<complexType name="Controller">
<sequence>
<element maxOccurs="unbounded" minOccurs="0" name="controller-category-metadata"
type="ibmrfidconfigadmin:ControllerCategoryMetaData" />
<element maxOccurs="1" minOccurs="0" name="controller-locations"
type="ibmrfidconfigadmin:ControllerLocations" />
</sequence>
<attribute name="controllerid" type="integer" use="required" />
<attribute name="controllername" type="ibmrfidconfigadmin:non-empty-string" use="required" />
<attribute name="macaddress" type="string" use="optional" />
<attribute name="alertlevel" type="string" use="optional"  default="error" />
<attribute name="config-group-name" type="ibmrfidconfigadmin:non-empty-string" use="required"/>
<attribute name="controlleridprefix" type="ibmrfidconfigadmin:non-empty-string"
use="optional" default="C" />
</complexType>
<!-- CONTROLLER CATEGORY METADATA -->
<complexType name="ControllerCategoryMetaData" >
<attributeGroup ref="ibmrfidconfigadmin:metadata-attrgroup" />
</complexType>
<!-- CONTROLLER LOCATION  -->
<complexType name="ControllerLocations" >
<sequence>
<element maxOccurs="unbounded" minOccurs="0" name="locationid"
type="ibmrfidconfigadmin:non-empty-string" />
</sequence>
</complexType>
<!-- CONTACT DEFINITION  -->
<complexType name="Contact">
<attribute name="name" type="ibmrfidconfigadmin:non-empty-string" use="required" />
<attribute name="email" type="string" use="optional" />
<attribute name="phone" type="string" use="optional"/>
<attribute name="mobile" type="string" use="optional"/>
<attribute name="pager" type="string" use="optional"/>
</complexType>
<!--*************** GROUP DEFINITIONS****************** -->
<attributeGroup name="agentattrgroup">
<attribute name="bundlename" type="string" use="optional" />
<attribute name="bundleversion" type="string" use="optional" />
<!-- attribute name="createDMSSoftware" type="boolean" use="optional" -->
<attribute name="name" type="ibmrfidconfigadmin:non-empty-string" use="required" />
<attribute name="config-group-type" type="ibmrfidconfigadmin:agentconfiggrouptypeEnum"
use="required" />
<attribute name="config-group-name" type="ibmrfidconfigadmin:non-empty-string" use="optional" />
</attributeGroup>
<attributeGroup name="metadata-attrgroup">
<attribute name="name" type="ibmrfidconfigadmin:non-empty-string" use="required"/>
<attribute name="value" type="string" use="optional"/>
<attribute name="description" type="string" use="optional"/>
</attributeGroup>
<attributeGroup name="configgrouptypemetadata-attrgroup">
<attribute name="name" type="ibmrfidconfigadmin:non-empty-string" use="required"/>
<attribute name="defaultvalue" type="string" use="optional"/>
<attribute name="description" type="string" use="optional"/>
</attributeGroup>
<!-- ***************ENUMERATION DEFINITIONS************* -->
<simpleType name="requestTypeEnum">
<restriction base="string">
<enumeration value="update" />
<enumeration value="create" />
<enumeration value="delete" />
</restriction>
</simpleType>
<simpleType name="alertlevelEnum">
<restriction base="string">
<enumeration value="error" />
<enumeration value="debug" />
<enumeration value="warning" />
<enumeration value="info" />
</restriction>
</simpleType>
<simpleType name="configgrouptypeEnum">
<restriction base="string">
<enumeration value="LocationType" />
<enumeration value="DeviceType" />
```

```
<enumeration value="ControllerType" />
</restriction>
</simpleType>
<simpleType name="agentconfiggrouptypeEnum">
<restriction base="string">
<enumeration value="LocationType" />
<enumeration value="DeviceType" />
<enumeration value="ControllerType" />
<enumeration value="" />
</restriction>
</simpleType>
<simpleType name="propertyTypeEnum">
<restriction base="string">
<enumeration value="boolean" />
<enumeration value="byte" />
<enumeration value="character" />
<enumeration value="double" />
<enumeration value="float" />
<enumeration value="integer" />
<enumeration value="long"/>
<enumeration value="short"/>
<enumeration value="string"/>
<enumeration value="Boolean" />
<enumeration value="Byte" />
<enumeration value="Character" />
<enumeration value="Double" />
<enumeration value="Float" />
<enumeration value="Integer" />
<enumeration value="Long"/>
<enumeration value="Short"/>
<enumeration value="String"/>
</restriction>
</simpleType>
<simpleType name='non-empty-string'>
<restriction base='string'>
<minLength value='1'/>
</restriction>
</simpleType>
</schema>
```

XML Configuration key concepts and samples

The **request** element

The request element defines the request type that the server executes when
receiving the XML configuration. The valid request types are create, update, and
delete. When receiving a create request type, the server attempts to create the
requested system object. If that system object already exists, the request type fails
with a "system object already exists" error. The update request type performs a
hard update, meaning that if the system object already exists, the system object is
updated. Otherwise, the system object is created. In most cases, use the update
request type. The delete request type deletes the specified system object. The other
attribute on the Request element is cascade. Cascade applies only to the update of
agent configurations. It is ignored with all other elements. When cascade is equal
to true, all update to any agents specified cause an update to this agent's
configuration in all configuration groups.

The **agentconfigurations** element

The agentconfiguration element defines one or more agents that are updated,
created, or deleted based on the request type. A subelement of the
agentconfigurations element is the configuration element. This element defines the
actual agent system object with its property set that the operation is performed
against. When defining properties, you must have an understanding of how to
define special properties such as ID and name. These properties are usually
substituted at runtime with real values. Below, is a list of macro names that are
substitutable at runtime. You may use any of these names when defining
properties.

String substitution macros

Table 54. String substitution macros for XML configuration file

ControllerAgent string substitution name (Macros)	Value
%PREMISES_IP%	WebSphere Premises Server IP address
%CONTROLLER_ID%	Controller ID from table sage.controller.controller_id
%CONTROLLER_NAME%	Controller name from table sage.controller.username
%LOGGING_THRESHOLD%	Logging threshold from table sage.controller.alertagentthreshold
%LOCATION_ID%	Location ID from table sage.location.location_id
%LOCATION_NAME%	Location name from table sage.location.username
%SELFTEST_MODE%	Self test mode from table sage.location.Isinselftestmode
%READER_ID%	Reader ID from table sage.reader.reader_id
%READER_NAME%	Reader name from table sage.reader.username
%READER_COM_PORT%	Reader serial port number from table sage.reader.serialport
%READER_IP%	Reader IP address from table sage.reader.ipaddress
%READER_REMOTE_PORT%	Reader IP port number from table sage.reader.ipport
%READER_TRANSPORT_CLASS%	Reader communication protocol package name from table sage.reader.commprotocol
%PRINTER_ID%	Printer ID from table sage.printer.printer_id
%PRINTER_NAME%	Printer name from table sage.printer.username
%PRINTER_COM_PORT%	Printer serial port number from table sage.printer.serialport
%PRINTER_IP%	Printer IP address from table sage.printer.ipaddress
%PRINTER_REMOTE_PORT%	Printer IP port number from table sage.printer.ipport
%PRINTER_TRANSPORT_CLASS%	Printer communication protocol package name from table sage.printer.commprotocol
%READERS_STR%	All reader IDs belong to specific edge id. separate with ","
%LOCATIONS_STR%	All location IDs belong to specific edge id. separate with ","

Sample agentconfigurations element

```
<agentconfigurations>
 <configuration name="HealthCheckAgent"
 factoryPid="com.ibm.rfid.agent.healthcheck.bundle.HealthCheckAgentManagedServiceFactoryActivator"
 config-group-type="LocationType">
   <properties>
     <property key="portal.id" value="%LOCATION_ID%"/>
     <property key="portal.initial" value="ON"/>
     <property key="portal.name" value="%LOCATION_NAME%"/>
     <property key="reader.id" value="%READER_ID%"/>
     <property key="tracing" value="false"/>
     <property key="device.names" value="motionsensor,barrier,switch,reset"/>
   </properties>
 </configuration>
</agentconfigurations>
```

The **configurationgroup** element

The configurationgroup element defines a configuration group. When defining a configuration group, you can define the agents to associate with the configuration group. The list of agents specified for a configuration must be a complete list of agents with their complete property set definition, not just a subset of the agents or their properties. Creating agents associated with a configuration group also creates the default agent definition using the specified properties. This agent is then available when other configuration groups of that type are created. IBM recommends that you create configuration groups first because all system objects must be associated with some existing configuration group.

The **device** element

The device element defines a device system object. If the device is of the `reader` or `printer` category, the XML must contain the following device metadata or the device will not operate:

COMMPROTOCOL with a value of TCPIP or SERIAL

If COMMPROTOCOL is TCPIP
- IPADDRESS with a valid IP address
- IPPORT with a valid IP port number

If COMMPROTOCOL is SERIAL
- SERIALPORT with a valid serial port number

Sample device configuration

```
<serverconfigurations>
 <devices>
  <device config-group-name="Samsys" deviceid="81" deviceidprefix="R" devicename="Door 1">
    <device-category-metadata name="IPADDRESS" value="127.0.0.1" description="ipaddress"/>
    <device-category-metadata name="IPPORT" value="2101" description="ipport"/>
    <device-category-metadata name="COMMPROTOCOL" value="TCPIP" description="protocol"/>
  </device>
 </devices>
</serverconfigurations>
```

Sample complete agent configuration

```
<ibmrfidconfigadmin:configurationAdmin
dest=""
dts="2001-12-31T12:00:00"
orig="" version="" xmlns:ibmrfidconfigadmin="http://www.ibm.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.ibm.com IBMRFIDConfigAdmin.xsd">
<requests>
<request type="update" cascade="true">
<agentconfigurations>
<configuration factoryPid="com.motorola.symbol.bsp.adapter.factory.SymbolBspAdapterFactory"
name="Symbol BSP" config-group-type="DeviceType" bundlename="" bundleversion="1.1">
<properties>
<property key="id" value="%READER_ID%" description="The identiifer." type="String"
cardinality="0" required="true"/>
<property key="idimportfilter" value="" description="The identiifer import filter."
type="String" cardinality="0" required="false"/>
<property key="idname" value="%READER_NAME%" description="The name prefix." type="String"
cardinality="0" required="false"/>
<property key="prefix" value="%READER_ID%" description="The notification prefix."
type="String" cardinality="0" required="true"/>
</properties>
</configuration>
<configuration factoryPid="com.motorola.symbol.bsp.device.factory.SymbolBspDeviceFactory"
name="SAMSys CHUMP" config-group-type="DeviceType" bundlename="" bundleversion="1.1">
<properties>
<property key="id" value="%READER_ID%" description="The identiifer." type="String"
cardinality="0" required="true"/>
<property key="idimportfilter" value="" description="The identiifer import filter."
type="String" cardinality="0" required="false"/>
<property key="idname" value="%READER_NAME%" description="The name prefix." type="String"
cardinality="0" required="false"/>
<property key="prefix" value="%READER_ID%" description="The notification prefix."
type="String" cardinality="0" required="true"/>
<property key="ParameterBlockAntenna0SetOnlyRequest" value="" description="Request
setting the parameter block information for only annenna 0 (starting at 0) at physical
address a0 command" type="Byte" cardinality="4" required="false"/>
<property key="ParameterBlockAntenna1SetOnlyRequest" value=""
description="Request setting the parameter block information for only annenna 1
(starting at 0) at physical address b0 command" type="Byte" cardinality="4"
required="false"/>
<property key="ParameterBlockAntenna2SetOnlyRequest" value="" description="Request
setting the parameter block information for only annenna 2 (starting at 0) at physical
address b0 command" type="Byte" cardinality="4" required="false"/>
<property key="ParameterBlockAntenna3SetOnlyRequest" value="" description="Request
```

```
setting the parameter block information for only annenna 3 (starting at 0) at physical
address b0 command" type="Byte" cardinality="4" required="false"/>
</properties>
</configuration>
<configuration factoryPid="com.motorola.symbol.bsp.gpio.profile.factory.SymbolBspGpioProfileFactory"
name="Symbol BSP" config-group-type="DeviceType" bundlename="" bundleversion="1.1">
<properties>
<property key="id" value="%READER_ID%" description="The identifier." type="String"
cardinality="0" required="true"/>
<property key="idimportfilter" value="" description="The identiifer import filter."
type="String" cardinality="0" required="false"/>
<property key="idname" value="%READER_NAME%" description="The name prefix." type="String"
cardinality="0" required="false"/>
<property key="prefix" value="%READER_ID%" description="The notification prefix."
type="String" cardinality="0" required="true"/>
<property key="Gpio/Output1Expression" value="" description="LDAP expression to
trigger the state of output pin 1 based on input pin and control values."
type="String" cardinality="0" required="false"/>
<property key="Gpio/Output2Expression" value="" description="LDAP expression to trigger
the state of output pin 2 based on input pin and control values." type="String"
cardinality="0" required="false"/>
<property key="Gpio/Output3Expression" value="" description="LDAP expression to trigger
the state of output pin 3 based on input pin and control values." type="String"
cardinality="0" required="false"/>
<property key="Gpio/Output4Expression" value="" description="LDAP expression to trigger the state of
output pin 4 based on input pin and control values." type="String" cardinality="0" required="false"/>
<property key="Gpio/Output5Expression" value="" description="LDAP expression to trigger the state of
output pin 5 based on input pin and control values." type="String" cardinality="0" required="false"/>
<property key="Gpio/Output6Expression" value="" description="LDAP expression to trigger the state of
output pin 6 based on input pin and control values." type="String" cardinality="0" required="false"/>
<property key="Gpio/Output7Expression" value="" description="LDAP expression to trigger the state of
output pin 7 based on input pin and control values." type="String" cardinality="0" required="false"/>
<property key="Gpio/Output8Expression" value="" description="LDAP expression to trigger the state of
output pin 8 based on input pin and control values." type="String" cardinality="0" required="false"/>
<property key="Gpio/Output9Expression" value="" description="LDAP expression to trigger the state of
output pin 9 based on input pin and control values." type="String" cardinality="0" required="false"/>
<property key="Gpio/Output10Expression" value="" description="LDAP expression to trigger the state of
output pin 10 based on input pin and control values." type="String" cardinality="0" required="false"/>
<property key="Gpio/Output11Expression" value="" description="LDAP expression to trigger the state of
output pin 11 based on input pin and control values." type="String" cardinality="0" required="false"/>
<property key="Gpio/Output12Expression" value="" description="LDAP expression to trigger the state of
output pin 12 based on input pin and control values." type="String" cardinality="0" required="false"/>
<property key="Gpio/Output13Expression" value="" description="LDAP expression to trigger the state of
output pin 13 based on input pin and control values." type="String" cardinality="0" required="false"/>
<property key="Gpio/Output14Expression" value="" description="LDAP expression to trigger the state of
output pin 14 based on input pin and control values." type="String" cardinality="0" required="false"/>
<property key="Gpio/Output15Expression" value="" description="LDAP expression to trigger the state of
output pin 15 based on input pin and control values." type="String" cardinality="0" required="false"/>
<property key="Gpio/Output16Expression" value="" description="LDAP expression to trigger the state of
output pin 16 based on input pin and control values." type="String" cardinality="0" required="false"/>
<property key="Gpio/Output17Expression" value="" description="LDAP expression to trigger the state of
output pin 17 based on input pin and control values." type="String" cardinality="0" required="false"/>
<property key="Gpio/Output18Expression" value="" description="LDAP expression to trigger the state of
output pin 18 based on input pin and control values." type="String" cardinality="0" required="false"/>
<property key="Gpio/Output19Expression" value="" description="LDAP expression to trigger the state of
output pin 19 based on input pin and control values." type="String" cardinality="0" required="false"/>
<property key="Gpio/Output20Expression" value="" description="LDAP expression to trigger the state of
output pin 20 based on input pin and control values." type="String" cardinality="0" required="false"/>
<property key="Gpio/Output21Expression" value="" description="LDAP expression to trigger the state of
output pin 21 based on input pin and control values." type="String" cardinality="0" required="false"/>
<property key="Gpio/Output22Expression" value="" description="LDAP expression to trigger the state of
output pin 22 based on input pin and control values." type="String" cardinality="0" required="false"/>
<property key="Gpio/Output23Expression" value="" description="LDAP expression to trigger the state of
output pin 23 based on input pin and control values." type="String" cardinality="0" required="false"/>
<property key="Gpio/Output24Expression" value="" description="LDAP expression to trigger the state of
output pin 24 based on input pin and control values." type="String" cardinality="0" required="false"/>
<property key="Gpio/Output25Expression" value="" description="LDAP expression to trigger the state of
output pin 25 based on input pin and control values." type="String" cardinality="0" required="false"/>
<property key="Gpio/Output26Expression" value="" description="LDAP expression to trigger the state of
output pin 26 based on input pin and control values." type="String" cardinality="0" required="false"/>
<property key="Gpio/Output27Expression" value="" description="LDAP expression to trigger the state of
output pin 27 based on input pin and control values." type="String" cardinality="0" required="false"/>
<property key="Gpio/Output28Expression" value="" description="LDAP expression to trigger the state of
output pin 28 based on input pin and control values." type="String" cardinality="0" required="false"/>
<property key="Gpio/Output29Expression" value="" description="LDAP expression to trigger the state of
output pin 29 based on input pin and control values." type="String" cardinality="0" required="false"/>
<property key="Gpio/Output30Expression" value="" description="LDAP expression to trigger the state of
output pin 30 based on input pin and control values." type="String" cardinality="0" required="false"/>
<property key="Gpio/Output31Expression" value="" description="LDAP expression to trigger the state of
output pin 31 based on input pin and control values." type="String" cardinality="0" required="false"/>
<property key="Gpio/Output32Expression" value="" description="LDAP expression to trigger the state of
output pin 32 based on input pin and control values." type="String" cardinality="0" required="false"/>
<property key="notificationrate" value="300" description="Notificationrate" type="Integer" cardinality="0"
required="false"/>
<property key="ControlProfilePrefix" value="%READER_ID%" description="Control profile prefix"
type="String" cardinality="0" required="false"/>
</properties>
</configuration>
<configuration
factoryPid="com.motorola.symbol.bsp.inventory.profile.factory.SymbolBspInventoryProfileFactory"
name="Symbol BSP" config-group-type="DeviceType" bundlename="" bundleversion="1.1">
<properties>
<property key="id" value="%READER_ID%" description="The identiifer." type="String" cardinality="0"
required="true"/>
<property key="idimportfilter" value="" description="The identiifer import filter." type="String"
cardinality="0" required="false"/>
<property key="idname" value="%READER_NAME%" description="The name prefix." type="String" cardinality="0"
required="false"/>
<property key="prefix" value="%READER_ID%" description="The notification prefix." type="String"
cardinality="0" required="true"/>
<property key="RfidInventory/TagReadingExpression" value="(b1=true)" description="" type="String"
cardinality="0" required="true"/>
<property key="RfidInventory/TagAggregatingExpression" value="" description="" type="String" cardinality="0"
required="true"/>
<property key="RfidInventory/TagMaskSetting" value="" description="" type="String" cardinality="0"
required="true"/>
<property key="RfidInventory/DuplicateFilteringExpression" value="(b1=true)" description="" type="String"
cardinality="0" required="true"/>
<property key="RfidInventory/AggregationMaskSetting" value="" description="" type="String" cardinality="0"
required="true"/>
<property key="pollingrate" value="100" description="Pollingrate" type="Integer" cardinality="0"
required="false"/>
<property key="GpioProfilePrefix" value="" description="Gpio profile prefix" type="String" cardinality="0"
required="false"/>
<property key="ControlProfilePrefix" value="%READER_ID%" description="Control profile prefix" type="String"
cardinality="0" required="false"/>
</properties>
</configuration>
<configuration factoryPid="com.motorola.symbol.bsp.transport.factory.SymbolBspTransportFactory"
name="Symbol BSP" config-group-type="DeviceType" bundlename="" bundleversion="1.1">
<properties>
<property key="id" value="%READER_ID%" description="The identiifer." type="String" cardinality="0"
required="true"/>
<property key="idimportfilter" value="" description="The identiifer import filter." type="String"
cardinality="0" required="false"/>
<property key="idname" value="%READER_NAME%" description="The name prefix." type="String" cardinality="0"
required="false"/>
<property key="prefix" value="%READER_ID%" description="The notification prefix." type="String"
```

```
cardinality="0" required="true"/>
<property key="host" value="symbolbsp" description="The host." type="String" cardinality="0"
required="false"/>
<property key="remoteport" value="3000" description="The remote port" type="Integer" cardinality="0"
required="false"/>
<property key="localport" value="-1" description="The local port." type="Integer" cardinality="0"
required="false"/>
<property key="linger" value="-1" description="The SL Linger time." type="Integer" cardinality="0"
required="false"/>
<property key="responsetimeout" value="4000" description="The response timeout." type="Long" cardinality="0"
required="false"/>
<property key="noactivitytimeout" value="10000" description="The no activity timeout." type="Long"
cardinality="0" required="false"/>
<property key="retrytime" value="1000" description="The retry time." type="Long" cardinality="0"
required="false"/>
<property key="connection" value="factory" description="" type="String" cardinality="0" required="true"/>
</properties>
</configuration>
</agentconfigurations>
<serverconfigurations>
<devices>
<device config-group-name="TestSamSys" deviceid="81" deviceidprefix="R" devicename="Door 1">
<device-category-metadata name="IPADDRESS" value="127.0.0.1" description="ipaddress"/>
<device-category-metadata name="IPPORT" value="2101" description="ipport"/>
<device-category-metadata name="COMMPROTOCOL" value="TCPIP" description="protocol"/>
</device>
<device config-group-name="TestSamSys" deviceid="82" deviceidprefix="R" devicename="Door 2">
<device-category-metadata name="IPADDRESS" value="127.0.0.2" description="ipaddress"/>
<device-category-metadata name="IPPORT" value="2102" description="ipport"/>
<device-category-metadata name="COMMPROTOCOL" value="TCPIP" description="protocol"/>
</device>
<device config-group-name="TestSamSys" deviceid="83" deviceidprefix="R" devicename="Door 3">
<device-category-metadata name="IPADDRESS" value="127.0.0.3" description="ipaddress"/>
<device-category-metadata name="IPPORT" value="2103" description="ipport"/>
<device-category-metadata name="COMMPROTOCOL" value="TCPIP" description="protocol"/>
</device>
<device config-group-name="TestSamSys" deviceid="91" deviceidprefix="R" devicename="Door 11">
<device-category-metadata name="IPADDRESS" value="127.0.0.1" description="ipaddress"/>
<device-category-metadata name="IPPORT" value="2201" description="ipport"/>
<device-category-metadata name="COMMPROTOCOL" value="TCPIP" description="protocol"/>
</device>
<device config-group-name="TestSamSys" deviceid="92" deviceidprefix="R" devicename="Door 12">
<device-category-metadata name="IPADDRESS" value="127.0.0.2" description="ipaddress"/>
<device-category-metadata name="IPPORT" value="2202" description="ipport"/>
<device-category-metadata name="COMMPROTOCOL" value="TCPIP" description="protocol"/>
</device>
<device config-group-name="TestSamSys" deviceid="93" deviceidprefix="R" devicename="Door 13">
<device-category-metadata name="IPADDRESS" value="127.0.0.3" description="ipaddress"/>
<device-category-metadata name="IPPORT" value="2203" description="ipport"/>
<device-category-metadata name="COMMPROTOCOL" value="TCPIP" description="protocol"/>
</device>
</devices>
<locations>
<location aliasname="Warehouse1-West - L80alias" config-group-name="Basic Dock Door Receiving"
iscontainerlocation="true" description="" isaddressable="false"
isselftestmode="false" locationid="80" locationidprefix="L"
name="Warehouse1-West - L80"
parentlocationref="Root"/>
<location aliasname="Warehouse1-East - L90alias"
config-group-name="Basic Dock Door Receiving"
iscontainerlocation="true" description="" isaddressable="false"
isselftestmode="false" locationid="90" locationidprefix="L"
name="Warehouse1-East - L90" parentlocationref="Root"/>
<location aliasname="L81-alias" config-group-name="Basic Dock Door Receiving"
iscontainerlocation="false" description="Door 1" deviceidref="R81"
isaddressable="false" isselftestmode="false" locationid="81"
locationidprefix="L" name="L81name"
parentlocationref="L80"/>
<location aliasname="L82-alias" config-group-name="Basic Dock Door Receiving"
iscontainerlocation="false" description="Door 2" deviceidref="R82"
isaddressable="false" isselftestmode="false" locationid="82"
locationidprefix="L" name="L82name" parentlocationref="L80"/>
<location aliasname="L83-alias" config-group-name="Basic Dock Door Receiving"
iscontainerlocation="false" description="Door 3" deviceidref="R83"
isaddressable="false" isselftestmode="false" locationid="83"
locationidprefix="L" name="L83name" parentlocationref="L80"/>
<location aliasname="L91-alias" config-group-name="Basic Dock Door Receiving"
iscontainerlocation="false" description="Door 11" deviceidref="R91"
isaddressable="false" isselftestmode="false" locationid="91"
locationidprefix="L" name="L91name" parentlocationref="L90"/>
<location aliasname="L92-alias" config-group-name="Basic Dock Door Receiving"
iscontainerlocation="false" description="Door 12" deviceidref="R92"
isaddressable="false" isselftestmode="false" locationid="92"
locationidprefix="L" name="L92name" parentlocationref="L90"/>
<location aliasname="L93-alias" config-group-name="Basic Dock Door Receiving"
iscontainerlocation="false" description="Door 13" deviceidref="R93"
isaddressable="false" isselftestmode="false" locationid="93"
locationidprefix="L" name="L93name" parentlocationref="L90"/>
</locations>
<controllers>
<controller alertlevel="error" config-group-name="Distribution Center"
controllerid="80" controlleridprefix="C" controllername="Warehouse1-West - C80"
macaddress="kjajafkdfd">
<controller-category-metadata description="Warehouse1 West"
name="westtestingmetafsys" value="westtestingmetavalue"/>
<controller-locations>
<locationid>L81</locationid>
<locationid>L82</locationid>
<locationid>L83</locationid>
</controller-locations>
</controller>
<controller alertlevel="error" config-group-name="Distribution Center"
controllerid="90" controlleridprefix="C" controllername="Warehouse1-East - C90"
macaddress="kjajafkdfd">
<controller-category-metadata description="Warehouse1 East"
name="easttestingmetadata" value="easttestingmetavalue"/>
<controller-locations>
<locationid>L91</locationid>
<locationid>L92</locationid>
<locationid>L93</locationid>
</controller-locations>
</controller>
</controllers>
</serverconfigurations>
</request>
</requests>
</ibmrfidconfigadmin:configurationAdmin>
```

Importing the XML configuration file using the console

This topic describes how to use the WebSphere Premises Server Administrative
Console to import the Data Capture and Delivery XML configuration file that
configures the server.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Click **Data Capture Configuration** → **Import Configurations** from the left navigation pane.
3. In the **XML File** field, enter the location and name of the XML configuration file or click **Browse** to search for and select it.
4. Click **Import**. If the XML imports successfully, a confirmation message displays.

Importing the XML configuration file using a command line

This topic describes how to use a command line utility to import the Data Capture and Delivery XML configuration file that configures the server.

1. Open a command prompt.
2. Run the following command:

   If the command is not run from the directory where the JAR file is located, enter the fully qualified path of the file when running the command: *Premises_Root*\premises\tools\xmlimport.

   ```
   java -jar XMLimport.jar premises_hostname XML_file_path filename.log
   ```

   where *premises_hostname* is the hostname for the target WebSphere Premises Server, *XML_file_path* is the fully qualified path of the XML configuration file, and *filename.log* is the name of the file used to log messages.

   The *filename.log* parameter is optional. If used, new messages will be added to the file. If the file does not exist, it will be created in the current directory. If the log file is not specified, messages will be written to the console.

Working with update sites

This section describes how to use the information provided in vendor-specific update sites to configure new agents and update existing agents. Device vendors can package their WebSphere Premises Server agent configuration information as an Eclipse update site. All update sites adhere to the OSGi Service Platform Service Compendium, which describes how to package the agent configuration.

Adding update sites

Use the WebSphere Premises Server Administrative Console to add new Data Capture and Delivery update sites to your network topology.

About this task

Before accessing device-specific download sites, you must define the updates sites.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Navigate to **Data Capture Configuration** → **Update Sites** from the left navigation pane. The Update Sites panel displays.
3. Click **New**. The Create Update Site panel displays.
4. Enter a name for the update site and then enter the URL to the vendor-specific download site.
5. Click **Create**. A new update site is created.

Modifying update sites

This topic describes how to modify information about an update site in your network topology using the WebSphere Premises Server Administrative Console.

About this task

Use the following steps to change information about an update site.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Click **Data Capture Configuration** ▸ **Update Sites** from the left navigation pane. The Update Sites panel displays.
3. Click on the update site for which you are modifying information. The Edit Update Site Details panel displays.
4. Make all necessary changes and click **Update**. The Update Site panel displays.

Deleting update sites

This topic describes how to delete an update site from your network topology using the WebSphere Premises Server Administrative Console.

About this task

Use the following steps to delete an update site from your network topology.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Click **Data Capture Configuration** ▸ **Update Sites** from the left navigation pane. The Update Sites panel displays.
3. Select the update site that you want to delete.
4. Click **Delete Selected**. A message displays asking you to confirm the deletion.
5. Click **OK** to delete the update site.

Downloading bundles

This topic describes how to download bundles from an update site using the WebSphere Premises Server Administrative Console.

Before you begin

Before downloading bundles from an update site, make sure that WebSphere Application Server is running.

About this task

The **Find and Install** function enables you to download Data Capture and Delivery bundles that are then loaded into the Bundle Repository Server. Multiple versions of bundles can be stored in the Bundle Repository Server.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Navigate to **Data Capture Configuration** ▸ **Find and Install** from the left navigation pane. The Find and Install panel displays.
3. Select the radio button for **Download Data Capture bundles** and click **Next**.
4. Select the update site to use for the bundles. Click **Next**.
5. Select a feature for the bundles. The list of features is retrieved from the update site. Click **Next**.
6. Accept the license agreement and click **Next**.
7. Confirm your selections and then click **Finish** to begin the download process.

What to do next

Once you have downloaded new bundles into the Bundle Repository Server, you need to create customized bundle list files in order to load the bundles to the Data Capture and Delivery controller. See "Installing the bundle loader and a bundle list" on page 72 for more information.

Managing event processing

You can manage the event flow in your network topology by using the WebSphere Premises Server Administrative Console to work with event templates and output channels.

The WebSphere Premises Server event model

WebSphere Premises Server uses an event format called the IBM Sensor Event. When the Data Capture and Delivery controller captures an event from a device, the event is converted to the IBM Sensor Event format. That format is then converted to sensor event XML and sent to the WebSphere Premises Server sensor event gateway. The WebSphere Premises Server sensor event gateway pushes the event to the WebSphere Application Server service integration bus (SIBus), ibmsensorevent, where WebSphere Premises Server task agents are listening for events.

WebSphere Premises Server task agents are message-driven beans (MDBs). They process events by registering with WebSphere Application Server for the desired topics. When a topic arrives, the MDB receives the event and processes it. A Persistence Manager listens on the SIBus for all messages destined for WebSphere Premises Server or the Data Capture and Delivery controller. When the Persistence Manager captures an event, it either persists the event to a local database or it can persist the event to the Electronic Product Code Information System (EPCIS) using the EPCIS Connector.

A Complex Event Processing (CEP) engine also listens on the SIBus for certain events. When it receives an event, the CEP engine responds either by generating a new event, which is pushed to the SIBus, or by calling actions that start processes on WebSphere Process Server.
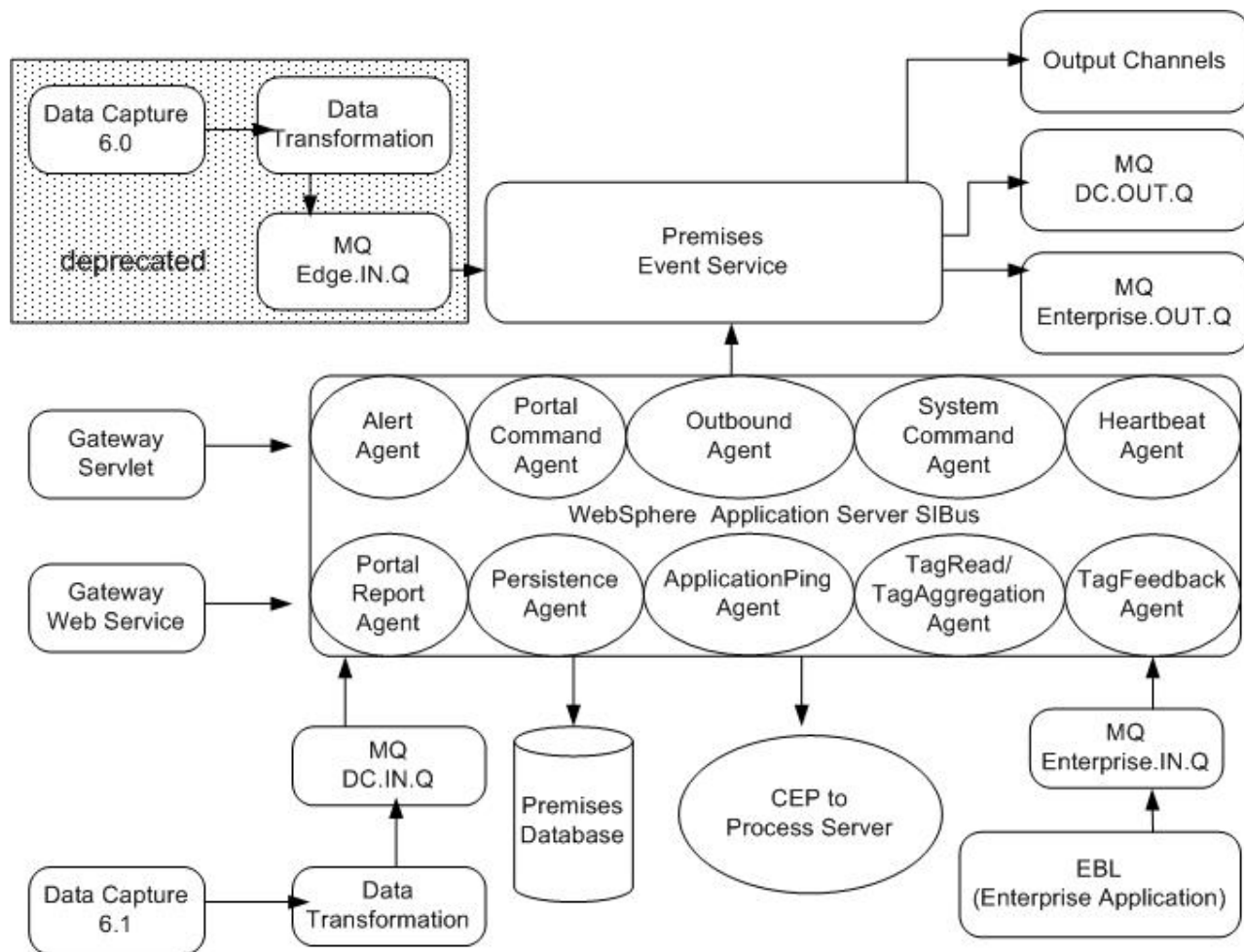
Figure 1. The event flow

You can use the WebSphere Premises Server Toolkit to develop your own use case. For more information refer to the WebSphere Premises Server Toolkit documentation.

Working with event templates

This topic contains information on managing event templates using the WebSphere Premises Server Administrative Console.

An *event* is a type of action that takes place in the WebSphere Premises Server network, such as a new tag read. An *event template* contains information specific to a particular event. You define event templates in the network topology so that the event information transmits across the appropriate communication channels. The information then coordinates with the Data Capture and Delivery controller, WebSphere Premises Server, and enterprise system.

To see what event templates are already defined for your topology, go to **Event Processing Configuration** → **Event Templates** in the WebSphere Premises Server Administrative Console.

Refer to these topics for instructions on how to create, modify, or delete event templates:

Adding event templates

Use the WebSphere Premises Server Administrative Console to add new event templates to your network topology definition.

About this task

When you create an event template, you can direct it to send events to an output channel to be forwarded to another destination, such as a Java Message Service queue. Event templates should map to WebSphere Premises Server topics that are used on the SIBus.

The format of the event template is: `target_ID/event_type`

The *target_ID* is the ID of the target system. If the target is not a Data Capture and Delivery environment, then this value should be `*`. If the target is a Data Capture and Delivery environment, then this value can be a location ID or a controller ID.

The *event_type* is comprised of elements in this format: `profile_id/type_of_event/event_name`

The *type_of_event* is usually a command or a report, and the *event_name* is usually a command or report name. Any element of the *event_type* can be set to the variable value, `*`. Setting this variable means that any value in the same position creates a match. For example, an *event_type* of `*/*/*/*` causes every event to be sent to the associated output channels.

See "Adding output channels to event templates" on page 182 for more information on adding output channels to existing event templates.

Note: Event templates for `tag_read` are deprecated.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Navigate to **Event Processing Configuration** → **Event Templates** in the left navigation pane. The Event Templates panel displays a list of currently defined event templates.
3. Scroll to the bottom of the page and click **New**. The Create Event Template panel displays.
4. In the **Event Template Name** field, enter a unique identifier for this event.
5. Enter a brief description of the event.
6. If desired, select the channels that you want to associate with the event from the **Available Channels** column and click the **->** (right arrow). The channels display in the **Selected Channels** column.
7. When you are done, click **Create Event Template**. The event template is saved.

Modifying event templates

Use the WebSphere Premises Server Administrative Console to modify existing event templates in your network topology definition.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Navigate to **Event Processing Configuration** → **Event Templates** in the left navigation pane. The Event Templates panel displays a list of currently defined event templates.

3. In the Actions column, click the **View Template Properties** link for the event template that you want to modify. The Event Template Detail panel displays.

4. Make the necessary changes and click **Update Event Template**. The changes are saved.

Deleting event templates

Use the WebSphere Premises Server Administrative Console to delete existing event templates from your network topology definition.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.

2. Navigate to **Event Processing Configuration** → **Event Templates** in the left navigation pane. The Event Templates panel displays a list of currently defined event templates.

3. In the Actions column, click the **View Template Properties** link for the event template that you want to modify. The Event Template Detail panel displays.

4. Click **Delete Event Template**. A confirmation message displays.

5. Click **OK** to delete the event template.

Event Template details

The following table defines the fields in the **Create Event Template** and **Event Template Detail** panels.

Fields

Field	Description
Event Template Name*	Enter a unique identifier for the event template you are defining. After you create the event template, you cannot modify this field.
Description	Enter a description of this event template.
Available Channels	The list of available channels to associate with the event you are defining. Select a channel and click the **->** (right arrow) to associate the channel with this event.
Selected Channels	The list of channels that are currently associated with the event. Click the **<-** (left arrow) to disassociate this channel with the event.

* Required field.

Working with output channels

This section describes managing output paths, or channels, for messages sent from the WebSphere Premises Server to the Data Capture and Delivery controller or enterprise using the WebSphere Premises Server Administrative Console.

This section contains the following topics:

Creating output channels

Use the WebSphere Premises Server Administrative Console to define the output channels for the WebSphere Premises Server.

About this task

These channels are output paths for messages sent from WebSphere Premises Server to either the Data Capture and Delivery controller or the enterprise. Use the Output Channels function to define these paths.

There are several types of output channels:
- **Email**, for email-based messages
- **HTTP**, for HTTP-based messages
- **JMS**, for Java Message Service messages
- **JMS Topic**, for Java Message Service topic messages
- **MQ**, for WebSphere MQ messages

Edge.out.channel enables tag data to be communicated between the WebSphere Premises Server and Data Capture and Delivery controllers, and is created by default. Follow these steps to create additional output channels:

1. If you are creating an output channel for e-mail, you must first create an e-mail session using the WebSphere Premises Server Administrative Console. Refer to the WebSphere Application Server Information Center topic on Configuring mail providers and sessions for more information. For other types of output channels, proceed to the next step.
2. Open the WebSphere Premises Server Administration Console. The Welcome page displays.
3. Navigate to **Event Processing Configuration** → **Output Channels** in the left navigation pane. The Output Channels panel displays.
4. Under **Create Output Channel**, select the type of output channel to create and click **New**. The Create New Channel panel displays.
5. In the **Channel ID** field, type a logical identifier for the new output channel.
6. Complete the remaining optional fields, and click **Create**. The new output channel displays in the Output Channels panel.
7. After you create an output channel, you can use it by adding it to an event template.

Adding output channels to event templates

Use the WebSphere Premises Server Administrative Console to add defined output channels to event templates.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Navigate to **Event Processing Configuration** → **Event Templates** in the left navigation pane. The Event Templates panel displays a list of currently defined event templates.
3. In the Actions column, click the **View Template Properties** link for the event template that you want to modify. The Event Template Detail panel displays.
4. Move the desired channels from the **Available Channels** column to the **Selected Channels** column using the arrow button.
5. When you have finished adding the channels and click **Update Event Template**. The changes are saved.

What to do next

If a desired output channel does not appear in the **Available Channels** column, it must be created. Refer to the instructions for "Creating output channels" on page 181.

Modifying output channels

Use the WebSphere Premises Server Administrative Console to modify the output channels for the WebSphere Premises Server.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Navigate to **Event Processing Configuration** → **Output Channels** in the left navigation pane. The Output Channels panel displays.
3. Click the output channel that you want to modify. The Modify Output Channel details panel displays.
4. Make the necessary changes and click **Update**. The changes are saved.

Deleting output channels

Use the WebSphere Premises Server Administrative Console to delete output channels for the WebSphere Premises Server.

About this task

Note: Do not delete *edge.out.channel* because that is the channel used to communicate with the Data Capture and Delivery runtime.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Navigate to **Event Processing Configuration** → **Output Channels** in the left navigation pane. The Output Channels panel displays.
3. Click the output channel that you want to delete. The Modify Output Channel details panel displays.
4. Click **Delete**. The output channel is deleted.

Results

Note: If you delete an output channel, all associations with event templates for that output channel are also deleted. If you recreate the output channel, you must add it to the event templates.

Output Channel details

The following table defines the fields in the Create New Channel panel.

Fields

Field	Description
Channel ID	Enter a unique identifier for this output channel. After you create the output channel, you cannot modify this field.
Description	Enter a description of the output channel.
XSL Transform	Enter an XSL style sheet transform, if desired. Applying an XSL transform to an output channel ensures that the outgoing message is received in the right format by the target application.
JNDI Session[E]	Enter a Java Naming and Directory session for the e-mail output channel, if desired.
Recipient[E]	Enter the e-mail recipient's name.
From Address[E]	Enter your e-mail address.
Subject[E]	Enter a subject for the e-mail.
Connection Factory[J]	Enter a Java Message Service connection factory, which are objects used to create connections to JMS destinations.
Topic Factory[JT]	Enter a Java Message Service topic connection factory, which are objects used to manage connections between JMS topics.

Field	Description
Topic[JT]	Enter a Java Message Service topic, which are objects used to manage message flow from publishers to subscribers.
URL[H]	Enter a destination URL for the message.
Queue[JM]	Enter a WebSphere MQ queue, which defines a point-to-point destination type.
Queue Manager[M]	Enter a WebSphere MQ queue manager, which controls access to queues and serves as a transaction coordinator for all queue operations.
Channel[M]	Enter a WebSphere MQ channel, which provides a communication path between queue managers.
Hostname[M]	Enter the host name of the MQ Manager server.
Port[M]	Enter the port of the MQ Manager server.
Uid[M]	Enter the user ID of the MQ Manager server.
Pwd[M]	Enter the password of the MQ Manager server.

[E] Email Output Channel only

[J] JMS Output Channel only

[JT] JMS Topic Output Channel only

[H] HTTP Output Channel only

[JM] JMS and MQSeries® Output Channels only

[M] MQ Output Channels only

Setting the XML converter property

The IBM Sensor Event format is converted to XML before it is sent to the WebSphere Premises Server sensor event gateway. You can configure the class of XML converter to use by modifying the value of the `com.ibm.sensorevent.converter` property in the SystemAgent.

Before you begin

See "Modifying agent properties for a PID" on page 106 for detailed steps on modifying an agent using the WebSphere Premises Server Administrative Console.

1. In the WebSphere Premises Server Administrative Console, navigate to **Agent Configuration** → **SystemAgent** → **com.ibm.premises.SystemAgent** .
2. Modify the **Value** field of the `com.ibm.sensorevent.converter` property.

   The default value is `com.ibm.sensorevent.model.converter.XMLConverter`.
3. Save your agent configuration changes.
4. Restart WebSphere Application Server.

Managing the EPC configuration

Use the EPC Configuration function in the WebSphere Premises Server Administrative Console to manage the process of converting product codes to Electronic Product Codes (EPCs) and manage the EPCglobal Company Prefix Index.

This process consists of four main parts:

- Pack type configuration - see "Working with pack types."
- Profile configuration - see "Working with profiles" on page 191.
- Serial number configuration - see "Working with serial numbers" on page 193.
- EPCglobal company prefix index - see "Working with the EPCglobal company prefix index" on page 196.

Working with pack types

This section contains information on managing pack types using the Profile Configuration feature in the WebSphere Premises Server Administrative Console.

About this task

A pack type is a type of container, such as a case or pallet. Each pack type is associated with various pieces of information that are required for converting customer-specific product codes to EPC format. This information includes an input type, which is the UCC.EAN format of the customer product code, and an encoding type, which defines an EPC algorithm to convert the input codes into EPC format. The pallet and case concept is a two-tiered approach to defining a containment hierarchy of items: pallets contain cases. You can, however, define terms beyond pallet and case to define your own containment hierarchy.

In a containment hierarchy, any pack type can contain zero or more pack types. For example, pack type A can contain both pack types B and C; and D does not contain any pack types. B and C are children of pack type A (the parent). The following example is a containment hierarchy cycle that is not valid: A contains B contains C contains A. The Print, Verify, and Ship Reference User Interface does not allow this type of containment configuration. Use the Verify panel in the Print, Verify, and Ship Reference User Interface to specify that any pack type with children in its containment hierarchy is a container of associated labels.

The following table shows the available input types and their corresponding encoding types:

Table 55. Input Types and Matching Encoding Types

Input Type	Encoding Type
DOD	• usdod-64 • usdod-96
GIAI	• giai-64 • giai-96
GID	• gid-96

Table 55. Input Types and Matching Encoding Types (continued)

Input Type	Encoding Type
GLN **Note:** This input type is supported only for printing. This type is not supported by the WebSphere Premises Server EPC Commissioning Member APIs.	• sgln-96 • sgln-64
GRAI	• grai-96 • grai-64
GTIN14	• sgtin-64 • sgtin-96
SSCC18	• sscc-96 • sscc-64

The Print, Verify, and Ship Reference User Interface includes twelve default pack types. The default GTIN14 pack types are:
- CASE64 - 64-bit pack type for cases
- CASE96 - 96-bit pack type for cases
- PALLET64 - 64-bit pack type for containers
- PALLET96 - 96-bit pack type for containers

The default SSCC18 pack types are:
- PALLET64-SSCC64 - 64-bit non-item pack type
- PALLET96-SSCC96 - 96-bit non-item pack type

The default DOD pack types are:
- DODPallet64 - 64-bit pack type for DOD containers
- DODCase64 - 64-bit pack type for DOD cases
- DODUIDItem64 - 64-bit pack type for DOD single-item shipments
- DODPallet96 - 96-bit pack type for DOD containers
- DODCase96 - 96-bit pack type for DOD cases
- DODUIDItem96 - 96-bit pack type for DOD single-item shipments

You can modify the default pack type or create any number of new ones for a particular customer. You associate pack types with profiles; therefore, for each created profile, you can create new pack types with which to print RFID tag labels. See "Configuring profiles" on page 192 for more information.

Adding pack types

Use the Profile Configuration feature in the WebSphere Premises Server Administrative Console to create new pack types for profiles. You use these pack types in the Print, Verify, and Ship Reference User Interface.
1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.

2. Click **EPC Configuration Profile Configuration** from the left panel. The EPC Profiles panel displays.

3. Click the profile for which you are creating a new pack type. The Edit EPC Profile Details Panel displays.

4. In the **Available Packaging Types** box, select **Add new packtype**. The Pack Type Configuration panel displays.

5. Enter the pack type in the **Packaging Type** field.

6. Type a brief description of this pack type in the **Description** field.

7. In the **Input Type** field, select the input format of the product codes you are including in this pack type.

8. In the **Company Prefix Length** field, select the number of digits in the company prefix for this pack type.

9. In the **Encoding Type** field, select the algorithm to use when converting from the specified input type to the EPC-compliant output type.

10. Select a filter value from the **Filter Value** field. Filter values are two- to four-digit codes that identify the pack type. In the EPCglobal standard, filter rules are used for filtering and pre-selecting basic logistic types such as inner packs, cases, and pallets.

11. Type a one-digit code from 0-9 in the **Indicator/Extension Digit** field, if necessary. The indicator digit is specific to the manufacturer and identifies packing levels for SGTIN encoding types. The extension digit is used by SSCC encoding types to extend the range of serial numbers.

12. If appropriate, select one or more pack types from the **Contained Pack Type** field. Use the <CTRL> key to select more than one pack type. A contained pack type refers to a pack type that is a subset of a larger pack type. For example, if you are creating pack type Pallet64-011, you might have a contained pack type of CASE64-001 because a case can be part of a larger pallet.

    Note: Any pack type can have zero or more contained pack types.

13. Select a print template from the **Default Print Template** field. You must have already created at least one print template on the Print Templates panel in the WebSphere Premises Server Administrative Console. For more information on creating print templates, see Creating print templates.

    Note: The template you select automatically displays in the **Label** field on the Print panel of the Print, Verify, and Ship Reference User Interface when you select this pack type.

14. Click **Create**. The pack type is saved and available for selection in the Print module of the Print, Verify, and Ship Reference User Interface.

15. Go to the next section, "Configuring profiles" on page 192, to create a customer profile containing these pack types.

Modifying pack types

Use the WebSphere Premises Server Administrative Console to modify your existing pack types.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.

2. Click **EPC Configuration → Profile Configuration** from the left navigation pane. The EPC Profiles panel displays.

3. From the **Profile Name** field, select the profile for which you are modifying the pack type. The EPC Profiles Details panel displays.

4. From the **Available Packaging Type** field, select the pack type that you want to modify. The Pack Type Configuration panel displays.

5. Make the necessary changes and click **Update**.

Deleting pack types

Use the WebSphere Premises Server Administrative Console to delete pack types from your network topology.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.

2. Click **EPC Configuration** → **Profile Configuration** from the left navigation pane.

3. From the **Profile Name** field, select the profile from which you are deleting the pack type. The EPC Profiles Details panel displays.

4. From the **Available Packaging Type** field, select the pack type that you want to delete. The Edit EPC Profile Details panel displays.

5. Make sure that this is the pack type that you want to delete, and click **Delete**. A confirmation message displays.

6. Click **OK** to delete the pack type.

Configuring pack types

Use the Profile Configuration feature in the WebSphere Premises Server Administrative Console to create pack types for a profile. These pack types can then be used in the Print, Verify, and Ship Reference User Interface.

About this task

A pack type is a type of container, such as a case or pallet. Each pack type is associated with various pieces of information that are required for converting customer-specific product codes to EPC format. This information includes an input type, which is the UCC.EAN format of the customer product code, and an encoding type, which defines an EPC algorithm to convert the input codes into EPC format. The pallet and case concept is a two-tiered approach to defining a containment hierarchy of items: pallets contain cases. You can, however, define terms beyond pallet and case to define your own containment hierarchy.

In a containment hierarchy, any pack type can contain zero or more pack types. For example, pack type A can contain both pack types B and C; and D does not contain any pack types. B and C are children of pack type A (the parent). The following example is a containment hierarchy cycle that is not valid: A contains B contains C contains A. The Print, Verify, and Ship Reference User Interface does not allow this type of containment configuration. Use the Verify panel in the Print, Verify, and Ship Reference User Interface to specify that any pack type with children in its containment hierarchy is a container of associated labels.

The following table shows the available input types and their corresponding encoding types:

Table 56. Input Types and Matching Encoding Types

Input Type	Encoding Type
DOD	• usdod-64 • usdod-96
GIAI	• giai-64 • giai-96

Table 56. Input Types and Matching Encoding Types (continued)

Input Type	Encoding Type
GID	• gid-96
GLN **Note:** This input type is supported only for printing. This type is not supported by the WebSphere Premises Server EPC Commissioning Member APIs.	• sgln-96 • sgln-64
GRAI	• grai-96 • grai-64
GTIN14	• sgtin-64 • sgtin-96
SSCC18	• sscc-96 • sscc-64

The Print, Verify, and Ship Reference User Interface includes twelve default pack types. The default GTIN14 pack types are:

- CASE64 - 64-bit pack type for cases
- CASE96 - 96-bit pack type for cases
- PALLET64 - 64-bit pack type for containers
- PALLET96 - 96-bit pack type for containers

The default SSCC18 pack types are:

- PALLET64-SSCC64 - 64-bit non-item pack type
- PALLET96-SSCC96 - 96-bit non-item pack type

The default DOD pack types are:

- DODPallet64 - 64-bit pack type for DOD containers
- DODCase64 - 64-bit pack type for DOD cases
- DODUIDItem64 - 64-bit pack type for DOD single-item shipments
- DODPallet96 - 96-bit pack type for DOD containers
- DODCase96 - 96-bit pack type for DOD cases
- DODUIDItem96 - 96-bit pack type for DOD single-item shipments

You can modify the default pack type or create any number of new ones for a particular customer. You associate pack types with profiles; therefore, for each created profile, you can create new pack types with which to print RFID tag labels. See "Configuring profiles" on page 192 for more information.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Click **EPC Configuration Profile Configuration** from the left panel. The EPC Profiles panel displays.

3. Click the profile for which you are creating a new pack type. The Edit EPC Profile Details Panel displays.
4. In the **Available Packaging Types** box, select **Add new packtype**. The Pack Type Configuration panel displays.
5. Enter the pack type in the **Packaging Type** field.
6. Type a brief description of this pack type in the **Description** field.
7. In the **Input Type** field, select the input format of the product codes you are including in this pack type.
8. In the **Company Prefix Length** field, select the number of digits in the company prefix for this pack type.
9. In the **Encoding Type** field, select the algorithm to use when converting from the specified input type to the EPC-compliant output type.
10. Select a filter value from the **Filter Value** field. Filter values are two- to four-digit codes that identify the pack type. In the EPCglobal standard, filter rules are used for filtering and pre-selecting basic logistic types such as inner packs, cases, and pallets.
11. Type a one-digit code from 0-9 in the **Indicator/Extension Digit** field, if necessary. The indicator digit is specific to the manufacturer and identifies packing levels for SGTIN encoding types. The extension digit is used by SSCC encoding types to extend the range of serial numbers.
12. If appropriate, select one or more pack types from the **Contained Pack Type** field. Use the <CTRL> key to select more than one pack type. A contained pack type refers to a pack type that is a subset of a larger pack type. For example, if you are creating pack type Pallet64-011, you might have a contained pack type of CASE64-001 because a case can be part of a larger pallet.

    Note: Any pack type can have zero or more contained pack types.
13. Select a print template from the **Default Print Template** field. You must have already created at least one print template on the Print Templates panel in the WebSphere Premises Server Administrative Console. For more information on creating print templates, see Creating print templates.

    Note: The template you select automatically displays in the **Label** field on the Print panel of the Print, Verify, and Ship Reference User Interface when you select this pack type.
14. Click **Create**. The pack type is saved and available for selection in the Print module of the Print, Verify, and Ship Reference User Interface.
15. Go to the next section, "Configuring profiles" on page 192, to create a customer profile containing these pack types.

Pack Type Configuration details

The following table defines the fields in the Pack Type Configuration Details panels.

Fields

Field	Description
Packaging Type	Select an existing pack type from the list to modify or delete it, or type a name for a new pack type.
Description	Type a brief description of the pack type.

Field	Description
Input Type	The UCC EAN format of the customer product code. See "Configuring pack types" on page 188 for a list of available input types.
Company Prefix Length	The number of digits in the company prefix.
Encoding Type	The electronic product code (EPC) algorithm used to convert the input codes into EPC format. See "Configuring pack types" on page 188 for a list of available encoding types.
Filter Value	The two- to four-digit codes for identifying the pack type. In the EPCglobal standard, filter rules are used for filtering and preselecting basic logistic types such as inner packs, cases, and pallets.
Indicator/Extension Digit	Type a one-digit code from 0-9 in the **Indicator/Extension Digit** field, if necessary. The indicator digit is specific to the manufacturer and identifies packing levels for SGTIN encoding types. The extension digit is used by SSCC encoding types to extend the range of serial numbers.
Contained Pack Type	A contained pack type refers to a pack type that is a subset of a larger pack type. For example, if you are creating pack type, Pallet64-011, you might have a contained pack type of CASE64-001 because a case may be part of a larger pallet.
Default Print Template	Select a print template from the **Default Print Template** field. You must have already created at least one print template in the Print Templates panel in the WebSphere Premises Server Administrative Console. See "Creating print templates" on page 359 for more information on creating print templates.

Working with profiles

This section contains information on managing electronic product code (EPC) tag profiles using the WebSphere Premises Server Administrative Console.

About this task

You can create any number of different pack types for a single customer. By creating a profile, you can associate all of a particular customer's pack types into a single record to simplify the process of printing RFID tag labels. After creating the profile, it is applied to a print job in the Print, Verify, and Ship Reference User Interface so that you can select from the list of pack types associated with that customer.

The Print, Verify, and Ship Reference User Interface comes with five default profiles installed:

- Default64 - default profile for 64-bit tags
- Default96 - default profile for 96-bit tags
- Cage64 - default profile for 64-bit DoD CAGE tags
- Cage96 - default profile for 96-bit DoD CAGE tags
- DoDAAC96 - default profile for 96-bit DoDAAC tags

Adding profiles

Use the WebSphere Premises Server Administrative Console to add new profiles to your network topology.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays. .
2. Click **EPC Configuration** → **Profile Configuration** from the left panel. The EPC Profiles panel displays.
3. Click **New**. The Create a New EPC Profile panel displays.
4. Type a name for this profile in the **Profile Name** field.
5. Type a brief description of the profile in the **Profile Description** field, if desired.
6. Enter a company prefix or a DoD CAGE/DoDAAC in the **Default Company Prefix/DoD CAGE/DoDAAC** field.
7. Click **Create**. The profile is saved and available in the Print module on the Print, Verify, and Ship Reference User Interface.

   Note: Now you can edit the profile to create pack types for this profile. For information about creating pack types, see Working with pack types.

Modifying profiles

Use the WebSphere Premises Server Administrative Console to modify existing profiles in your network topology.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Click **EPC Configuration** → **Profile Configuration** from the left navigation pane. The EPC Profiles panel displays.
3. Click on the profile that you want to modify. The Edit EPC Profile details panel displays.
4. Make the necessary changes and click **Update**.

Deleting profiles

Use the WebSphere Premises Server Administrative Console to delete electronic product code (EPC) profiles from the network topology.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Click **EPC Configuration** → **Profile Configuration** from the left navigation pane. The EPC Profiles panel displays.
3. Click on the profile that you want to delete. The Edit EPC Profile details panel displays.
4. Click **Delete**. A confirmation message displays.
5. Click **OK** to delete the profile.

Configuring profiles

Use the Profile Configuration feature on the WebSphere Premises Server Administrative Console to create a customer profile to use in the Print, Verify, and Ship Reference User Interface.

About this task

You can create any number of different pack types for a single customer. By creating a profile, you can associate all of a particular customer's pack types into a single record to simplify the process of printing RFID tag labels. After creating the profile, it is applied to a print job in the Print, Verify, and Ship Reference User Interface so that you can select from the list of pack types associated with that customer.

The Print, Verify, and Ship Reference User Interface comes with five default profiles installed:

- Default64 - default profile for 64-bit tags
- Default96 - default profile for 96-bit tags
- Cage64 - default profile for 64-bit DoD CAGE tags
- Cage96 - default profile for 96-bit DoD CAGE tags
- DoDAAC96 - default profile for 96-bit DoDAAC tags

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays. .
2. Click **EPC Configuration** → **Profile Configuration** from the left panel. The EPC Profiles panel displays.
3. Click **New**. The Create a New EPC Profile panel displays.
4. Type a name for this profile in the **Profile Name** field.
5. Type a brief description of the profile in the **Profile Description** field, if desired.
6. Enter a company prefix or a DoD CAGE/DoDAAC in the **Default Company Prefix/DoD CAGE/DoDAAC** field.
7. Click **Create**. The profile is saved and available in the Print module on the Print, Verify, and Ship Reference User Interface.

   Note: Now you can edit the profile to create pack types for this profile. For information about creating pack types, see Working with pack types.

Profile configuration details

The following table defines the fields on the Profile Configuration Details panels.

Fields

Field	Description
Profile Name	Type a name for this profile.
Profile Description	Type a brief description of the profile.
Default Company Prefix/DoD CAGE/DoDAAC	Enter a default company prefix or a DoD CAGE/DoDAAC.
Available Pack Types	Select one or more pack types to associate with this profile.

Working with serial numbers

This section contains information on managing electronic product code (EPC) serial numbers using the WebSphere Premises Server Administrative Console.

About this task

After you create a customer's pack types and associated profile, you can configure two other important pieces of information: product identification number or DoD CAGE/DoDAAC and EPC serial number. This information is required to uniquely identify a product for RFID tagging. Because there might be more than one pack type associated with a product, a product can have a range of serial numbers.

This process is required only if you want to manually assign serial numbers to your products. If you do not manually assign serial numbers, they are automatically assigned in increments of **1**, starting with **1**.

Adding serial numbers

Use the WebSphere Premises Server Administrative Console to add new serial numbers to your network topology.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays. .
2. Click **EPC Configuration** → **Serial Number Configuration** from the left panel. The Serial Number Profiles panel displays.
3. Select an ID URI type and click **New**. The Create a New Serial Number Profile panel displays with the EPCglobal ID URI type you chose.
4. Complete the fields to configure the new serial number. For information about these fields, see the Serial number profile details panel.
5. Click **Create**. The configuration is saved.
6. Repeat this procedure for each new serial number.

Modifying serial numbers

Use the WebSphere Premises Server Administrative Console to modify existing electronic product code (EPC) serial numbers.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Click **EPC Configuration** → **Serial Number Configuration** from the left panel. The Serial Number Profiles panel displays.
3. Click the **EPCglobal ID URI** type that you want to modify. The Edit Serial Number Profile Details panel displays.
4. Make the necessary changes and click **Update**.

Deleting serial numbers

Use the WebSphere Premises Server Administrative Console to delete electronic product code (EPC) serial numbers from your network topology.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Click **EPC Configuration** → **Serial Number Configuration** from the left panel. The Serial Number Profiles panel displays.
3. Select the **EPCglobal ID URI** type that you want to delete. The Edit Serial Number Profile Details panel displays.
4. Click **Delete**. A confirmation message displays.
5. Click **OK** to delete the serial number.

Configuring serial numbers

Use the Serial Number Configuration feature in the WebSphere Premises Server Administrative Console to determine the EPC serial numbers associated with each customer's products.

About this task

After you create a customer's pack types and associated profile, you can configure two other important pieces of information: product identification number or DoD CAGE/DoDAAC and EPC serial number. This information is required to uniquely identify a product for RFID tagging. Because there might be more than one pack type associated with a product, a product can have a range of serial numbers.

This process is required only if you want to manually assign serial numbers to your products. If you do not manually assign serial numbers, they are

automatically assigned in increments of **1**, starting with **1**.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays. .
2. Click **EPC Configuration** → **Serial Number Configuration** from the left panel. The Serial Number Profiles panel displays.
3. Select an ID URI type and click **New**. The Create a New Serial Number Profile panel displays with the EPCglobal ID URI type you chose.
4. Complete the fields to configure the new serial number. For information about these fields, see the Serial number profile details panel.
5. Click **Create**. The configuration is saved.
6. Repeat this procedure for each new serial number.

Serial Number Profile details

The following table defines the fields on the Create New Serial Number Profile and Edit Serial Number Profile panels.

Fields

Field	Description
EPCglobal ID URI type	The ID URI that you indicated displays. This ID is the universal resource identifier for the serial number.
EAN, UCC company prefix	(For ID URI types *sgtin*, *sscc*, *grai*, and *giai*.) The company prefix that is part of the URI. It is associated with a specific pack type.
Extension digit	(For ID URI type *sscc*.) While similar in function to an indicator digit, see below, EAN.UCC gives them different names.
Indicator digit	(For ID URI type *sgtin*.) A numeric value in the URI that differentiates between containers.
Asset type	(For ID URI type *grai*.) A numeric value used to define a returnable asset such as a pallet, keg, or other carrier.
Item reference	(For ID URI type *sgtin*.) The reference number to associate with the product for which you are creating or modifying the serial number.
Dept. of Defense CAGE/DoDAAC	(For ID URI type *usdod*.) CAGE, Commercial And Government Entity, is a five-position, alphanumeric string that uniquely identifies a company that is registered to do business with the U.S Dept. of Defense. It serves the same purpose as a EAN.UCC company prefix, but the numbers are managed by the DoD, not EAN.UCC. DoDAAC (Dept. of Defense Activity Address Code) is a unique six-position, alphanumeric string that uniquely identifies departments, locations, units, and so on within the military. This identifier serves the same purpose as a company prefix, but it is managed by the DoD, not EAN.UCC. CAGE is a company prefix for civilian suppliers to the DoD, DoDAAC is a company prefix for military divisions within the DoD.
EPC global General Manager Number	(For ID URI type *gid*.) The EPCglobal general manager number is a number assigned by EPCglobal to a subscriber who has requested it for creating a GID. It is similar to a company prefix in that it is a six- through 12-digit number, but you cannot use a company prefix as a general manager number; you must request a separate one from EPCglobal.

Field	Description
Object class	(For ID URI type *gid*.) Object class is a numeric string that identifies a "class" of similar objects for which you can create a GID. The general manager number + object class + serial number creates a unique GID that can be used to encode an EPC that uses GID-96 encoding.
Allocate to	Enter the item to which you are assigning this serial number. This field enables you to manage serial number ranges for a given product across one or more locations.
Description	Enter a description of the item to which you are allocating the serial number.
Start serial number	Enter the starting EPC serial number.
End serial number	Enter the ending EPC serial number.
Increment	Enter the number by which to increase the serial number for each new serial number within the range.

Working with the EPCglobal company prefix index

This section contains information about managing the EPCglobal Company Prefix Index that is used to map or translate an EAN.UCC company prefix to an index value when printing 64-bit tags. Use the WebSphere Premises Server Administrative Console to manage the company prefix index.

EPCglobal maintains a database of these index translations, and updates them periodically. To retrieve the latest company index translations, click **Refresh** on the EPCglobal Company Prefix Index Translations panel.

When you add new company prefixes to the index, you are only adding them to a copy of the index on your local database. Therefore, when you modify the EAN.UCC Company Prefix field or delete a company prefix from the index, only the index on your local database is updated.

CAUTION:
Be careful when refreshing this index. If you add an index value and company prefix to this table to ship 64-bit tags and that index value and company prefix has not been assigned to you through EPCglobal, clicking refresh could overwrite your company prefix with the EPCglobal company prefix associated with that index value.

This section contains the following topics:

Adding company prefixes
Use the WebSphere Premises Server Administrative Console to add new company prefixes to your local database of the EPCglobal Company Prefix Index.

About this task

EPCglobal maintains a database of these index translations, and updates them periodically. To retrieve the latest company index prefix translations from EPCglobal, click **Refresh** on the EPCglobal Company Prefix Index Translations panel. The codes you add only update your local database; they are not added to the EPCglobal Company Prefix Index.

CAUTION:

Be careful when refreshing this index. If you add an index value and company prefix to this table to ship 64-bit tags and that index value and company prefix has not been assigned to you through EPCglobal, clicking refresh could overwrite your company prefix with the EPCglobal company prefix associated with that index value.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Click **EPC Configuration → Company Prefix Index Translation** from the left panel. The EPCglobal Company Prefix Index Translations panel displays.
3. Click **New** to add a new Company Prefix Index Translation.
4. Enter the new code in the **EPCglobal Company Prefix Index** field.
5. In the **EAN.UCC Company Prefix** field, enter the number to associate with the EPCglobal code.
6. Click **Create**.

Modifying company prefixes

This topic describes how to change the EAN.UCC company prefix for an existing company prefix in your local database of the EPCglobal Company Prefix Index. Use the WebSphere Premises Server Administrative Console to modify existing company prefixes.

About this task

EPCglobal maintains a database of these index translations, and updates them periodically. To retrieve the latest company index prefix translations from EPCglobal, click **Refresh** on the EPCglobal Company Prefix Index Translations panel. The codes you add only update your local database; they are not added to the EPCglobal Company Prefix Index.

CAUTION:

Be careful when refreshing this index. If you have added an index value and company prefix to this table to ship 64-bit tags and this index value and company prefix has not been assigned to you through EPCglobal, clicking refresh could overwrite your company prefix with the EPCglobal company prefix associated with that index value.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Click **EPC Configuration → Company Prefix Index Translation** from the left panel. The EPCglobal Company Prefix Index Translations panel displays.
3. Select the EPCglobal company prefix for which you are modifying the translation. The Edit EPCglobal Company Prefix Index Translation panel displays.
4. In the **EAN.UCC Company Prefix** field, enter the new number that you want to associate with the EPCglobal code.
5. Click **Update**.

Deleting company prefixes

This topic describes how to delete a company prefix from your local database of the EPCglobal Company Prefix Index. Because the index assignment of the company prefix is managed by EPCglobal, this procedure only removes the company prefix from your local database. Use the WebSphere Premises Server Administrative Console to delete a company prefix.

Before you begin

When you retrieve the most current index from EPCglobal, it overrides any changes that you made to your local database.

CAUTION:
Be careful when refreshing this index. If you have added an index value and company prefix to this table to ship 64-bit tags and that index value and company prefix has not been assigned to you through EPCglobal, clicking refresh could overwrite your company prefix with the EPCglobal company prefix associated with that index value.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Click **EPC Configuration** → **Company Prefix Index Translation** from the left panel. The EPCglobal Company Prefix Index Translations panel displays.
3. Select the EPCglobal company prefix that you want to delete and click **Delete**. A confirmation message displays.
4. Click **OK** to delete the company prefix from your local database.

Configuring EPC commissioning details

To print RFID tag labels, you must convert non-EPC product codes that customers currently use to Electronic Product Code (EPC) format.

EPC is the worldwide standard for RFID set by EPCglobal. The IBM Print, Verify, and Ship solution is based on EPC Generation 1 Tag Data Standard, version 1.1, revision 1.27.

Use the EPC Commissioning Configuration section in the WebSphere Premises Server Administrative Console for defining the behavior for the commissioning process -- the process of converting product codes into EPC codes.

The EPC Commissioning Configuration process consists of the following main steps:

1. Configure pack types -- Create pack types, such as case and container, that are specific to each supplier. In the WebSphere Premises Server Administrative Console, pack types define the UCC.EAN formatted product code that is currently used by the customer and the desired encoding type that is used to convert the product codes to EPC-compliant codes, or commissioned output. Refer to "Configuring pack types" on page 188 for more information.
2. Configure profiles -- Create profiles that contain all of the available pack types for a given customer. Refer to "Configuring profiles" on page 192 for more information.
3. Configure serial numbers -- Associate a customer's products with a range of EPC serial numbers. Refer to "Configuring serial numbers" on page 194 for more information.

Managing printing

This topic contains information on the different ways you can print tags using the WebSphere Premises Server.

Using the WebSphere Premises Server Administrative Console, you can define devices as printers and then set up print templates for those printers to use.

There are two ways to handle print jobs with WebSphere Premises Server:

- Logical printers - These are predefined printer devices, such as Loftware Labeling System by Loftware, Inc. or BarTender by Seagull Scientific, Inc, that allow tag printing through a third-party software system.
- Inbound and outbound printing using print profiles - This feature uses a publish/subscribe method to send and receive messages through the WebSphere Application Server service integration bus (SIBus).

Configuring logical printers

Use the WebSphere Premises Server Administrative Console to add and configure logical tag printers in your network topology.

About this task

If you configure a logical tag printer, such as Loftware or BarTender, the print request is sent to the appropriate print server, which retrieves the appropriate print template from WebSphere Premises Server. The print server then sends the request to the physical tag printer and the job prints.

1. Define your printer device. Choose either Loftware or BarTender for the configuration group.
2. Create a print template with the label information.

Print profile support

The print profile application program interface (API) supports outbound and inbound printing and provides abstract and concrete methods.

For information about the WebSphere Premises Server Java API, refer to the WebSphere Premises Server API documentation.

For more information on predefined agents and their topics, refer to "Predefined task agents" on page 215.

Inbound printing

WebSphere Premises Server listens to the inbound print profile topics. Inbound message are processed by a message-driven bean (MDB) which updates the appropriate tables with the received information. The inbound print profile can update the status for a single tag or a print job.

The inbound API concrete method publishes a print job or tag status to these topics on the WebSphere Application Server SIBus.

Updating individual tag status
Topic name: ibmse/*device_ID*/RfidWrite/signal/labelprint/tag/status

Event process: Uses a MDB to send the updated status of a tag to the back-end database; updates the status column of SAGE.PRINTDATA.

Updating the print job status
Topic name: ibmse/*device_ID*/RfidWrite/signal/labelprint/job/status

Event process: Uses a MDB to send the updated status of a print job to the back-end database; updates the status column of SAGE.PRINTJOB.

You can also use a servlet to update the status of inbound print profile topics. The servlet can be accessed at the following URL, where *Premises_Server* is the host name or IP address of your WebSphere Premises Server: http:// *Premises_Server*:9080/ibmse/eventpublish

See "Configuration samples for print profile support" on page 202 for examples of the servlet URLs and XML for updating the print job or tag status.

Outbound printing

Print jobs submitted from Print, Verify, and Ship and bound to a printer device type (outbound print profile) publish to the following topics on the WebSphere Application Server service integration bus (SIBus). Printer vendors can use the abstract method to implement outbound printing and subscribe to these print topics using the API.

Printing a label
> Topic name: ibmse/*DeviceID*/RfidWrite/command/labelprint/job/print

> Event process: This topic accepts print requests submitted by Print, Verify, and Ship.

Canceling a print job
> Topic name: ibmse/*DeviceID*/RfidWrite/command/labelprint/job/cancel

> Event process: This topic cancels a submitted print job.

Reprinting a label
> Topic name: ibmse/*DeviceID*/RfidWrite/command/labelprint/job/reprint

> Event process: This topic reprints the label for a supplied tag URI if you request a reprint in Print, Verify, and Ship. The Print, Verify, and Ship reprint function accepts the tag URI and generates a new print job with one tag.

Creating a print profile device
Use these steps to create and configure a print profile device.
1. Import the device configuration XML using the WebSphere Premises Server Administrative Console. See "Configuration samples for print profile support" on page 202 for an example of the input XML file.
2. Create a new device configuration group for the print profile device.
   a. In the WebSphere Premises Server Administrative Console, under **Data Capture Configuration** in the left navigation pane, click **Devices**. The Devices panel displays.
   b. Under **Configuration Groups**, click **Create**. The New Device Configuration Group panel displays.
   c. Enter the information for the new configuration group, making sure to select a category of **Printer**. You do not need to select a **Configuration Group Agent** to associate with the configuration group.
   d. Click **Create**. The new print profile configuration group displays in the list of configuration groups.
3. Create a new device associated with the new print profile configuration group.
   a. In the same WebSphere Premises Server Administrative Console panel, under **Devices**, click **New**. The Create Device panel displays.
   b. Enter the information for the new print profile device, making sure to select the configuration group you created.
   c. Click **Create**. The new printer device displays in the list of devices.

4. Create a new print template for the print profile configuration group.

Creating a custom print profile driver

Printer vendors can use the print profile API to develop customized message-driven beans (MDBs) to meet their printing requirements.

1. Turn off the default print driver.
    a. Log in to the WebSphere Application Server administrative console.
    b. Navigate to **Resources** › **JMS** › **Activation specifications** and click **LabelPrintJobCommandAS**.
    c. Enter `ibmse=off` in **Message selector** field.
    d. Restart WebSphere Application Server.
2. Develop a new MDB that listens for the outbound print profile topic.
3. Develop a new class by extending the LabelPrintProfile abstract class.
4. Use the call print, reprint or cancel print methods, as needed.
5. Create a new topic with the correct topic name using the WebSphere Application Server administrative console.
6. Create new activation specifications using the WebSphere Application Server administrative console.

Sample print profile code

```
public class DefaultPrintProfileDriver extends LabelPrintProfile{

public void labelprintjob(String print_job_id, Map metadata, String XML) {
 transform(String xml, String xslUrl)
}
 public void labelprintjob_cancel(String print_job_id) {
  transform(String xml, String xslUrl)
 }

 public void labelprintjob_reprint(String print_job_id, Map metadata, String XML) {
  transform(String xml, String xslUrl)
 }
```

Print profile status servlet

The print profile status servlet receives and processes XML-formatted status messages about WebSphere Premises Server print jobs or individual tags.

The XML message must be bundled into a URL for the servlet. The URL must contain the following parameters:

eventType
>   A type identifier, either RfidWrite/signal/labelprint/job/status for job status or RfidWrite/signal/labelprint/tag/status for tag status.

eventTopic
>   A topic identifier, either ibmse/*printer_name*/RfidWrite/signal/labelprint/job/status for job status, or ibmse/*printer_name*/RfidWrite/signal/labelprint/tag/status for tag status, where *printer_name* is the name of the printer device as configured in the WebSphere Premises Server Administrative Console.

eventXml
>   The XML message containing the job or tag status information.

See "Configuration samples for print profile support" on page 202 for examples of the servlet URLs and XML for updating the print job or tag status.

Configuration samples for print profile support

Use these sample files for print profile support.

- "Sample XML generated from the printer driver before the XSL transformation"
- "Sample XSLT to transform the XML generated by the printer driver"
- "Sample XML file after transformation"
- "Sample XML to define the printer device metadata" on page 203
- "Sample XML to update the print job status" on page 203
- "Sample XML to update tag status" on page 203
- "Sample servlet URL to update the print job status" on page 204
- "Sample servlet URL to update tag status" on page 204

Sample XML generated from the printer driver before the XSL transformation

```
<?xml version="1.0" encoding="UTF-8"?>
<labels _PRINTERNAME="P4" _JOBNAME="1191438711797">
<label _FORMAT="file://SampleCase.zpl">
<variable name="epcdata">sgtin-64:2.1234567.100150.2</variable>
<variable name="manufacturername">Widget Makers, Inc.</variable>
<variable name="barcodedata">11234567001507</variable>
<variable name="EPC">907ce30e6c000002</variable>
<variable name="productquantity">50</variable>
<variable name="productname">Widgets</variable>
<variable name="productdescription">1/2 inch Steel Widgets</variable>
<variable name="manufacturerid">098574</variable>
</label>
</labels>
```

Sample XSLT to transform the XML generated by the printer driver

```
<?xml version="1.0" encoding="UTF-8"?>
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
<xsl:output indent="yes" method="xml"/>
<xsl:param name="attribute" select="'_PRINTERNAME'" />
<xsl:param name="newvalue" select="'P10XXX'"/>
<xsl:template match="node()|@*">
<xsl:copy>
<xsl:apply-templates select="@*|node()"/>
</xsl:copy>
</xsl:template>
<!-- This is a generic search replace of attribute values -->
<xsl:template match="@*" >
<xsl:attribute name="{name()}">
<xsl:choose>
<xsl:when test="(name()=$attribute)"><xsl:value-of select="$newvalue"/></xsl:when>
<xsl:otherwise><xsl:value-of select="."/></xsl:otherwise>
</xsl:choose>
</xsl:attribute>
</xsl:template>
</xsl:stylesheet>
```

Sample XML file after transformation

```
<?xml version="1.0" encoding="UTF-8"?>
<labels _PRINTERNAME="P10XXX" _JOBNAME="1191438711797">
<label _FORMAT="file://SampleCase.zpl">
<variable name="epcdata">sgtin-64:2.1234567.100150.2</variable>
<variable name="manufacturername">Widget Makers, Inc.</variable>
<variable name="barcodedata">11234567001507</variable>
<variable name="EPC">907ce30e6c000002</variable>
<variable name="productquantity">50</variable>
<variable name="productname">Widgets</variable>
<variable name="productdescription">1/2 inch Steel Widgets</variable>
<variable name="manufacturerid">098574</variable>
</label>
</labels>
```

Sample XML to define the printer device metadata

Note: If you would like to get a device configuration group name from the metadata published to the WebSphere Application Server SIBus, the key name is DEVICE_CONFIGURATION_GROUP_NAME.

```
<?xml version="1.0" encoding="UTF-8"?>
<ibmrfidconfigadmin:configurationAdmin dest="prem" dts="2001-12-31T12:00:00"
    orig="dms" version="" xmlns:ibmrfidconfigadmin="http://www.ibm.com"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.ibm.com IBMRFIDConfigAdmin.xsd ">
<requests>
<request type="update">
<serverconfigurations>
<categories>
<category config-group-type="DeviceType" name="Printer">
<category-metadata defaultvalue="rr" name="Print XML Location URL" />
<category-metadata defaultvalue="rr" name="XSLT File URL" />
</category>
</categories>
</serverconfigurations>
</request>
</requests>
</ibmrfidconfigadmin:configurationAdmin>
```

Sample XML to update the print job status

Tip: Replace the variable, *printer name*, with the name of your printer.

```
<CommonBaseEvent creationTime="2008-04-25T19:28:54.781Z" globalInstanceId="123456789"
priority="50" version="1.0.1">
<extendedDataElements name="ibmse_payloadMetaData" type="noValue">
</extendedDataElements>
<extendedDataElements name="ibmse_payload" type="string">
<values>com.ibm.sensorevent.model.payload.Payload</values>
<children name="ibmse/printer name/RfidWrite/signal/labelprint/job/status" type="noValue">
<children name="STATUS" type="string">
<values>PRINT: Submitted Job</values>
</children>
<children name="JobID" type="string">
<values>1208787033984</values>
</children>
</children>
</extendedDataElements>
<situation categoryName="ReportSituation">
<situationType xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="ReportSituation"
  reasoningScope="EXTERNAL" reportCategory="LOG"/>
</situation>
<CommonBaseEvent>
```

Sample XML to update tag status

Tip: Replace the variable, *printer name*, with the name of your printer.

```
<CommonBaseEvent creationTime=" 2008-04-25T19:28:54.781Z" globalInstanceId="123456789"
priority="50" version="1.0.1">
<extendedDataElements name="ibmse_payloadMetaData" type="noValue">
</extendedDataElements>
<extendedDataElements name="ibmse_payload" type="string">
<values>com.ibm.sensorevent.model.payload.Payload</values>
<children name="ibmse/printer name/RfidWrite/signal/labelprint/tag/status" type="noValue">
<children name="STATUS" type="string">
<values>PRINT: Submitted Job</values>
</children>
<children name="TAGID" type="string">
<values>1208787033984</values>
</children>
</children>
</extendedDataElements>
<situation categoryName="ReportSituation">
<situationType xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="ReportSituation"
  reasoningScope="EXTERNAL" reportCategory="LOG"/>
</situation>
<CommonBaseEvent>
```

Sample servlet URL to update the print job status

The parameters marked in bold type are required, and the following variables should be replaced with the correct values for your environment.

- *Premises_Server* - the host name or IP address of your WebSphere Premises Server
- *device_ID* - the name of the printer
- *status of print job* - a string of text describing the updated status. For example, `PRINT: TEST JOB VALIDATED`
- *job_ID* - ID number of the print job

http://*Premises_Server*:9080/ibmse/eventpublish?**eventType**=RfidWrite/signal/labelprint/job/status&**eventTopic**=ibmse/*device_ID*/RfidWrite/signal/labelprint/job/status &**eventXml**=<CommonBaseEvent><extendedDataElements name="ibmse_payloadMetaData" type="noValue"></extendedDataElements><extendedDataElements name="ibmse_payload" type="string"><values>com.ibm.sensorevent.model.payload.Payload</values><children name="RfidWrite/signal/labelprint/job/status" type="noValue"><children name="STATUS" type="string"><values>*status of print job*</values></children><children name="JOBID" type="string"><values>*job_ID*</values></children></children></extendedDataElements></CommonBaseEvent>

Sample servlet URL to update tag status

The parameters marked in bold type are required, and the following variables should be replaced with the correct values for your environment.

- *Premises_Server* - the host name or IP address of your WebSphere Premises Server
- *device_ID* - the name of the printer
- *status of tag* - a string of text describing the updated status. For example, `PRINT: TEST TAG VALIDATED`
- *tag_ID* - ID number of the tag

http://*Premises_Server*:9080/ibmse/eventpublish?**eventType**=RfidWrite/signal/labelprint/tag/status&**eventTopic**=ibmse/*device_ID*/RfidWrite/signal/labelprint/tag/status &**eventXml**=<CommonBaseEvent><extendedDataElements name="ibmse_payloadMetaData" type="noValue"></extendedDataElements><extendedDataElements name="ibmse_payload" type="string"><values>com.ibm.sensorevent.model.payload.Payload</values><children name="RfidWrite/signal/labelprint/tag/status" type="noValue"><children name="STATUS" type="string"><values>*status of tag*</values></children><children name="TAGID" type="string"><values>*tag_ID*</values></children></children></extendedDataElements></CommonBaseEvent>

Working with print templates

This section contains information on managing print templates using the WebSphere Premises Server Administrative Console.

A print template in the WebSphere Premises Server Administrative Console consists of a template name, a printer type, and a template file location that reference an existing print template stored in another file. A print template file for a physical tag printer is written in a printer-specific language and contains

instructions unique to that printer to define the layout of the fields that are being printed on the label. Sample print templates are provided in the following directories:

> **Windows** *IBM_RFID_HOME*\premises\pvs\templates
>
> **Linux** *IBM_RFID_HOME*/premises/pvs/templates

They can be customized to meet your specific label requirements.

A print template for a tag printer must be stored on the file system of the printer software. For example, the .lwl Loftware print template must be on the Loftware server to access it and the .btw Bartender print template must be on the Bartender server to access it. A print template for a physical tag printer can be stored on your IBM HTTP Server or on your local file system. The IBM HTTP Server can be on either the same server as WebSphere Premises Server or on another server in the RFID network.

To submit print jobs from the Print, Verify, and Ship Reference User Interface, you must create a corresponding properties file that contains static data required for shipping, such as customer name and address, after you define the print template.

This section contains the following topics:

Adding print templates

Use the WebSphere Premises Server Administrative Console to add new print templates to your network topology.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Under **Data Capture Configuration**, click **Print Templates** in the left navigation panel. The Print Templates panel displays.
3. Click **New**. The Create a New Print Template panel displays.
4. Enter a name for the print template. This name should be the same as the file name of a properties file that is located in the Print, Verify, and Ship application labels directory. The contents of the properties file determines the fields that are provided in the XML print job stream and the fields specified must match those defined in the label file used by the printer, which is specified in the **Properties Location URL** field. See "Creating properties files for print templates" on page 360 for more information.
5. Select a printer configuration group.
6. In the **Properties Location URL** field, enter the label file name as file://*label_file_name*. This label file name is included in the XML print job stream as the value for the _FORMAT attribute of the `<label>` tag. This value is assumed to be significant to the print handler software (for example, it might correspond to the name of a label).
7. Click **Create**. The print template displays in the list of print templates.
8. Create the properties file for the print template if you want to submit print jobs from the Print, Verify, and Ship Reference User Interface. See "Creating properties files for print templates" on page 360 for more information.

Modifying print templates

Use the WebSphere Premises Server Administrative Console to modify existing print templates.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.

2. Under **Data Capture Configuration**, click **Print Templates** in the left navigation panel. The Print Templates panel displays.

3. Click the print template that you want to modify. The Edit Print Template Details panel displays.

4. Make the necessary changes and click **Update**.

Deleting print templates

Use the WebSphere Premises Server Administrative Console to delete existing print templates from your network topology.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.

2. Under **Data Capture Configuration**, click **Print Templates** in the left navigation panel. The Print Templates panel displays.

3. Click on the print template that you want to delete. The Edit Print Template Details panel displays.

4. Click **Delete**. A confirmation message displays.

5. Click **OK** to delete the profile.

Print template details

The following table defines the fields on the Create a New Print Template and Edit Print Template Details panels.

Fields

Field	Description
Print Template Name	Type a unique identifier for this template.
Configuration Groups	Select the type of tag printer for which you are creating the print template. The tag printer types display in the Print Templates panel.
Properties Location URL	Enter the location of the properties file for the tag printer; for example, enter: file://SampleCaseTag.lwl.

Managing ALE

This topic provides information on the ALE Administrative Console, which allows you to administer the Application Level Events (ALE) server.

The ALE Administrative Console is installed with WebSphere Premises Server and can be accessed by entering the following URL into a browser: http://*localhost:portnumber*/ale/admin, where *localhost* and *portnumber* are the hostname and port number of the computer hosting WebSphere Premises Server.

The ALE Administrative Console contains the following pages:

Server Requests
Allows you to submit commands to the ALE server and view responses. Submit commands by attaching a predefined XML file to the request. The XML file should conform with the XML and SOAP Bindings defined in Part II of EPCglobal's ALE 1.1 Specification.

Readers
Allows you to view all readers known to the system. This includes base readers, composite readers, and reader simulators.

Reports

Allows you to view incoming ECReports from the ALE server. To receive reports, start the TCP Callback and make a subscription, for example, through the Server Requests page, to a defined ECSpec using the appropriate notification URI, such as tcp://*hostname:port*.

Reader Simulators

Allows you to create reader simulators and associate them with the desired tag simulators. ECSpecs may then be defined referencing these simulators as logical readers. You may also import and export reader simulator configurations.

Tag Simulators

Allows you to create simulated EPC Class 1, Gen 2 tags. These may then be added to the fields of reader simulators. You may also import and export tag simulator configurations.

Reporting

This section contains the following topics that you can use to gather information about your WebSphere Premises Server system configuration.

Viewing tag read reports

Use the WebSphere Premises Server Administrative Console to view tag read and aggregated tag read events that have registered in your WebSphere Premises Server network.

Before you begin

By setting parameters in the SystemAgent, you can determine whether your tags persist to a database or to an EPCIS, and you can determine the type of events persisted, such as tag reads or aggregated tag reads. For details on how to do this, see "Managing persistence" on page 210.

To determine the current status of the persistence parameter, view the SystemAgent configuration in the WebSphere Premises Server Administrative Console by navigating to **Agent Configuration** → **SystemAgent** → **com.ibm.premises.SystemAgent** .

About this task

WebSphere Premises Server uses Business Intelligence and Reporting Tools (BIRT), an Eclipse-based open source reporting system, to run and display the tag read reports within the WebSphere Premises Server Administrative Console.

The reports you run are stored in a location that is defined by the com.ibm.premises.report.location parameter in the SystemAgent. Modify the value of this parameter if you would like your reports stored in a location other than the default directory. Remember to use only US English ASCII characters in directory paths.

Note: If you do change the value of this property, the files and folders in the installed reports must also be moved. Otherwise, the standard RFID tag read event reports will not be found.

The default location of stored reports is:

Windows *IBM_RFID_HOME*/reports

Linux *IBM_RFID_HOME*\reports

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Under **Reporting**, click **RFID Tag Read Events** in the left navigation pane. The **RFID Tag Read Events** panel displays filter fields for you to search your tags.
3. Enter filter criteria and click **Search** to display tag read events matching your criteria.

   When the report displays, you can perform these actions:
   - Click an event ID to display the report containing detailed information about the event.
   - Click a tag ID to display the report containing detailed information about the RFID tag. This option is available from either the main **RFID Tag Read Events** report, or from the **RFID Tag Read Event Details** report.
   - Click**Show XML** in the **RFID Tag Read Event Details** panel to display the report containing complete event XML.

   Refer to "Available actions after searching" on page 209 for more details on what you can do with your generated reports.

RFID Tag Read Events details

This topic explains the available options in the RFID Tag Read Events panel.

Available fields before searching

No tags are displayed before you search. You can filter the tags before searching. You can also view tag history for a specific location or all locations and for a particular date or range of dates. The default format for the date fields is yyyy-MM-dd. The system administrator can change the date field format by setting the com.ibm.rfid.premises.taghistory.search.filter.date.format property in the SystemAgent.

Table 57. Available fields before searching

Field		Description
Location		Use this optional field to indicate the location for which you are viewing tag history. The default is **All locations**. Click the drop-down arrow and select a specific location from the list. If you search by location, all tags for the selected location and its contained locations are displayed.
Filter		To search for a particular tag in a long list of tags, enter the tag ID in this field to scroll to that tag. To show all tags, leave this field blank and click **Search**.
Start Date		Enter the date for which you are viewing tag history or click the calendar icon and select the date. This date can also indicate the start date for a range of dates. If you enter a value here and leave the **End Date** field empty, all tags from this date forward are displayed. Optional.
End Date		Enter the date through which you are viewing tag history or click the calendar icon and select the date. If you also entered the start date, this date is the end date for a range of dates. If you enter a value here and leave the **Start Date** field empty, all tags through this date are displayed. Optional.

Table 57. Available fields before searching (continued)

Field		Description
Page Size		A number that indicates how many events are displayed on each page. The default page size is 50.

Available actions after searching

After you click **Search**, the following actions are available in the **RFID Tag Read Events** report results to display more detailed reports.

- Click an event ID to display the report containing detailed information about the event.
- Click a tag ID to display the report containing detailed information about the RFID tag. This option is available from either the main **RFID Tag Read Events** report, or from the **RFID Tag Read Event Details** report.
- Click**Show XML** in the **RFID Tag Read Event Details** panel to display the report containing complete event XML.

Note: The event XML is encoded, which is the required format for WebSphere Premises Server.

Each report page contains a banner of common report functions:

Note: These functions are unmodified and provided "as-is" by BIRT. You may notice that some of the toolbar functions may not work as expected. For example, links in exported reports may not be valid.

Toggle table of contents
> Displays a table of contents when the page contains multiple rows. Only the **RFID Tag Read Events** report contains table of contents information. The other reports do not, so their table of contents will be empty.

Run report
> Runs the report again. Do not modify any parameters displayed in the Run Report dialog. Instead, click **OK** to continue.

Export data
> Exports the report data to a file.

Export report
> Exports the report to another format, such as Microsoft Excel.

Print report
> Prints the report in HTML or PDF format.

Print report on the server
> Print the report, as displayed, to an attached printer.

Page selection
> Provides navigation among the pages in a report such as next or previous page, first or last page, or you can go to a specific page number.

Disabling tag aggregation

The Tag Aggregation function enables edge controllers to capture and group tag information from one event to another, to process those tags as a unit, and to use that grouped information.

About this task

Tag aggregation is turned on by default.

To disable tag aggregation, you must disable the TagAggregationAgent. You do this by setting `location.association=NONE` in the properties for the tag aggregation agent. For instructions on how to modify agent properties, refer to "Modifying agents by downloading agent properties" on page 107 and "Modifying agent properties for a PID" on page 106.

Managing persistence

This topic describes how to configure event persistence.

You can change how tag reads and events persist by modifying values in the SystemAgent.

Note: After modifying the SystemAgent, you must restart the WebSphere Premises Server.

Persisting events to the database

If you want all of your events saved to the database, set the value of the `com.ibm.sensorevent.persistence.db` property to `true` in the SystemAgent. If this property is set to any value other than `true`, all events are not saved to the database. The default value is `true`.

Persisting events to an EPCIS

If you set the value of `com.ibm.sensorevent.persistence.epcis` to `true`, then all events are sent to the EPCIS Connector. If you set the value to `false`, then the events are not sent to the EPCIS Connector. The default value is `false`.

For more information on using the EPCIS Connector, refer to the topic on the "EPCIS Connector sample application" on page 375.

Filtering persisted events
About this task

To filter persisted events, administrators can change the message selector value in the PersistenceAS activation specification in the WebSphere Application Server administrative console.

1. Open the WebSphere Application Server administrative console.
2. Navigate to **Resources** → **JMS** → **Activation specifications** and click **PersistenceAS**.
3. Edit the **Message selector** field to the desired filter value. The default value limits the events persisted to tag read and aggregated tag read events:

```
ibmse='RfidInventory/TagReport' OR
ibmse='RfidInventory/TagAggregationReport' OR ibmse LIKE
 '%/report/TagReport' OR ibmse LIKE '%/report/TagAggregationReport'
```

Understanding Application Ping

Application Ping is the functionality of the edge controller to check the availability of the entire RFID system.

Overview

The concept of Application Ping is similar to the concept of the Internet Control Message Protocol (ICMP), which is a protocol for controlling messages reporting errors between a host server and a gateway. Application Ping uses an agent on the edge controller to periodically check whether the whole RFID system is available by sending out an Application Ping Request on the MicroBroker bus. The Application Ping Request travels from the edge controller through WebSphere Premises Server to the back-end of the RFID system. The back-end system then responds to the Application Ping Request with an Application Ping Response message, which includes any errors from the back-end devices. WebSphere Premises Server routes the Application Ping Response back to the originating edge controller.

If there is no Application Ping Response to the Application Ping Request, then the edge controller does not recognize the RFID system as available.

Application Ping configuration settings

The setting for Application Ping is configurable in the SystemAgent. The possible values for the `com.ibm.rfid.applping.shortcut` property are `true` or `false`.

A value of `false` means that the Application Ping Request is passed through WebSphere Premises Server and answered by the back-end RFID system. A value of `true` means that the Application Ping Request is answered by WebSphere Premises Server.

The default value is `true`.

To view the Application Ping configuration settings in the WebSphere Premises Server Administrative Console, navigate to **Agent Configuration** ⊁ **SystemAgent**. Look for `com.ibm.rfid.applping.shortcut` in the **Name** column. The current set value for each configuration variable is in the **Value** column.

Setting the delete filter for Data Capture and Delivery

The delete filter for Data Capture and Delivery is an LDAP filter that is used to clear configurations from the Data Capture and Delivery device.

The delete filter must be set correctly so that duplicate configurations are not stored in ConfigAdmin, causing duplicate agents that can compete for the same resources. For example, if a reader's configuration is not deleted, then when the Data Capture and Delivery controller starts it will load a second copy of the reader configuration, creating a second agent. Both agents will try to open the same port on the same reader at the same IP address.

To view the delete filter configuration settings in the SystemAgent, navigate to **Agent Configuration** ⊁ **SystemAgent** ⊁ **com.ibm.premises.SystemAgent** .

Delete filter configuration settings

The setting for the delete filter is configurable in the SystemAgent.
- To delete all configurations except for the bundle.loader and edge.config, and therefore to delete configurations for any additional third party agents such as readers, set the filter value to this:

```
(!(|(service.pid=com.ibm.rfid.bundle.loader)
(service.pid=com.ibm.rfid.edge.config)))
```

> **Note:** This option is the best filter to use unless there are configurations that should be saved. For IBM RFID agents, only the bundle.loader and edge.config configurations must be saved. If you are storing any additional settings in ConfigAdmin that should *not* be deleted, modify this filter or use a different one.

- To delete only the IBM RFID agent configurations (except for bundle.loader and edge.config) and to leave all other configurations in ConfigAdmin, set the filter value to this:

```
(&(service.pid=com.ibm.rfid*)
(!(|(service.pid=com.ibm.rfid.bundle.loader)(service.pid=com.ibm.rfid.edge.config))))
```

- To delete only IBM RFID agent configurations (except for bundle.loader and edge.config) and also to delete all configurations for `com.sirit*`, `com.intermec*`, `com.motorola.symbol*`, and `service.pid=com.alien*`, set the filter value to this:

```
(|(|(|(|(|(service.pid=com.sirit*)
(service.pid=com.intermec*))(service.pid=com.motorola.symbol*))(service.pid=com.alien*))
(service.pid=org.eclipse.soda.dk*))(&(service.pid=com.ibm.rfid*)
(!(|(service.pid=com.ibm.rfid.bundle.loader)(service.pid=com.ibm.rfid.edge.config)))))
```

Using the simulated reader

A simulated reader helps you to verify that the WebSphere Premises Server and related software, such as WebSphere MQ and DB2 for Linux, UNIX, and Windows, are correctly installed and configured.

Indicate how long you want the simulated reader to run by setting the `com.ibm.rfid.simulated.reader.timeout` property in the SystemAgent. For more information and instructions on how to verify that WebSphere Premises Server was correctly installed, refer to "Verifying the installation" on page 71.

This section contains the following topics:

Starting a simulated reader

This topic describes how to start a simulated reader using the WebSphere Premises Server Administrative Console.

Before you begin

Be sure that the property, `com.ibm.rfid.applping.shortcut`, in the SystemAgent is set to `true`. If you have to change the value to `true`, restart WebSphere Application Server before continuing.

About this task

Use the start function to begin the tag-reading process that verifies that all software is installed and configured correctly.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. In the left navigation panel, navigate to **Verification** ⊁ **Simulated Reader**. The Simulated Reader panel displays.
3. In the **Reader** field, click the drop-down arrow and select the simulated reader that you want to start.
4. Click **Start Reader**. The **Reader Status** icon displays the status of the simulated reader: reader status unknown, reader off, or reader on.

Stopping a simulated reader

This topic describes how to stop a simulated reader using the WebSphere Premises Server Administrative Console.

About this task

Use the stop function to end the tag-reading process of the simulated reader.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. In the left navigation panel, click **Verification** › **Simulated Reader**. The Simulated Reader panel displays.
3. In the **Reader** field, click the drop-down arrow and select the simulated reader that you are stopping.
4. Click **Stop Reader**. The **Reader Status** icon displays the status of the simulated reader: reader status unknown, reader off, or reader on.

Resetting a simulated reader

This topic describes how to reset a simulated reader using the WebSphere Premises Server Administrative Console.

About this task

Use the **Reset Reader** button to reset the WebSphere Premises Server Administrative Console when the reader does not respond to a start or stop request.

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. In the left navigation panel, click **Verification** › **Simulated Reader**. The Simulated Reader panel displays.
3. In the **Reader** field, click the drop-down arrow and select the simulated reader that you want to reset.
4. Click **Reset Reader**. The **Reader Status** icon displays the status of the simulated reader: reader status unknown, reader off, or reader on.

Running the simulated reader and simulated WebSphere Premises Server

This topic describes how to run the simulated reader and simulated WebSphere Premises Server.

About this task

Use these steps to run the simulated reader and simulated WebSphere Premises Server together on the same server.

1. If you have run previous versions of Data Capture and Delivery on the machine or if you encounter problems with MicroBroker connections, make sure you clear the MicroBroker and workspace directory from the directory where you are running the script. Only clear the workspace directory if you are *not* using the workspace (it will only contain a .metadata subdirectory).
2. Follow the steps in "Launching the Simulated Reader and simulated WebSphere Premises Server on the local system" on page 64.

What to do next

If you want to run only the simulated reader, follow the steps in "Launching the Simulated Reader and I/O Simulator interface while connecting to a remote WebSphere Premises Server or Premises Simulator" on page 64.

Chapter 5. Developing

This section describes the development environments and code provided with WebSphere Premises Server and how you can use them.

Toolkits

WebSphere Premises Server provides toolkits that help you develop a solution for your environment.

These toolkits are:

WebSphere Premises Server Toolkit
Enables developers to create and test custom WebSphere Premises Server applications and use cases in the Rational Application Developer for WebSphere Software. For more information on using this toolkit, see the documentation that is installed with the toolkit.

IBM Data Capture and Delivery Toolkit for WebSphere Premises Server
Enables developers to create OSGi bundles and test them on a workstation. It also helps developers deploy bundles to edge devices and WebSphere Premises Server and manage them. For more information on using this toolkit, see the documentation available on the toolkit CD.

For information on how to install these toolkits, see "Installing the toolkits" on page 61.

Predefined task agents

These agents process predefined events in WebSphere Premises Server. This topic lists the agent, its publish/subscribe topic, and the event that it processes.

Alert event
Topic name: ibmse/*/dccontroller/report/diagnostic/alert/*

Event process: Sends a heartbeat message to the event service and handles by the existing internal alert event handler.

Application ping event (from Data Capture and Delivery to WebSphere Premises Server)
Topic name: ibmse/*/dccontroller/command/diagnostic/applping

Event process: Sends the event to the outbound event agent. If `com.ibm.rfid.applping.shortcut=true`, then the application pong message goes to the event server. The default target destination is the DC.OUT.Q queue. If `com.ibm.rfid.applping.shortcut=false`, then the application ping message goes to the event server. The default target destination is the ENTERPRISE.OUT.Q queue.

Application pong event (from WebSphere Premises Server to Data Capture and Delivery)
Topic name: ibmse/*/dccontroller/command/diagnostic/applpong

Event process: Sends the application pong message to the outbound event agent.

Heartbeat event

> Topic name: ibmse/*/dccontroller/report/diagnostic/heartbeat

> Event process: Sends a heartbeat message to the event service and handles by the existing internal heartbeat event handler.

Line printer command event (for the WebSphere Premises Server Printing API event) Topic name: ibmse/*/RfidWrite/command/labelprint//*

> Event process: See the WebSphere Premises Server API documentation.

Line printer signal event (for the WebSphere Premises Server Printing API event) Topic name: ibmse/*/RfidWrite/signal/labelprint//*

> Event process: See the WebSphere Premises Server API documentation.

Persistence event

> Topic name: ibmse//*

> Event process: See "Filtering persisted events" on page 210 for more information.

Portal command event

> Topic name: ibmse/*/*/command/portalcontrol/activation

> Event process: Converts a portal alias to a portal and sends the event to the outbound event agent. The default target destination is the DC.OUT.Q queue.

Portal report event

> Topic name: ibmse/*/*/report/portal

> Event process: Converts a portal id to a portal alias and sends the event to the outbound event agent. The default target destination is the ENTERPRISE.OUT.Q queue.

Outbound event

> Topic name: ibmse/*/outbound

> Event process: Sends the event message to the outbound channel of the event server.

System command event

> Topic name: ibmse/*/dccontroller/command/system/*

> Event process: Sends the event to the outbound event agent. The default target destination is the DC.OUT.Q queue.

Tag aggregation event

> Topic name: ibmse//RfidInventory/TagAggregationReport

> Event process: Converts a portal alias to a portal id and sends the event to the outbound event agent. The default target destination is the ENTERPRISE.OUT.Q queue.

Tag feedback event

> Topic name: ibmse//report/tag/feedback

> Event process: Converts a portal alias to a portal id and sends the event to the outbound event agent. The default target destination is the DC.OUT.Q queue.

Tag read event

> Topic name: ibmse//RfidInventory/TagReport

If it is raw tag read, then the topic is ibmse/*deviceId*/RfidInventory/
TagReport.

If it is tag read, the topic is ibmse/*portId*/*applicationId*/RfidInventory/
TagReport.

Event process: Converts a portal alias to a portal id and sends the event to
the outbound event agent. The default target destination is the
ENTERPRISE.OUT.Q queue.

IBM Sensor Event

The IBM Sensor Event is the event format used by WebSphere Premises Server.

A sensor event is an event detected by a sensor device and reported.

The IBM Sensor Event (IBMSensorEvent class) has three sections:
- **Header** - contains information about the who, what, and where of an event
- **Payload metadata** - provides a way for users to pass data about the payload
  (additional data about the event)
- **Payload** - contains the actual data that was captured from the sensor device
  (event data)

See the Example event format in the WebSphere Premises Server Toolkit
documentation for an example of this event format.

Sensor event gateway

The sensor event gateway is the entry point to publishing sensor events to the
WebSphere Application Server service integration bus (SIBus), ibmsensorevent.

The sensor event gateway provides two WebSphere MQ event handlers to process
events in DC.IN.Q and ENTERPRISE.IN.Q, and two event handlers that process
events that come into the SIBus queues, Dc.In.Bus.Queue and
Enterprise.In.Bus.Queue.

The sensor event gateway also provides servlet and Web services interfaces for you
to write and send your own events using HTTP servlet or Web services protocols
from any device or programming language to publish your defined events to the
SIBus through the sensor event gateway.

Each of these entry points converts the sensor event XML to an ibmsensorevent
object to send to the SIBus. All events in the ibmsensorevent SIBus are
ibmsensorevent objects.

You can publish events to the sensor event gateway one of five ways:
- Write an OSGi agent and install it on the Data Capture and Delivery controller.
- Write MQ JMS code to send to the DC.IN.Q queue.
- Write Java code to HTTP GET or POST to send to the event gateway servlet.
- Write a Web service by using the event gateway Web Services Description
  Language (WSDL) file.
- Generate ECReports XML using the ALE ECReports Servlet.

Event gateway servlet

The event gateway servlet is only for sensor events *upstream* to WebSphere Premises Server.

If you want to send events *downstream* to Data Capture and Delivery, use the WebSphere Premises Server application program interface (API). For more information on using the APIs, refer to the WebSphere Premises Server API documentation.

Event gateway servlet code:

```
HTTP Get
http://premises_host:premises_port/ibmse/eventpublish?eventtype=
eventtype&eventtopic=topicname&eventxml=eventstring
HTTP Post
Form Action: /ibmse/eventpublish
Parameter: eventtype
Parameter: eventtopic
Parameter: eventxml
```

Response if the event XML is null:

```
SC_BAD_REQUEST (400) and no message body.
```

Response if the event XML is not sensor event XML:

```
SC_OK (200) and message body is "Can not convert event xml to sensor event object.
Publish to deadletter topic".
```

Response if the event XML is sensor event XML:

```
SC_OK (200) and message body is "Publish event to topic topic_name"
```

Example of a Java client using the event gateway servlet

```
/*********************************************************************************
 * Licensed Materials - Property of IBM
 * 5724-L17 WebSphere Premises Server
 * (c) Copyright IBM Corp. 2008  All rights reserved.
 *
 * US Government Users Restricted Rights - Use, duplication or disclosure
 * restricted by GSA ADP Schedule Contract with IBM Corp.
 *
 * DISCLAIMER OF WARRANTIES.  The following code is sample code created by
 * IBM Corporation.  This sample code is part of the WebSphere Premises Server
 * and is warranted to perform its intended function only if used un-modified.
 * If you modify this code then it is considered provided "AS IS", without
 * warranty of any kind.  Notwithstanding the foregoing, IBM shall not be liable
 * for any damages arising out of your use of the sample code, even if they have
 * been advised of the possibility of such damages.
 *********************************************************************************/

package com.ibm.sensorevent.servlet.simulator;

import com.ibm.sensorevent.model.ISensorEvent;
import com.ibm.sensorevent.model.IBMSensorEvent;
import com.ibm.sensorevent.model.converter.CBEConverter;
import com.ibm.sensorevent.model.payload.*;
import java.net.HttpURLConnection;
import java.net.URL;
import java.net.URLEncoder;
import java.io.BufferedReader;
import java.io.InputStreamReader;
import java.io.DataOutputStream;

public class ApplicationPingEventServletClientTester {
 private final static String urlString = "http://localhost:9080/ibmse/eventpublish";
 public final static String CONTENT_TYPE_FORM = "application/x-www-form-urlencoded";
 public final static String CONTENT_TYPE_XML = "text/xml";

 public static void main(String args[]) {
  try {
   ISensorEvent ise = IBMSensorEvent.getApplicationPingInstance();
   ise.getHeader().setSourceId("E2");
   ApplicationPingPayload payload = (ApplicationPingPayload) ise.getPayload();
   payload.setValue("1,Edge_EdgeName1 (E1)-2007-10-17T0:56:49.176");
   System.out.println(ise);
   System.out.println();
```

```
        CBEConverter converter = CBEConverter.getInstance();
        String xml = converter.toXMLString(ise);

        URL url = new URL(urlString);
        HttpURLConnection connection = (HttpURLConnection) url.openConnection();
        connection.setRequestMethod("POST");
        connection.setRequestProperty("Content-Type", CONTENT_TYPE_FORM);
        connection.setUseCaches(false);
        connection.setDoInput(true);
        connection.setDoOutput(true);
        connection.connect();

        StringBuffer data = new StringBuffer();
        data.append("eventXml=" + URLEncoder.encode(xml, "UTF-8"));
        DataOutputStream dos = new DataOutputStream(connection.getOutputStream());
            dos.writeBytes(data.toString());
        dos.flush();
        dos.close();

        System.out.println("result code: " + connection.getResponseCode() + " " + connection.getResponseMessage() );
        if (connection.getResponseCode() == 200) {
          InputStreamReader in = new InputStreamReader(connection.getInputStream());
          BufferedReader dis = new BufferedReader(in);
          System.out.println("result: " + dis.readLine());
        }
      } catch (Exception e) {
        e.printStackTrace();
      }
    }
  }
}
```

Gateway Web service

WebSphere Premises Server provides a gateway Web services interface for you to
write and send events.

To avoid overloading, two methods for the gateway Web service are provided:

```
public int publish ( string sensoreventXML );
public int sensoreventpublish (string eventType , string eventTopic ,string sensoreventXML );
```

Return codes:

```
0: success
-1: failure
-2: deadletter
```

Web service endpoint: http://localhost:*port*/ibmse/services/EventPublish

Web service WSDL: http://localhost:*port*//ibmse/services/EventPublish?wsdl

Example of the gateway Web service WSDL

```
/*******************************************************************************
 * Licensed Materials - Property of IBM
 * 5724-L17 WebSphere Premises Server
 * (c) Copyright IBM Corp. 2008  All rights reserved.
 *
 * US Government Users Restricted Rights - Use, duplication or disclosure
 * restricted by GSA ADP Schedule Contract with IBM Corp.
 *
 * DISCLAIMER OF WARRANTIES.  The following code is sample code created by
 * IBM Corporation.  This sample code is part of the WebSphere Premises Server
 * and is warranted to perform its intended function only if used un-modified.
 * If you modify this code then it is considered provided "AS IS", without
 * warranty of any kind.  Notwithstanding the foregoing, IBM shall not be liable
 * for any damages arising out of your use of the sample code, even if they have
 * been advised of the possibility of such damages.
 *******************************************************************************/
package com.ibm.sensorevent.ws.simulator;

import java.io.Serializable;

import javax.xml.namespace.QName;
import javax.xml.rpc.Service;
import javax.xml.rpc.ServiceFactory;
import javax.xml.rpc.Call;
import javax.xml.rpc.encoding.XMLType;
import javax.xml.rpc.ParameterMode;

import com.ibm.sensorevent.model.IBMSensorEvent;
import com.ibm.sensorevent.model.ISensorEvent;
import com.ibm.sensorevent.model.converter.CBEConverter;
```

```
import com.ibm.sensorevent.model.payload.PortalReportPayload;

public class publishClient  implements Serializable {
 private static final long serialVersionUID = 0L;
 public static String wsdlURL="http://localhost:9080/ibmse/services/EventPublish?wsdl";
 public static String endpoint="http://localhost:9080/ibmse/services/EventPublish";

 public publishClient(){
  super();
 }

 public String createSensorEvent() {
  String xml = null;
  try {
   ISensorEvent ise = IBMSensorEvent.getPortalReportInstance("EDDR/report/portal");
   ise.getHeader().setSourceId("P2");

   PortalReportPayload payload = (PortalReportPayload) ise.getPayload();
   payload.setValue("ON");

   System.out.println(ise);
   System.out.println();
   CBEConverter converter = CBEConverter.getInstance();
   xml = converter.toXMLString(ise);
  } catch (Exception e) {
   e.printStackTrace();
  }

  return xml;

 }

 public void DIIPublish(String xml) {
  try{
   // publish to sensor event web service
         // Define the service.

         QName serviceName = new QName("http://gateway.sensorevent.ibm.com","EventPublishService");
         Service service = ServiceFactory.newInstance().createService(serviceName);
         Call call = (Call) service.createCall();
         call.setProperty(Call.ENCODINGSTYLE_URI_PROPERTY, "");
         call.setProperty(Call.OPERATION_STYLE_PROPERTY, "wrapped");
         call.setTargetEndpointAddress(endpoint);
         call.removeAllParameters();
         QName portName = new QName("http://gateway.sensorevent.ibm.com","EventPublish");
         call.setPortTypeName(portName);
         QName operationName = new QName("http://gateway.sensorevent.ibm.com", "publish");
         call.setOperationName(operationName);
         call.addParameter(
                 "sensoreventXML",   // parameter name
                 XMLType.XSD_STRING, // parameter XML type QName
                 String.class,       // parameter Java type class
                 ParameterMode.IN);  // parameter mode
         call.setReturnType(XMLType.XSD_STRING);
         Object[] args = { xml };
         System.out.println("response = " + (String) call.invoke(args));
  } catch (Exception e) {
   e.printStackTrace();
  }
 }

 public static void main(String[] args) {
  publishClient client = new publishClient();
  String eventxml = client.createSensorEvent();
  client.DIIPublish(eventxml);
 }
}
```

Example of a Java client using the gateway Web service

```
/*
 * IBM Confidential OCO Source Material
 * (C) COPYRIGHT International Business Machines Corp., 2007.
 * The source code for this program is not published or otherwise divested
 * of its trade secrets, irrespective of what has been deposited with the
 * U. S. Copyright Office.
 */
package com.ibm.sensorevent.ws.simulator;

import java.io.Serializable;

import javax.xml.namespace.QName;
import javax.xml.rpc.Service;
import javax.xml.rpc.ServiceFactory;
import javax.xml.rpc.Call;
import javax.xml.rpc.encoding.XMLType;
import javax.xml.rpc.ParameterMode;

import com.ibm.sensorevent.model.IBMSensorEvent;
import com.ibm.sensorevent.model.ISensorEvent;
```

```java
import com.ibm.sensorevent.model.converter.CBEConverter;
import com.ibm.sensorevent.model.payload.PortalReportPayload;

public class publishClient  implements Serializable {

 private static final long serialVersionUID = 0L;
 public static String wsdlURL="http://localhost:9082/ibmse/services/EventPublish?wsdl";
 public static String endpoint="http://localhost:9082/ibmse/services/EventPublish";
/**
 * @param args
 */
 public publishClient(){
  super();
 }

 public String createSensorEvent (){
  String xml = null;
  try{

   ISensorEvent ise = IBMSensorEvent.getPortalReportInstance("EDDR/report/portal");

   ise.getHeader().setAssetId("ASSED_ID_VALUE");
   //ise.getHeader().setEventType("EDDR/report/portal");
   ise.getHeader().setGeoLocation("GEO_LOCATION_VALUE");
   ise.getHeader().setOriginatingEventId("ORIGINATING_EVENT_ID_VALUE");
   ise.getHeader().setPriority((short) 75);
   ise.getHeader().setSourceId("P2");
   //ise.getHeader().setTargetId("PremisesServer");
   ise.getHeader().setDateTime(System.currentTimeMillis());

   PortalReportPayload payload = (PortalReportPayload) ise.getPayload();
   payload.setValue("ON");

   System.out.println(ise);
   System.out.println();
   CBEConverter converter = CBEConverter.getInstance();
   xml = converter.toXMLString(ise);
   //System.out.println(xml);

  } catch ( Exception e){
        //System.out.println("exception = " + e.getMessage());
   e.printStackTrace();
  }

  return xml;

 }

 public void DIIPublish(String xml){
  try{
   // publish to sensor event web service
         // Define the service.

          QName serviceName = new QName("http://gateway.sensorevent.ibm.com","EventPublishService");
          Service service = ServiceFactory.newInstance().createService(serviceName);
          Call call = (Call) service.createCall();
          call.setProperty(Call.ENCODINGSTYLE_URI_PROPERTY, "");
          call.setProperty(Call.OPERATION_STYLE_PROPERTY, "wrapped");
          call.setTargetEndpointAddress(endpoint);
          call.removeAllParameters();
          QName portName = new QName("http://gateway.sensorevent.ibm.com","EventPublish");
          call.setPortTypeName(portName);
          QName operationName = new QName("http://gateway.sensorevent.ibm.com", "publish");
          call.setOperationName(operationName);
          call.addParameter(
                  "sensoreventXML",   // parameter name
                  XMLType.XSD_STRING, // parameter XML type QName
                  String.class,       // parameter Java type class
                  ParameterMode.IN);  // parameter mode
          call.setReturnType(XMLType.XSD_STRING);
          Object[] args = { xml };
          System.out.println("response = " + (String) call.invoke(args));

  } catch ( Exception e){
        //System.out.println("exception = " + e.getMessage());
   e.printStackTrace();
  }


 }


 public static void main(String[] args) {
  publishClient client = new publishClient();
  String eventxml = client.createSensorEvent();
  client.DIIPublish(eventxml);
 }

}
```

Event handlers

The sensor event gateway provides four event handlers to process events.

- A WebSphere MQ input handler for the DC.IN.Q queue. It converts sensor event XML strings to ibmsensorevent objects to send to the SIBus.
- A WebSphere MQ input handler for the ENTERPRISE.IN.Q queue. It converts sensor event XML strings to ibmsensorevent objects to send to the SIBus.
- An input handler for the Dc.In.Bus.Queue for processing events that come onto this SIBus queue.
- An input handler for the Enterprise.In.Bus.Queue for processing events that come onto this SIBus queue.

The queues that are predefined on the SIBus can be used to integrate third party or user applications with the WebSphere Premises Server generated events. The third party or user application can reside on the same WebSphere Application Server as the WebSphere Premises Server or on another WebSphere Application Server that is a member of the ibmsensorevent SIBus.

ALE 1.1 ECReports servlet

The ECReports servlet is installed with WebSphere Premises Server and allows ALE 1.1 implementations to send ECReports to the sensor event gateway. The servlet accepts XML as input and converts it into an IBMSensorEvent that is then placed on the SIBus.

ECReports are sent to the servlet using the POST method in the body of the HTTP request that is called by the ALE 1.1 implementation. The corresponding IBMSensorEvents are published by the servlet to the SIBus with the topic ibmse/EDDR/report/TagAggregationReport.

The ECReports servlet can also be used to get ALE events from Data Capture and Delivery to WebSphere Premises Server ALE.

Notes:

- Use unique tag names in the ECReport. If a tag name is duplicated in an ECReport, only the last statistic in the report that corresponds to that tag will be saved.
- There is no one-to-one mapping for ECReport to IBMSensorEvent. Data that is present in the ECReport may not have a corresponding place in the IBMSensorEvent. This information is placed in the payload metadata as key/value pairs.
- If the same tag is read by multiple readers, the tag read will have multiple sets of statistics. Only the last occurrence of a statistic for the tag read of any key is captured in the metadata; all previous duplicate statistics will be overwritten. For example, lastsightingtime appears several times in the sample ECReport, but only the last occurrence would be saved in the payload metadata.

Accessing the servlet

The servlet is installed with WebSphere Premises Server. To access the servlet, enter the following URL into a browser: http://*localhost*:9080/ibmse/ECReport.

Working with the ECReports servlet

This topic includes an example of an ECReport XML received by the servlet to create an IBMSensorEvent, and an example of the corresponding IBMSensorEvent.

The following is an example of the ECReport XML that is sent to the servlet from an ALE 1.1 implementation.

```xml
<?xml version="1.0"?>
<ECReports xmlns="urn:epcglobal:ale:xsd:1" schemaVersion="1.1"
   creationDate="2008-02-19T10:54:06.444-05:00" specName="ECSpec1"
   date="2008-02-19T10:54:06.444-05:00" ALEID="ALEID_1"
   totalMilliseconds="5000" terminationCondition="DURATION">
   <reports>
      <report reportName="ReportName1">
         <group>
            <groupList>
               <member>
                  <tag>
                     urn:epc:tag:sgtin-96:3.0037000.006542.773346595
                  </tag>
                  <extension>
                     <fieldList>
                        <field>
                           <name>quantity</name>
                           <value>10</value>
                           <fieldspec>
                              <fieldname>03.0.32</fieldname>
                              <datatype>uint</datatype>
                              <format>decimal</format>
                           </fieldspec>
                        </field>
                     </fieldList>
                     <stats>
                        <stat>
                           <profile>TagTimestamps</profile>
                           <firstSightingTime>
                              2008-02-19T10:54:06.444-05:00
                           </firstSightingTime>
                           <lastSightingTime>
                              2008-02-19T10:54:06.455-05:00
                           </lastSightingTime>
                        </stat>
                        <stat>
                           <profile>IBMTagTimestamps</profile>
                           <statBlocks>
                              <statBlock>
                                 <readerName>R1</readerName>
                                 <firstSightingTime>
                                    2008-02-19T10:54:06.444-05:00
                                 </firstSightingTime>
                                 <lastSightingTime>
                                    2008-02-19T10:54:06.455-05:00
                                 </lastSightingTime>
                              </statBlock>
                              <statBlock>
                                 <readerName>R2</readerName>
                                 <firstSightingTime>
                                    2008-02-19T10:54:06.444-05:00
                                 </firstSightingTime>
                                 <lastSightingTime>
                                    2008-02-19T10:54:06.455-05:00
                                 </lastSightingTime>
                              </statBlock>
                           </statBlocks>
                           <firstSightingTime>
                              2008-02-19T10:54:06.444-05:00
                           </firstSightingTime>
                           <lastSightingTime>
                              2008-02-19T10:54:06.455-05:00
                           </lastSightingTime>
                        </stat>
                        <stat>
                           <profile>IBMTagCounts</profile>
                           <statBlocks>
                              <statBlock>
                                 <readerName>R1</readerName>
                                 <count>10</count>
                              </statBlock>
                              <statBlock>
                                 <readerName>R2</readerName>
                                 <count>6</count>
                              </statBlock>
                           </statBlocks>
                           <count>2</count>
                        </stat>
                        <stat>
```

```
                              <profile>IBMTagAntennas</profile>
                              <statBlocks>
                                 <statBlock>
                                    <readerName>R1</readerName>
                                    <antennas>
                                       <antenna>0</antenna>
                                       <antenna>1</antenna>
                                    </antennas>
                                 </statBlock>
                                 <statBlock>
                                    <readerName>R2</readerName>
                                    <antennas>
                                       <antenna>1</antenna>
                                    </antennas>
                                 </statBlock>
                              </statBlocks>
                           </stat>
                           <stat>
                              <profile>IBMReaderNames</profile>
                              <statBlocks>
                                 <statBlock>
                                    <readerName>R1</readerName>
                                 </statBlock>
                                 <statBlock>
                                    <readerName>R2</readerName>
                                 </statBlock>
                              </statBlocks>
                           </stat>
                        </stats>
                     </extension>
                  </member>
               </groupList>
               <groupCount>
                  <count>1</count>
               </groupCount>
            </group>
         </report>
         <report reportName="ReportName2" />
      </reports>
   <ECSpec creationDate="2008-02-19T10:54:06.444-05:00"
      schemaVersion="1.1">
      <logicalReaders>
         <logicalReader>R1</logicalReader>
      </logicalReaders>
      <boundarySpec>
         <repeatPeriod unit="MS">10000</repeatPeriod>
         <duration unit="MS">5000</duration>
      </boundarySpec>
      <reportSpecs>
         <reportSpec reportName="ReportName1">
            <reportSet set="CURRENT" />
            <output includeTag="true" includeCount="true" />
         </reportSpec>
      </reportSpecs>
   </ECSpec>
</ECReports>
```

The following is an example of the IBMSensorEvent generated using the ECReports sample above.

```
version: 6.1
name: ibmse_header
      attributes: {
      name: sourceId, value: ALEID_1, type: 18
      name: eventType, value: EDDR/report/TaggregationReport, type: 18
      name: priority, value: 70, type: 16
      name: dateTime, value: 2008-07-03T10:12:35.015Z, type: 5
      name: eventId, value: IBMSensorEvent_8c77d029-276b-418a-88e4-a64662905dc7, type: 18}
      groups: {
      name: sourceComponent
            attributes: {
            name: componentType, value: none, type: 18
            name: locationType, value: Unknown, type: 18
            name: componentIdType, value: Application, type: 18
            name: location, value: none, type: 18
            name: subComponent, value: none, type: 18
            name: component, value: none, type: 18
            name: application, value: IBM WebSphere Premises Server, type: 18}
            groups: {}}
name: ibmse_payloadMetaData
      attributes: {
      name: lastSightingTime, value: 2008-02-19T23:54:06.455+08:00, type: 18
      name: antennas, value: 1, type: 18
      name: CreationDate, value: 2008-02-19T23:54:06.444+08:00, type: 18
      name: reportnames, value: ReportName1, ReportName2, , type: 18
      name: count, value: 6, type: 18
      name: firstSightingTime, value: 2008-02-19T23:54:06.444+08:00, type: 18}
      groups: {}
name: ibmse_payload
```

```
        attributes: {
        name: AGGCOUNT, value: 1, type: 12}
        groups: {
        name: EDDR/report/TaggregationReport
              attributes: {}
              groups: {
              name: tagread_1
                    attributes: {
                    name: ANTENNA, value: 1, type: 12
                    name: DISCOVERED, value: 2008-07-03T10:12:35.031Z, type: 5
                    name: COUNT, value: 2, type: 12
                    name: reader, value: R1, type: 18}
                    groups: {
                    name: tag
                          attributes: {
                          name: rawuri, value: urn:epc:raw:96.x30740242200663802E185523, type: 18
                          name: taguri, value: urn:epc:tag:sgtin-96:3.0037000.006542.773346595, type: 18
                          name: iduri, value: urn:epc:id:sgtin:0037000.006542.773346595, type: 18
                          name: tagid, value: 30740242200663802E185523, type: 18}
                          groups: {}}}}
payloadClassName: com.ibm.sensorevent.model.payload.PassiveRFIDAggregatedTagReadPayload
```

WebSphere Premises Server API

The WebSphere Premises Server application program interface (API) enables customers to create custom applications that interface with a WebSphere Premises Server. Use the WebSphere Premises Server Toolkit to create applications using the WebSphere Premises Server API.

The APIs provide access to a wide range of WebSphere Premises Server information, and can be applied to a wide variety of usage scenarios. WebSphere Premises Server ships a working example of one such scenario, the Print, Verify, and Ship Reference User Interface. The Print, Verify, and Ship Reference User Interface demonstrates a scenario for printing tags, verifying tags that are affixed to containers, and then registering the shipment of those containers. The Print, Verify, and Ship Reference User Interface is a working example of a J2EE servlet and JSP application that makes numerous calls to the WebSphere Premises Server API.

You can use the WebSphere Premises Server API to communicate with the WebSphere Premises Server Application Level Events (ALE) engine using Simple Object Access Protocol (SOAP) calls. You can also use the WebSphere Premises Server API to communicate with any Electronic Product Code Information System (EPCIS) by creating and sending Object and Aggregate Events.

You can also use the API to develop a new print profile for WebSphere Premises Server to use. For more information on using print profiles, refer to "Print profile support" on page 199.

The WebSphere Premises Server API enables the following read-only queries:
- Get details on devices.
- Get device status.
- Get device types.
- Get pack types.
- Get supply chain profiles.
- Get device print job details.
- Get location details.
- Get controller details.

The WebSphere Premises Server API enables the following basic commands:
- Start or stop tag readers.

- Control the light tree through reject or accept commands.
- Submit a print job.

You can run Java APIs both remotely (different WebSphere Application Server) and locally (using the same WebSphere Application Server as WebSphere Premises Server).

For more information about the WebSphere Premises Server Java API, refer to the WebSphere Premises Server API documentation.

Note: The WebSphere Premises Server API requires Java 1.5. You must use Java version 1.5 to program applications using the WebSphere Premises Server API. You can use the WebSphere Premises Server API to program many types of applications including J2EE applications, portlets, and standalone Java applications.

Integrating an enterprise system using APIs

The Enterprise Business Logic application submits events to the WebSphere Premises Server using WebSphere Premises Server API and IBM Sensor Events.

Following are some of the inbound events to the WebSphere Premises Server:

Portal ON/OFF
> WebSphere Premises Server API can be used to submit this event to the WebSphere Premises Server.

Portal (Location) ON

> To get premisesaccess object in the case of WebSphere Premises Server is local to the Enterprise Business Logic (EBL).

> `PremisesAccess premisesAccess = PremisesContext.getPremisesAccess();`

> To get premisesaccess object in the case of WebSphere Premises Server is remote to the EBL.

> `PremisesAccess premisesAccess = PremisesContext.getPremisesAccess(<Server Name>)`

> To Send Start Portal (Location)

> `premisesAccess.startLocation(locationid);`

Portal (Location) OFF

> To get premisesaccess object in the case of WebSphere Premises Server is local to the EBL.

> `PremisesAccess premisesAccess = PremisesContext.getPremisesAccess();`

> To get premisesaccess object in the case of WebSphere Premises Server is remote to the EBL.

> `PremisesAccess premisesAccess = PremisesContext.getPremisesAccess(<Server Name>)`

> To Send Start Portal (Location)

> `premisesAccess.stopLocation(locationid);`

Accept/Reject
> Server API can be used to submit this event to the WebSphere Premises Server.

Send Accept Message to Light Tree Agent

> To get premisesaccess object in the case of WebSphere Premises Server is local to the EBL.

```
            PremisesAccess premisesAccess = PremisesContext.getPremisesAccess();
```

To get premisesaccess object in the case of WebSphere Premises Server is remote to the EBL.

```
            PremisesAccess premisesAccess = PremisesContext.getPremisesAccess(<Server Name>)
```

To Send Start Portal (Location)

```
            premisesAccess. sendAcceptToLightStack (locationid);
```

Send Reject Message to Light Tree Agent

To get premisesaccess object in the case of WebSphere Premises Server is local to the EBL.

```
            PremisesAccess premisesAccess = PremisesContext.getPremisesAccess();
```

To get premisesaccess object in the case of WebSphere Premises Server is remote to the EBL. PremisesAccess premisesAccess = PremisesContext.getPremisesAccess(<Server Name>)

To Send Start Portal (Location)

```
            premisesAccess. sendRejectToLightStack (locationid);
```

Sample

In order to process Application Ping and send ApplPong to Data Capture and Delivery, you need to develop new MDB. The following is a sample of MDB code. The sample requires *IBM_RFID_HOME*\RFID\premises\api\lib\ ibmse_event_model.jar and *IBM_RFID_HOME*\RFID\premises\api\lib\ ibmse_event_model_uuid.jar as J2EE Module Dependencies.

```java
/***********************************************************************************
 * Licensed Materials - Property of IBM
 * 5724-L17 WebSphere Premises Server
 * (c) Copyright IBM Corp. 2008  All rights reserved.
 *
 * US Government Users Restricted Rights - Use, duplication or disclosure
 * restricted by GSA ADP Schedule Contract with IBM Corp.
 *
 * DISCLAIMER OF WARRANTIES.  The following code is sample code created by
 * IBM Corporation.  This sample code is part of the WebSphere Premises Server
 * and is warranted to perform its intended function only if used un-modified.
 * If you modify this code then it is considered provided "AS IS", without
 * warranty of any kind.  Notwithstanding the foregoing, IBM shall not be liable
 * for any damages arising out of your use of the sample code, even if they have
 * been advised of the possibility of such damages.
 ***********************************************************************************/

import java.text.SimpleDateFormat;
import java.util.Date;
import java.util.Hashtable;

import javax.jms.JMSException;
import javax.jms.Queue;
import javax.jms.QueueConnection;
import javax.jms.QueueConnectionFactory;
import javax.jms.QueueSender;
import javax.jms.QueueSession;
import javax.jms.TextMessage;
import javax.naming.InitialContext;
import javax.naming.NamingException;

import com.ibm.sensorevent.model.IBMSensorEvent;
import com.ibm.sensorevent.model.IConstants;
import com.ibm.sensorevent.model.ISensorEvent;
import com.ibm.sensorevent.model.converter.XMLConverter;
import com.ibm.sensorevent.model.generic.SensorEventException;
import com.ibm.sensorevent.model.payload.ApplicationPongPayload;

/**
 * Bean implementation class for Enterprise Bean: SimulatedBusBackEnd
 */
public class SimulatedBusBackEndBean implements javax.ejb.MessageDrivenBean,javax.jms.MessageListener {

 private static final long serialVersionUID = 6285653378773758308L;
 private javax.ejb.MessageDrivenContext fMessageDrivenCtx;

 private static final String VALUE = "value";
```

```
private static final String RESPONSE_QUEUE_NAME = "ENTERPRISE.IN.Q";
private static final String RESPONSE_VALUE = "REJECTED";
private static final String RESPONSE_PARAMETER = "IBMSE_EBL_TEST_RESPONSE";
private static final String TAG_REPORT = "TagReport";
private static final String TAG_AGGREGATION_REPORT = "TagAggregationReport";
private static final String TAG_FEEDBACK_EVENT_TYPE_SUFFIX = "/report/tag/feedback";
private static final String APP_PONG_EVENT_TYPE_SUFFIX = "/dccontroller/report/diagnostic/applpong";
private static final String APP_PING = "applping";

private static final String CLASS_NAME = "com.ibmse.ebl.test.SimulatedBusBackEndBean";
private Logger logger = Logger.getLogger(CLASS_NAME);


protected InitialContext context;
private static Hashtable<String,Object> jndiObjects ;
private static final String QCF_JNDI_NAME="jms/ibmsensoreventQCF";
private static final String Queue_JNDI_NAME="jms/enterprise.in.bus.q";
/**
 * getMessageDrivenContext
 */
public javax.ejb.MessageDrivenContext getMessageDrivenContext() {
 return fMessageDrivenCtx;
}

/**
 * setMessageDrivenContext
 */
public void setMessageDrivenContext(javax.ejb.MessageDrivenContext ctx) {
 fMessageDrivenCtx = ctx;
}

/**
 * ejbCreate
 */
public void ejbCreate() {
}

/**
 * onMessage
 */
public void onMessage(javax.jms.Message msg) {
 String incomingXML;
 try {
  incomingXML = ((TextMessage) msg).getText();
  if (logger.isLoggable(Level.FINE))
   logger.fine("received message XML: "+incomingXML);

  // Investigate incoming message
  XMLConverter converter = (XMLConverter)XMLConverter.getInstance();
  ISensorEvent fromPremISE = converter.toIBMSensorEvent(incomingXML);

  // Process EventType
  String originatingEventType = fromPremISE.getHeader().getEventType();
  if(originatingEventType.indexOf(APP_PING)!=-1) {
   sendApplicationPong(fromPremISE);
  }

 } catch (JMSException e) {
  e.printStackTrace();
 } catch (SensorEventException e) {
  e.printStackTrace();
 }
}

/**
 * ejbRemove
 */
public void ejbRemove() {
}

/**
 * sendApplicationPong
 * @param fromPremISE
 */
public void sendApplicationPong(ISensorEvent fromPremISE) {

 try {
  String originatingEventId = fromPremISE.getHeader().getEventId();

  // Create response XML
  ISensorEvent responseISE = IBMSensorEvent.getApplicationPongInstance(APP_PONG_EVENT_TYPE_SUFFIX);
  responseISE.getHeader().setAssetId(fromPremISE.getHeader().getAssetId());
  responseISE.getHeader().setGeoLocation(fromPremISE.getHeader().getGeoLocation());
  responseISE.getHeader().setOriginatingEventId(originatingEventId);
  responseISE.getHeader().setPriority(IConstants.PRIORITY_DEFAULT);
  responseISE.getHeader().setSourceId(fromPremISE.getHeader().getTargetId());
  responseISE.getHeader().setTargetId(fromPremISE.getHeader().getSourceId());

  ApplicationPongPayload newpayload = (ApplicationPongPayload) responseISE.getPayload();
  String eventType = fromPremISE.getHeader().getEventType();
  String pingValue = fromPremISE.getPayload().getGroup(eventType).getStringAttributeValue(VALUE);
```

```
      newpayload.setValue(pingValue + getApplicationPingEntry());

      XMLConverter converter = (XMLConverter)XMLConverter.getInstance();
      String responseXML = converter.toXMLString(responseISE);
      if (logger.isLoggable(Level.FINE))
       logger.fine("response XML: "+responseXML);

      // Send response XML
      // MQHelper.send(RESPONSE_QUEUE_NAME, responseXML);
      send(responseXML);
     } catch (SensorEventException e) {
      e.printStackTrace();
     }
     if (logger.isLoggable(Level.FINE))
      logger.exiting(CLASS_NAME, "sendApplicationPong");
   }

   /**
    * getApplicationPingEntry
    * @return
    */
   private String getApplicationPingEntry(){
    String entry= ", Premises";
    SimpleDateFormat formatter = new SimpleDateFormat("yyyy-MM-dd'T'HH:mm:ss.SSS");
    String dateTime = formatter.format(new Date());
    entry+= "-" + dateTime;
    return entry;
   }

   private void send(String msg){
    QueueConnection queueConnection = null;
    QueueSession queueSession = null;
    QueueSender queueSender = null;

    try{
     QueueConnectionFactory connectionFactory =
       (QueueConnectionFactory)getRemoteObject(QCF_JNDI_NAME);

     Queue queue =
       (Queue)getRemoteObject(Queue_JNDI_NAME);

     queueConnection = connectionFactory.createQueueConnection();

     queueSession =
      queueConnection.createQueueSession(false,QueueSession.AUTO_ACKNOWLEDGE);

     queueSender =
      queueSession.createSender(queue);

     TextMessage message = queueSession.createTextMessage(msg);
     queueConnection.start();
     queueSender.send(message);
    } catch(Exception e ) {
     e.printStackTrace();

    } finally {
     if(queueSender != null)
     {
      try { queueSender.close(); }
      catch(Exception e) { }
     }
     if(queueConnection != null)
     {
      try { queueSession.close(); }
      catch(Exception e) { }
     }
     if(queueConnection != null)
     {
      try { queueConnection.close(); }
      catch(Exception e) { }
     }
    }
   }

   protected Object getRemoteObject(String ejbRef) throws Exception
   {
    synchronized (this) {
     if (jndiObjects == null) {
      jndiObjects = new Hashtable<String,Object>();
     }
    }

    synchronized (jndiObjects) {
     if (jndiObjects.containsKey(ejbRef)) {
      return jndiObjects.get(ejbRef);
     }
    }

    Object obj = null;
    synchronized (jndiObjects) {
     // defect 146354
```

```
  try {
   obj = getInitialContext().lookup("java:comp/env/" + ejbRef);
  } catch(Exception e) {
   obj = getInitialContext().lookup(ejbRef);
  }
  //obj = getInitialContext().lookup(ejbRef);
  jndiObjects.put(ejbRef, obj);
 }
 return obj;
}

protected synchronized InitialContext getInitialContext() throws NamingException
{
 if(context == null)
 {
  context = new InitialContext();
 }
 return context;
}
}
```

Modifying the EJB deployment descriptor

After creating the message-driven beans (MDBs), modify the EJB deployment
descriptor.

Before you begin

Create the MDBs.

1. Go to the EJB Project.
2. Click **Deployment Descriptor**.
3. Select **Bean**.
4. Select **MDB Bean**.
5. Select **JCA Adapter section**.
6. Enter the following values:
   a. ActivationSpec JNDI: eis/EnterpriseOutBusAS
   b. Destination JNDI Name: jms/enterprise.out.bus.q
7. Save your changes.

Chapter 6. Tuning

Use these topics to adjust the configuration and improve the performance of the WebSphere Premises Server infrastructure and components.

Changing MQ settings to improve performance

Modify these MQ settings to improve your performance.

1. Change the enterpriseOutputListener and enterpriseInputListener properties.

   a. In the WebSphere Application Server administrative console, click **Application servers** › **server1** › **Messaging** › **Message Listener Service** › **Listener Ports**.

   b. Click **enterpriseOutputListener** and change the maximum sessions to **3**, maximum retries to **2**, and maximum messages to **10**.

   c. Click **enterpriseInputListener** and change the maximum sessions to **2**, maximum retries to **2**, and maximum messages to **10**.

2. Modify the **Log buffer pages** setting in the queue manager.

   > **Windows** > **Windows**

   a. In the MQ Explorer, right-click **IBM.DC.QM** and select **Properties**.

   b. Click **Log**, and then change the value of **Log buffer pages** to 4096.

   c. Click **OK**.

   > **Linux** > **Linux**

   a. Open the qm.ini file in a text editor.

   b. Modify the setting for log buffer pages to `LogBufferPages=4096`.

   c. Save your changes.

   Refer to the Queue manager configuration files topic in the WebSphere MQ information center for more details about the queue manager configuration file settings.

3. Modify the **TCP keepalive** setting in the queue manager.

   The TCP keepalive setting determines whether TCP/IP periodically checks to make sure that the other end of the connection is still available. If the other end is not available, the channel is closed.

   > **Windows** > **Windows**

   a. In the MQ Explorer, right-click **IBM.DC.QM** and select **Properties**.

   b. Click **TCP**, and then change the value of **TCP keepalive** to Yes.

   c. Click **OK**.

   > **Linux** > **Linux**

   a. Open the qm.ini file in a text editor.

   b. Modify the setting for TCP keepalive to `KeepAlive = Yes`.

   c. Save your changes.

   Refer to the Queue manager configuration files topic in the WebSphere MQ information center for more details about the queue manager configuration file settings.

4. Modify the **Max channels** setting in the queue manager.

   > **Windows** > **Windows**

   a. In the MQ Explorer, right-click **IBM.DC.QM** and select **Properties**.

b. Click **Channels** and change the value of the **Max channels** to 1000.

c. Click **OK**.

▶ Linux   ▶ Linux

a. Open the qm.ini file in a text editor.

b. Modify the setting for maximum channels to `MaxChannels=1000`.

c. Save your changes.

Refer to the Queue manager configuration files topic in the WebSphere MQ information center for more details about the queue manager configuration file settings.

5. Restart the IBM.DC.QM queue manager.

6. Modify the **Purge policy** setting of the queue connection factory connection pool.

a. In the WebSphere Application Server administrative console, click **Resources → JMS → Queue connection factories**.

b. Click **IBMDCQM**.

c. Under **Additional Properties**, click **Connection pool**.

d. Set the **Purge policy** to **EntirePool**. When the purge policy is set to **EntirePool**, the WebSphere connection pool manager flushes the entire connection pool when a fatal connection error, such as Reason Code 2009, occurs. This prevents the application from getting other bad connections from the pool.

e. Save your configuration changes and restart WebSphere Application Server.

Increasing memory used by Data Transformation

This topic explains how to increase the amount of memory that is used by Data Transformation.

About this task

Do the following to increase memory:

1. Open the following files:

   ▶ Windows   *IBM_RFID_HOME*\IBM\RFID\dts\dts.bat

   ▶ Windows   *IBM_RFID_HOME*\IBM\RFID\dts\DTSWin32Service.bat

   ▶ Linux   *IBM_RFID_HOME*/IBM/RFID/dts/dts.sh

   ▶ Linux   *IBM_RFID_HOME*/IBM/RFID/dts/dts_service.sh
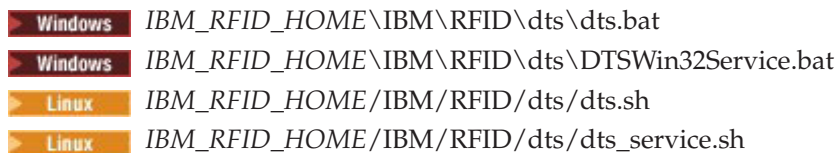
2. Change the minimum and maximum memory for Data Transformation in each of these files from 64 to **256**.

Example

For the dts.bat, dts.sh, and dts_service.sh files, the code should look similar to this before you make the memory change:

```
"%JCLPATH%\java" -Xmx64M -Xms64M -jar org.eclipse.osgi_3.3.0.v20070530.jar -console
```

And then it should look similar to this after you have made the change:

```
"%JCLPATH%\java" -Xmx256M -Xms256M -jar org.eclipse.osgi_3.3.0.v20070530.jar -console
```

For the DTSWin32Service.bat file, the code should look similar to this before you make the memory change:

```
"%JCLPATH%\javaw" -Xrs -Xmx64M -Xms64M -Xgcpolicy:optavgpause -Xlp
-Dcom.ibm.rfid.win32service.sessionkey=%1
%VMOPTIONS% -jar org.eclipse.osgi_3.3.0.v20070530.jar >>..\logs\DTSRuntime.log 2>&1
```

And then it should look similar to this after you have made the change:

```
"%JCLPATH%\javaw" -Xrs -Xmx256M -Xms256M -Xgcpolicy:optavgpause -Xlp
-Dcom.ibm.rfid.win32service.sessionkey=%1
%VMOPTIONS% -jar org.eclipse.osgi_3.3.0.v20070530.jar >>..\logs\DTSRuntime.log 2>&1
```

Tuning the databases to improve performance

Use the steps in this topic to improve your WebSphere Premises Server database performance.
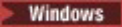
Note: If you have installed Location Awareness Services for WebSphere Premises Server, the default installation can support small scenarios, using between 100 and 200 tags. To use Location Awareness Services for WebSphere Premises Server in a production environment or to use it with more tags, tune your ATLASDB database for additional buffer pools, and add more hard drives to avoid bottlenecks.

Tuning DB2 for Linux, UNIX, and Windows

To tune your WebSphere Premises Server DB2 database, you can either run a script or issue the commands from the DB2 command line.

If you are using a local DB2 database, use the scripts provided on the DVDs. The scripts are located in these paths:

Before installation:

> **Windows** On CD 2 in db_script\performance_tuning_db2.bat
>
> **Linux** On CD 3 in db_script/performance_tuning_db2.sh

After installation:

> **Windows** *IBM_RFID_HOME*\premises\install\db\
> performance_tuning_db2.bat
>
> **Linux** *IBM_RFID_HOME*/premises/install/db/performance_tuning_db2.sh

If you have a remote DB2 database, you may prefer to run the commands from the DB2 command line:

```
db2 connect to IBMRFID
db2 update database configuration using locklist 50000 immediate
db2 update database configuration using maxlocks 95 immediate
db2 update database configuration using maxappls 75 immediate
db2 update database configuration using avg_appls 40 immediate
db2 alter bufferpool IBMDEFAULTBP immediate size 20000
```

Chapter 7. Location Awareness Services for WebSphere Premises Server

After you have installed Location Awareness Services for WebSphere Premises Server, use these topics to access the component information:

Overview

This section provides an overview of Location Awareness Services for WebSphere Premises Server components.

What is Location Awareness Services for WebSphere Premises Server?

Location Awareness Services for WebSphere Premises Server allows companies to continuously track active tags in real time in predefined areas of refineries, plants, and office buildings. Third-party asset location systems provide the tags, which may be carried by employees or visitors, or fixed to assets. Third-party systems also include reader infrastructure and a location engine, which is software that calculates tag positions based on the tag signals received by different readers. The Location Awareness Services for WebSphere Premises Server solution works with these systems to visualize locations that are being monitored and to display the current position of personnel or assets carrying the tags.

Location Awareness Services for WebSphere Premises Server provides a visual console that automatically locates the tags that are monitored in real time, allowing for real time response to emergency situations or security breaches. Personnel or assets can be monitored in virtual danger zones and Location Awareness Services for WebSphere Premises Server will send safety and security breach alerts if assets or personnel are not qualified for entry or exit. Zones are virtual areas that can have rules or permissions assigned to them, and may vary over time. For example, temporary dangerous construction zones may be created.

The solution does the following:
* Cooperates with third-party position determination systems to acquire information about the current location of personnel or assets.
* Allows visualizing monitored areas and the current position of personnel and assets within these areas.
* Supports the rule-based specification of supervision policies.
* Supports a flexible alerting concept.
* Supports integration with existing human resource or asset management applications.
* Supports flexible reporting on monitored areas, providing the current or historical position of personnel and assets within these areas.
* Offers Web services that allow the whole solution or part of its functionality to be used in Service Oriented Architecture (SOA) applications.

An adapter (not shown in Figure 2 on page 236) gathers data from real time location systems (RTLS) monitoring the area and sends the data to Location Awareness Services for WebSphere Premises Server, which stores information in the resources database and performs runtime processing, such as determining

235

when zones are entered or exited, checking business rules, and calling registered programs in case of business rule violations. Information in the resources database, such as position coordinates and zones, is displayed on the Spatial Management Client. The configuration table in this same database is used to define, update, and display administration and operation information through portlets in the WebSphere Application Server administrative console. You can also use the WebSphere Application Server administrative console to define business rules, notification programs, and various system properties.
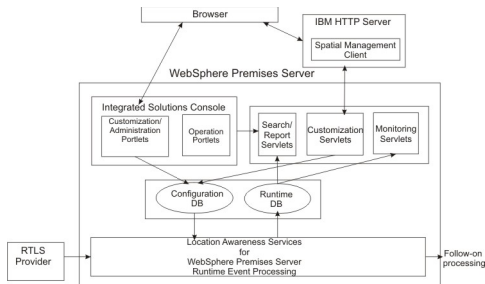
Figure 2. Overview of Location Awareness Services for WebSphere Premises Server

How the data is used

This section provides a brief overview of how the data provided to Location Awareness Services for WebSphere Premises Server is used. Each item that is represented is described in greater detail in the sections that follow.

Data is used in Location Awareness Services for WebSphere Premises Server as follows (see Figure 3 on page 237):

1. A third-party event provider sends provider-specific data.

   Location Awareness Services for WebSphere Premises Server regularly receives data from the event providers, which usually are connected to a number of event devices (receivers). The receivers regularly receive signals from active tags that are usually attached to assets or carried by people. The event providers consolidate the signals that are received and create fixed-format messages that are generated from the signals. Each of these messages contains details about a single tag, including tag ID and current position.

2. Location Awareness Services for WebSphere Premises Server recognizes the event and transforms it to a provider independent format that is used throughout the internal processing of Location Awareness Services for WebSphere Premises Server.

3. The event is linked to a zone. Because zones can overlap, a location event can affect multiple zones.

4. Rules are checked and, if necessary, an alert event is issued.

5. The event is sent to the subscribing programs and notification programs. See "Location Awareness Services for WebSphere Premises Server events" on page 250 for more information.
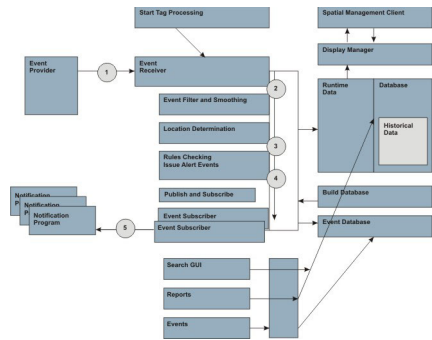
Figure 3. Data flow and usage

Roles and access

This topic lists the groups, allowed actions, and role associated with the Location Awareness Services for WebSphere Premises Server portlets, servlets, and Web services.

Portlets

Table 58. Groups, actions, and roles for portlets

Portlet name	Default groups	Allowed action	Roles
Boundary Zones	lasadministergrp, laslocategrp	view and change settings	lasadminister, laslocate
Business Rules	lasadministergrp, lasconfiguregrp	view and change settings	lasadminister, lasconfigure
CEI Events	lasadministergrp, lasmonitorgrp	view and change settings	lasadminister, lasmonitor
Classes/Items Manager	lasadministergrp, lasmonitorgrp	view settings	lasadminister, lasmonitor
	lasadministergrp, lasregistrategrp	view and change settings	lasadminister, lasregistrate
Control Processing	lasoperategrp	view and change settings	lasadminister, lasoperate
Devices	lasadministergrp, laslocategrp	view and change settings	lasadminister, laslocate
Event Provider	lasadministergrp, laslocategrp	view and change settings	lasadminister, laslocate
Gate Manager	lasadministergrp, laslocategrp	view and change settings	lasadminister, laslocate
Groups Manager	lasadministergrp, lasregistrategrp	view and change settings	lasadminister, lasregistrate
Mail Host Configuration	lasadministergrp, lasconfiguregrp	view and change settings	lasadminister, lasconfigure
Mail Receiver Configuration	lasadministergrp, lasconfiguregrp	view and change settings	lasadminister, lasconfigure
Notification Channels	lasadministergrp, lasconfiguregrp	view and change settings	lasadminister, lasconfigure

Table 58. Groups, actions, and roles for portlets (continued)

Portlet name	Default groups	Allowed action	Roles
Notification Program Manager	lasadministergrp, lasconfiguregrp	view and change settings	lasadminister, lasconfigure
Registration Units	lasadministergrp, laslocategrp	view and change settings	lasadminister, laslocate
Reports Administration	lasadministergrp, lasconfiguregrp	view and change settings	lasadminister, lasconfigure
Reports Operation	lasadministergrp, lasmonitorgrp, lasoperategrp	perform reports	lasadminister, lasmonitor, lasoperate
Search Tags	lasadministergrp, lasmonitorgrp	perform searches	lasadminister, lasmonitor
System Properties	lasadministergrp, lascustomizegrp	view and change settings	lasadminister, lascustomize

Servlets

Table 59. Groups, actions, and roles for servlets

Servlet name	Default groups	Allowed action	Roles
LasVisualizationEAR	lassmcadministergrp, lasmonitorgrp	can use the Spatial Management Client, but cannot change the configuration	allrole
	lassmcadministergrp, lasmonitorgrp	view zones and areas	getrole
	lassmcadministergrp	change zones and areas	putrole
AtlasReportingServletEAR	lassmcadministergrp, lasmonitorgrp, lasoperategrp, lasadministergrp	view reports	getrole
TagProcessingServlet	lasoperategrp	view and change settings	allrole
db2AssetMgmtEAR	lassmcadministergrp, lasmonitorgrp	view and change settings	allrole

Web services

Table 60. Groups, actions, and roles for Web services

Web service name	Default groups	Allowed action	Roles
LasQueryEAR	lassmcadministergrp, lasmonitorgrp	view tag details and reports	allrole
LasEventHandlingEAR	lassmcadministergrp	view and change settings	allrole

Web service name	Default groups	Allowed action	Roles
AtlasImportEAR	lassmcadministergrp	view and change settings	writerole
	lassmcadministergrp, lasmonitorgrp	view settings	viewrole
PremisesCEPRuleDefinitionEJBEAR	lassmcadministergrp	change settings	allrole

Defining Location Awareness Services for WebSphere Premises Server

This section explains the structure of Location Awareness Services for WebSphere Premises Server and how to define it.

Figure 4 shows the structure of Location Awareness Services for WebSphere Premises Server and how the topological items are related.
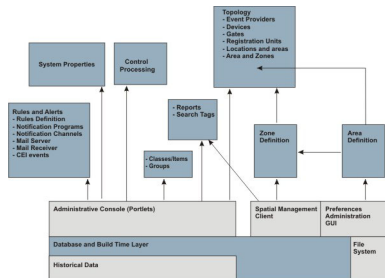
Figure 4. Structure of Location Awareness Services for WebSphere Premises Server

The following user interfaces are provided with Location Awareness Services for WebSphere Premises Server:

- Preferences Administration GUI

  The Preferences Administration GUI allows you to define areas and subareas and set preferences for those areas, such as scaling and coordinate transformation values. You can also define the SVG images for your areas.

- Spatial Management Client

  The Spatial Management Client allows you to define zones and provides a visualization of the defined topology with the tags and their current positions. You can see if a tag has violated a business rule. You can also search for items and request reports.

  There are two versions of the Spatial Management Client: one that allows you to both define and delete zones and monitor tags, and one that only allows you to monitor tags.

- Location Awareness Services for WebSphere Premises Server Administrative Console

  The Location Awareness Services for WebSphere Premises Server Administrative Console is based on WebSphere Application Server and consists of portlets that allow you to define the topology of a location where assets and personnel are tracked. You can use the portlets to define the items, such as assets and personnel, and the rules that control compliance with safety and security regulations. You can also set or change Location Awareness Services for

WebSphere Premises Server system properties. Additional portlets are available to view, maintain, and search events and also to generate and view reports on tag activity.

To define Location Awareness Services for WebSphere Premises Server, complete the following steps using the GUIs and Location Awareness Services for WebSphere Premises Server Administrative Console:

- Define areas and subareas for the location. Do so by creating scalable vector graphic (SVG) images of the areas that you want to monitor and point to them in the Preferences Administration GUI. Because the Spatial Management Client is typically accessed through IBM HTTP Server, store the SVG images and item icons on the Location Awareness Services for WebSphere Premises Server on which the IBM HTTP Server is located.
- Define zones in the administration version of the Spatial Management Client. Zones are related to the area in which they are created.
- Define the location topology in the Location Awareness Services for WebSphere Premises Server Administrative Console:
    - Define the location event providers and associated devices:
        1. Define location event providers.
        2. Define devices per location event provider (if required).
    - Define the registration units you want to use to define items.
    - Define any boundary zones.
    - Define gates.
- Define the item class hierarchy of items to be tracked, such as `Person` and `Asset` classes in the Location Awareness Services for WebSphere Premises Server Administrative Console.
- Define the item groups to be used and the relationship between the groups in the Location Awareness Services for WebSphere Premises Server Administrative Console.
- Register the items to be tracked by the system and the association of items to classes and groups in the Location Awareness Services for WebSphere Premises Server Administrative Console.
- Define the business rules that determine the item tracking behavior of the system in the Location Awareness Services for WebSphere Premises Server Administrative Console. For example, you might define a rule that allows only those persons belonging to a specific group, such as `Security`, to enter a specific zone, such as `HazardousZone`. You can also set system properties to determine the alert behavior for other rules, such as a low battery threshold.
- Define the programs or web services to be called for filtered alerts in the Location Awareness Services for WebSphere Premises Server Administrative Console. For a predefined e-mail notification program, define who to notify about alerts.
- Define the customized reports available for this installation.

Topology
This topic lists the location topology to be defined.

Define the location topology:

Event providers:

This topic explains third-party event providers that are mainly for location events.

Location Awareness Services for WebSphere Premises Server relies on third-party *event providers* to provide tag position data. The third-party hardware and software must be installed and configured to work before configuring Location Awareness Services for WebSphere Premises Server. In general, sufficient hardware must be available to calculate three-dimensional position data for each tag, and it must be installed and configured to provide the necessary positional data.

Event providers monitor areas and feed Location Awareness Services for WebSphere Premises Server with tag location data. In turn, devices read the tag signals and send those to the event provider. Device receivers are always associated to an event provider (hub). Event providers are not part of Location Awareness Services for WebSphere Premises Server, so they must be defined within Location Awareness Services for WebSphere Premises Server. They must be configured for an existing area so that Location Awareness Services for WebSphere Premises Server can track tags within that area. They are defined in the Location Awareness Services for WebSphere Premises Server Administrative Console.

Event providers can be set up and calibrated so that they deliver absolute coordinates or coordinates can be transformed to fit the Spatial Management Client display. Coordinates can be transformed in the following ways:

- *Base point displacement:* Maps the first coordinate system to that of the second one.
- *Scaling:* Scales the coordinate systems if they use different scale units.
- *Rotation:* Makes axes of the coordinate systems congruent.
- *Permutation of axes:* Makes X and Y coordinates in both systems point in the same directions.
- *Smoothing algorithm:* Smooths position estimates.

Such transformation rules must be configured for each event provider.

Devices:

This topic explains devices and device groups and their importance within Location Awareness Services for WebSphere Premises Server.

Devices can be either readers or a device group to which you can associate several readers. Devices represent physical or logical equipment from event providers that provide location data for tags. Devices can be readers that are simple devices or logical device groups (virtual groups) that are used to group the devices into logical units. For example, by grouping the devices into logical units, you can optimize location calculation.

Devices are always related to an event provider (hub). After defining an event provider, you can define the devices. After defining the devices, you can then define gates, registration units based on devices or device groups, or barrier zones with relation to devices.

Gates:

This topic explains gates and their role in controlling access within zones for Location Awareness Services for WebSphere Premises Server.

Gates provide access control for the entry way and exit of a zone. With gates, you can associate one device that specifically monitors the entry to or exit from a zone. Gates are defined after defining the devices for the event provider (hub).

When monitoring zones in areas, you will need to define the gate twice, for the zone and for the area. Otherwise, Location Awareness Services for WebSphere Premises Server cannot correctly monitor tag counts for the zone and area.

Registration units:

This topic defines registration units and explains their purpose.

Registration units are location event providers that you designate for the specific purpose of registering tag IDs with Location Awareness Services for WebSphere Premises Server when you create items. For example, you can define a hub as a registration unit and then use it to read tags when defining items, which means you do not have to enter the tag IDs manually.

Locations and areas:

A *location* is made up of many *areas*, each of which represents a real physical space within the location to be monitored. *Subareas* are areas nested inside of other areas.

Areas are graphically represented and are the container for all zones. Areas have a flat lower and an optionally flat upper boundary.

Define an area by creating an SVG file of the area and then importing it into the Spatial Management Client by referencing it in the Preferences Administration GUI. See "Defining areas and subareas" on page 252.

Zones:

This topic defines and explains zones, including boundary zones, and describes how to monitor the entrances and exits of different classes of zones.

Zones are designated logical sections within areas that are associated with those areas and for which rules can be defined. Zones can overlay each other and are the units on which rules can be performed and on which counts and statistics for a tag entering or leaving can be calculated.

Zones within an area are defined with the Spatial Management Client and can be of different types. An entire area can also be considered a zone. You cannot change its size in the Spatial Management Client and it is not displayed as a colored region. However, rules can be attached to it.

Within the IBM Location Awareness Services for WebSphere Premises Server system, zones are used for different purposes. Depending on their purpose, they are classified into one or several of the following zone classes:

Alarm zones
> Alarm zones are the most common type of zone. Access restriction rules or similar rules can be triggered when an item (usually a person or asset) enters or exits a zone of this class. The restriction rules can be set for all other zone types as well, but they have additional semantics, as described in the following definitions.

Privacy zones
> Currently privacy zones behave like alarm zones.

Shadow zones
> Tags entering shadow zones might not be visible temporarily because they are out of reach of the tag reader infrastructure or the signals are shielded.

Location Awareness Services for WebSphere Premises Server assumes that a tag continues to be in the shadow zone at the last reported position after it has been seen. No alert is generated if the tag is no longer visible.

Boundary zones

These zones are used for implementing access control to areas that are not covered by event devices and therefore cannot be controlled completely or directly. See "Monitoring the entrance and exit of zones that are not fully covered by devices" on page 245.

Note: In the Spatial Management Client, the term *barrier zone* is a synonym for a *boundary zone*.

Exit zones

These zones are used to determine if a tag has passed and no signals can be received thereafter. They indicate that an item has left the premises and so there is no reason to be concerned about not receiving a signal.

Monitoring the entry and exit in an area

The following example describes how an item (person or asset) might be tracked when entering and exiting a zone. Assume you have X (0.0, 0, 100, 100, and 100) and Y (100 and 0) coordinates representing the area MyZone. Whenever a tag is visible within these coordinates and a signal comes from the related hub, Location Awareness Services for WebSphere Premises Server registers the tag within the zone.

Consider the following scenarios:

1. The tag enters the area and follows the path indicated in the graphic below. If the tag is no longer visible, Location Awareness Services for WebSphere Premises Server stores information about the last location where the tag was seen (indicated by the small circle at right edge of the area), and after a configurable time generates an event indicating that the tag is not responsive and was last seen at the stored location.
2. The tag follows the path in the graphic below and is last seen in an exit zone. Location Awareness Services for WebSphere Premises Server no longer displays the tag in the area and recognizes that the tag has left the area.
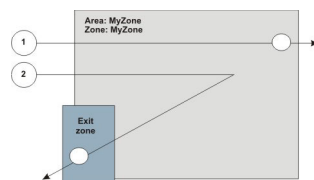
So that Location Awareness Services for WebSphere Premises Server knows that tags have left an area, you should define exit zones. Otherwise Location Awareness Services for WebSphere Premises Server assumes that the tag is still at the edge of the area, but not responsive anymore.

Monitoring the entry and exit in an area (gates)

You can also define one device to be responsible for reporting the entry or exit to or from an area or zone. Do this by creating a *gate*. You define a event provider and then define a device to monitor the gate. You then specify whether the device monitors tags that are entering the zone (IN) or tags that are exiting the zone

(OUT). When the device sees a tag that fits the parameter you specified (IN or OUT), it reports the event and generate an alert if a rule is broken.

When monitoring zones in areas, define the gate for the zone and for the area. Otherwise, Location Awareness Services for WebSphere Premises Server cannot correctly monitor tag counts for the zone and area.

Consider the following scenario for a zone inside of an area that is not fully monitored by devices:

1. Create one gate to monitor tags with device A that enter the zone. Define the gate twice, once for the zone and once for the area.
2. Create another gate to monitor tags with device B that leave the zone. Also define this gate twice, once for the zone and once for the area.
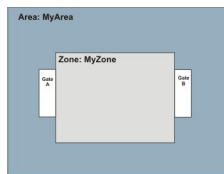
Monitoring zones that are fully covered by devices

The following graphic depicts a zone in which devices can cover all of the areas. The following example describes how Location Awareness Services for WebSphere Premises Server tracks a tag that follows the path indicated by the arrow.

1. When the tag reaches the first point (indicated by a circle), Location Awareness Services for WebSphere Premises Server generates an event internally that indicates that the tag entered the zone and checks whether any existing rules apply to the situation. The tag count for the zone increases by 1.
2. Within the `FullyCovered` zone, Location Awareness Services for WebSphere Premises Server can usually track the position of the tag continuously. If Location Awareness Services for WebSphere Premises Server loses contact with the tag, an `AtlasTagNotResponsive` event is generated, indicating an abnormal condition. Within the zone, no location-dependent rules are checked.
3. When the tag leaves the zone (indicated by the second circle) Location Awareness Services for WebSphere Premises Server generates an event indicating that the tag left the zone and checks whether any existing rules apply to this situation. The zone tag count decreases by 1 when the tag leaves the zone.
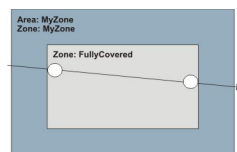
Thus, zones that are fully covered by devices allow you to fully track the activity of a tag. This type of zone is usually an alarm zone, where you define business rules for monitoring activity within the zone.

Monitoring shadow zones

The following scenarios describe situations in which zones are not completely covered by devices.

Assume you want to monitor a closed room in which the tags cannot be seen in all sections at all times. For example, the room might contain metal, which reflects signals in a certain section of the zone so that signals are too low to register, or a chimney is located above the devices in one section.

The following graphic depicts two scenarios:

1. The entry and exit for the zone are fully covered:
   - Entry to the zone (indicated by the first circle) and exit from the zone (indicated by the second circle) are covered by devices. However, there are spots in the zone (indicated as "Not Covered") where signals from the tag cannot be received.
   - Location Awareness Services for WebSphere Premises Server assumes that a tag continues to be in the shadow zone at the last reported position after it has been seen. No alert is generated if the tag is no longer visible.

     Note: This situation is different from the situation described in "Monitoring the entry and exit in an area" on page 243.
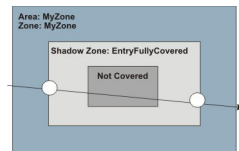
2. The entry into the zone is not fully covered:
   In this special scenario, you must define a zone or zones outside of the entry area to monitor tags that enter or exit the zone. Solutions include the following:
   - Two boundary zones
   - Single boundary zone
   - Mixed approach of zones

Monitoring the entrance and exit of zones that are not fully covered by devices

Some zones are not fully covered by event devices; however, a precise count of tags within a zone is still needed. To accomplish this, the entrance and exit of the zone must be monitored. To monitor these zones, you define *boundary zones* around or at the entrance of the zone to be monitored.

Boundary zones can be related to a target zone in the following ways:
- **Outer boundary zone:** The tag is assumed to be out of the target zone.
- **Inner boundary zone:** The tag is assumed to be in the target zone, even it is not visible.
- **Single boundary zone:** The tag is assumed to be in the target zone, even it is not visible. However, you do not use an outer boundary in this case.

As shown in the following figures, target zones can be monitored by one or more inner and outer boundary zones, or multiple target zones can share the same inner or outer boundary zones.
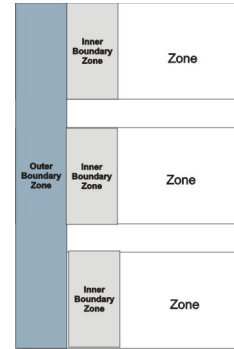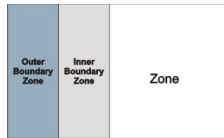
You can use a single boundary zone to monitor the entrance of the target zone and an exit zone to monitor the exit. If no exit zone is defined, Location Awareness Services for WebSphere Premises Server assumes that the tag remains in the zone, even though it cannot see it.
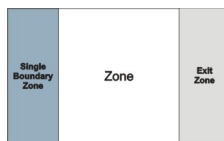
Sample zone layout

The following figure combines different zones in one area. Notice that you can overlap zones. You can open an overlapping area to see different graphical representations, and for each zone you can see summary counts for the all child zones of the area in focus. However, note that you cannot see details for more than one zone at a time.
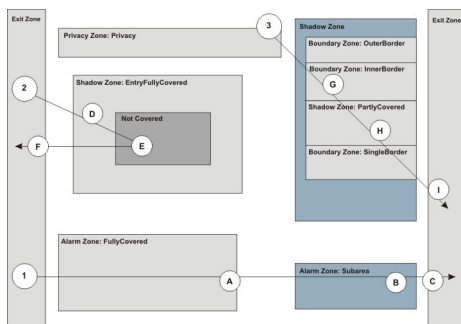
In the graphic, the arrows represent persons with tags walking through the area. The circles represent points along the path they take:

1. A person walks from the left exit zone to the right exit zone, passing through two zones:
   - When the person reaches point **A**, the tag is seen by the devices and Location Awareness Services for WebSphere Premises Server knows that the tag is in the `FullyCovered` alarm zone.
   - When the person reaches point **B**, the tag is seen by the devices and Location Awareness Services for WebSphere Premises Server knows that the tag is in

the Subarea alarm zone. Because Subarea is another zone, if you had imported and defined the image of the other area, you could navigate to it and see the tag there as well.

- When the person reaches point **C**, the tag is seen by the devices and Location Awareness Services for WebSphere Premises Server knows that the tag is in the right exit zone. When the tag is no longer seen in the exit zone, Location Awareness Services for WebSphere Premises Server removes the tag from the area and assumes that the tag has left the area.

2. A person walks from the left exit zone into the shadow zone and then exits through the left exit zone:

- When the person reaches point **D**, the tag is seen by the devices and Location Awareness Services for WebSphere Premises Server knows that the tag is in the EntryFullyCovered shadow zone.

- When the tag reaches point **E**, the tag is no longer seen. Because it is in a shadow zone, Location Awareness Services for WebSphere Premises Server does not expect the tag to respond and does not generate an alert event. Location Awareness Services for WebSphere Premises Server continues to assume that the tag is in the EntryFullycovered shadow zone.

- When the tag reaches point **F**, the tag is seen by the devices and Location Awareness Services for WebSphere Premises Server knows that the tag is in the left exit zone. When the tag is no longer seen in the exit zone, Location Awareness Services for WebSphere Premises Server removes the tag from the area and assumes that the tag has left the area.

3. A person walks from a privacy zone within the area to the right exit zone, passing through several zones:

- When the person reaches point **G**, the tag is seen by the devices and Location Awareness Services for WebSphere Premises Server knows that the tag is in the InnerBorder boundary zone. Because this zone is a border area for the PartlyCovered alarm zone, Location Awareness Services for WebSphere Premises Server assumes that the tag is within this area.

- When the person reaches point **H**, the tag might not be seen by a device, but Location Awareness Services for WebSphere Premises Server assumes that the tag is in the area because it was last seen in the InnerBorder boundary zone. Also, because these zones overlap a shadow zone, the TagNotResponsive alert event is not issued.

- When the person reaches point **I**, the tag is seen by the devices and Location Awareness Services for WebSphere Premises Server knows that the tag is in the right exit zone. When the tag is no longer seen in the exit zone, Location Awareness Services for WebSphere Premises Server removes the tag from the area and assumes that the tag has left the area.

Items

This topic explains items and their importance within Location Awareness Services for WebSphere Premises Server.

Items represent the entities within a location that can be equipped with tags so that you can track their positions. Each item has attributes, including the tag ID, label, and icon link update interval. An item also has key properties that are required to set the item apart and properties that complete the description. Key properties and properties vary by class. A key property for a person might be a social security number and a property might be a person's first name.

When defining items for the first time, you can use a registration unit or external device to read the tag IDs into the system or you can enter them manually.

People and assets are the most common items that are monitored by Location Awareness Services for WebSphere Premises Server; however, tags can also be attached to other items like product parts being consumed in discrete manufacturing processes like vehicle assembly. Therefore, Location Awareness Services for WebSphere Premises Server uses the term *item* for everything that can be equipped with a tag.

Item classes

This topic describes item classes and subclasses and their importance within Location Awareness Services for WebSphere Premises Server.

Item classes define items through a set of properties and attributes for them. For example, you might have the following classes: Person and Asset. Within these classes, you can also have subclasses with extended properties and attributes. For example, the Person class might have the subclass Administrators.

Items must belong to a class. Once an item is created and assigned to a class, you cannot move the item to another class. Because classes are in the form of a tree-structured hierarchy, an item cannot belong to more than one class directly. However, an item is automatically considered to be an instance of any superclasses of the given class. Items have the attributes defined for the class that they belong to. Class attributes are either defined directly for the class, or are inherited from its superclasses (if any).

Using the example of the Person class and the Administrator subclass, if a tag is assigned to class Administrator, it is also considered to be an instance of the superclass Person. Therefore the rule, "let me know when a Person enters the HAZARD zone," triggers an alert for Administrators as well as any other subclasses of "Person."

All classes have some common attributes, such as an icon label and tag ID. You can define required, or key, properties such as social security number or first name and last name, as well as optional properties such as telephone number. You can also define properties that are specific to your organization.

One specific property for all classes is the container attribute. If this is set, all items of the class are potential containers and can contain other items.

Subclasses inherit the properties of the parent (superclass), but you can also define new properties for them.

Important: Properties for subclasses cannot have the same name as properties in parent classes. Also, once items or subclasses are defined for a class or subclass, you cannot change the class attributes.

Groups

This topic defines a group and how it functions within Location Awareness Services for WebSphere Premises Server.

Groups are containers that allow grouping of items from different classes for common rules, searches, or so forth. For example, the `Fire Brigade` group can contain fire fighters (persons) and fire extinguishers (assets). Such containers are often referred to as *views* because you can view the items from a distinct perspective.

An item can belong to one or more groups; however, it does not have to belong to a group. A group can be a member of one or more groups; however, it does not have to be a member of another group.

You can specify that a group hierarchy be used by setting the `HierarchicalGroups` property in "System Properties" on page 291. The default value for `HierarchicalGroups` property is `Yes`, meaning group hierarchy is used.

Important: When group hierarchy is used (the default), this enforces a tree-like group hierarchy, which means that you cannot assign an item to more than one group and you cannot make a group a member of multiple groups. The characteristic of a group, when group hierarchy is used, is more similar to a class than a container.

You can select a group color in the Group Manager portlet if the `HierarchicalGroups` property is set to *true*. The color then displays behind all group member icons on the Spatial Management Client.

Rules

This topic explains different types of rules and how they trigger Location Awareness Services for WebSphere Premises Server events.

Rules define conditions and policies that need to be met. For example, rules can be used to restrict access to certain zones or to limit the amount of time an item stays in a zone. Business rules are implemented based on a generic Complex Event Processing (CEP) engine which facilitates the development of additional rule types. Events (alerts) occur when rules are violated. Events are published and saved in the event database. Subscriber programs can subscribe to Location Awareness Services for WebSphere Premises Server events. Violations of rules related to items can also be displayed in the Spatial Management Client.

Location Awareness Services for WebSphere Premises Server rules typically refer to the aspects of the real world as it is modeled in Location Awareness Services for WebSphere Premises Server - items and persons equipped with tags and the topology of the location to be monitored. Some basic rule types are supported by Location Awareness Services for WebSphere Premises Server and you can use portlet-based user interfaces to create instances of these rule types. An example of a rule type is "must not enter" whereas an example of a related rule instance is "members of the Visitor class must not enter protected zones". The following rules are related to zones and can be set and maintained in "Business Rules" on page 282 in the Location Awareness Services for WebSphere Premises Server Administrative Console:

- Zone entry and exit rules

  When a tag is considered to have entered or exited a zone is also affected by the `MaxUnrecognizedMovement` system property. See "System Properties" on page 291.

- Visitor escorting rules

  This rule checks whether a visitor is accompanied in specified zones by an escort. The visitor must belong to container classes, the escort must not contain a container class, and the `DynamicContainerSupportOn` system property must be selected. See "System Properties" on page 291.

- Duration of stay rules

  When an item is in a zone longer than specified by the rule, an alert is triggered for the tag.

- Maximum items per zone rules

When a defined threshold of items in a zone is exceeded, an alert is triggered.

The following global rule types do not have different instances, but can be customized in the "System Properties" on page 291 portlet in the Location Awareness Services for WebSphere Premises Server Administrative Console:

- Tag not responsive rule

  When a tag is no longer detected by the event provider, an alert is triggered. See `MaxUnrecognizedMovement` and `TagNotResponsiveAlertAction` in "System Properties" on page 291 for more information. In addition, the tag icon fades on the Spatial Management Client.

- Tag battery low rule

  When a tag has a low or empty battery, a BatteryLowAlert or BatteryExhaustedAlert is issued. See `BatterylowAlertAction` in "System Properties" on page 291 for more information. In addition, the Spatial Management Client displays a small battery icon.

- Unknown tag rule

  When a tag is detected that is not related to a defined item, an UnknownTagAlert is generated. See `UnknownTagalertAction` in "System Properties" on page 291 for more information. In addition, the Spatial Management Client displays an unknown tag icon.

- Stationary tag rule

  If a tag that belongs to a class that is defined as stationary moves, an alert is generated. The movement must exceed the value specified in the `MaxUnrecognizedMovement` system property.

  To avoid a flooding condition of stationary alerts, if the tag moves twice the amount of units defined in `MaxToleratedMovement`, then a stationary alert will be generated once every 5 minutes.

Location Awareness Services for WebSphere Premises Server events

This topic explains Location Awareness Services for WebSphere Premises Server event details and notification programs to subscribe events.

The main purpose of monitoring items is to make sure that the position of a tagged item conforms to the awareness and security rules defined for the monitored locations. Nonconformance to such security or business rules triggers alerts that inform security staff or automated emergency systems about the event. In addition to the Spatial Management Client, other subscriber programs can also subscribe to Location Awareness Services for WebSphere Premises Server events.

Event details

A subscriber must have sufficient information about the event to trigger corrective action or inform others sufficiently. Event information includes the following:

- Type of event:
  - Event types pertaining to the tag battery level:
    - `LasBatteryExhausted` - indicates that the tag battery is completely exhausted on the tagged asset.
    - `LasBatteryLow` - indicates that the tag battery is low on the tagged asset.
  - `LasDurationOfStay` - indicates that a tag has stayed longer in a zone than allowed.

- – `LasEventProviderDiagnostic` - a diagnostic message coming from an event provider.
  - – `LasIBMInfrastructure` - indicates that there is a problem in the middleware infrastructure.
  - – `LasMissingEscort` - indicates that an item defined as "must be escorted" is missing the required proximity of an escort longer than allowed.
  - – `LasStationaryTagMoves` - indicates that a tag that is defined as stationary has moved.
  - – `LasTagNotResponsive` - indicates that no signal is being received from the tag.
  - – `LasUnknownTag` - indicates an unknown tag is found.
  - – `LasZoneEntry` - indicates that an unauthorized tag entered the zone.
  - – `LasZoneExit` - indicates that an unauthorized tag exited the zone.
- • Alert details are shown about the event dependent on event type. For example, they might include the following information:
  - – Tag ID
  - – Icon label (as tag identification)
  - – Last valid time that the tag was reported
  - – Last valid position where the tag was reported
  - – Battery level
  - – Zone or area exit time or entry time
  - – Groups of which the tag is a member (if a subscriber is interested only in specific groups)
  - – Class to which the tag is related (if a subscriber is interested only in a specific class)
  - – Specific message text that describes the situation
  - – Event history (status of event, time handled, and how it was handled)
- • If the event was triggered independent of a specific tag, but is related to third-party infrastructure elements, the following information that is necessary to identify the failing element is provided:
  - – Event time
  - – Hub name

  Depending on the situation and the information given by the event provider, more details might be in the specific message text.

Notification programs to subscribe events

The *event group*, or group of persistent related events, with its related messages queues is defined during installation and configuration. A filter is defined that identifies which Location Awareness Services for WebSphere Premises Server alert messages are routed to these queues. As a result, an application can query the Common Event Infrastructure (CEI) event database, where all Location Awareness Services for WebSphere Premises Server events are stored, for events or a *subscriber program* can subscribe to the topic related to the event group.

When installing Location Awareness Services for WebSphere Premises Server, a predefined subscriber program listens to all events on the `All events` group. It dispatches the arriving events to the Location Awareness Services for WebSphere Premises Server *notification programs*. The notification programs are the programs and web services that can be triggered when an event occurs. For example, a notification program might be an e-mail program that notifies authorized

personnel of an event. By default, Location Awareness Services for WebSphere Premises Server has only one event group defined: All events. However, you can add additional subscribers as a customization task.

Finally, you define *notification channels* for a given subscriber (defined as attributes for a channel definition) to specify the program that should be called for an event.

Customization tasks include the following:
- Implementing a new notification program and deploying it.
- Deploying a new program or web service that is called on entry of an event.

See "Defining how to handle alerts" on page 288 for details about these tasks.

To publish and subscribe, administrators can perform the following tasks (based on a set of event group topics) in the Location Awareness Services for WebSphere Premises Server Administrative Console, specifically in "Notification Program Manager" on page 288 and "Notification Channels" on page 289:
- Define programs or services to be triggered.
- Define the channels triggering the program.

Administering

Perform administration tasks for Location Awareness Services for WebSphere Premises Server using the Spatial Management Client and the Location Awareness Services for WebSphere Premises Server Administrative Console.

Defining areas and subareas

Use the Preferences Administration GUI to define areas and subareas.

1. Import an SVG image of the area. See "Importing a graphic of your area."
2. Use the "Preferences Administration GUI" on page 261 to reference the graphic and set preferences, such as scaling and coordinate transformations, for the area. See "Transforming coordinates for your areas" on page 255.
3. Optionally, use the "Preferences Administration GUI" on page 261 to nest another area inside of an existing area or create a subarea. Use the following fields in the GUI:
   a. In **Parent SVG area name**, enter the name of the parent area. For example, Matrix.

      Note: Area names must be unique across the installation.
   b. In **X offset value**, enter the X offset value in units for placement of the subarea within the parent area. For example, if you want to nest the subarea 40 feet inside the X axis of the existing area, enter 40.
   c. In **Y offset value**, enter the Y offset value in units for placement of the subarea within the parent area. For example, if you want the subarea 20 feet inside the Y axis of the existing area, enter 20.
4. Save your preferences and exit the GUI.
5. Open the Spatial Management Client and verify that your settings are correct. See "Starting the Spatial Management Client (administration)" on page 263.

Importing a graphic of your area
This topic describes how to import and convert a graphic of your area.

Before you begin

Make sure that you have installed Adobe SVG viewer and Internet Explorer 6.0.

1. Convert the graphic to an SVG (Scalable Vector Graphics) format and copy the SVG file to the svg directory of the Spatial Management Client.

   The directory is usually located in the *IHS_HOME*/htdocs/en_US/Tracking GUI/ path.

   Restriction: Using SVGs larger than 4 MB is not recommended.

2. Import the graphic of the area by referencing the SVG file in the **SVG path** field in the "Preferences Administration GUI" on page 261.

   Make sure you scale the graphic correctly in the Preferences Administration GUI before creating zones in the area using the Spatial Management Client.

Converting a graphic to SVG format

You can import any graphic format supported by the SVG specification. All conformant SVG implementations must support PNG (Portable Network Graphics), JPEG (Joint Photographic Experts Group), and SVG images. The Adobe SVG viewer required by Location Awareness Services for WebSphere Premises Server also supports GIF (Graphics Interchange Format) images. Graphic formats, such as CAD, TIFF, or BMP, can be converted to one of the supported formats: PNG, JPEG, or SVG. Use a graphic editing tool such as CorelDraw, Adobe Photoshop, or Adobe Illustrator to perform these conversions.

Tip: Starting from a bitmap format results in lower quality. Vector formats result in higher quality.

Restriction: Using SVGs larger than 4 MB is not recommended.

Converting a vector format to SVG:
About this task

If the input format is a vector graphic, such as CAD, convert the graphic directly to SVG.

1. Import the graphic into a graphic editing tool, such as Adobe PhotoShop.
2. Prepare the graphic to be used in the Spatial Management Client by making the file as small as possible. The larger the graphic file, the more time it takes to load and render in the GUI. Do the following:
   - Remove excess layers of detail from the graphic before converting it. Layers of unwanted details such as plumbing, electrical, landscaping, and wall types, can be hidden under the layers of the basic area shape.
   - If possible, remove extra rooms or areas from your CAD drawing. For example, export only a room if you do not need the entire floor.
   - Do not embed fonts in the SVG file if given a choice; use system fonts instead. Embedding fonts significantly increases the file size.
   - Pre-scale the image so that the longest axis is no more than 600 pixels in length.
3. Make sure the upper-left corner of the graphic is the position you want to be 0, 0 on the X, Y coordinates in the Spatial Management Client. If it is not, crop the graphic until the positioning is correct.
4. Write down the graphic width and height values for later use.
5. Export the file as an SVG file. For example, floor1.svg.

6. Open the SVG file in a text editor, add the `onload` attribute, and modify the width and height, as necessary:

```
<svg onload="clearSvgArray(evt)" width="width" height="height" viewBox="0 0 width height">
```

Note: Make sure the graphic *width* and *height* values are those you wrote down while using the graphic editing tool. You can round the values to whole numbers if preferred.

For example:

```
<svg onload="clearSvgArray(evt)" width="586" height="452" viewBox="0 0 586 452">
```

Note: Because a PDF is vector-based, you can also convert PDF files to the SVG format. However, with the PDF format you cannot alter or delete unnecessary layers, and so the file size is larger.

Converting a bitmap format to SVG:
About this task

If the input format is a bitmap, you can convert the graphic to a PNG or JPEG format, which can then be linked to an SVG container graphic. Complete the following steps:

1. Import the graphic into a graphic editing tool, such as Adobe PhotoShop.
2. Prepare the graphic to be used in the Spatial Management Client by making the file as small as possible. The larger the graphic file, the more time it takes to load and render in the GUI. Do the following:
   - Remove excess layers of detail from the graphics before converting them. Layers of unwanted details such as plumbing, electrical, landscaping, and wall types, can be hidden under the layers of the basic area shape.
   - Pre-scale the image so that the longest axis is no more than 600 pixels in length.
   - Change the image bit depth of bitmap formats so that they are as small as possible. For example, in a simple line bitmap graphic, the graphic does not have to have a 24-bit depth when a 1-bit depth conveys the same image.
3. Make sure the upper-left corner of the graphic is the position you want to be 0, 0 on the X, Y coordinates in the Spatial Management Client. If it is not, crop the graphic until the positioning is correct.
4. Write down the graphic width and height values for later use.
5. Export the file as a PNG or JPEG format. For example, floor1.jpg.
6. Open an empty file in a text editor and create an SVG container file for the graphic by copying the following:

```
<svg onload="clearSvgArray(evt)" width="width" height="height" viewBox="0 0 width height">

 <g>
   <image height="height" width="width" xlink:href="file_name"></image>
 </g>
</svg>
```

Note: The graphic *width* and *height* values are those you wrote down while using the graphic editing tool.

For example:

```
<svg onload="clearSvgArray(evt)" width="586" height="452" viewBox="0 0 586 452">

 <g>
   <image height="452" width="586" xlink:href="floor1.jpg"></image>
 </g>
</svg>
```

7. Save the file as an SVG file. For example, floor1.svg.

Transforming coordinates for your areas

This topic explains how to transform coordinates so that an area displays properly on the Spatial Management Client.

Usually the map on the Spatial Management Client relates to the coordinate system of the event provider (hub) in such a way that the logical 0.0 point is either in the bottom left or top left corner (abstracting from the offset). In those cases it would be sufficient to define a scaling factor when defining the area and X and Y offsets. If your default 0.0 is in the top left corner and you want to change it to the bottom left, specify `cartesian` when defining the area.

The detailed information in this topic is necessary for more complex situations, where one hub is related to different maps with various orientation, overlap, and so on.

There can be up to three types of coordinate systems in an Location Awareness Services for WebSphere Premises Server environment:

1. The systems defined by the location event providers.
2. The systems defined by Location Awareness Services for WebSphere Premises Server in the Spatial Management Client. The point of origin of the coordinate system defined by the Spatial Management Client is the upper-left corner, with the Y-axis pointing downwards and the X-axis pointing to the right.
3. Logical reference systems.

The following figure shows a simple scenario that demonstrates why at least one coordinate transformation is required in almost all cases.
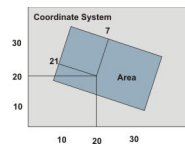
The point has coordinates 20, 20 in the location event provider coordinate system. These coordinates must be translated to Spatial Management Client coordinates which are 7, 21 in this sample. Depending on the complexity of the setup, separate logical reference systems might be needed. In many cases, such as in the sample illustrated here, a system defined by the location event provider or the Spatial Management Client can be used as a reference system. In some setups, the systems might even be identical.

When the systems are identical, no coordinate transformation is needed. If either system acts as a reference system, one coordinate transformation must be made. If there is a separate reference system, two transformations must be made: one between the location event provider and the Location Awareness Services for WebSphere Premises Server server and one between the Location Awareness Services for WebSphere Premises Server server and the Spatial Management Client.

Processing coordinates

Location events from location event providers are processed by Location Awareness Services for WebSphere Premises Server and transformed as required:
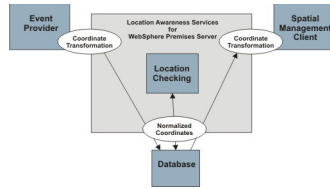
1. Coordinates from a location event provider are transformed before they are stored in the Location Awareness Services for WebSphere Premises Server database.
2. Internal server side processing, such as location checking, is based on those normalized coordinates.
3. Location Awareness Services for WebSphere Premises Server also transforms tag positions when sending them to the Spatial Management Client.

Configuring coordinate transformations

The location event provider transformation rules are specified in the Location Awareness Services for WebSphere Premises Server Administrative Console, specifically in the **Event Provider** portlet. In the **Coordinate Transformation** section of the Details view you can supply values for the following base transformation operations:

- **Horizontal Rotation:** Rotates the X-Y plane around the point of origin.
- **X-Y Permutation:** Permutates, or switches, the X and Y axis.
- **X Offset:** Displaces the area in the X direction.
- **Y Offset:** Displaces the area in the Y direction.
- **Scaling:** Scales the area to a larger or smaller size.

The transformations apply only to the X and Y coordinates. There is no need for three dimensional transformations because all components can be configured so that the Z-axis of their coordinate systems points upward.

The following samples show the effects that different values have.

Input coordinates are transformed based on the values of the listed parameters. Input coordinates (X,Y,Z) are converted to (X′,Y′,Z′) according to the following rules:

- X′ =
  - Scaling * (X * cos(HorizontalRotation) + Y * sin(HorizontalRotation)) + XOffset (if X and Y axis are *not* permuted)
  - Scaling * (-X * sin(HorizontalRotation) + Y * cos(HorizontalRotation)) + YOffset (if X and Y axis are permuted)
- Y′ =
  - Scaling * (-X * sin(HorizontalRotation) + Y * cos(HorizontalRotation)) + YOffset (if X and Y axis are *not* permuted)
  - Scaling * (X * cos(HorizontalRotation) + Y * sin(HorizontalRotation)) + XOffset (if X and Y axis are permuted)
- Z′ = Scaling * Z (sin() and cos() are the standard trigonometric functions)

In the Spatial Management Client, you cannot configure horizontal rotation and axis permutation. However, you can specify the following base transformations when you define a new area in the Preferences Administration GUI:

- **X Offset value:** Displacement in X direction.
- **Y Offset value:** Displacement in Y direction.
- **Area scale:** Scaling factor.

As a consequence, areas must be aligned with either the location event provider's coordinate system or the intermediate reference system.

Location event provider and area configurations

The following figures show the different location event provider and area configurations that can occur. The location event provider-defined coordinate system is depicted in light gray and the coordinate system defined in the Spatial Management Client for the area is in blue.
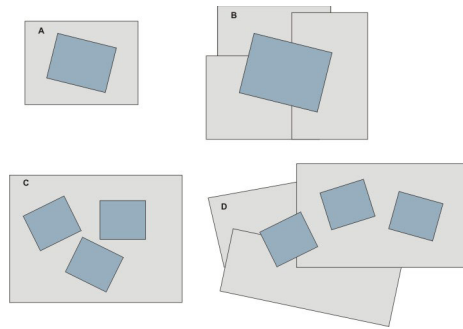
Scenarios A and B depict a single location event provider configuration and scenario C depicts a configuration where all location event providers refer to the same coordinate system.

In scenarios C and D, the X and Y axes of all areas must be aligned. In other words, the X axis of each area must point in the same direction and the Y axis of each area must point in the same direction.

The following table summarizes the scenarios depicted above and shows which system should be used as a reference system:

Case	Location event providers	Area	Reference system	Comment
A	1	1	Location event provider or Spatial Management Client	When the Spatial Management Client is used frequently by multiple users, use the GUI's coordinate system as the reference. In all other cases, use the location event provider's coordinate system to reduce the number of transformations.

Case	Location event providers	Area	Reference system	Comment
B	None	1	Spatial Management Client	
C	1	None	Location event provider	
D	None	Multiple	Separate reference system	The separate coordinate system can coincide with the coordinate system of the location event provider, the Spatial Management Client, or both.

In scenarios A, B, and C, a separate reference system can also be used. However, doing so increases the number of required transformations.

Transformation samples

The following figures show some basic transformation scenarios. The original coordinate system is labeled with a "1", such as X-1, Y-1. The target system is labeled with a "2", such as X-2, Y-2. The scaling factor depends on the base units of both systems. The configuration settings are shown in the tables.

Table 61. Sample 1

Configuration setting	Value
Rotation	0
X-Y permutation	No
X-offset	dx
Y-offset	dy
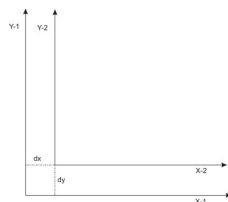
Table 62. Sample 2

Configuration setting	Value
Rotation	0
X-Y permutation	Yes
X-offset	dy
Y-offset	dx
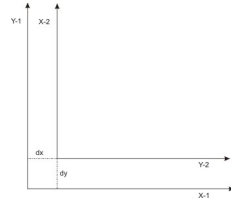
Table 63. Sample 3

Configuration setting	Value
Rotation	90
X-Y permutation	No
X-offset	dx
Y-offset	dy
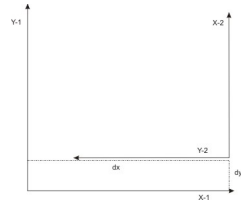
Table 64. Sample 4

Configuration setting	Value
Rotation	90
X-Y permutation	Yes
X-offset	dy
Y-offset	dx
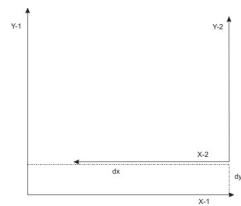
Table 65. Sample 5

Configuration setting	Value
Rotation	180
X-Y permutation	No
X-offset	dx
Y-offset	dy
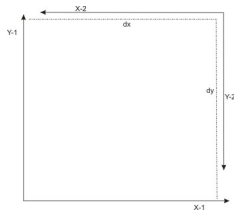
Table 66. Sample 6

Configuration setting	Value
Rotation	180
X-Y permutation	Yes
X-offset	dy
Y-offset	dx
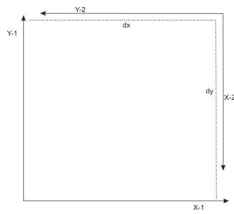
Table 67. Sample 7

Configuration setting	Value
Rotation	270
X-Y permutation	No
X-offset	dx
Y-offset	dy
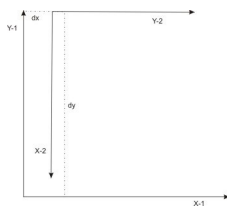
Table 68. Sample 8

Configuration setting	Value
Rotation	270
X-Y permutation	Yes
X-offset	dy
Y-offset	dx
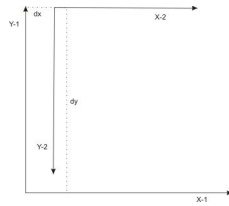
The transformation shown in the last sample occurs frequently in Location Awareness Services for WebSphere Premises Server configurations. The target coordinate system is like that defined by the Spatial Management Client, with the point of origin in the *upper-left* corner, with the Y axis pointing downward, and the X axis pointing to the right.

Preferences Administration GUI

This topic describes how to use the Preferences Administration GUI to define your Spatial Management Client and build time preferences for Location Awareness Services for WebSphere Premises Server.

It is necessary to define your preferences only once per server installation instance for the installation entries.

Open the Preferences Administration GUI by opening the following URL: http://*fully_qualified_host_name*/Tracking GUI/AtlasPrefsAdmin.html

Spatial Management Client

The Spatial Management Client is a monitoring application that polls every *n* seconds for new data in a defined area, as specified in the prefsV3.xml file. The default value is to poll every second.

Note: Some browser functions are not supported. For example, using the **Back**, **Forward**, and **Refresh** buttons in the browser can lead to inconsistent displays of areas, tags, and menu options.

Before setting your preferences, update the *http_root*\htdocs\en_us\Tracking GUI\xml\prefsV3.xml file with the IP address or fully qualified host name of your Location Awareness Services for WebSphere Premises Server server. Doing so automatically updates some of the **Build time** fields.

Note: When you update, ensure that you merge the contents of the old prefsV3.xml file, rather than simply replacing the previous contents. The list must be consistent with the related tables in the Location Awareness Services for WebSphere Premises Server database.

Define your preferences in the Preferences Administration GUI by entering information in the following **Build time** fields:

Note: Make sure you define your preferences and set your area, icon, and overview scale values correctly before you create zones.

Build time

Build time preferences are defined only when a new area or subarea is added. These preferences determine how the areas, zones, and resources display in the Spatial Management Client.

- **Area SVG:** Select an area from the menu or create or delete one.
  - Click **New** to create a new area.
  - Click **Cancel** to cancel your action without saving.
  - Click **Delete** to delete an area.

  Notes:
  - Defining an area with an SVG that is greater than 4 MB is not recommended.
  - Deleting an area also deletes its subareas.
- **SVG path:** Enter the relative path to the area scalable vector graphic (SVG) file. For example, `./svg/Matrix.svg`.
- **SVG overview path:** Enter the relative path to the area SVG overview file, which is the graphic file used for the overview window in the Spatial Management Client. For example, `./svg/Matrix.svg`.
- **SVG width:** Enter the width of the SVG file in pixels.
- **SVG height:** Enter the height of the SVG file in pixels.
- **Minimum Z:** Enter the minimum Z value, or height, for this area.
- **Maximum Z:** Enter the maximum Z value, or height, for this area.
- **Enter the width the drawing represents:** Enter the value in units that the drawing represents. For example, if the drawing represents an area that is 40 feet wide, enter `40`.

  Note: If you enter the drawing width, **Area Scale** is automatically filled in with a scale determined by the drawing width.
- **Area scale:** Enter the scale factor to use to scale the coordinate display in feet for the SVG file representation. As you move the cursor over the drawing, X and Y coordinates are visible. Move it over an area of the graphic that you know the coordinates for and adjust this value so the values match the scale of the drawing.

  Note: If you enter the area scale value, the drawing width also adjusts. The current width and height are calculated and displayed at the current scale.
- **Overview scale:** Scale the overview window to the size you want it.
- **Parent SVG area name:** If this area is to be used as a subarea, enter the name of the parent area. Otherwise leave this entry blank.

  Note: Area names must be unique across the Location Awareness Services for WebSphere Premises Server installation.
- **X offset value:** Enter the X offset value in units for placement of the subarea within the parent area. Otherwise enter `0`.
- **Y offset value:** Enter the Y offset value in units for placement of the subarea within the parent area. Otherwise enter `0`.
- **Cartesian coordinate system:** Check this box to turn on the Cartesian coordinate system, which flips the area coordinate system so that the X0 and Y0 coordinates are located in the lower-left corner of the drawing with X positive going right and Y positive going up. This system matches the X0 and Y0 coordinate system of many third-party location event providers.

The other parameters on the Preferences Administration GUI are described in the section about installing the Spatial Management Client.

Starting the Spatial Management Client (administration)

This topic provides steps for starting the Spatial Management Client if you are an administrator.

About this task

Complete the following steps to start the Spatial Management Client:

1. Start the Spatial Management Client by typing the following URL in a browser: http://*fully_qualified_host_name*/Tracking GUI/AtlasAdmin.html. If you are not an administrator, see "Starting the Spatial Management Client" on page 307.

2. Enter your user name, and password if security is enabled, and click **OK**. Your individual preferences are displayed. You can save your preferences for each area you view by clicking **Save** under **DEFAULT VIEW**. Setting preferences prevents rescaling and repositioning each time you view an area of interest.

3. In **AREA**, select the area that you want to monitor from the drop-down list.

4. In **TAGS**, select the class of tags that you want to monitor. For example, select **Asset** to view all hardware that has been defined or **All** to view all tags.

5. In **ZONES**, under **Visible**, select the category of zones that you want to view.

6. In **ALERTS**, turn the alert sound on or off and choose whether to hide or view all alerts. You can also click **Acknowledge All Alerts** to acknowledge and turn off all current alerts.

7. In **DEFAULT VIEW**, click **Save** to save the current pan and zoom settings. You can customize the view and scale of the area without having to repeat the process every time you log in to the Spatial Management Client.

   The **OVERVIEW** window provides a view of the entire area. Drag the blue box around the overview window and notice that the main graphic window of the Spatial Management Client reflects the highlighted area. The box size is controlled by the zoom slider and zoom box controls below. The upper-left corner of the blue box and the upper-left corner of the main graphic window are the same point.

   See Spatial Management Client (administration) for more information.

8. To start monitoring tags in the GUI, start the tag processing servlet:

   a. Open the WebSphere Application Server administrative console and click **Control Processing**.

   b. Select the WebSphere Application Server that is related to your installation and click **Start Selected**.

   If you do not start the tag processing servlet, tags are displayed at their last reported location.

Results

In the Spatial Management Client, the defined tags are displayed with the icons you define, either for the item or the class. These icons move on the Spatial Management Client according to the reported coordinates. If you turn alerts on, a red circle highlights the tag icon when an alert related to the tag is reported. You can click the icon and see the alert details and acknowledge the alert. The circle goes away when you acknowledge the alert.

In some cases the tags fade, which means that there is no current position information available about the tag. Location Awareness Services for WebSphere Premises Server assumes that the tag remains at the last reported position. Use the InactivityDelay system property to set the length of time after which a tag starts

to fade. To avoid moving tags away from the last reported position, set this parameter to a high value. See "System Properties" on page 291 for a complete list of system properties.

Defining zones

This topic describes how to define zones for Location Awareness Services for WebSphere Premises Server.

Use the "Spatial Management Client (administration)" to define zones for Location Awareness Services for WebSphere Premises Server.

Spatial Management Client (administration)

This topic describes the administration version of the Spatial Management Client.

The Spatial Management Client provides a state of the art visual interface which shows the location of tags in real time, allowing an authorized user to monitor employees, contractors, and visitors in hazardous areas, to respond immediately to emergencies, and to locate high-value assets. With the administrative version of the GUI, you can also create or delete zones for special monitoring.

Notes: For optimal GUI performance:
- Use only Internet Explorer 6.0 with the Adobe Scalable Vector Graphics (SVG) Viewer for your browser.
- Maximize the Spatial Management Client for the best results.
- Restart the GUI whenever you change the screen resolution.
- Do not use browser functions. For example, using the **Back**, **Forward**, and **Refresh** buttons in the browser can lead to inconsistent displays of areas, tags, and menu options.

For keyboard accessibility of the GUI, edit the Mouse settings.
1. Select **Start** → **Settings** → **Control Panel** → **Accessibility Options**.
2. On the Mouse tab, select **Use MouseKeys**. This option allows you to control the pointer with the numeric keypad on your keyboard.

The Spatial Management Client retrieves all tags for an area in the following cases:
- When an area is opened
- When the class filter is changed
- Every n polling intervals. The value of n is set according to the `<DisplayRefreshCounter>` parameter in the prefsV3.xml file. If this parameter is not present in the prefsV3.xml file or it is set to 0, then a full redraw is not scheduled on the Spatial Management Client.

In all other cases, tags are only refreshed when they change their position or they change their alert state.

If you experience problems with the Spatial Management Client, refer to the troubleshooting tips in the product documentation for possible solutions.
- **AREA**

  Select the area that you want to monitor from the drop-down list.
- **TAGS**

  Select the class of tags that you want to monitor. For example, select **Asset** to view all hardware that has been defined.
- **ZONES**

Visible: Select the category of zones to view.

- **ALERTS**

  Sound: Turn the alert sound **On** or **Off**.

  Hide: To view all alerts, select **No**. To hide all alerts, select **Yes**.

  Tag filter: Filter the tags displayed. The options are **2d/2d**, **p-data**, **inactive**, **alerts only**, and **all**.

  Note: These tag filters do not affect the zone tag count. They only affect what you can see on the map. For example, if there are three tags in zone Z and one of them has no accurate location information (it has only proximity data) and you filter the tags by p-data, only one tag remains visible on the map, but the tag count for zone Z still shows 3.

- **DEFAULT VIEW**

  Click **Save** to save the current scaling, positioning, and menu settings to your user preferences. You can customize the view and scale of the drawing without having to repeat the process every time you start the Spatial Management Client.

- **OVERVIEW**

  This window provides a view of the entire area. Drag the box around the overview window and notice that the main graphic window of the Spatial Management Client reflects the highlighted area. The box size is controlled by the zoom slider and zoom box controls below. The upper-left corner of the box and the upper-left corner of the main graphic window are the same point.

- **Cluster view**

  When several tags are close together and cannot be distinguished from each other, the cluster icon displays to indicate that there are several icons overlaying each other. Icons might overlay because the icons are too large, the current zoom is not close enough, or the tags are reported to have the same coordinates. To correct overlaying tags, try one of the following:

  – Downscale the size of the icons until they do not overlay each other.

    To configure the size of the icons that display in the cluster view of the main window:

    - Press the Ctrl key plus the space bar to display the Tag Zoom Control window. Then click **Up** to enlarge the icons or **Down** to shrink the icons. Icons resize immediately.

    - To close the dialog window, close the window or press the Ctrl key plus the space bar again. You can save the configured icon size with your user preferences.

  – Zoom closer to the icons until you can distinguish them from each other.

  – Click the cluster icon to get a list of icons within the cluster. A window opens to display all the icons of the cluster and the information for each tag according to the current configuration (for example, labels, X and Y coordinates, and alerts). To see more information about a tag, click the appropriate icon and the information appears in the detail view while the cluster view window closes.

- **Zoom selection rectangle**

  Click on the dotted rectangle (zoom selection rectangle) and move the pointer to the main graphic window where you can click and drag to create a zoom selection rectangle. When you release the mouse, the window zooms into the selected area.

- **Zoom slider**

Use the slider to enlarge or shrink the current image in the main window. You can drag the slider button, click on the hashed lines, or click the magnifying glass icon to change the zoom.

Note: When you have highly magnified an area, the blue box in the overview window might not be able to represent the area and it becomes a small black rectangle and no longer zooms. You can still drag the box to pan another area.

- **Count**

  The Count window is a draggable window (click and press Shift to drag) that provides a list of areas, subareas, and zones and the number of tags currently in them. Only those zones that match the type of zones set to visible in the **ZONES** drop down menu are displayed.
  - Click the area or zone name to display a current tag count window that lists the number of tags in the area and zone. All subareas and zones are listed under the area they are associated with.
  - Click **Hide** to hide the area or zone or **Show** to display the area or zone on the main window.

  Note: Only content filters, such as filtering for all the tags in the Person class, affect the zone count. Technical filters for details about the tags (2d/3d, p-data, and so on) apply to the visibility of the tags on the map, but they do not affect the zone counts.

- **Evacuation View**

  Click this button to open a new window that displays the zones within the selected area and the number of tags within the zones. Click a zone to expand details about the tags within the zone. You can open multiple evacuation views at one time.

  The tags shown within the zones will be filtered based on any search criteria you specify in the main view and you can click the pause button in the evacuation view to pause and view the tag information at a specific instance. You can also open the evacuation view when you are replaying data.

  If you want to view an evacuation view for another area, you must open another instance of the Spatial Management Client.

- **Search**

  Click this button to search by class, group, or tag properties, or a combination of them.

  Note: The search is *not* case sensitive. Also, the **AND** and **OR** only apply to the filter attributes within the class, group, and tag criteria. When you search by a combination of class, group, and tag criteria, they are always combined by **AND**.
  - **Class Properties**

    Select a class or classes to search for. Enter your search criteria. Click **AND** if all the search criteria you enter must be found or click **OR** to display search results for any search criteria that you enter.
  - **Group Properties**

    Select the group to search for. Click **AND** if all the search criteria you enter must be found or click **OR** to display search results for any search criteria that you enter.
  - **Tag Properties**

To search for a specific tag, click **Tag** and enter the search criteria. Click **AND** if all the search criteria you enter must be found or click **OR** to display search results for any search criteria that you enter.

Click **Search** to search for the specified criteria or click **Reset** to clear all entries and perform a new search. Search results are displayed in a table or list format. When you select a tag in the table or list, the tag will be highlighted by a circle in the Spatial Management Client. If the tag is located in a different area, the area will open in the Spatial Management Client. Click **Save** to save the results to a file or close the window to exit without saving.

- **Replay**

  Click this button to replay tag movements and events that occurred during a specific time frame.

  A window displays. Enter the start and end date and time for the period of time you want to replay and click **Enable Replay Console**.

  Select the area for which you want to display tag movements and events. Then click **Play** in the replay dialog to the right of the main window to watch the tag movements and events that occurred in the area during the specified time frame. Click **Pause** to pause events and **Resume** to resume playing them. Click **Exit** to close the replay dialog and to return to the current area and time.

  Note: Times are relative to times on the database server. The machines that host the database server and WebSphere Application Server must be set to the same time zone.

- **Group Color On/Off**

  Click this button to turn group color on or off. The color associated with the group in the Groups Manager portlet is seen as a colored rectangle behind the tag icon. Group color is off by default.

- **Acknowledge All Alerts**

  Click this button to acknowledge and turn off all current alerts.

Tags

For tags displayed on the Spatial Management Client, use the following features:

- **Tag Details:** Click a tag to display details about the tag including its tag ID, coordinates, and the class it belongs to. If there is an alert associated with the tag, you can acknowledge it by clicking **Acknowledge Alert**.
- **Label:** Hold down the Ctrl key and click a tag to display the Label window. Select the information to be displayed for the tag when you hover over it. For example, select **Label** to display the label text defined for the item, select **Tag ID** to display the tag ID, or select **X**, **Y**, or **Z** to display location coordinates for the tag.

Zones

Note: In the Spatial Management Client, the term *barrier zone* is a synonym for a *boundary zone*, which is defined in the **Boundary Zones** portlet.

For zones displayed on the Spatial Management Client, use the following features:

- **Zone details:** Click a zone to display details about the zone including name, function, coordinates, and number of tags in the zone.

  This feature also allows following actions for a zone:

– **Hide zone:**: If you select this, the zone is hidden (but tags are still displayed). To show the zone again, use the **Count** window.
– **Show all tags**: This option lists all tags that are currently in the selected zone in a table similar to the **Search** results window. All selected filters for the zone apply to the search results as well (such as the class and tag properties).

- **Creating a zone:** Create a zone in the Spatial Management Client by holding down the Shift key and clicking on the main window to enter coordinates for the zone. The first click is represented by a small green dot; the second and subsequent clicks connect lines that outline the area. After all lines are selected, the area of the zone is automatically shaded. Release the Shift key and click once more to finish creating the zone.

  Note: When you are pressing the Shift key, you can also click on tag icons to select the coordinate as a point in the zone.

  In the Zone Creation window, enter the following information about the zone:
  – **Choose zone type:** Select the type of zone you are creating.
  – **Name:** Enter a unique name for the zone.

    Note: If you enter the name of an existing zone, you overwrite the existing zone. Make sure your name is unique.
  – **Min Z:** Enter the minimum height of the zone.
  – **Max Z:** Enter the maximum height of the zone.

- **Modifying a zone:** You can modify an existing zone in the Spatial Management Client by holding down the Shift key and clicking on the main window to enter new coordinates for the zone. The first click is represented by a small green dot and the second and subsequent clicks will be connected by lines and the area of the zone is shaded. Release the **Shift** key and click once more to finish creating the zone.

  In the Zone Creation window, enter the following information about the zone:
  – **Choose zone type:** Select the type of zone you are creating.
  – **Name:** Enter the name of the existing zone you are modifying.
  – **Min Z:** Enter the minimum height of the zone.
  – **Max Z:** Enter the maximum height of the zone.

- **Delete a zone:** Hold down the Alt key and click a zone to delete it.

Restrictions on new areas and zones
This topic lists restrictions that exist for new areas and zones.

When you define a new area or zone, existing tags and tag to zone relationships will not be displayed or logged for the new area or zone. For example, you will need to recreate boundary zones and gates and review any historical data you are interested in. New alerts and tag data will be read and analyzed; however, old events will not be reanalyzed to determine whether a tag is within a newly defined area or zone.

For example, consider the following scenarios:
- If three-dimensional tag coordinates are read from the tag, the tag will be displayed and counted in the new area or zone.
- If only one device reads the tag, indicating its presence in the zone, the tag will not be shown or counted in the new area or zone.

- If no information is received from the tag but it was last seen in a location that would be inside the new area or zone, the tag will not be shown or counted in the area or zone.
- If no information is received from the tag, but it had passed a gate or barrier zone previously that you have now defined for the new area or zone, then the tag will not be shown or counted in the new zone.

To summarize, old location events that were received by devices that are now in a newly defined area or zone are ignored by the new area or zone. Only new events will be analyzed and displayed for the new area or zone. This also applies to zone-related rules. Since rules evaluate zone entry and exit event, they are not triggered until a tag enters or leaves a zone.

Furthermore, area and zone names must be unique across the Location Awareness Services for WebSphere Premises Server installation.

Defining the topology

This topic lists the portlets you can use to define the Location Awareness Services for WebSphere Premises Server topology (event providers, devices, gates, registration units, and boundary zones).

Event providers provide Location Awareness Services for WebSphere Premises Server with position data for the tags. Use the following portlet to define these providers and relate them to specific areas:
- "Event Provider" on page 270

  Log in to WebSphere Application Server administrative console and click **Topology** → **Event Provider** to access this page.

A device relates to a hub, and a hub has a coordinate system. A hub can relate to multiple areas. If a tag or device position is within the area and the hub relates to this area, then the tag or device can be seen in the area. Use the following portlet to define devices and assign them to a hub:
- "Devices" on page 272

  Log in to WebSphere Application Server administrative console and click **Topology** → **Location Devices** to access this page.

Gates provide access control for the entryways and exits of a zone. See "Monitoring the entry and exit in an area (gates)" on page 243. Use the following portlet to define these gates:
- "Gate Manager" on page 273

  Log in to the WebSphere Application Server administrative console and click **Topology** → **Gate Manager** to access this page.

Registration units read tag IDs and make them available to you for item definition. Use the following portlet to define these units:
- "Registration Units" on page 274

  Log in to the WebSphere Application Server administrative console and click **Topology** → **Registration Units** to access this page.

Boundary zones provide access control for areas that are not fully covered by devices. See "Monitoring the entrance and exit of zones that are not fully covered by devices" on page 245. Use the following portlet to define these boundary zones:
- "Boundary Zones" on page 275

Log in to the WebSphere Application Server administrative console and click **Topology** → **Boundary Zones** to access this page.

Event Provider

Use this page to define the event providers for your areas and zones.

Note: Currently location event providers are the only type of supported event provider.

Location event providers provide Location Awareness Services for WebSphere Premises Server with tag location data.

Click **Add** to define a new event provider or click **Delete** to delete an existing provider. Click **Edit** to edit details for an existing event provider.

Add new event provider

Complete the following fields to define a new event provider:

Note: You need to have defined an area before you can relate a location event provider to it.

- **Hub Base Parameters:** These parameters are used to define the event provider.
  - **Name*:** Enter a name for the event provider.
  - **Description:** Enter a description of the event provider.
  - **Related App Server ID*:** Enter the IP address for the related WebSphere Application Server.
- **Connectivity:**
  - **Connection Type*:** Select the type of connection to make to the event provider: socket, WebSphere MQ, or WebSphere Internal Messaging.
  - **Parameters:** This value is prepopulated based on your selection of a connection type:

    Note: Brackets [ ] indicate optional key value pairs.
    - **Socket**

      IPAddress=*hub_IP*;Port=*hub_listener*
    - **WebSphere MQ**

      HostName=*queue_manager_host_name*;QueueManager=*queue_manager_name*;Queue=*queue_name*
      [;TransportType=Client;Channel=*server_connection_channel*;Port=*listener_port*]
      [;UserID=*MQ_user_ID*;Password=*MQ_password*]
    - **WebSphere Internal Messaging**

      HostName=*WAS_host_name*;BusName=*bus_name*;Queue=*queue_name*;
      Port=*port_number*[;UserID=*WAS_user_ID*;Password=*WAS_password*]
- **Input Event Conversion:** Choose an input event conversion method from the list of available methods. Input event conversion methods transform provider-specific events into Location Awareness Services for WebSphere Premises Server internal events. Different event providers require different conversion methods.
  - **Implementation Name:** Location Awareness Services for WebSphere Premises Server is the default implementation name. Select **Custom** to use your own implementation name.
  - **Implementation Class:** This value is pre-populated based on your selection of an implementation name. This is the Java implementation class used for conversion. The default class is com.ibm.atlas.event.conversion.LASEventConverter.

If you selected **Custom** as the implementation name, you can enter the name of your own implementation class. Your class must be in the *was_root*\lib\ext directory on your Location Awareness Services for WebSphere Premises Server server.

– **Parameters:** This value is pre-populated based on your selection of an implementation name; however, you have to instantiate the template by replacing placeholder values with valid values.

All event converters shipped with Location Awareness Services for WebSphere Premises Server support the optional parameter `IDPrefix=`*string*. This parameter can be used for making tag IDs unique across a multi-event provider installation. The provider tag IDs are prefixed by the value specified in the `IDPrefix` parameter throughout Location Awareness Services for WebSphere Premises Server.

The `com.ibm.atlas.event.conversion.LASEventConverter` implementation class supports the following parameters:

- `ignoreTagIDs=`*name of file containing tag IDs* - For this parameter, enter the name of a file that contains tag IDs that should be ignored.

- `providerLocale=`*ISO-639 code* - This parameter is relevant if the actual locale is different from the default locale and, for example, numeric values need to be converted.

Parameters in square brackets ([*parameter*]) in the parameter template are optional. In general, parameters are keyword-value pairs separated by semi-colons (`;`).

Note: Whenever you add real values to the parameter template, remember to remove the square brackets.

Note: Contact your IBM Services representative in order to use a custom implementation.

- **Transformation options:** These parameters are used to convert the coordinates returned by the location event provider into appropriate coordinates for the area, and therefore to transform the area displayed on the Spatial Management Client. You can shift or displace the area, change its scale, rotate it, or juxtapose its position.

  – **X Offset:** Enter a value to offset the area on the X-axis. The offset value can be negative or positive and is `0.0` by default, indicating no offset.

  – **Y Offset:** Enter a value to offset the area on the Y-axis. The offset value can be negative or positive and is `0.0` by default, indicating no offset.

  – **Z Offset:** Enter a value to offset the area on the Z-axis. The offset value can be negative or positive and is `0.0` by default, indicating no offset.

  – **Scaling:** Enter a value greater than `0` to change the scale of the area. The default value is `1.0`, or no scaling.

  – **Horizontal Rotation:** Enter a value between `0` and `360` to rotate the area. This value specifies an angle in degrees and has a default value of `0`, or no rotation.

  – **X-Y Permutation:** Select this box to switch the X and Y coordinates.

- **Smoothing Algorithm:** No default smoothing algorithm is selected when you create a new provider. Instead, the **Implementation Name** field is pre-filled with a value of `None`, indicating that no smoothing is applied.

- **Implementation Name:** Select the name of the smoothing algorithm implementation to use. The other fields are pre-populated when you select an implementation name other than **Custom**. Select **Custom** to use your own smoothing algorithm.
- **Implementation Class:** This value is pre-populated based on your selection of an implementation name; however, you can modify the value. This is the Java implementation class used by the smoothing algorithm. The default class is `com.ibm.atlas.smoothing.SmoothingMovingAverage`. Leave the field empty if you do not want to specify a smoothing algorithm.

  If you selected **Custom** as the implementation name, you can enter the name of your own implementation class. Your class must reside in the *was_root*\lib\ext directory on your Location Awareness Services for WebSphere Premises Server server.
- **Parameters:** This value is pre-populated based on your selection of an implementation name; however, you can modify the value. These are the customization parameters for the smoothing algorithm. Specify them in the *keyword=value;keyword=value* format. For `com.ibm.atlas.smoothing.SmoothingMovingAverage`, specify the following parameters:
  - **TimeSeriesLength=**_value_ - This value specifies the amount of historical time that is taken into consideration and must be an integer greater than 0.
  - **Weights=**_values_ - These values allow you to weight past positions when calculating a new position. They must be decimal values between 0 and 1 that are comma-separated. The sum of the values must be 1.

  For example, `TimeSeriesLength=5;Weights=0.10, 0.15, 0.20, 0.25, 0.30`. In this example, 5 seconds are taken into consideration and the greatest weight is given to the most recent second.
- **Associated Areas:** Select the areas you want to associate with the transformation.

  After you switch to this area in the Spatial Management Client, you might still see tags moving around – even after you have removed the association between an area and a location event provider instance. This can happen even if there is no longer an association between the area and a location event provider instance. An internal cleanup is made when you delete the area; however, this strange effect cannot be suppressed due to the manner in which Location Awareness Services for WebSphere Premises Server internally maintains tag-to-area associations.

Click **Save** to save your settings or click **Cancel** to exit without saving your changes. Click **Reload** to refresh the options that are available from the menus and to reset the fields to their original state.

Note: Fields marked with an asterisk (*) are required. All other fields are optional.

Devices
Use this page to define your devices and assign them to a hub (event provider).

Devices can be either readers or a device group to which you can associate several readers. Devices must be defined here if they play a specific role. For example, if a reader represents part of a gate or if a device group represents part of a boundary zone.

A device relates to a hub, and a hub has a coordinate system. A hub can relate to multiple areas. If a tag or device position is within the area and the hub relates to this area, then the tag or device can be seen in the area.

Click **Add** to define a new device or click **Delete** to delete an existing device. Click **Edit** to edit details for an existing device.

Note: Before you can add a new device, you must have defined an event provider in the **Topology > Event Provider** page.

Add a new device or edit an existing device

Complete the following fields to define a new device or to update an existing one:
- **Name*:** Enter a unique meaningful name for the device.
- **Definition:** Enter a description of the device.
- **ID:** Enter a unique ID per event provider for the device. An ID can be a number greater than 0. Do not use 0.
- **Type*:** Choose either **Device Group** or **Reader** for the device type. If you choose **Device Group**, you can associate other devices with this group.
- **Hub*:** Select the type of event provider to use for the device.
- **Device Location:** Choose one of the following:
  - **No Location** - No position for the device is defined.
  - **Static Location** - Position is defined by X, Y, and Z coordinates. The coordinates are for the hub to which the device belongs. Static locations are recommended for fixed devices.
  - **Dynamic Location** - Position is related to a tag ID. Dynamic locations are recommended for devices associated with a mobile and active tag.
- **Associated Devices:** If you are in the process of defining a device group, you can assign other already defined readers to this group. Use the arrows to associate devices with your device group or to remove associated readers from the group.

Click **Save** to save your settings or click **Cancel** to exit without saving your changes.

Note: Fields marked with an asterisk (*) are required. All other fields are optional.

Gate Manager
Use this page to define gates.

A *gate* allows you to have only one device that specifically monitors the entry to or exit from a zone.

When monitoring zones in areas, define the gate twice: once for the zone and once for the area. Otherwise, Location Awareness Services for WebSphere Premises Server cannot correctly monitor tag counts for the zone and area.

Click **Add** to define a new gate, click an existing gate to edit it, or select a gate and click **Delete** to delete it.

Add new gate

Complete the following fields to create a gate:

Note: Before you can add a new gate, you must have defined all devices for the associated event provider from the **Topology > Devices** page.

- **Name*:** Enter a unique, meaningful name for the gate.
- **Description:** Enter a description of the gate.
- **Area*:** Select the area to associate with the gate.

   Note: For scenarios where proximity data (p-data) is used for tag positions, be sure that the gate you define belongs to the area itself, and not to a zone within the area. Otherwise, the tags may not be visible in the Spatial Management Client.

- **Zone:** Select the zone to associate with the gate. If no zone is selected, the definition applies to the whole area.
- **Hub*:** Select the event provider to associate with the gate.
- **Device*:** Select the name of the device you have already defined using the **Devices** portlet.
- **Role*:** Select the role of the gate.
   - Select **IN** to specify that the associated device monitors tags entering the gate. When the device sees a tag in the associated zone, it considers the tag to be inside the zone. The coordinates of the tag are those reported by the location event provider. An event or alert is logged to indicate that the tag left the zone.
   - Select **OUT** to specify that the associated device monitors tags exiting the gate. When the device sees a tag, it considers the tag to be outside of the zone being monitored. An event or alert is logged to report that the tag left the zone.
   - Select **IN/OUT** to specify that a tag is:
      - Logged in to the zone associated with the device as long as it is "seen" by this device only
      - Logged out if it is not seen by the device anymore (after some delay) or if it is seen by any other devices

Click **Save** to save your settings or click **Cancel** to exit without saving the changes. Click **Reload** to clear the fields or click **Back** to go back to the previous step.

Note: Fields marked with an asterisk (*) are required. All other fields are optional.

Registration Units

Use this page to define the registration units for your areas and zones.

You can designate a registration unit to provide a way to register tag IDs with Location Awareness Services for WebSphere Premises Server when you create items. For example, you can define an event provider as a registration unit and then its signals can be used to read tag IDs into Location Awareness Services for WebSphere Premises Server when defining items; you do not have to enter the tag IDs manually.

Note: When defining a location event provider as a registration unit, you should already have defined it in the **Event Provider** portlet before you define it as a registration unit.

   If you define a device group or a single device as a registration unit, the remaining devices of the event provider can be used for regular monitoring.

Otherwise, if you designate the entire event provider as a registration unit, do not use it for real-time tag reporting.

Click **Add** to define a new registration unit or click **Delete** to delete an existing registration unit. Click **Edit** to edit details for an existing registration unit.

Add new registration unit

Complete the following fields to create a new registration unit:
- **Unit Name*:** Enter a unique, meaningful name for your registration unit.
- **Description:** Enter a description for the registration unit.
- **Hub*:** Choose an event provider from the list of defined providers.
- **Device:** Choose the associated device (which can be a device group or a simple device) from the list, if applicable. Devices are listed only if they have been previously defined.

Click **Save** to save your settings or click **Cancel** to exit without saving the changes. Click **Reload** to refresh the options available from the menus and to reset the fields to their original state.

Note: Fields marked with an asterisk (*) are required. All other fields are optional.

Boundary Zones
Use this page to define boundary zones for critical zones in your area.

You use boundary zones to monitor areas that are not fully covered by devices. For example, inner and outer boundary zones can be set up at the entrance and exit of areas that are not fully covered by devices. They provide position data on tags entering and leaving those areas. If an item is detected in the outer zone and then in the inner zone, and eventually disappears or cannot be located, Location Awareness Services for WebSphere Premises Server assumes that the item is now within the area protected by the two zones. As a result of this function, inner and outer boundaries can be used to implement a light barrier.

Click **Add** to define a new boundary zone.

Add new boundary

Adding a new boundary definition consists of two steps: first, you define the zone that makes up the boundary, and then you define the zone within the boundary. The latter zone is called a *related zone*. Complete the following fields to create a new boundary zone.

Note:
- Create all boundary zones and related zones in the Spatial Management Client before you define them here. In the Spatial Management Client, the term *barrier zone* is a synonym for a *boundary zone*.
- Do not define a zone as a boundary zone of itself.
- **Area:** Select the area in which you are defining the boundary zone.
- **Zone:** Select the zone you are defining as a boundary zone. It must be in the area you selected.
- **Boundary Type:** Select the type of boundary zone you are defining:
  - **Inner** - A zone where tags are considered to be in the target zone, even if not visible. Use an **Outer** boundary zone with this type of zone.

- **Outer** - A zone where tags are considered to be out of the target zone. Use an **Inner** boundary zone with this type of zone.
  - **Single** - A zone where tags are considered to be in the target zone, even if not visible. Do *not* use an **Outer** boundary zone with this type of zone.
- **Related Area:** Select the area of the related zone.
- **Related Zone:** Select the related zone.

Click **Save** to save your settings or click **Cancel** to exit without saving your changes. Click **Reload** to refresh the options that are available from the menus and to reset the fields to their original state.

Planning for classes and items

This topic describes how to plan effectively for Location Awareness Services for WebSphere Premises Server classes and items.

To plan effectively for Location Awareness Services for WebSphere Premises Server classes and items, consider some basic rules and concepts behind the Location Awareness Services for WebSphere Premises Server classes as described below.

Class structure

When defining classes and items, start by defining your class hierarchy along with attributes and properties. Then, you can associate items with the classes. Location Awareness Services for WebSphere Premises Server classes make up a hierarchical tree, so remember the following:

- When you delete a class, it also deletes all subclasses and items belonging to the deleted class or subclass.
- When you add a subclass, it inherits all properties from the parent class. These inherited properties cannot be changed at the subclass level.
- When maintaining class properties, keep the following points in mind:
  - Make sure you identify whether subclasses have been defined for the class and whether items were defined for the class or subclass.
  - Make sure you use unique property names throughout the class hierarchy. For example, if the class *Employee* has a property named `BadgeNumber` and if the subclass, *SecurityPersonnel*, represents guards who have special badges in addition to the normal employee badge, give the special badge number a unique property name such as `SecurityBadgeNumber`.
  - Changes to key properties are restricted when the class or subclass has items defined. Therefore, the following restrictions apply:
    - Adding key properties is allowed only if no items are defined for the class or any of its subclasses.
    - Deleting key properties is allowed only if no items are defined for the class or any of its subclasses.
    - Changes to key properties are usually allowed only if they are less restrictive.
    - Renaming key properties is allowed.
    - You can only change a key property type from any value to a string. The values are kept.
  - Changes to other properties are restricted when the class or subclass has items defined. Therefore, the following restrictions apply:

- Adding other properties is allowed only if no items are defined for the class or any of its subclasses.
- Deleting other properties is allowed only if no items are defined for the class or any of its subclasses.
- Changes to other properties are usually allowed only if they are less restrictive.
- Renaming other properties is allowed.
- You can only change a property type from any value to a string. The values are kept.
- Changing a property from mandatory to optional is allowed, but you cannot make an optional property mandatory.
- Minimize the number of levels in your class hierarchy. Too many levels can make the display unusable and can decrease performance.

Class name length

Depending on font size and screen resolution, long class names might be truncated in the Spatial Management Client and Location Awareness Services for WebSphere Premises Server Administrative Console.

Subclasses are shown with an indentation that depends on the level in the class hierarchy. In order to display the full names, use the following guidelines:
- Top-level classes should not be longer than 15 to 20 characters (depending on your resolution).
- The name length should decrease by about 20 percent per level.

Defining classes, items, and groups

This topic lists the portlets you use to define classes, items, and groups.

About this task

Use the following portlets to define classes, items, and groups:
- "Classes/Items Manager"

  Log in to the WebSphere Application Server administrative console and click **Tag Registration** → **Classes/Items** to access this page.
- "Groups Manager" on page 281

  Log in to the WebSphere Application Server administrative console and click **Tag Registration** → **Groups** to access this page.

Classes/Items Manager
Use this page to define classes and individual items for a class, for example, Asset and Person.

You can define classes or subclasses depending on your needs and then define individual items for those classes.

Click **Add Child Class** to define a new class; or click an existing class to edit the fields or to define new items for the class.

Note: If items are associated with the class or any of its subclasses, you can change the **Description**, **Icon Link**, **Update Interval**, **Stationary**, **Container** and **Edge Length** attributes. All other attributes and properties are read-only and cannot be changed.

Therefore, to change the class, complete the following steps:

1. Delete the items associated with the class.
2. Change the class.
3. Add the items associated with the class.

When you delete a group, class, or zone, any rules you created that refer to those entities are not automatically deleted. You need to clean up any related rules when you delete a group, class, or zone. If you create a new group, class, or zone with the same name as one you deleted, and you have not cleaned up the old related rules, then the old rules will not apply, even if you intended them to be applicable.

Rules related to items and its properties are always triggered when an item with the properties matches the condition.

Class Details View

Click the **Class Details View** tab to view the details for a class. This view opens automatically when you click **Add Child Class** or click an existing class.

Complete or edit the following fields:
- **Class Name*:** Enter a unique, meaningful name for the class.
- **Description:** Enter a description of the class.
- **Icon Link:** Enter the file name of the graphic icon to display for this class of items. All items in the class are displayed in the Spatial Management Client with the icon.
- **Update Interval:** Enter the number of seconds Location Awareness Services for WebSphere Premises Server waits before processing location data and updating the location of the icon on the Spatial Management Client. Set this field to a higher number for items that move slowly or not at all to reduce server load. For example, if the tagged item is a mainframe computer, set the field to a higher number because it does not make sense to check its position each second.
- **Stationary:** Check this field if the class is made up of items that should not be removed from a specific location, such as hardware assets.
- **Container:** Check this field to define items in this class as containers. This means they can contain other items.
- **Edge Length:** Enter the size of the container (assume it is a cube). This value allows rules checking in later releases, such as when an item cannot leave a container.

You can define key properties, properties, or child classes for each class you create. From the menu, choose from the following actions:
- **Add Key Property**

  Key properties are mandatory for a class item. Define key properties so that all members of the class can be clearly identified. For example, a person's social security number is an adequate key property, but a person's first and last names are not adequate key properties, even when used together, because there might be two people using the same first and last names.

  Important: Make sure to define key properties with unique names.
  - **Name:** Enter a unique name for the property.

– **Type:** Select the type of value that should be entered for the property. For example, you can choose among the following types:
  - **text** - A text field. For example, select this type for a name property.
  - **textarea** - A text field with space for more characters. For example, select this type for an address property.
  - **checkbox** - A check box. For example, select this type for a property where the default is true or false.
  - **integer** - A field that allows only numeric values.
  - **date** - A calendar. Select this type for a property that will always be a date. When entering this property, click **PickDate** to select the date from the calendar or **ClearDate** to clear your selection.

Beside each property that you want to delete, click **Mark for Deletion**; then click **Save** to save your changes.

Note: You cannot delete a key property if there are any items, subclasses, or items in a subclass defined.

- **Add Property**

  Properties can either be optional or mandatory for a class item.

  Important: Make sure to define properties with unique names.
  – **Name:** Enter a unique name for the property.
  – **Type:** Select the type of value that should be entered for the property. For example, you can choose between the following types:
    - **text** - A text field. For example, select this type for a name property.
    - **textarea** - A text field with space for more characters. For example, select this type for an address property.
    - **checkbox** - A check box. For example, select this type for a property where the default is true or false.
    - **integer** - A field that allows only numeric values.
    - **date** - A calendar. Select this type for a property that will always be a date. When entering this property, click **PickDate** to select the date from the calendar or **ClearDate** to clear your selection.
  – **Min Occurs:** Enter a value indicating the minimum occurrences of the property. This value should be less than or equal to the **Max Occurs** setting. For example, enter 0 if the property is optional and 1 if it is required.
  – **Max Occurs:** This property cannot be modified. The value is 1, indicating that it can occur only one time.
  – **Default Value:** Enter a default value for the property. For example, for the Company property, enter the name of your company. This value can be modified when you create an item for the class.

  Beside each property that you want to delete, click **Mark for Deletion**; then click **Save** to save your changes.

- **Add Child Class**

  Enter the values for the class, including defining key properties, properties, and child classes (also called subclasses) for each child class, as necessary.

- **Save**

  Click **Save** to save the class or child class you are creating, as well as all key properties and properties defined for the class.

- **Delete**

Click **Delete** to delete the class, its sub classes, and all items in the class. All subclasses and items in the class are deleted.

- **Reload**

  Click **Reload** to refresh the options available from the menus and to reset the fields to their original state.

Item View

Click the **Item View** tab to view the items that have been defined for a class. You can add or edit new items for a class, assign items to groups, or delete selected items. If the item is defined as a container class, you can assign other items to the container item.

Items in this view are sorted by tag ID in ascending order. Items that do not have a tag ID are listed at the end.

Select **Add Item** to create a new item. Complete the following fields:

- **Registration Unit:** (Optional) If a registration unit has been defined and you are using it to read tag IDs into Location Awareness Services for WebSphere Premises Server, select the registration unit. This field is not always available.
- **Tag ID:** Enter the tag ID for the item.

  Enter the tag ID manually or use an external device, such as a bar code reader. Additionally, if you defined a registration unit, you can select the appropriate tag ID from the tags that are read by the registration unit.
- **Icon Link:** Enter the name of the graphic icon file. By default, the icon associated with the class displays for the item.
- **Icon Label**: Enter a label to identify the item. The label helps you quickly identify tags in Location Awareness Services for WebSphere Premises Server alerts, in search results, and on the Spatial Management Client, which allows you to view an icon label beside the tag. If an item is created or modified using import, you can specify rules for automatic label creation, such as building a label consisting of a person's first name, middle name, and last name. If the item is defined as a container class, the value for **Edge Length** is prefilled with the edge length defined for the class and can be modified for the single item.

Complete any additional fields, which vary by class.

Click **Save** to save your settings or click **Cancel** to exit without saving.

After an item is defined, you can complete the following actions:

- **Delete Items**

  Under **Choose Action**, select **Delete Items** to delete selected items.
- **Edit Properties**

  Click **Edit Properties** to edit an existing item.
- **Edit Groups**

  Click **Edit Groups** to assign the item to a group or to remove it from a group.

  Note: You can select one or multiple groups, dependent on the HierarchicalGroups system property.

  Click **Save** to save your settings or click **Cancel** to exit without saving.
- **Edit Container** (only available if the item is a container)

Click **Edit Container** to assign items to the container. A list of items that can be assigned to the container are listed, as well as a list of any items that have already been assigned to the container, if any. The items are listed by class.

Note: To assign items to the container, select one or more items under containable items. To remove assigned items from the container, select one or more items under direct children.

Click **Save** to save your settings or click **Cancel** to exit without saving.

Filtering the Item View

You can also filter the item view. Enter a string in the text field and then click **Apply Filter**. The items will be filtered according to the string you enter. If any of the property values or tag IDs for an item contains the string, the item will be shown. Click **Clear Filter** to clear the filter criteria.

Note: Fields marked with an asterisk (*) are required. All other fields are optional.

Groups Manager

Use this page to define groups.

Click **Add** to define a new group or click an existing group to edit it. You can also use this page to view items in a group, add an item to a group, and remove an item from a group.

Add new group

Click **Add** and then enter values in the following fields to create a group:
- **Group Name*:** Enter a unique, meaningful name for the group.
- **Description:** Enter a description of the group.
- **Group Color:** Select the color that you want to use to identify the group. You can only assign a group color if the system property `HierarchicalGroups` is set to `Y`. The icons of group members are outlined in the selected color in the Spatial Management Client.

Click the arrows to add or remove groups to or from the **Group Members** column. The **Selectable Groups** column lists all defined groups.

Click **Save** to save the group you are creating or click **Delete** to delete the group.

Note: Fields marked with an asterisk (*) are required. All other fields are optional.

View items in a group

Complete the following steps to view items in a group:
1. In the Group Manager portlet, click the group for which you want to modify the item membership.
2. Click **ItemsView**.
3. Optionally, to reduce the items to choose from or to search on specific criteria, enter search criteria in the **Filter Items over properties** field and click **Apply Filter**.
4. In the **Only show items of the following class** field, select the class for which you want to view items or select **All classes**.

Add items to a group

Complete the following steps to add an item to a group:

1. Click the group you want to add items to and then click **ItemsView**.
2. In the **Possible Group Members** column, select the item or items you want to add to the group and click the left arrow button (<<). The item now appears in the **Group Members** column.

   Note: If the **Possible Group Members** column is not visible, click **Show possible group members**. To hide the column, click **Hide possible group members**. Any filter criteria you have specified applies to all items on the groups portlet and, therefore, also limits the list of possible group members.

3. When you finish adding items, click **Save**.

Remove an item from a group

Complete the following steps to remove an item from a group:

1. Click the group you want to remove items from and then click **ItemsView**.
2. In the **Group Members** column, select the item or items you want to remove from the group and click the right arrow button (>>). The item is removed from the **Group Members** column.
3. When you finish removing items, click **Save**.

Defining rules

This topic lists the portlet you use to define rules.

Rules define conditions and policies that need to be met. For example, rules can be used to restrict access to certain zones or to limit the amount of time an item stays in a zone. Business rules are implemented based on a generic Complex Event Processing (CEP) engine which facilitates the development of additional rule types. Events (alerts) occur when rules are violated. Events are published and saved in the event database. Subscriber programs can subscribe to Location Awareness Services for WebSphere Premises Server events. Violations of rules related to items can also be displayed in the Spatial Management Client.

To define rules, use the following portlet:

- "Business Rules"

  Log in to the WebSphere Application Server administrative console and click **Rules/Alerts** → **Business Rules** to access this page.

Business Rules

Use this page to define the business rules for your zones. Rules define the circumstances that trigger alerts.

Note: You need to define a zone before you can define a rule for it.

When you define a rule, you can check for future events, but not for events that have already happened. For example, if a person is already in Zone A and you then define a rule that items defined in the Person class cannot enter Zone A, the result is no alert. No alert occurs because rule checking is triggered by zone entry and exits events, which did not occur in this situation. The logic is similar with a

rule for duration of stay. If a person has already been in Zone A for 30 minutes, and you define a rule that the person cannot stay in Zone A for longer than 10 minutes, no alert occurs.

Click the type of business rule you want to work with. Business rule types include:

- **"Zone Access Restriction" on page 284** - Define rules indicating persons and items that are not allowed to enter zones during specified time frames.
- **"Zone Exit Restriction" on page 284** - Define rules indicating persons and items that are not allowed to leave zones during specified time frames.
- **"Duration of Stay in Zone" on page 285** - Define rules indicating how long persons or items can remain in a zone before an alert is triggered.
- **"Maximum Items per Zone Threshold" on page 285** - Define rules indicating the maximum number of items or persons that can be in a zone at one time.
- **"Visitor Escorting" on page 286** - Define rules indicating how visitors to the location will be escorted. For example, you can specify who will escort visitors or how far away from an employee a visitor can be before an alert is triggered.
- **"Items Association" on page 287** - Define rules indicating associations between items.

A list of rules displays that are of the business type you selected. Click **Add** to define a new rule. Click **Delete** to delete an existing rule or click **Edit** to edit details for an existing rule.

The following fields are available for all business rules except for Visitor Escorting:

- **Activity**

  Specify the time frame when the rule should be applied. You can specify to **Always** apply the rule, to apply it **From** a specific date and time (*yyyy/mm/dd hh:mm:ss*) **To** another specific date and time, or to specify a repetitive time frame for the new rule to be applied, for example outside of normal work hours on all weekdays and all day on weekends. You can also choose to **Invert** the time frame, meaning that the rule only applies during times outside the specified time frame.

  > **Note:** Times are relative to times on the database server. The machines that host the database server and WebSphere Application Server must be set to the same time zone.

  For example, if you check **Monday** and specify `08:00` as the start time and `17:00` as the end time, the rule is active on Mondays between the hours of 8 am and 5 pm. If you choose to **Invert** the rule, then it applies on Mondays except between the hours of 8 am and 5 pm (instead the rule applies from midnight to 8 am and from 5 pm to midnight).

- **Actors**

  Specify the class, group, and other filter criteria for items to which the rule applies. You can specify all three, if needed. If you specify a **Class**, then all class-specific **Attributes** are selectable. Otherwise, only the tag ID and label attributes are selectable. If you select criteria for **Inclusion**, the rule applies for all items that match the filter criteria specified. If you select **Exclusion**, the rule applies to all items except those matching the filter criteria. If no **Class**, **Group**, or **Attribute** is specified in both the **Inclusion** and the **Exclusion** sections, the rule applies to every defined item.

  For example, if you want the rule to apply to all items in the Person class, except for those in the Security group, specify the **Class** value as **Person** for

inclusion and the **Group** value as **Security** for exclusion. You can also exclude the rule from applying to specific people or items by filling in the **Zone** values in the **Exclusion** column.

- **Zones**

  Specify the **Zone** and **Zone Type** to which the rule is restricted. Similar to **Actors**, you can specify **Zones** for **Inclusion** and **Exclusion** by filling in the values in the respective columns. In both cases, you can select a single zone or all zones.

Zone Access Restriction

This rule type allows you to specify the times when specific classes or groups of persons or items cannot enter specific zones.

Complete the following fields to create a new rule:

- **Identification**

  Enter a **Name** and **Description** for the new rule.
- **Activity**
- **Actors**
- **Zones**
- **Alert Actions**

  Specify the alert action to take when the rule is violated. You can specify a combination of the following actions:

  - **Display Alert** displays the issue in the Spatial Management Client.
  - **Log Alert** sends the alert to CEI. You can also define a notification channel to call a program as a result of this alert. For example, the alert action could be to send an email.
  - **Customized Notification** calls a notification program outside of CEI and requires special customization.

Zone Exit Restriction

This rule type allows you to specify the times when specific classes or groups of persons or items must not leave specific zones.

Complete the following fields to create a new rule:

- **Identification**

  Enter a **Name** and **Description** for the new rule.
- **Activity**
- **Actors**
- **Zones**
- **Alert Actions**

  Specify the alert action to take when the rule is violated. You can specify a combination of the following actions:

  - **Display Alert** displays the issue in the Spatial Management Client.
  - **Log Alert** sends the alert to CEI. You can also define a notification channel to call a program as a result of this alert. For example, the alert action could be to send an email.
  - **Customized Notification** calls a notification program outside of CEI and requires special customization.

Duration of Stay in Zone

This rule type allows you to specify how long specified persons or items that can be in a specific zone at one time before an alert is triggered.

Complete the following fields to create a new rule:
- **Identification**

  Enter a **Name** and **Description** for the new rule.
- **Activity**
- **Actors**
- **Zones**
- **Additional Parameters**

  Specify the **Maximum duration of stay, in seconds** that an actor can stay in the zone during the specified time. For example, if you specify 120, then if a specified actor stays in the zone for more than 120 seconds, an alert will be triggered.
- **Alert Actions**

  Specify the alert action to take when the rule is violated. You can specify a combination of the following actions:
  - **Display Alert** displays the issue in the Spatial Management Client.
  - **Log Alert** sends the alert to CEI with a `LasDurationOfStay` event type. You can also define a notification channel to call a program as a result of this alert. For example, the alert action could be to send an email.
  - **Customized Notification** calls a notification program outside of CEI and requires special customization.

Maximum Items per Zone Threshold

This rule type allows you to specify the maximum number of persons or items satisfying the specified criteria that can be in a specific zone at one time.

Complete the following fields to create a new rule:
- **Identification**

  Enter a **Name** and **Description** for the new rule.
- **Activity**
- **Actors**
- **Zones**
- **Additional Parameters**

  Specify the **Maximum number of actors** that can be in the zone during the specified time. For example, if you specify 10 then if more than 10 actors are in the zone at one time during the specified time frame, an alert will be triggered.
- **Alert Actions**

  Specify the alert action to take when the rule is violated. You can specify a combination of the following actions:
  - **Display Alert** displays the issue in the Spatial Management Client.
  - **Log Alert** sends the alert to CEI. You can also define a notification channel to call a program as a result of this alert. For example, the alert action could be to send an email.
  - **Customized Notification** calls a notification program outside of CEI and requires special customization.

Visitor Escorting

This rule type allows you to specify rules that enforce the escorting of visitors and that govern how visitors will be escorted at the location. This rule type has less configuration options than the others, and its activity cannot be temporarily restricted.

Complete the following fields to create a new rule:

- **Identification**

  Enter a **Name** and **Description** for the new rule.

- **Visitor**

  Specify the tag ID, class, or group of persons or items to be escorted. You can specify an individual person or item by specifying the **Tag ID** or you can specify a **Class** or **Group** of persons or items to which the rule applies.

  Note: The visitor must belong to container classes, the escort must not contain a container class, and the DynamicContainerSupportOn system property must be selected.

- **Escort**

  Specify the tag ID, class, or group of persons or items that will escort the visitor. You can specify an individual person or item by specifying the **Tag ID** or you can specify a **Class** or **Group** of persons or items to which the rule applies. For example, you could specify that a class of persons could escort the visitor.

  Note: The visitor must belong to container classes, the escort must not contain a container class, and the DynamicContainerSupportOn system property must be selected.

- **Zone Selection**

  Specify the **Zone** and **Zone Type** to which the rule applies. In other words, specify the zones in which the visitor must be escorted.

- **Additional Parameters**

  Specify the **Maximum tolerated distance, in units** that the visitor can be away from the escort. For example, if you specify 10, then if the visitor is more than 10 feet away from an escort, an alert will be triggered.

  Note: Currently, the edge length of the visitor (who is in the container class) determines the maximum tolerated distance.

  Specify the **Maximum tolerated rule violation time, in seconds** that the visitor can be away from an escort before an alert is triggered. For example, if you specify 120, then if the visitor is more than 10 feet away from an escort for more than 120 seconds, an alert will be triggered.

- **Alert Actions**

  Specify the alert action to take when the rule is violated. You can specify a combination of the following actions:

  - **Display Alert** displays the issue in the Spatial Management Client.
  - **Log Alert** sends the alert to CEI. You can also define a notification channel to call a program as a result of this alert. For example, the alert action could be to send an email.
  - **Customized Notification** calls a notification program outside of CEI and requires special customization.

Items Association

This rule type allows creating associations between items. An association is created when two items fulfilling the specified filtering criteria are close to each other for a configurable period of time. Even though the rule can be applied to classes and group of items, associations are always created between two individuals.

Complete the following fields to create a new rule:

- **Identification**

  Enter a **Name** and **Description** for the new rule.

- **Base Item**

  Specify the tag ID, class, or group of persons or items to which other items are to be associated. You can specify an individual person or item by specifying the **Tag ID** or you can specify a **Class** or **Group** of persons or items to which the rule applies. There can be multiple base items.

  Notes:

    – The base items must be members of classes that have been specified as containers, and the system property `DynamicContainerSupportOn` must be selected.
    – The edge length must be greater than zero.

- **Associated Item**

  Specify the tag ID, class, or group of persons or items to be associated with others. You can specify an individual person or item by specifying the **Tag ID** or you can specify a **Class** or **Group** of persons or items to which the rule applies. There can be multiple associated items. The item to be associated must not be a container item.

- **Zone Selection**

  Specify the **Zone** and **Zone Type** to which the rule applies.

- **Additional Parameters**

  Specify the **Maximum distance, in units** that the base item and the associated item may be apart and still be associated. For example, if you specify 10, then an association only takes place if the associated item is within a radius of 10 from the base item.

  Note: Currently, the edge length of the base item (that is in the container class) determines the maximum distance.

  Specify the **Minimum time of being together, in seconds**. This means the minimum period of time that both items must be close to each other before an association is created and an alert is triggered. For example, if you specify 120, then two items must be not more than 10 feet away from each other for at least 120 seconds before an alert will be triggered.

- **Alert Actions**

  Specify the alert action to take when the rule is violated. You can specify a combination of the following actions:

  – **Display Alert** displays the issue in the Spatial Management Client.
  – **Log Alert** sends the alert to CEI. You can also define a notification channel to call a program as a result of this alert. For example, the alert action could be to send an email.
  – **Customized Notification** calls a notification program outside of CEI and requires special customization.

Tips for using this rule:

- Both the container tag and the associated tag must move into the target zone *after* the zone-related rule has been defined.
- The associated tag must be ″inside″ the edge length of the container tag longer than the minimum time without interruption.
- The base item must be the last item moving because the association rule is evaluated when the container items move.

Click **Save** to save your settings or click **Cancel** to exit without saving the changes. Click **Delete** to delete the rule.

Note: Fields marked with an asterisk (*) are required. All other fields are optional.

Defining how to handle alerts

This topic helps you define how to handle alerts with Location Awareness Services for WebSphere Premises Server.

Alerts are generated when a rule has been broken within Location Awareness Services for WebSphere Premises Server or when there are diagnostic events from an event provider. These alerts are persisted to an event database to which you can subscribe. You define how to react to alerts by defining notification programs and notification channels. An email service is provided as a sample notification program.

Use the following portlets to define how alerts are handled:
- "Notification Program Manager"

  Log in to the WebSphere Application Server administrative console and click **Rules/Alerts** ▸ **Notification Programs** to access this page.
- "Notification Channels" on page 289

  Log in to the WebSphere Application Server administrative console and click **Rules/Alerts** ▸ **Notification Channels** to access this page.
- "Mail Host Configuration" on page 289

  Log in to the WebSphere Application Server administrative console and click **Rules/Alerts** ▸ **Mail Server** to access this page.
- "Mail Receiver Configuration" on page 290

  Log in to the WebSphere Application Server administrative console and click **Rules/Alerts** ▸ **Mail Receiver** to access this page.

Notification Program Manager
Use this page to define notification programs.

A notification program is a program or Web service that can be triggered when an event is logged.

Click **Add** to define a new program or click **Delete** to delete an existing program. Click **Edit** to edit details for an existing program.

Add new notification program

Complete the following fields to create a new notification program:

- **Notification Program Name*:** Enter the name of the program. For a Web service, enter the URL for the Web service. For a batch program, enter the file name of the batch program.
- **Notification Program Description:** Enter a description of the program.
- **Notification Program Call Type:** Select **Web Service** or **Command**.
- **Notification Program Call Details*:** Complete this field depending on the call type. If the program is a command, enter the directory where the program is located. If the program is a Web service, enter the name of the Web service method to be called.

Click **Save** to save your settings or click **Cancel** to exit without saving the changes.

Note: Fields marked with an asterisk (*) are required. All other fields are optional.

Notification Channels

Use this page to define notification channels.

Notification channels define the filter criteria for a given subscriber that should be called for an event. A subscriber is a program subscribing all, or a defined subset of, the events arriving for a given event group. It dispatches the arriving events to Location Awareness Services for WebSphere Premises Server notification programs, which are programs or Web services that can be triggered when an event is logged.

Click **Add** to define a new channel or click **Delete** to delete an existing program. Click **Edit** to edit details for an existing program.

Add new notification channel

Complete the following fields to create a new notification channel:

Note: A subscriber program must exist before you can add a new notification channel.
- **Subscriber:** Select the subscriber program.
- **Program:** Select a notification program.
- **Description:** Enter a description of the program.

Complete the following fields to create a notification channel matching the filter criteria you selected. Only a positive match for valid criteria will produce valid results.
- **Tag ID:** Enter the tag ID of a person or asset.
- **Tag Label:** Enter the label of the tag.
- **Tag Class:** Enter a class of items to search for.
- **Tag Group:** Enter a group to search for.
- **Zone:** Enter a zone for the events.
- **Event Type:** Select a type of event to search for.
- **Acknowledged:** Select **All (*)** to filter all events, **Acknowledged** to filter only the events that have been acknowledged, or **Active** to filter only the events that have not been acknowledged.

Click **Save** to save your settings or click **Cancel** to exit without saving the changes.

Mail Host Configuration
Use this page to define the mail servers for your alerts.

Click **Add** to define a new mail server or click **Delete** to delete an existing server. Click **Edit** to edit details for an existing server.

Add new mail host configuration

Complete the following fields to define a new mail server:
- **Host Address*:** Enter the fully qualified host name or IP address of the mail server.
- **Port*:** Enter the mail server port number.
- **Default Sender*:** Enter the name of the default sender.
- **Default Subject:** Enter a default subject for the alert.

Click **Save** to save your settings or click **Cancel** to exit without saving your changes.

Note: Fields marked with an asterisk (*) are required. All other fields are optional.

Mail Receiver Configuration
Use this page to define the individuals or groups who will receive alert notification. Also specify what types of alerts to send notification of and when to send them.

Click **Add** to define a new mail receiver or click **Delete** to delete an existing receiver. Click **Edit** to edit details for an existing receiver.

Add new mail receiver

Complete the following fields to create a new mail receiver:

Note: Times are relative to times on the database server. The machines that host the database server and WebSphere Application Server must be set to the same time zone.
- **Receiver Name*:** Enter the name of the receiver.
- **Receiver Address*:** Enter the e-mail address of the receiver.
- **Week Days:** Select the days of the week when e-mail should be sent to the receiver.
- **Start Time*:** Enter a start time after which e-mail can be sent to the receiver each day. Use the format hour, minute, and second (HH:MM:SS).
- **End Time*:** Enter an end time after which e-mail should not be sent to the receiver each day. Use the format hour, minute, and second (HH:MM:SS).
- **Alert Types*:** Select the type of alert event to send to the receiver.
- **Mail Host*:** Enter the fully qualified host name of the mail server.

Click **Save** to save your settings or click **Cancel** to exit without saving your changes.

Note: Fields marked with an asterisk (*) are required. All other fields are optional.

Setting system properties
This topic lists the portlet you use to set system properties.

About this task

You can set Location Awareness Services for WebSphere Premises Server system properties using the following portlet:

- "System Properties"

    Log in to the WebSphere Application Server administrative console and click **System Properties** to access this page.

System Properties

Use this page to set system properties. System properties are unique and predefined.

You can edit the properties on this page. Click **Save** to save the changes.

The following system properties are used:

Table 69. Default system properties

Name	Type	Default	Description
LasVersion	String	current version number	Shows the Location Awareness Services for WebSphere Premises Server version that is installed. This property is read-only.
AllEventsGroup	String	All events	Name of the events group that holds all Location Awareness Services for WebSphere Premises Server events.
BIRTViewerURL	String	http://localhost:9080/birt-viewer/ frameset?__report=	Use this URL to view BIRT reports. If WebSphere Application Server was installed using different ports or if the BIRT engine was installed on a different WebSphere Application Server system, modify the value of this URL to point to the correct location.
BatteryExhaustedAlertAction	String	Event	Alert action if the battery of a tag is completely exhausted. The alert generates an event. Valid values are `Event`, `Display`, `Event, Display`, and `Display, Event`. In the Spatial Management Client, the battery icon displays.
BatteryLowAlertAction	String	Event	Alert action if the battery of a tag is low. The alert generates an event. When the alert is triggered, you will not receive another alert unless the battery rises above the threshold and then triggers it again. Valid values are `Event`, `Display`, `Event, Display`, and `Display, Event`. In the Spatial Management Client, the battery icon displays.

Table 69. Default system properties (continued)

Name	Type	Default	Description
BatteryThreshold	Integer	1	Battery threshold that triggers an alert when the battery is underrun. The battery status can be: • 3, which is full or completely charged • 2, which is high or sufficiently charged • 1, which is low or somewhat charged • 0, which is empty or not charged
ContainerSupportOn	Boolean	The box is not checked, which means No	Turns container processing on during runtime processing, meaning you can add an item to a container. The box can either be checked to mean Yes or not checked to mean No. Use this property in scenarios with containers equipped with active tags and content items without active tags. Once entered to a container, the content items should inherit the container position. **Note:** This property should not be selected at the same time as DynamicContainerSupportOn. If it is, the ContainerSupportOn property will be ignored.
CurrentSVGDir	String	.//svg	Defines the directory below AtlasDirectory, which is used to hold the historical SVGs temporarily for replay.
DefaultDateFormat	String	MM/dd/yyyy	Format used to display dates and accept date input in Location Awareness Services for WebSphere Premises Server. By specifying MM/dd/yyyy as the pattern for data pertaining to dates, • Input to the GUI, such as 01/12/2008, will be interpreted as January 12, 2008 (not December 1, 2008). • Output from the GUI will be displayed in the specified pattern format, for example 01/12/2008. For detailed information on time format syntax, refer to the Java API for SimpleDateFormat.

Table 69. Default system properties (continued)

Name	Type	Default	Description
DynamicContainerSupportOn	Boolean	The box is checked, which means Yes	Turns on dynamic container processing. The box can either be checked to mean Yes or not checked to mean No. With this flag set, Location Awareness Services for WebSphere Premises Server is able to detect by position whether a tag is near a container (using its edge length) and will add an item to or remove an item from a container. Use this property if both the container and the content items are equipped with active tags. Each item can be tracked individually. This is also prerequisite for the escorting and association rule. **Notes:** • If you have a lot of container items, this setting will have an impact on performance. Enable this option only if you use this kind of dynamic container assignment often, or if you have defined escorting rules. • When the content item is not seen by the RTLS system, it will not inherit the container position but will stay on the last seen position. To force inheritance of the container position, see ContainerSupportOn. • This property should not be selected at the same time as ContainerSupportOn. If it is, the ContainerSupportOn property will be ignored.
HierarchicalGroups	Boolean	The box is checked, which means Yes	Specifies whether or not to use hierarchical groups. The box can either be checked to mean Yes or not checked to mean No. **Note:** When you uncheck this box to set this value to No, specifying that you do not want to use hierarchical groups, you cannot switch back to Yes. Also, once you uncheck the box, you may have to wait up to one minute for the changes in the setting to take effect.
InactivityDelay	Integer	60	Time in seconds that Location Awareness Services for WebSphere Premises Server waits before displaying a tag as inactive in the Spatial Management Client if no new position coordinates are received. **Note:** The value specified for this property will be added to the value specified for the WatchdogDelay property.

Table 69. Default system properties (continued)

Name	Type	Default	Description
IsStationaryRuleAlertAction	String	None	Defines whether an event is generated if an item that is defined as stationary is moving. Valid values are `Event`, `Display`, `Event, Display`, and `Display, Event`. If a class that is defined as stationary moves twice the amount of feet defined in MaxToleratedMovement, an event is generated once every 5 minutes to avoid flooding stationary events when an item is moving. An event could be similar to the following example:`Item with tag [00000017] with label [alabelele], defined as stationary has moved at [Tue Jan 22 22:56:56 CET 2008]. Details: Position [38.30, 38.30, 0.00], Classes: [Asset], Groups: [Laptop]`
LasDirectory	String	C://IBMHttpServer// htdocs//en_US	Directory that holds subdirectories, such as archive and search, that are the default values for the Location Awareness Services for WebSphere Premises Server Administrative Console. The specified directory must already exist.
LogHistory	Boolean	The box is not checked, which means No	Specifies whether to save runtime data for the tags. The box can either be checked to mean Yes or not checked to mean No.
MaxToleratedMovement	Integer	2	Number of feet an item can move without generating an alert when belonging to a class that is defined as stationary. To avoid a flooding condition of stationary alerts, if an item moves twice the amount of units defined, then a stationary alert will be generated once every 5 minutes.
MaxUnrecognizedMovement	Integer	1	Number of feet an item can move before it is identified as moving. Movements within the specified number of feet are not reported. This property also affects when a tag is identified as having entered or exited a zone. A tag is considered to have entered or exited a zone if its coordinates are inside or outside of the zone by at least 50 percent of this value. For example, if this value is set to 1 and a tag's coordinates indicate that the tag is inside the zone by at least six inches, the tag is considered to have entered the zone.
MinRefreshInterval	Integer	10	Time in seconds after which the tag position is updated. At least every n seconds (as specified with this parameter), the tag position is updated. If you receive updates in shorter intervals, they are used and the tag position is updated more often.

Table 69. Default system properties (continued)

Name	Type	Default	Description
MissingReadsTolerance	Integer	30	Time in seconds during which missing readings from tags are tolerated. The value specified for this property will be added to the value specified for the WatchdogDelay property and a no TagNotResponsiveAlert is generated. The system checks regularly for unresponsive tags, every *value of WatchdogDelay* seconds. Also, the system is looking for tags that have not been seen in the last *value of MissingReadsTolerance* seconds. So, it may take up to *value of WatchdogDelay* plus *value of MissingReadsTolerance* seconds until this condition is detected. If this function is critical, the value of WatchdogDelay should be smaller than that of MissingReadsTolerance.
MultiTaggingSupportOn	Boolean	The box is not checked, which means No	Indicates whether one item can be related to multiple tags. The box can either be checked to mean Yes or not checked to mean No.
NumOfBadMsgIgnored	Integer	10	Time in seconds after which low quality messages are ignored when they follow good quality messages.
NumberOfEventsPerTag	Boolean	50	Defines how many events are listed in the tag details window on the Spatial Management Client.
Performance4Report	Boolean	The box is not checked, which means No	Indicates whether performance statistics are written for report operations. The box can either be checked to mean Yes or not checked to mean No.
Performance4Search	Boolean	The box is not checked, which means No	Indicates whether performance statistics are written for search operations. The box can either be checked to mean Yes or not checked to mean No.
Performance4TagProcessing	Boolean	The box is not checked, which means No	Indicates whether performance statistics are written for tag processing. The box can either be checked to mean Yes or not checked to mean No.
ProximityAlertAction	String	Event, Display	Alert action when a tag enters or leaves a restricted area. Valid values are Event, Display, Event, Display, and Display, Event. In the Spatial Management Client, the tag icon flashes or is highlighted.
RunPerformanceTest	Boolean	The box is not checked, which means No	Specifies whether to check performance options. Use this property when debugging. The box can either be checked to mean Yes or not checked to mean No.
SimulatorFileDirectory	String	C:/IBMAtlas/Simulator/	Target directory for files with recorded data.

Table 69. Default system properties (continued)

Name	Type	Default	Description
SimulatorFileExtension	String	.txt	The file extension of the files with recorded data. A timestamp is used in the file names.
SimulatorFileLength	Integer	20	The length defines the size of the simulator file in kilobytes (KB). When the defined size is exceeded, a new simulator file is created with a new suffix. This value can be set to no more than 100.
SimulatorFileSwitchInterval	Integer	10800	Time in seconds after which Location Awareness Services for WebSphere Premises Server switches to a new output file.
SimulatorRecordingOn	Boolean	The box is not checked, which means No	Turns recording on or off. The box can either be checked to mean Yes to turn the recording on, or not checked to mean No and recording is not turned on.
TagNotResponsiveAlertAction	String	Event	Alert action if a tag is not responsive. The alert generates an event. Valid values are Event, Display, Event, Display, and Display, Event. In the Spatial Management Client, the tag icon fades.
UnknownIconLabel	String	Unknown Tag	Label of the unknown tags.
UnknownTagAlertAction	String	Event	Alert action if an unknown tag is found. The alert generates an event. Valid values are Event, Display, Event, Display, and Display, Event. In the Spatial Management Client, the unknown tag icon displays.
UnknownTagIcon	String	unknownTag.jpg	Graphical representation of the unknown tags.
WASBootstrapAddress	String	localhost 2809	Defines the bootstrap address for WebSphere Application Server if it is different than the default (such as 2810 in case of multiple servers on the same machine). The bootstrap address is used to retrieve and send alert events.
WatchdogDelay	Integer	60	Time in seconds during which non-zone-related business rules are checked. For example, if this value is set to 60, then tags will be checked every 60 seconds, whether they are responsive or not. **Note:** If another property that delays checking is set, then action will not be taken on a tag until after the accumulation of delays.

Formatting data types for importing data to Location Awareness Services for WebSphere Premises Server

This section provides information about data types and values for importing data to Location Awareness Services for WebSphere Premises Server.

Table 70. Data Types and values

Name (in ClassesItemsManager)	Type	Format	Example
checkbox	boolean	true | false	true, false
date	date	MM/dd/YYYY	11/20/2008
text / textbox	string	any string (must not contain ″or′)	John
integer	integer	any integer	-1

Importing resource data to Location Awareness Services for WebSphere Premises Server

This topic describes how to import resource data into Location Awareness Services for WebSphere Premises Server.

Location Awareness Services for WebSphere Premises Server provides an application that acts as an intermediary component between an enterprise's legacy systems and Location Awareness Services for WebSphere Premises Server to allow information about tagged items (people or assets) to be imported into Location Awareness Services for WebSphere Premises Server and, subsequently, to be updated or deleted. The application reads records from comma-separated values (CSV) files that are provided by the existing enterprise application and forms a Java Message Service (JMS) request. The application sends the JMS request to Location Awareness Services for WebSphere Premises Server through the messaging engine and then logs the responses in a log file.

Configuring properties

1. Configure the properties in the following properties files:

   Data_Export.properties
   > Contains properties that identify JMS resources and the location of the CSV and class properties files. A sample is provided in *LAS_HOME*\AtlasIntegrator\Data_Export.properties. A sample CSV file and its associated properties files are also provided in the same location.

   > Verify that the following properties are set correctly:
   > - `batchsize`: Enter the size of the JMS batch. For example, a value of `50` means that AtlasIntegrator sends packets of 50 items for import.
   >
   >   **Note:** Set this number to a low value, such as `20`, if you experience timeouts (for example, if you get a message saying that no response was received from WebSphere Application Server).
   > - `locale_language`: Specify the language corresponding to the data you wish to import. The language value should be a valid ISO language code, such as `en` for English or `de` for German.
   > - `locale_country`: Specify the country corresponding to the data you wish to import. The country value is a valid ISO country code. These

codes are the uppercase, two-letter codes as defined by ISO-3166. For example, `US` for the United States or `DE` for Germany.

- `locale_variant`: Specify the variant. The variant value is vendor or browser-specific code. For example, use `WIN` for Windows, `MAC` for Macintosh, and `POSIX` for POSIX. If you are unsure about the system you are using, leave this property empty.
- `CSV`: Enter the location of the CSV file.

  Note: The following conventions must be followed in the CSV file:
  - Each row must contain exactly one data row. You can use the new line character (\n) to force a new data row. If you want to include the new line character in a data cell without forcing a new row, enclose the contents of the data cell in double quotation marks (`"item1/nitem2"`).
  - The data cells of a data row must be delimited by a comma. A comma forces a new data cell. If you want to include a comma without forcing a new data cell, enclose the contents of the data cell in double quotation marks (`"item1,item2"`).
  - If you need to use double quotation marks in a data cell without indicating the beginning or end of the data cell contents, enclose the contents of the data cell in double quotation marks (`"Error: "error_message""`).

- `log`: Enter the location of the log file.
- `hostname`: Enter the fully qualified host name or IP address of the provider of the Service Integration bus.
- `secure`: Specify whether security has been enabled for WebSphere Application Server. The default value is `no`.

  Note: If security has been enabled for WebSphere Application Server, the Data_Export.bat file may need to be edited. The default configuration points to the sample key store and trust store files provided with WebSphere Application Server. If you use different key and trust stores or different passwords for these files, edit the Data_Export.bat file as needed. The trace.log file contains detailed logs about the communication process, including possible security related issues.

- `port`: Enter the SIB_ENDPOINT_ADDRESS of your messaging engine. The default value is 7276. If security has been enabled for WebSphere Application Server, enter the SIB_ENDPOINT_SECURE_ADDRESS of your messaging engine, which is usually 7286.
- `request_q`: Enter the name of the request queue, such as `AtlasImportRequestQ`.
- `response_q`: Enter the name of the response queue, such as `AtlasImportResponseQ`.
- `propertiesFileLocation`: Enter the directory that contains the ClassMapping.properties file and the *class_name*.properties files. Leave this property empty to specify the current directory from which the import application (Data_Export.bat) is running.
- `class`: Enter the column in the CSV data file that contains class names. This value must be specified in the `attrib`*N* format, where *N* is the integer representing the column number. For example, if the class names are in column 7, then `class=attrib7`.

- `action`: Enter the action to be performed on the record being sent to ATLAS. Valid values include:
  - `createUpdate`: Create a new record if the tagged item does not already exist in the Location Awareness Services for WebSphere Premises Server database. Otherwise, update the existing record.
  - `create`: Create a new record if the tagged item does not exist in the Location Awareness Services for WebSphere Premises Server database. Otherwise, return an error.
  - `update`: Update an existing record in the Location Awareness Services for WebSphere Premises Server database. If the record does not exist, return an error.
  - `delete`: Delete an existing record from the Location Awareness Services for WebSphere Premises Server database. If the record does not exist, return an error.

  If you do not specify an action, the default action is `createUpdate`.
- `group`: Enter the column in the CSV data file that contains group names. This value must be specified in the `attrib`N format, where N is the integer representing the column number. For example, if the group names are in column 8, then `group=attrib8`.

  Note: If you want to retain the relationship of an item to multiple groups during the import and `HierarchicalGroups` is set to `off`, you can specify multiple groups names in this column, separating the group names with a pipe symbol (|).
- `defaultClass`: Enter the name of the class that new records from the CSV file are added to if the corresponding class name specified in the CSV file is not found in the ClassMapping.properties file. For example, if a record in the CSV file contains the class name `RESOURCE SECURITY` and that class name is not found in the ClassMapping.properties file, the record is added to the class specified in this property. For example, `defaultClass=Contractor`.
- `defaultGroup`: Enter the name of the group that new records from the CSV file are added to if group information is not specified. For example, if a record in the CSV file does not contain group information, the record is added to the group specified in this property. For example, `defaultGroup=Contractor`.
- `tagId`: Enter the column in the CSV data file that contains tag ID values. This value must be specified in the `attrib`N format, where N is the integer representing the column number. For example, if the tag IDs are in column 13, then `tagID=attrib13`.
- `mq_response_timeout(secs)`: The Location Awareness Services for WebSphere Premises Server imports client sends a JMS request containing a batch of ten records from the CSV data file to Location Awareness Services for WebSphere Premises Server. Enter the number of seconds that the Location Awareness Services for WebSphere Premises Server imports client waits for the JMS response from ATLAS. The default value for this property is 60 seconds.

ClassMapping.properties

Provides a mapping from the names in the `class` column of the CSV data file to class names that are defined within the Location Awareness Services for WebSphere Premises Server database. See "Planning for classes and items" on page 276 for tips on defining the Location

Awareness Services for WebSphere Premises Server class hierarchy. For example, a ClassMapping.properties file might read as follows:

```
ACME INC.=Employee
Sunspot Heating and Cooling=Contractor
```

This file indicates that the records with `ACME INC.` in the class column are to be assigned to the Location Awareness Services for WebSphere Premises Server class `Employee` and those records with `Sunspot Heating and Cooling` are to be assigned to the Location Awareness Services for WebSphere Premises Server class `Contractor`.

class_name.**properties**

Provides the attribute details about any class. A sample is provided in *LAS_HOME*\AtlasIntegrator\Person.properties. The file name of the class properties file should be the class name. There should be one file for each Location Awareness Services for WebSphere Premises Server class.

Verify that the following properties are set correctly:

- `label`: Enter the attributes and text strings, separated by a plus sign (+), that automatically fill the tag label field and surround blank spaces with quotation marks. For example, `attrib5+" "+attrib6+" "+attrib4`.
- `icon`: Enter the attributes and text strings, separated by a plus sign (+), that represent the name of the graphic file that will represent the class items in the Spatial Management Client. For example, if the value of `attrib3` is `Susan`, which represents a specific item in the Person class, the following entry will equate to `Susan.png`: `attrib3+".png"`. Surround extensions with quotation marks.
- `attribN`: Enter the name of an attribute and its corresponding Location Awareness Services for WebSphere Premises Server property name, where *N* corresponds to the column in the CSV file that contains the information. For example, `attrib2=First Name` indicates that column 2 in the CSV file contains the first name of the item and is mapped to the Location Awareness Services for WebSphere Premises Server property named `First Name`.
- `KeyProperties`: Enter the list of attributes, separated by commas, that represents key properties. For example, `attrib5,attrib3`.

2. Run the data import application from the *LAS_HOME* directory, specifying your messaging engine user ID and password:

```
Data_Export.bat user_ID password [Data_Export.properties ClassMapping.properties]
```

Tip:

- Because the Data_Export.properties and ClassMapping.properties files are entered as parameters to the import application, you can replace these file names of these properties with names that are more meaningful to you. This allows you to set up a series of properties files with different names that reflect different tasks or mappings. For example, you could distinguish between the initial import of enterprise data and later maintenance imports.
- This command assumes that the import application is running from the AtlasIntegrator directory. If the Data_Export.properties file is not in the same location as the import application, provide the complete directory path. For example:

```
Data_Export.bat user_ID password D:\Properties\Data_Export.properties
ClassMapping.properties
```

- If the remaining properties files, such as ClassMapping.properties and
  class_name.properties, are not in the same location as the import
  application, the directory location can be specified in the
  `propertiesFileLocation` in the Data_Export.properties file. For example,
  if the ClassMapping.properties file and the *class_name*.properties files
  are located in D:\Properties, set `propertiesFileLocation=D:\\`
  `Properties\\`. If the ClassMapping.properties file and the
  class_name.properties file are located in the same directory as the
  Data_Export application, leave the value for `proertiesFileLocation`
  empty: `propertiesFileLocation=`.

3. Look at the log file specified in Data_Export.properties file to verify that the
   import application ran successfully.

   Note: Look at the trace.log file if you are experiencing connection problems.

Using the dispatcher

This topic describes the dispatcher application and how to utilize it.

The dispatcher is a standalone application that acts as an intermediary between
large Location Awareness Services for WebSphere Premises Server event providers,
such as hubs that process more than 300 messages per second, and one or more
devices. The dispatcher retrieves all location messages from the event providers it
is connected to and distributes them to one or more Location Awareness Services
for WebSphere Premises Server devices. Using the dispatcher enables Location
Awareness Services for WebSphere Premises Server to increase the number of
location messages it processes.

The dispatcher is shipped with Location Awareness Services for WebSphere
Premises Server and is located in the *LAS_HOME*\samples\
AtlasStandaloneDispatcher directory.

Communicating with event providers

The dispatcher connects to the event providers as a socket server using the IP
address and port that are specified in the dispatcher.bat file. When the dispatcher
establishes a connection, it receives all location messages sent by the provider and
distributes them to the connected devices. Each device receives a subset of the
location messages from the event provider.

If the dispatcher cannot connect, it tries again every 30 seconds. If an existing
connection to an event provider drops, the dispatcher tries to reconnect in time
intervals increasing from one to 30 seconds.

Communicating with event devices

The dispatcher communicates with a device as if it were an event provider. The
dispatcher waits for a device, which is a client application to the dispatcher, to
connect. You specify the number of clients and associated ports that can connect to
the dispatcher in the dispatcher.bat file. Each client must use an individual port.

When the dispatcher connects to a device, it forwards all location messages
assigned to that device. All messages have the same format and content as when
they are received from the event providers.

How location messages are assigned to a device

The dispatcher supports two simple algorithms for assigning location messages to a device: modulo (the suggested algorithm) and round robin. You specify the algorithm that you want to use in the Dispatcher.bat file.

- **Modulo** - This algorithm uses the last digit or letter of a location message's tag ID. The number of active devices determines which device the message is assigned to.

  If there are no active Location Awareness Services for WebSphere Premises Server devices, the dispatcher discards the location messages from the provider. The dispatcher considers only active devices, and forwards all messages arriving from the location event providers to them. If a device cannot keep up with the number of messages provided, the dispatcher queues the outstanding messages.

- **Round robin** - Using this algorithm, if *N* Location Awareness Services for WebSphere Premises Server devices are connected to the dispatcher, each gets every *N*th location message.

- **Hash map** - Setting this algorithm means that the set of available tag IDs is evenly distributed to the different devices and that messages referring to the same tag ID always go to the same device.

Note: In a production environment, use the modulo or the hash map algorithm. These dispatching algorithms work better with filtering and position smoothing within Location Awareness Services for WebSphere Premises Server. You might use the round robin algorithm in a test environment where you use fewer tags to generate test data.

Configuring the dispatcher application

This topic describes how to configure the dispatcher application.

Before you begin

Before using the standalone dispatcher application, make sure that each location event provider is defined in the Location Event Provider portlet.

About this task

This topic explains how to configure Location Awareness Services for WebSphere Premises Server ports to use the standalone dispatcher. When using Location Awareness Services for WebSphere Premises Server with the standalone dispatcher, not directly connected to the location event provider, you must configure a provider definition for each Location Awareness Services for WebSphere Premises Server port. These definitions must be identical except for the provider port number, which varies as specified for the dispatcher. All definitions must point to the same provider IP address, and the same areas must be assigned to all provider ports. For more information about the dispatcher, refer to "Using the dispatcher" on page 301.

1. Copy the contents of the *LAS_HOME*\samples\AtlasStandaloneDispatcher directory to a separate directory on your system.
2. Make a backup of the sample Dispatcher.bat file.
3. Edit the Dispatcher.bat file, providing the following parameters for each location event provider:

   - `TagIDPosition` - Specify the position of the tag ID in the input event. The default is 3.

- `Separator` - This is the separator between units of information in the input event. The default is `;` (a semi-colon).
- `HubIP` - Specify the IP address of the machine hosting the location event provider.
- `HubPort` - Specify the port number that the location event provider listens on. Typically, the port is `5117`.
- `AtlasPorts` - Specify a list of the ports that the dispatcher listens to. Separate each port number with a comma.
- `Logging` - This parameter is optional. Specify `on` to enable logging or `off` to disable logging. By default, this parameter is set to `off`. If logging is enabled, the output is logged in the SysOut file. Only enable logging for debugging purposes.
- `Algorithm` - This parameter is optional. Specify the dispatching algorithm that you want to use. By default, this parameter is set to `MODULO`.

Note: Look over the parameters to ensure that they comply with these guidelines:
- Parameter keywords and the predefined values are case-sensitive.
- Keywords and values cannot contain any blank spaces.

If you start the dispatcher without entering any parameters, a usage message is displayed. You can also enter `?`, `help`, or `h` to display the usage statement. If you enter incomplete or erroneous parameters, you receive an error message.

4. Start the dispatcher application by running the Dispatcher.bat file from a command line.
5. Stop the dispatcher by typing `stop` or `s` from a command line.

Backing up and restoring data

This topic describes how you back up historical and event data for Location Awareness Services for WebSphere Premises Server.

About this task

You are responsible to back up historical and event data for Location Awareness Services for WebSphere Premises Server. This data is stored in the Location Awareness Services for WebSphere Premises Server databases and the CEI events database. You can use the database management system (DBMS) to automatically schedule backups, archive, and delete tasks or you can manually back up these databases.

Go online to see the DB2 information center for more information.

Note: Once you make a backup you can replay the transaction logs that were used during the online backup. The data stored in the backup image will be replayed. However, if you wish to replay transactions after you back up databases, ensure that your log files are in the path where they were archived and that the subdirectories are in the data directory, such as in C:\DB2_Archived_Logs\DB2\ATLASDB\NODE0000.

Backing up your databases while online
Before you begin

Prior to backing up your system, make sure that:

- The DB2 backup batch files are in the same directory and that the log files are also created in the directory where the batch files are located. The DB2 scripts are shipped with Location Awareness Services for WebSphere Premises Server in the *LAS_HOME*\DB2\Backup Restore directory.
- The following directories exist:
  - C:\DB2_Database_Backups: Directory where the database backups are stored
  - C:\DB2_Archived_Logs: Directory where DB2 stores the archived log files
  - C:\DB2_LOGTEMP: Directory where temporary log files are created during the roll forward operation of logs stored in the database backup image

About this task

The following instructions describe how to back up your databases when you are online, which allows you to be connected to the database. To perform a backup, do the following:

1. Set up the environment by running the DoSetupBackup.bat script. It calls the setupbackup.bat script.
2. Schedule online backups of the ATLASDB and EVENT databases using the Windows `at` command and the `DoONLINEBackups_Runstats.bat` command from the C:\DB2_Backup_Scripts directory:

   Note: The `DoONLINEBackups_Runstats.bat` command also updates statistics for the tables in both databases after the backups are done. The script can also be run manually from a command prompt in the directory where the file is located and calls the following scripts:
   - OnlineBackup_Databases.bat: Creates an offline backup of the ATLASDB and EVENT databases
   - ATLASDB_RUNSTATS.bat: Updates the statistics for the ATLASDB database
   - EventDB_RUNSTATS.bat: Updates the statistics for the EVENT database

   a. To run a weekly backup at 00:30 on Sunday morning, run the following command:
      ```
      at 00:30 /every:Sunday "C:\DB2_BACKUP_SCRIPTS\DoOnlineBackups_Runstats.bat"
      ```
   b. To run a backup every day at 00:30, run the following command (on one line):
      ```
      C:\DB2_Backup_Scripts>at 00:30 /every:Sunday,Monday,Tuesday,Wednesday,
      Thursday,Friday,Saturday "C:\DB2_BACKUP_SCRIPTS\DoOnlineBackups_Runstats.bat"
      ```
   c. To delete an entry from the `at` list, run the following commands:
      1) Run `at` to list the scheduled tasks:
         ```
         at
         ```
      2) Use the ID from the list to delete the entry:
         ```
         at task_ID /DELETE
         ```
      3) Run `at` again to verify that there are no entries in the list:
         ```
         at
         ```

Backing up your databases while offline
Before you begin

Prior to backing up your system, ensure that:
- All backup scripts are located in the C:\DB2_Backup_Scripts directory. The scripts for offline backups are shipped with ATLAS in the *LAS_HOME*\DB2\ Backup Restore\OFFLINE (cold) backups directory.
- No users are active in the system and that WebSphere Application Server is not running.
- The following directories exist:
    - C:\DB2_Database_Backups: Directory where the database backups are stored

About this task

The following instructions describe how to back up your databases when you are offline, which means that users cannot be connected to the database.

Note: To turn off log archiving and allow only offline backups, run the DoTurnOffArchiving.bat script.

To make a backup, do the following:

Schedule offline backups of the ATLASDB and EVENT databases using the Windows at command and the `DoBackups_Runstats.bat` command from the C:\DB2_Backup_Scripts directory:

Note: The `DoBackups_Runstats.bat` command also updates statistics for the tables in both databases after the backups are done. The script can also be run manually from a command prompt in the directory where the file is located and calls the following scripts:
- Backup_Databases.bat: Creates an online backup of the ATLASDB and EVENT databases
- ATLASDB_RUNSTATS.bat: Updates the statistics for the ATLASDB database
- EventDB_RUNSTATS.bat: Updates the statistics for the EVENT database

1. To run a backup weekly at 00:30 on Sunday morning, run the following command:

   ```
   at 00:30 /every:Sunday "C:\DB2_BACKUP_SCRIPTS\DoBackups_Runstats.bat"
   ```

2. To run a backup every day at 00:30, run the following command (on one line):

   ```
   C:\DB2_Backup_Scripts>at 00:30 /every:Sunday,Monday,Tuesday,Wednesday,Thursday,
   Friday,Saturday "C:\DB2_BACKUP_SCRIPTS\DoBackups_Runstats.bat"
   ```

3. To delete an entry from the at list, run the following commands:
   a. Run at to list the scheduled tasks:

      ```
      at
      ```

   b. Use the ID from the list to delete the entry:

      ```
      at task_ID /DELETE
      ```

   c. Run at again to verify there are no entries in the list:

      ```
      at
      ```

Restoring databases
Before you begin

Prior to running the script, verify the following:
* The database you are restoring was dropped.
* There is only one backup image file in the path of the database backup. For example, the ATLASDB database should only have one data directory with one backup file in that directory, such as C:\DB2_Database_Backups\ATLASDB.0\ DB2\NODE0000\CATN0000\20060330.

About this task

To restore a single database, run the DoRestoreOneDB.bat script from a command line, which calls the RestoreToNewDatabase.bat script.

Scheduling deletion of tag data

This topic describes how to set up a regular schedule for deleting historical tag data.

About this task

Currently Location Awareness Services for WebSphere Premises Server does not automatically archive historical data. Therefore, it is necessary to delete historical data on a regular basis to increase performance. You can schedule tag data to be deleted on a regular basis using the ATLASDB_DEL_TAG_HISTORY_SCHEDULE.bat script. The script schedules a task to delete all historical data entries that are older than eight hours and for which newer data is available. This allows you to consistently delete historical data.

To retain historical data for a longer period of time, you must archive and back up your data separately.

Complete the following steps to set up a regular deletion process for historical data:

1. Create a directory named C:\tools\history and copy all files from the *LAS_HOME*DB2\Tools\History to the new directory. To create the directory in a different location, edit ATLASDB_DEL_TAG_HISTORY_SCHEDULE.bat with the new location.
2. Edit ATLASDB_DEL_TAG_HISTORY.bat to specify your DB2 installation directory.
3. Edit ATLASDB_DEL_TAG_HISTORY_SCHEDULE.bat to enter your DB2 for Linux, UNIX, and Windows user ID and password.
4. (Optional) This script deletes all historical data entries that are older than eight hours and for which newer data is available. If you want to change the schedule, for example to delete data every six hours, edit the 8 hour entry in the insert and the delete statements.
5. Run ATLASDB_DEL_TAG_HISTORY_SCHEDULE.bat to schedule the deletion task.

   Note: After running this script, you must either manually edit each task to change the schedule or you must delete the scheduled tasks and then rerun this script after editing it.

Each time the deletion task runs, it will log results into the
C:\tools\history\ATLASDB_DEL_TAG_HISTORY_DATA.txt file.

Operating

Use the Spatial Management Client and the Location Awareness Services for
WebSphere Premises Server Administrative Console to perform daily operation
tasks for Location Awareness Services for WebSphere Premises Server.

Starting the Spatial Management Client

This topic describes how to start the Spatial Management Client.

About this task

Start the Spatial Management Client by completing the following steps:

1. Start the Spatial Management Client by typing the following URL in a browser:
   http://*fully_qualified_host_name*/Tracking GUI/AtlasMonitor.html If you are an
   administrator, see "Starting the Spatial Management Client (administration)" on
   page 263.
2. Enter your user name, and password if security is enabled, and click **OK**. Your
   individual preferences are displayed. You can save your preferences for each
   area you view by clicking **Save** under **DEFAULT VIEW**. Setting preferences
   prevents rescaling and repositioning each time you view an area of interest.
3. In **AREA**, select the area that you want to monitor from the drop-down list.
4. In **TAGS**, select the class of tags that you want to monitor. For example, select
   Asset to view all hardware that has been defined or **All** to view all tags.
5. In **ZONES**, under **Visible**, select the category of zones that you want to view.
6. In **ALERTS**, turn the alert sound on or off and choose whether to hide or view
   all alerts. You can also click **Acknowledge All Alerts** to acknowledge and turn
   off all current alerts.
7. In **DEFAULT VIEW**, click **Save** to save the current pan and zoom settings. You
   can customize the view and scale of the area without having to repeat the
   process every time you log in to the Spatial Management Client.

   The **OVERVIEW** window provides a view of the entire area. Drag the blue box
   around the overview window and notice that the main graphic window of the
   Spatial Management Client reflects the highlighted area. The box size is
   controlled by the zoom slider and zoom box controls below. The upper-left
   corner of the blue box and the upper-left corner of the main graphic window
   are the same point.

   See Spatial Management Client for more information.
8. To start monitoring tags in the GUI, start the tag processing servlet:
   a. Open the WebSphere Application Server administrative console and click
      Control Processing.
   b. Select the WebSphere Application Server that is related to your installation
      and click **Start Selected**.

   If you do not start the tag processing servlet, tags are displayed at their last
   reported location.

Results

In the Spatial Management Client, the defined tags are displayed with the icons
you define, either for the item or the class. These icons move on the Spatial

Management Client according to the reported coordinates. If you turn alerts on, a red circle highlights the tag icon when an alert related to the tag is reported. You can click the icon and see the alert details and acknowledge the alert. The circle goes away when you acknowledge the alert.

In some cases the tags fade, which means that there is no current position information available about the tag. Location Awareness Services for WebSphere Premises Server assumes that the tag remains at the last reported position. Use the InactivityDelay system property to set the length of time after which a tag starts to fade. To avoid moving tags away from the last reported position, set this parameter to a high value. See "System Properties" on page 291 for a complete list of system properties.

Spatial Management Client

This topic describes the Spatial Management Client.

The Spatial Management Client provides a state of the art visual interface which shows the location of tags in real time, allowing an authorized user to monitor employees, contractors, and visitors in hazardous areas, to respond immediately to emergencies, and to locate high-value assets.

Notes: For optimal GUI performance:

- Use only Internet Explorer 6.0 with the Adobe Scalable Vector Graphics (SVG) Viewer for your browser.
- Maximize the Spatial Management Client for the best results.
- Restart the GUI whenever you change the screen resolution.
- Do not use browser functions. For example, using the **Back**, **Forward**, and **Refresh** buttons in the browser can lead to inconsistent displays of areas, tags, and menu options.

For keyboard accessibility of the GUI, edit the Mouse settings.

1. Select **Start** → **Settings** → **Control Panel** → **Accessibility Options**.
2. On the Mouse tab, select **Use MouseKeys**. This option allows you to control the pointer with the numeric keypad on your keyboard.

The Spatial Management Client retrieves all tags for an area in the following cases:

- When an area is opened
- When the class filter is changed
- Every n polling intervals. The value of n is set according to the <DisplayRefreshCounter> parameter in the prefsV3.xml file. If this parameter is not present in the prefsV3.xml file or it is set to 0, then a full redraw is not scheduled on the Spatial Management Client.

In all other cases, tags are only refreshed when they change their position or they change their alert state.

If you experience problems with the Spatial Management Client, refer to the troubleshooting tips in the product documentation for possible solutions.

- **AREA**

  Select the area that you want to monitor from the drop-down list.
- **TAGS**

  Select the class of tags that you want to monitor. For example, select **Asset** to view all hardware that has been defined.

- **ZONES**

  Visible: Select the category of zones to view.

- **ALERTS**

  Sound: Turn the alert sound **On** or **Off**.

  Hide: To view all alerts, select **No**. To hide all alerts, select **Yes**.

  Tag filter: Filter the tags displayed. The options are **2d/2d**, **p-data**, **inactive**, **alerts only**, and **all**.

  Note: These tag filters do not affect the zone tag count. They only affect what you can see on the map. For example, if there are three tags in zone Z and one of them has no accurate location information (it has only proximity data) and you filter the tags by p-data, only one tag remains visible on the map, but the tag count for zone Z still shows 3.

- **DEFAULT VIEW**

  Click **Save** to save the current scaling, positioning, and menu settings to your user preferences. You can customize the view and scale of the drawing without having to repeat the process every time you start the Spatial Management Client.

- **OVERVIEW**

  This window provides a view of the entire area. Drag the box around the overview window and notice that the main graphic window of the Spatial Management Client reflects the highlighted area. The box size is controlled by the zoom slider and zoom box controls below. The upper-left corner of the box and the upper-left corner of the main graphic window are the same point.

- **Cluster view**

  When several tags are close together and cannot be distinguished from each other, the cluster icon displays to indicate that there are several icons overlaying each other. Icons might overlay because the icons are too large, the current zoom is not close enough, or the tags are reported to have the same coordinates. To correct overlaying tags, try one of the following:

  – Downscale the size of the icons until they do not overlay each other.

    To configure the size of the icons that display in the cluster view of the main window:

    - Press the Ctrl key plus the space bar to display the Tag Zoom Control window. Then click **Up** to enlarge the icons or **Down** to shrink the icons. Icons resize immediately.

    - To close the dialog window, close the window or press the Ctrl key plus the space bar again. You can save the configured icon size with your user preferences.

  – Zoom closer to the icons until you can distinguish them from each other.

  – Click the cluster icon to get a list of icons within the cluster. A window opens to display all the icons of the cluster and the information for each tag according to the current configuration (for example, labels, X and Y coordinates, and alerts). To see more information about a tag, click the appropriate icon and the information appears in the detail view while the cluster view window closes.

- **Zoom selection rectangle**

  Click on the dotted rectangle (zoom selection rectangle) and move the pointer to the main graphic window where you can click and drag to create a zoom selection rectangle. When you release the mouse, the window zooms into the selected area.

- **Zoom slider**

Use the slider to enlarge or shrink the current image in the main window. You can drag the slider button, click on the hashed lines, or click the magnifying glass icon to change the zoom.

Note: When you have highly magnified an area, the blue box in the overview window might not be able to represent the area and it becomes a small black rectangle and no longer zooms. You can still drag the box to pan another area.

- **Count**

  The Count window is a draggable window (click and press Shift to drag) that provides a list of areas, subareas, and zones and the number of tags currently in them. Only those zones that match the type of zones set to visible in the **ZONES** drop down menu are displayed.

  - Click the area or zone name to display a current tag count window that lists the number of tags in the area and zone. All subareas and zones are listed under the area they are associated with.
  - Click **Hide** to hide the area or zone or **Show** to display the area or zone on the main window.

  Note: Only content filters, such as filtering for all the tags in the Person class, affect the zone count. Technical filters for details about the tags (2d/3d, p-data, and so on) apply to the visibility of the tags on the map, but they do not affect the zone counts.

- **Evacuation View**

  Click this button to open a new window that displays the zones within the selected area and the number of tags within the zones. Click a zone to expand details about the tags within the zone. You can open multiple evacuation views at one time.

  The tags shown within the zones will be filtered based on any search criteria you specify in the main view and you can click the pause button in the evacuation view to pause and view the tag information at a specific instance. You can also open the evacuation view when you are replaying data.

  If you want to view an evacuation view for another area, you must open another instance of the Spatial Management Client.

- **Search**

  Click this button to search by class, group, or tag properties, or a combination of them.

  Note: The search is *not* case sensitive. Also, the **AND** and **OR** only apply to the filter attributes within the class, group, and tag criteria. When you search by a combination of class, group, and tag criteria, they are always combined by **AND**.

  - **Class Properties**

    Select a class or classes to search for. Enter your search criteria. Click **AND** if all the search criteria you enter must be found or click **OR** to display search results for any search criteria that you enter.

  - **Group Properties**

    Select the group to search for. Click **AND** if all the search criteria you enter must be found or click **OR** to display search results for any search criteria that you enter.

  - **Tag Properties**

To search for a specific tag, click **Tag** and enter the search criteria. Click **AND** if all the search criteria you enter must be found or click **OR** to display search results for any search criteria that you enter.

Click **Search** to search for the specified criteria or click **Reset** to clear all entries and perform a new search. Search results are displayed in a table or list format. When you select a tag in the table or list, the tag will be highlighted by a circle in the Spatial Management Client. If the tag is located in a different area, the area will open in the Spatial Management Client. Click **Save** to save the results to a file or close the window to exit without saving.

- **Replay**

  Click this button to replay tag movements and events that occurred during a specific time frame.

  A window displays. Enter the start and end date and time for the period of time you want to replay and click **Enable Replay Console**.

  Select the area for which you want to display tag movements and events. Then click **Play** in the replay dialog to the right of the main window to watch the tag movements and events that occurred in the area during the specified time frame. Click **Pause** to pause events and **Resume** to resume playing them. Click **Exit** to close the replay dialog and to return to the current area and time.

  Note: Times are relative to times on the database server. The machines that host the database server and WebSphere Application Server must be set to the same time zone.

- **Group Color On/Off**

  Click this button to turn group color on or off. The color associated with the group in the Groups Manager portlet is seen as a colored rectangle behind the tag icon. Group color is off by default.

- **Acknowledge All Alerts**

  Click this button to acknowledge and turn off all current alerts.

Tags

For tags displayed on the Spatial Management Client, use the following features:

- **Tag Details:** Click a tag to display details about the tag including its tag ID, coordinates, and the class it belongs to. If there is an alert associated with the tag, you can acknowledge it by clicking **Acknowledge Alert**.
- **Label:** Hold down the Ctrl key and click a tag to display the Label window. Select the information to be displayed for the tag when you hover over it. For example, select **Label** to display the label text defined for the item, select **Tag ID** to display the tag ID, or select **X**, **Y**, or **Z** to display location coordinates for the tag.

Zones

Note: In the Spatial Management Client, the term *barrier zone* is a synonym for a *boundary zone*, which is defined in the **Boundary Zones** portlet.

For zones that are displayed on the Spatial Management Client, use the following features:

- **Zone details:** Click a zone to display details about the zone including name, function, coordinates, and number of tags in the zone.

  This feature also allows following actions for a zone:

- **Hide zone::** If you select this, the zone is hidden (but tags are still displayed). To show the zone again, use the **Count** window.
- **Show all tags:** This option lists all tags that are currently in the selected zone in a table similar to the **Search** results window. All selected filters for the zone apply to the search results as well (such as the class and tag properties).

Starting and stopping tag processing

This topic lists the portlet you use to start or stop the tag processing servlet.

Use the following portlet to start or stop the tag processing servlet:
- "Control Processing"

  Log in to the WebSphere Application Server administrative console and click **Control Processing** to access this page.

Control Processing

Use this page to start or stop reporting tags from servers that are associated with your event providers. All Location Awareness Services for WebSphere Premises Server servers associated with event providers are displayed on this page, along with their status.

Select a server and click **Start Selected** to start a server or click **Stop Selected** to stop a server. If there is only one server in the list, the server is preselected by default.

Click **Refresh Status** to refresh the status of a single server.

Note: If the status of a server is listed as **Unknown**, then the status could not be calculated. Check the configuration of the specific server.

Click **Refresh List** to refresh the entire list of servers, such as when location event providers have been added or deleted. This action will not refresh the status of the servers in the list, as indicated by the status changing to "—", which means that status was not calculated.

Configure the port, URL, user ID, and password of the TagProcessingServlet by clicking the wrench symbol in the upper right corner of the portlet. The port and URL fields are mandatory and must not be empty. The user ID and password fields can be empty if the target server is running without WebSphere Application Server security enabled. The changes apply to the current user only. The user ID and password requested are the user ID and the password of the current user. If those values change, the values have to be changed in this page as well.

Replaying tag movements and events

This topic explains replaying tag movements and events and how to do it.

Location Awareness Services for WebSphere Premises Server allows you to replay tag movements and events. For example, you might use this feature to replay events that led to a recent alert or you might use it to replay an evacuation drill to identify improvements to procedures or the need for more training.

Important: Replaying tag movements and events can severely impact performance. To avoid large amounts of historical data, schedule deletion of data after n number of hours. The amount of data stored on your system

depends on the number of tags tracked in Location Awareness Services for WebSphere Premises Server and on the database system.

Replay is based on historical administrative data (such as about zones, classes, rules, and so forth) and historical runtime data (such as tag movements, zone entry events, and rule-based events). Historical data is stored in the Location Awareness Services for WebSphere Premises Server database and is used to replay specific periods of time. For runtime data to be available for the replay, the `LogHistory` property must be set to `Y` during the time frame that will be replayed later. See "System Properties" on page 291.

You can view events that were logged during the period of time you are replaying on the Spatial Management Client or in the "CEI Events" portlet.

For details on how to replay events, see the **Replay** section in the Spatial Management Client topic.

Handling alerts

This topic contains information about the portlet and tools provided by Location Awareness Services for WebSphere Premises Server for handling alerts.

Use the following portlet to acknowledge alerts:

- "CEI Events"

  Log in to the WebSphere Application Server administrative console and click **Rules/Alerts** → **Cei Events** to access this page.

CEI Events

Use this page to handle events logged by Location Awareness Services for WebSphere Premises Server.

Location Awareness Services for WebSphere Premises Server events are logged to the event database and displayed in this portlet. Specify a filter for the events you want to view and then scroll through the events to view them.

Set filter

Complete the following fields to create a filter for events. You do not have to complete all of the fields in order to create a filter, but you should fill in the ones you find necessary to get the desired results.

Note: The filter criteria is specific to the type of event.

- **Tag ID:** Enter the tag ID of a person or asset.
- **Tag Label:** Enter the label of the tag.
- **Tag Class:** Enter a class of items to search for.
- **Tag Group:** Enter a group to search for.
- **Zone:** Enter a zone for which to display events.
- **Event Type:** Select a type of event to search for.
- **Acknowledged:** Select **All** to display all events, **Acknowledged** to display only the events that have been acknowledged, or **Active** to display only the events that have not been acknowledged.
- **Event After:** Enter the month (MM), day (DD), and year (YYYY) from which to start your search. Only events logged after this date are displayed.

- **Event Before:** Enter the month (MM), day (DD), and year (YYYY) to end your search. Only events logged before this date are displayed.
- **Hub:** Select all hubs or select a specific hub for which to display events.

  Note: The filter only shows events that have attributes set for the corresponding fields. A normal zone entry event does not have hub information set, so no events are shown. Select **all (*)** to view all events.

Click **Set Filter** to save your settings or click **Clear Filter** to exit without saving the changes.

Display view

The events that match your filter criteria are then displayed. Scroll through the pages of events by clicking **First**, **Previous**, **Next**, and **Last**.

On this page you can do the following:
- Select **Delete** to delete the selected event or **Delete All** to delete all events.
- Select **Archive** to save the selected event to an archive or **Archive All** to archive all events.
- Select **Mark as acknowledged** to indicate that an event has been completed or **Acknowledge All** to acknowledge all events.
- Click **Set Filter** to create a filter for events that display on this page. When there are many events, this feature enables you to display only those that interest you.
- Click **Details** next to each event to display the date, type, severity, priority, and status of the event.

Searching tags

This topic identifies the portlet and other search mechanisms that are available in Location Awareness Services for WebSphere Premises Server for searching tags.

Use the following portlet to search for events:
- "Search Tags"

  Log in to the WebSphere Application Server administrative console and click **Search/Reports** → **Search Tags** to access this page.

You can also use the search feature provided with the Spatial Management Client by opening the following URL: http://fully_qualified_host_name/Tracking GUI/AtlasMonitor.html. You can search by class, group, or tag properties, or a combination of them. If you search by class, group, and tag properties, only those tags that match the combined search criteria are displayed.

Search Tags

Use this page to search all existing tags that are active.

You can search by class, group, or tag properties or a combination of them. If you search by class, group, and tag properties, only those tags that match the combined search criteria are displayed.

Search results are displayed in a table or list format. Click **Save** to save the results to a file or close the window to exit without saving.

Note: The search is *not* case sensitive. Also, the **AND** and **OR** only apply to the filter attributes within the class, group, and tag criteria. When you search by a combination of class, group, and tag criteria, they are always combined by **AND**.

Restriction: Partial searches are not supported. Search results return only an exact match for your criteria. For example, if you want to search for the last name "MacDonald", a search string such as "Mac" or "Mac%" will not find the tag.

History

Select **History** if you want to search on historical data from a specific date and time you enter. Do not select this field if you want to search on current data.
- **Date:** Click **PickDate** to select the date to search on. You can click **ClearDate** to reset the field.
- **Time:** Enter the time to search on in the format of hour, minute, and second (HH:MM:SS). Valid values for hour are 0-23 and valid values for minute and second are 0-59.

Click **Reload** to load the data for the date and time you selected. Then enter your search criteria.

Class Properties

Select **Class Properties** and select a class or classes to search for. Complete the fields, which vary by class, with your search criteria.

Click **AND relation** if all the search criteria you enter must be found or click **OR relation** to display search results for any search criteria that you enter.

Group Properties

Select **Group Properties** and then select the group to search for.

Tag Properties

Select **Tag Properties** and complete the following fields to search by class:
- **Tag ID:** Enter the tag ID to search for.
- **Battery:** Enter the status of the battery of the tag.
- **Alert:** Enter the type of alert to search for.
- **Area Name:** Enter the area where the tag you are searching for is located.

  Note: Area names must be unique across the Location Awareness Services for WebSphere Premises Server installation.

  Note: If Tag criteria are selected and Area Name is set to NONE, tags that are sending signals but are not in any area are returned. This can happen if a tag is in an area for which no zones are defined, but tag signals could still be received.
- **Icon Label:** Enter the icon label associated with the tag you are searching for.

Click **AND relation** if all the search criteria you enter must be found or click **OR relation** to display search results for any search criteria that you enter.

Click **Search** to search for the specified criteria or click **Reset** to clear all entries and perform a new search. Click **Reload** to refresh the options and to reset the fields to their original state.

Generating reports

This topic lists the portlets you use to generate and manage reports on data within Location Awareness Services for WebSphere Premises Server.

These portlets run only on the same server with WebSphere Application Server.

Use the following portlets to generate and manage reports:

- Reports Administration

  Log in to the WebSphere Application Server administrative console and click **Reports** ▸ **Reports Administration** to access this page.

- Reports Operation

  Log in to the WebSphere Application Server administrative console and click **Reports** ▸ **Reports Operation** to access this page.

Reports Administration

Use this page to create and manage customized reports from data that has been collected.

Based on data that has been collected, you can create customized reports, such as: Battery life reports, Tag count by zone reports, and Area and zone list reports.

Functions that you can use to manage an existing report or add a new report include:

- **Add:** Add a new report.
- **Delete:** Delete a report.
- **Reload:** Reload the data from the database.
- **Edit:** Edit the report details.

Adding a new report

Click **Add** and then complete the following fields to create a new report.

- **Report Name*:** Enter a report name. For example, `Battery life`.
- **Report File Name*:** Enter a report file name. For example, `BatteryLifeReport.rptdesign`.
- **Report File Path*:** Enter a file path for the report file. For example, `C:\tools\reports\`
- **Role Name:** Enter the role name for the report. For example, `lasmonitor`.
- **Description:** Enter the report description. For example, `Reports all tags which are equal or below the system property BatteryThreshold`.

Click **Save** to save your report.

Note: Fields marked with an asterisk (*) are required. All other fields are optional.

Reports Operation

Use this page to select and view customized reports.

The reports are listed in table format by **Report Name** and **Description**.

If you enable WebSphere Application Server security, access to the reports are granted on role-based security. When you log in with a user ID that is in a group that has the associated role, then you can view the reports associated with that specific role as well as view all reports that have not been associated with any role.

If you do not enable WebSphere Application Server security, all reports can be viewed regardless of their specified roles because role-based security will not be applied.

Click **Display** to display the selected report or click **Reload** to reload the data from the database.

Developing

Use Web services to customize Location Awareness Services for WebSphere Premises Server.

Web services

Web services are self-contained, modular applications that can be described, published, located, and invoked over a network. They implement Service Oriented Architecture (SOA), which supports the connecting or sharing of resources and data in a flexible and standardized manner. Services are described and organized to support their dynamic, automated discovery and reuse.

Tip: See the WebSphere Application Server information center for more information about implementing Web service applications.

The following WSDL (Web Services Description Language) files are provided by Location Awareness Services for WebSphere Premises Server:
- http://*host_name*:9080/PremisesCEPRuleInstantiationWebServiceEJBHttpRouter/services/RuleInstantiationWS?wsdl
- http://*host_name*:9080/AtlasImportEJBHttpRouter/services/LasItemRegistration?wsdl
- http://*host_name*:9080/AtlasImportEJBHttpRouter/services/LasItemDetail?wsdl
- http://*host_name*:9080/AtlasImportEJBHttpRouter/services/LasItemMetaData?wsdl
- http://*host_name*:9080/LasEventHandlingEJBHttpRouter/services/LasEventHandling?wsdl
- http://*host_name*:9080/LasQueryEJBHttpRouter/services/LasQuery?wsdl
- http://*host_name*/wsdl/EMailHandler.wsdl

This XML-based language is used to create a description of an underlying application. It is this description that turns an application into a Web service, by acting as the interface between the underlying application and other Web-enabled applications.

The following Web services are provided by Location Awareness Services for WebSphere Premises Server:
- "LasRuleServices" on page 318
- "LasItemRegistrationServices" on page 323
- "LasItemDetailServices" on page 325
- "LasItemMetaDataServices" on page 326

- "LasEventHandlingServices" on page 326
- "LasQueryServices" on page 327
- "handleEvent" on page 327

Security
Location Awareness Services for WebSphere Premises Server supports HTTPS transport binding for its Web services.

If security is enabled for WebSphere Application Server, the Web services are available only through HTTPS and a secure port (usually 9443). Location Awareness Services for WebSphere Premises Server Web services are secured by HTTP Basic Authentication as well. This means that authorization occurs using the user name and password provided in the HTTP headers.

HTTPS

HTTPS is a well-known and often-used mechanism to secure HTTP Internet and intranet communications. HTTPS is based on a Secure Sockets Layer (SSL) or Transport Layer Security (TLS) that runs beneath HTTP. HTTPS encrypts the entire HTTP data packet. It also provides security features including party identification and message integrity. Mutual authentication (where the client authenticates to the server and the server authenticates to the client) is possible. If you intend to access Web services protected by HTTPS, certificate stores must be prepared on the client side.

For more information on these topics, see Using HTTP to transport Web services and Invoking outbound services over HTTPS in the WebSphere Application Server information center.

Localization and input parameters
All the Web services (except for LasRuleServices) have *locale_descriptor* as input parameter.

This parameter allows you to specify:
- Language
- Country
- Vendor specific information (such as operating system)

This descriptor enables the server to parse the values it receives from clients and return localized values (such as item properties). The format for the returned values is in the same locale. If the returned value is a message, then the message is translated according to the language of the specified locale, if a translation is available.

The property values must use strings for the locale provided in the *locale_descriptor* input parameter. This applies to integer and double properties.

Timestamp input parameters (such as *lastUpdateTime*, *start_time*, and *end_time*) are locale independent. This means that they are bound to the server time zone and a specific formatting pattern as returned by the server: *yyyy-mm-dd hh:mm:ss.fffffffff*, where *fffffffff* indicates nanoseconds.

LasRuleServices
The following Web services allow you to create, deploy, update, undeploy, hold, and delete rule instances.

createRuleInstance:
Purpose

Rules are created in the Location Awareness Services for WebSphere Premises Server database, but will not take affect until they are deployed.

Important: To use createRuleInstance for "LasRuleServices" on page 318, you must provide the Web service interface with internal information on zone IDs, class IDs, group IDs, and item IDs. You can obtain this information by browsing the following ATLASDB tables and by invoking another Web service.

- For zone IDs: Browse the ATLASDB.ZONES table for information on zone IDs.
- For class IDs: Browse the ATLASDB.CLASSES table for information on class IDs.
- For group IDs: Browse the ATLASDB.GROUPS table for information on group IDs.
- For item IDs: Invoke the Web service "viewItem" on page 325 of "LasItemDetailServices" on page 325 to obtain the item IDs.

createRuleInstance *type name description attributes deploy*

type: For a description of each of the rule types, see "Business Rules" on page 282. The following is a list of valid rule types:
- Visitor Escorting
- Duration of Stay in Zone
- Maximum Items per Zone Threshold
- Zone Access Restriction
- Zone Exit Restriction

name: The unique name for this rule. The maximum name length size is 64 bytes. Quotation marks cannot be used.

description: A description of the rule.

attributes: Attributes for the rule that are specified by keyword and values. For more information on attributes for specified rule types, see Table 71 on page 320 and Table 72 on page 321.

deploy: Indicates whether the rule is to be deployed. Valid values are 0 or 1.

The following tables contain lists of keyword and example values for the *attributes* parameter. For additional information on defining rules, see "Business Rules" on page 282.

Table 71 on page 320 for **Visitor Escorting** contains a list of valid keywords. It is important to note that all the keywords are required.

Table 71. Keyword-values for createRuleInstance for Visitor Escorting rules

Keyword	Example value	Value description
zoneType	1	The following are valid values for zoneType: • 1 : Indicates that the value for the zone parameter represents the zone ID. • 2 : Indicates that the value of the zone parameter represents a zone class ID.
zone	2	Depending on zoneType, this value represents either the zone ID or a zone class ID.
alertActions	3	This value is a sum of the following possible values: • 1 = log alert • 2 = display alert • 4 = custom notification In this example, the resulting value 3 is the sum of the value for a log alert (1) and a display alert (2).
itemType1	3	Keyword itemType1 corresponds to the Visitor. Keyword itemType2 corresponds to the Escort. Possible values can be one of the following: • 1 = item ID • 3 = class ID • 4 = group ID
itemType2	1	
item1	1	Depending on itemType, this value represents either an item ID, a class ID, or a group ID.
item2	4343	
additionalParameter1	30	This value is the maximum tolerated distance, in units, that the visitor can be away from the escort. **Note:** Currently, the edge length of the visitor (who is in the container class) determines the maximum tolerated distance.
additionalParameter2	400	This value is the tolerated rule violation time, in seconds.

For **Duration of Stay in Zone**, **Maximum Items per Zone Threshold**, **Zone Access Restriction**, and **Zone Exit Restriction**, Table 72 on page 321 contains a list of valid keywords for the attributes parameter. However, only activityPattern is required by all the specified rule types. The additionalParameter1 keyword is required but only valid for **Duration of Stay in Zone** and **Maximum Items per Zone Threshold**.

Table 72. Keyword-values for createRuleInstance for rule types: Duration of Stay in Zone, Maximum Items per Zone Threshold, Zone Access Restriction, and Zone Exit Restriction

Keyword	Example value	Value description
activityPattern	A:	This keyword is required. The activityPattern specifies the time frame when the rule should be applied. The following is a list of values for the rule's activity pattern: • **A:** – **Always active**. • **D:**2008/02/17-19:26:00;2008/02/25-19:26:00; – **Discretely active**. For this example, the rule is active only for the specified time from February 17, 2008, at 7:26:00 p.m. through February, 25, 2008 at 7:26:00 p.m. • **R:**2+[08:00:00-09:00:00];3-[08:00:00-09:00:00]; – **Repetitively active**. For this example, the rule is repetitively active on Tuesdays from 8:00:00 a.m. to 9:00:00 a.m. and on Wednesdays except from 8:00:00 a.m. to 9:00:00 a.m.
class1	1	This value represents the class ID to be included or excluded.
exclClass1		Class parameters are used to define the actor for a rule. [1]
group1	3	This value represents the group ID to be included or excluded.
exclGroup1		Group parameters are used to define the actor for a rule. [1]
attrName1	TagID, Label	This value represents the name of the attribute used for the inclusion or exclusion filter.
exclattrName1		Attribute name parameters are used to define the actor for a rule. [1,2]
attrOperator1	endsWith >= contains	This value represents the operator used for the inclusion or exclusion filter. The supported operator values are: • equals • equalsIgnoreCase • unequals • unequalsIgnoreCase • > • >= • < • <= • startsWith • endsWith • contains
exclattrOperator1		Attribute operator parameters are used to define the actor for a rule. [1,2]

Table 72. Keyword-values for createRuleInstance for rule types: Duration of Stay in Zone, Maximum Items per Zone Threshold, Zone Access Restriction, and Zone Exit Restriction (continued)

Keyword	Example value	Value description
attrValue1 exclattrValue1	133	The attribute value used for the inclusion or exclusion filter. Attribute value parameters are used to define the actor for a rule. [1] [2]
Zone exclZone	2	Represents the zone ID to be included or excluded. [3]
zoneType exclZoneType	6	Represents the zone class ID to be included or excluded. [3]
alertActions	3	This value is a sum of the following possible values: • 1 = log alert • 2 = display alert • 4 = custom notification In this example, the resulting value 3 is the sum of the value for a log alert (1) and a display alert (2).
additionalParameter1	30	This keyword is required but only valid for the following rule types: • **Maximum Items per Zone Threshold**. Specify the maximum number of actors. • **Duration of Stay in Zone**. Specify the maximum duration of stay in seconds.

deployRuleInstance:

---

1. The following applies when defining an actor:
   - It is possible to define an actor by inclusion, exclusion, or both.
   - Specification of an actor is required.
   - Actor specification includes at least class or group or attribute specification, or any combination of them.
   - You can specify one attribute as the filter criteria. This can be an attribute independent of class (for example, TagID or Label) or an attribute of the selected class. (You can retrieve this by the metadata of the item.)

2. When filtering by attribute, the name, operator, and value keywords all need to be defined for the rule.
   - The following expression describes which keywords must be defined when filtering by attribute:
   ```
   (attrName1 AND attrOperator1 AND attrValue1) OR
   (exclattrName1 AND exclattrOperator1 AND exclattrValue1)
   ```
   - It is possible to use both the include and the exclude attributes in one rule.
   - The name should be a valid attribute name for the specified class. The operator should be valid for the type of attribute.

3. When filtering by using the zone related keywords, you can only define Zone or zoneType, but not both keywords for the rule.
   - The following expression describes restrictions for using the Zone and zoneType keywords: `(zoneType XOR zone) OR (exclZoneType XOR exclZone)`.
   - It is possible to use both the include and the exclude zone related keywords in one rule.

Purpose

This Web service deploys a rule instance to the CEP runtime engine.

deployRuleInstance *type name*

undeployRuleInstance:
Purpose

This Web service removes a rule instance from the CEP runtime engine.

undeployRuleInstance *type name*

updateRuleInstance:
Purpose

This Web Service updates a rule instance.

Note: When a rule instance is updated, the old version is deleted and a new instance is created. This does not occur within a transaction.

updateRuleInstance *type name description attributes deploy*

For a detailed description of *type*, *name*, *description*, *attributes*, and *deploy* parameters, see "createRuleInstance" on page 319.

deleteRuleInstance:
Purpose

This Web service deletes a rule instance, removing it from the database and from the CEP runtime engine.

deleteRuleInstance *type name*

LasItemRegistrationServices
Location Awareness Services for WebSphere Premises Server provides Web services to assist you in defining, updating, and deleting items in your installation.

When using these Web services, you can specify items by supplying the key properties that match the item class or by specifying the item ID. Location Awareness Services for WebSphere Premises Server only checks for the attributes relevant to the specified class. If additional attributes are provided, they are ignored.

Note:

- Any dates must be supplied in the *MM/dd/yyyy* (month/day/year) format.
- The timestamp parameter, `LastUpdateTime`, makes sure that you have the most recent version of the item before you attempt to update or delete it. Timestamp input parameters are bound to the server time zone.
- You can only specify one instance of a key property attribute, but there can be multiple instances of other property attributes (according to the class schema).

createItem:

Purpose

This Web service creates items in the Location Awareness Services for WebSphere Premises Server database.

createItem *class_name key_attributes optional_attributes related_groups locale_descriptor*

Note:
- All key attributes must be filled with a string that matches the defined data type.
- If a hierarchical groups is set to yes, only the first group will be taken.
- If a *parent_item_ID* and *parent_tag_ID* are set (as optional properties), the parent must exist and be part of a container class.

The output from the Web service is the item ID and the timestamp of the last update.

updateItem:
Purpose

This Web service updates optional attributes for an item in the Location Awareness Services for WebSphere Premises Server database. Key properties cannot be changed with this service. Use the UpdateItemById Web service to update key properties. You only need to provide the optional attibutes you want to change. To blank out existing attributes, provide blank or null values. A list of groups always replaces the old list of groups.

updateItem *class_name key_attributes optional_attributes related_groups locale_descriptor*

Note:
- All key attributes must be filled with a string that matches the defined data type.
- If a hierarchical groups is set to yes, only the first group will be taken.
- If a *parent_item_ID* and *parent_tag_ID* are set (as optional properties), the parent must exist and be part of a container class.

The output from the Web service is the item ID and the timestamp of the last update.

updateItemById:
Purpose

This Web service allows you to update key attributes for an item in the Location Awareness Services for WebSphere Premises Server database. You only need to provide the attributes you want to change. To blank out existing attributes, provide blank or null values. A list of groups always replaces the old list of groups. To remove group assignments, set a blank list.

updateItemById *item_ID key_attributes optional_attributes related_groups last_update_time locale_descriptor*

Note:
- All key attributes must be filled with a string that matches the defined data type.

- If a hierarchical groups is set to yes, only the first group will be taken.
- If a *parent_item_ID* and *parent_tag_ID* are set (as optional properties), the parent must exist and be part of a container class.

The output from the Web service is the item ID and the timestamp of the last update.

deleteItem:
Purpose

This Web service deletes items from the Location Awareness Services for WebSphere Premises Server database. All dependent records such as group relations or parent item relationships will be deleted as well. The history entries remain.

deleteItem *class_name key_attributes locale_descriptor*

Note: All key attributes must be filled with a string that matches the defined data type.

deleteItemById:
Purpose

This Web service allows you to delete an item in the Location Awareness Services for WebSphere Premises Server database. All dependent records, such as group relations or parent item relationships, are deleted as well. History entries remain.

deleteItemById *item_ID last_update_time locale_descriptor*

The output from the Web service is the item ID.

Note: The item ID must match an existing item in Location Awareness Services for WebSphere Premises Server.

registerItem:
Purpose

This Web service changes an item's tag ID, which might already be defined in the Location Awareness Services for WebSphere Premises Server database.

registerItem *item_ID tag_ID last_update_time locale_descriptor*

Note: To unregister a tag ID, enter blanks or " as the tag ID.

The output from the Web service is the item ID and the timestamp of the last update.

LasItemDetailServices

The following Web Services allow you to obtain information about items.

viewItem:
Purpose

This Web service returns all tag attributes for an item, including tag attributes. If a timestamp is entered, it returns the historical attributes. It does not return the current position or outstanding events.

viewItem *class_name key_attributes timestamp locale_descriptor*

The output from the Web service is the item ID, class name, key attributes, optional attributes, assigned group, and the timestamp of the last update.

viewItemById:
Purpose

This Web service returns all tag attributes for an item, including tag attributes. If a timestamp is entered, it returns the historical attributes. It does not return the current position or outstanding events.

viewItemById *item_ID timestamp*

The output from the Web service is the item ID, class name, key attributes, optional attributes, assigned groups, and the timestamp of the last update.

LasItemMetaDataServices

The following Web service allows you to query Location Awareness Services for WebSphere Premises Server metadata.

getItemClassDefinitions:
Purpose

This Web service returns a list of all classes and their attributes. The information is a prerequisite, so run this Web service prior to creating or updating items.

getItemClassDefinitions *locale_descriptor*

The output from the Web service is an array of item classes in the following format:
- LasItemClass
  - Class name
  - Parent class name (can be empty)
  - Key properties (consisting of name and type)
  - Other properties (consisting of name, type, minimum number of occurrences, and maximum number of occurrences)

LasEventHandlingServices

The following Web services allow you acknowledge events.

issueEvent:
Purpose

This Web service issues an event, such as LasTagNotResponsive, in Location Awareness Services for WebSphere Premises Server.

issueEvent *keyword_value_pairs locale_descriptor*

Note:
- The value for the *keyword_value_pairs* variables is an array of properties describing the event. For example:
  ```
  "AlertType", "LasTagNotResponsive"
  "MessageType", "LasTagNotResponsive"
  "TagId", "00000007"
  ```

```
"ZoneName", "Zonename"
"EventTime", "12:12:30"
"TagLabel", "taglabel"
"TagClass", "Person"
"TagGroup", "Security"
```

acknowledgeEvent:
Purpose

This Web service acknowledges a concrete event by its global instance ID. This ID is returned as part of the tag details.

acknowledgeEvent *global_instance_ID user_name*

acknowledgeEventForTag:
Purpose

This service acknowledges all active events for a given tag ID.

acknowledgeEventForTag *tag_ID user_name*

LasQueryServices
The following Web service allows you to query tag data.

getTagDetails:
Purpose

This Web service returns the current or historical positions, events, and zones for a given tag. It does not include the tag attributes.

getTagDetails *tag_ID time locale_descriptor*

Output consists of the following information about the tag:
- Class name
- Item ID
- Tag ID
- Event list (including global instance ID and message)
- Coordinates
- Battery
- Item label (including icon link, parent ID, and tag ID of parent)
- Time last seen
- List of zones

handleEvent
Purpose

This Web service is a sample Web service that triggers an e-mail based on an event. This service is called when it is configured as a subscriber for events and if the configured event filter matches the incoming event.

handleEvent *string serialized_common_base_event locale_descriptor*

Information about the event is returned.

Use cases

This section contains possible use cases for Location Awareness Services for WebSphere Premises Server.

SOA integration

In this release, Location Awareness Services for WebSphere Premises Server aligns with the Service Oriented Architecture (SOA) approach by enabling alert-driven business processes.

Location Awareness Services for WebSphere Premises Server is able to call Web services and trigger a business process in case of a business alert. To set this up, customers must register a Web service and define proprietary filter criteria for the Web service to be called. Then when Location Awareness Services for WebSphere Premises Server issues an alert via CEI, a MDB listener is called, which checks whether the filter criteria for a Web service are met and calls the Web service with the common base event containing the details of the alert.

Additionally, other existing interfaces are available for use with the Web interfaces. These interfaces include:

- WebSphere MQ to import data and location events.
- Servlet interfaces to maintain and query areas and zones, monitor tag details, acknowledge alerts, and retrieve metadata for items.

Location Awareness Services for WebSphere Premises Server provides sample Web services and customers can also create their own. The following scenarios provide examples of how you might use the provided Web services in a warehouse environment to implement business processes.

Integrating supply chain management

The following scenarios describe how you might use Location Awareness Services for WebSphere Premises Server to integrate supply chain management business processes in a warehouse environment to track the arrival, storage, and decommissioning of goods.

This scenario consists of the following phases:

1. When new goods are ordered, the arriving pallet of goods must be placed in a specific zone. The position of the pallet is stored in Location Awareness Services for WebSphere Premises Server.
2. When the zone is full of goods, a sub business process is started to move the pallets of goods to another storage location.
3. When the pallets of goods leave the warehouse, the contents are unregistered. In order to track a pallet of goods, the position of the pallet must be printed on the order.

The following scenarios include examples of how you might use the "Web services" on page 317 that are supplied with Location Awareness Services for WebSphere Premises Server in the business processes.

Arriving goods

When an order arrives through the electronically available shipment manifest, the pallet tags that will arrive are registered in Location Awareness Services for WebSphere Premises Server. You can do this using the LasItemRegistrationServices - createItem Web service.

Rules that govern the arrival and storage of the goods must already exist. If they do not, you can define rules using the LasRuleServices - createRuleInstance Web service. For example, you can define what types of goods must be placed in what zone. You can also specify that goods of a specific type must not enter or leave specific zones or that palettes in specific zones cannot contain more than a specified number of tags of a specific type.

When the palette passes the entry gate or dock receiving door, any defined business processes are triggered in WebSphere Premises Server, Data Capture and Delivery, and Location Awareness Services for WebSphere Premises Server.

For example, when a forklift picks up a palette with a certain tag ID, WebSphere Premises Server can send a pickup event to Location Awareness Services for WebSphere Premises Server using a WebSphere MQ request. During the move, rules correlate the pallet tag ID and its properties to the forklift's position. (For example, if the item has already been defined as part of a group, such as "flammable group", and the forklift moves to a restricted area where the pallet is not allowed to go because of its flammable content, an alert is triggered based on the defined business rules for zone entry or exit.) When the forklift releases the pallet, a message can be sent to Location Awareness Services for WebSphere Premises Server specifying the position of the pallet.

Zone is full

Location Awareness Services for WebSphere Premises Server evaluates business rules constantly. If more pallets are stored in a zone than is allowed by the business rules, an alert is issued that can trigger other business processes. You can do this using the subscriberService Web service. For example, the business process might cause the pallets stored in the zone to be emptied.

Decommissioning goods

If a pallet is scheduled to be picked up at the position where it is currently stored and moved elsewhere, the supply chain management business process issues a request to Location Awareness Services for WebSphere Premises Server for the location of the pallet tag ID (you can use the LasQueryServices - getTagDetails Web service) and also sends information such as the pallet tag ID and location to the pick up team. When the pallet passes the dock door on the way out, the supply chain management business processes trigger the appropriate business services and sends a message to Location Awareness Services for WebSphere Premises Server indicating that the pallet tag ID has left the area or zone. If the pallet is leaving the premises WebSphere Premises Server can decommission the pallet's tag ID by using the ItemRegisterService Web service.

It is also possible to request the duration time per pallet in a specific zone by requesting a report. You can use the LasQueryServices - getTimeReportByTag Web service.

Granting access to visitors

The following scenarios describe how you might use Location Awareness Services for WebSphere Premises Server to track the movements of visitors on the premises.

In this scenario a contractor is ordered to temporarily work in special areas or zones of a company's premises. In order to track the contractor, the following actions must be taken:

- Register the contractor in the system.
- Grant access to the contractor to enter specific zones.
- Specify the zones where the contractor must be escorted by someone else.
- Specify the items, such as work-specific tools, that must remain in the work zone.

At the end of the temporary work assignment, the following actions must be taken:

- Unregister the contractor.
- Check the duration that the contractor remains in the work zone.

The following scenario includes examples of how you might use the "Web services" on page 317 that are supplied with Location Awareness Services for WebSphere Premises Server in the business processes.

For example, when contractors arrive at the company's premises, they receive a tag ID and predefined business rules are activated. These business rules identify areas and zones of the company's premises where contractors are allowed to enter or where they require escorting. Contractor-specific rules can be created as part of the business process as needed. You can define business rules using the LasRuleServices - createRuleInstance Web service.

The contractors are registered in Location Awareness Services for WebSphere Premises Server, for example using the LasItemRegistrationServices - createItem Web service.

When the contractors enter the premises or the zones defined for escorting, an escort can be informed automatically using the SubscriberService Web service of a contractor's arrival.

When the contractors enter the work zone, Location Awareness Services for WebSphere Premises Server can verify that the relevant work tools are available for every worker in the zone. Otherwise they can be dispatched using the SubscriberService Web service. The number of tools can also be counted using the LasQueryServices - getTimeReportByZone Web service.

When the job is done and the contract ends, the contractors are unregistered using the LasItemRegistrationServices - registeritem Web service. A tools check can be performed for the work area using the ItemsInZoneService Web service and a final billing for the contractors' working hours is kicked off using the LasQueryServices - getTimeReportByTag Web service. Any contractor-specific rules can be deleted using the LasRuleServices - deleteRuleInstance Web service.

Using containers

Location Awareness Services for WebSphere Premises Server allows you to use containment relationships to track items. For example, a containment relationship makes it easier to track items being shipped together, such as on a pallet.

About this task

Containment relationships are based on:

- Defined containment classes. You can define containers in Location Awareness Services for WebSphere Premises Server by explicitly defining specific item classes (new or existing) in the "Classes/Items Manager" on page 277 portlet and specifying them as container classes or by importing containment relationships with a CSV file. Items in container classes can contain other items. For example, the item "palette1" is associated with the class "palettes". The item "palette1" contains item "screwdriver42".

  You can dissolve containment relationships by editing the properties of the class to remove the container classification.

- External events that are processed by Location Awareness Services for WebSphere Premises Server. For example, if the position of item indicates it is inside the container, it is automatically associated with the container. This requires that containers be precisely defined with spatial dimensions and the system property `ContainerSupportOn` must checked. Since containers can be mobile, the spatial area occupied by them can change over time. Also, devices, such as complex Data Capture and Delivery devices, can be set up to deliver special events to indicate a container relationship. Containers cannot add other containers dynamically.

Using containers also allows you to visualize the location of all contained items, even if they are not tagged or their tags are not visible to a tag reader. In this case, when the container moves, Location Awareness Services for WebSphere Premises Server assumes the contained items also move. Also, if a container enters or leaves a zone, Location Awareness Services for WebSphere Premises Server assumes all contained items also enter or leave the zone and all rules apply to both the container and contained items. Rules can also be defined to prevent items from being removed from a container or added to a container.

It is important to note that the last reported position of a container and the position of its content can differ. This might be the case if the items in the container and the container itself are actively tagged. If contained items are removed from the container's location, you might want to remove the containment relationship and track all items separately. If the tags of the contained items are not visible or are read from a different tag reader than that of the container, the position coordinates might be read as being located outside of the container. In this case, you might want to define business rules that cause the position of the tagged items in the container to be ignored.

The following restrictions apply to containers and contained items:

- Contained items do not need to be equipped with active tags; however, if contained items are equipped with active tags, the container must also be equipped with an active tag.
- If both containers and contained items are equipped with active tags, the same technology must be used for all tags and the accuracy and send frequency of the tags must be identical.
- Location Awareness Services for WebSphere Premises Server assumes all containers are cubes; therefore specify a cube size that will most closely resemble the actual size of the container.

Defining a container and assigning items

This topic describes how to define a container class and container. It also describes how to assign items to the container.

About this task

Perform the following steps in the "Classes/Items Manager" on page 277 portlet to create a class of items that can contain other items and containers.

1. Log in to the WebSphere Application Server administrative console and click **Tag Registration** › **Classes/Items** to access this page.
2. Click the **Class Details View** tab.
3. Click **Add Child Class** to define a new class.
4. Fill in the values for the class, making sure to select **Container** to specify the items in the class can contain other items. Also, make sure to enter the correct spatial measurements in **Default-Edge-Length** for the size of the containers in the class.
5. Save your settings.
6. Now, add an item to the container class you created.
   a. Click the **Item View** tab.
   b. Click **Add New Item** to define a new item in the class you created.
   c. Fill in the values for the item. If the edge length of the container is different than the class default, make sure to enter a value for **Edge Length**.
   d. Save your settings.
7. Assign items to the container.
   a. Click the **Item View** tab.
   b. Click **Edit Container** next to the new container item you created. A list of items are displayed that can be assigned to the container, as well as a list of any items that are already assigned to the container, if any.
   c. Select one or multiple items to assign to the container.
   d. Save your settings and verify the items are now listed as being assigned to the container.

Converting an existing class to a container class

This topic describes how to define an existing class as a container class.

About this task

Perform the following steps in the "Classes/Items Manager" on page 277 portlet to edit an existing class so that it can contain other items and containers.

1. Log in to the WebSphere Application Server administrative console and click **Tag Registration** › **Classes/Items** to access this page.
2. Click the **Class Details View** tab.
3. Click an existing class to modify its properties and specify it as a container class.
4. Select **Container** to specify the class can contain items.
5. Make sure to enter the correct spatial measurements in **Default-Edge-Length** for the size of the containers in the class.
6. Save your settings.

Results

Any item defined for the class can now contain other items.

Removing the container property from the class

This topic describes how to specify that items belonging to the class can no longer contain other items.

About this task

Perform the following steps in the "Classes/Items Manager" on page 277 portlet.

1. Log in to the WebSphere Application Server administrative console and click **Tag Registration** → **Classes/Items** to access this page.
2. Click the **Class Details View** tab.
3. Click an existing class to modify its properties and specify that it is no longer a container class.
4. Deselect **Container** to specify the class can no longer contain items.
5. Save your settings.

Results

Any item defined for the class can no longer contain other items. Existing container relationships will be dissolved.

Importing a containment relationship

This topic describes how to import containment relationships with a CSV file.

Before you begin

You can import items into a container using a CSV file. However, before completing these steps, make sure the container item that you are adding items to has already been defined.

1. Configure the properties in Data_Export.properties, ClassMapping.properties, and *class_name*.properties as specified in "Importing resource data to Location Awareness Services for WebSphere Premises Server" on page 297. In the *class_name*.properties file, in addition to the other necessary values, set the following values for `attribN`:
    - Enter `attribN=EdgeLength` to map to the column in the CSV file that contains the item's edge length, if it has been specified.
    - Enter `attribN=ContainerTagId` to map to the column of the CSV file that indicates the tag ID of the container item.
    - Enter `attribN=removeFromContainer` to map to the column of the CSV file that indicates whether the item should be removed from the container item. The value in the column must be set to `yes` for the item to be removed.
2. Then run the data import application, as specified in "Importing resource data to Location Awareness Services for WebSphere Premises Server" on page 297.

Sending events to establish containment relationships

This topic describes how external events can be sent, such as by a Data Capture and Delivery device, to establish relationships.

Before you begin

In order to send external events that can define a containment relationship, you must have defined a location event provider with the proper converter.

About this task

The XML of the event must contain the following information:

- The tag ID of the container is indicated in the `location` attribute of the `event`.
- The tag ID of the contained item is indicated in the `tagid` attribute of `rfid-tag-data`.

Example

For example:

```
<?xml version="1.0" encoding="UTF-8"?>
<ibmprem:ibm-premises-unified-format xmlns:ibmprem="http://www.ibm.com"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 dts="2007-01-29T11:18:22" messageId="Event_1170008750248226334"
 xsi:schemaLocation="http://www.ibm.com IBMPremisesUnifiedMessageFormat.xsd">
 <event eventId="Event_1170008750248226334" location="ErfF1"
  type="tag_read_external">
  <argument name="sessionid"
   value="L15@1170066396687||1170066406828" />
  <argument name="direction" value="world2forklift" />
  <rfid-tag-data antenna="0" count="1" discovered="1170066396890"
   reader="R12" tagid="331505d7941f7900000003a5" />
 </event>
</ibmprem:ibm-premises-unified-format>
```

Evacuating locations

In case there is an emergency in a location and it is necessary to track the evacuation of employees from endangered zones, Location Awareness Services for WebSphere Premises Server provides an evacuation view that allows companies to monitor tagged items. The evacuation view displays all the zones in the selected area and the number of tags within the zones.

About this task

To monitor evacuation of a location, follow this procedure.

1. Open the Spatial Management Client.
2. Click **Evacuation View**. The Evacuation View window opens and shows the zones within the selected area.

   Note: If you want to view an evacuation view for another area, you can open another instance of the Spatial Management Client.
3. Click a zone to expand details about the tags within the zone. The tags shown within the zones will be filtered based on any search criteria you specify in the main view.

What to do next

You can also open the evacuation view when you are replaying data. This allows you to view evacuation patterns and response times by replaying and pausing data from specific areas and zones.

Troubleshooting

This section includes topics for troubleshooting Location Awareness Services for WebSphere Premises Server.

Logging

If you are unable to resolve technical problems, this topic describes log files, and the process for gathering log files and sending them to your IBM services representative.

Logging levels

The following table lists the available log levels and their meanings.

Table 73. Available log levels and descriptions

Log level	Description
OFF	No events are logged.
FATAL	Task cannot continue and component cannot function.
ERROR	Task cannot continue, but component can still function.
WARN	Potential error or impending error.
INFO	General information outlining overall task progress.
CONFIG	Configuration change or status.
DETAIL	General information detailing subtask progress.
FINE	Trace information - general trace + method entry / exit / return values.
FINER	Trace information - detailed trace.
FINEST	Trace information - a more detailed trace that includes all the detail that is needed to debug problems.
ALL	All events are logged. Can provide a more detailed trace than FINEST.

A message is logged if the logging request's priority is greater than or equal to the currently assigned priority of the utilized logger. For example, if you have a logger with an assigned log level of INFO, then an ERROR request will pass the approval, but a DETAIL request will be blocked. Level ALL causes a logger to accept all logging request; OFF blocks all requests.

Configuring logging

Follow these steps for configuring logging:

1. Modify the *WAS_HOME*\lib\ext\log4j.properties file to modify logging for the Location Awareness Services for WebSphere Premises Server components.
2. Restart WebSphere Application Server.

Log files are stored in the *WAS_HOME*\profiles*profile_name*\logs directory.

Turning off logging

For Location Awareness Services for WebSphere Premises Server, logging is performed within the Apache log4j framework that has been designed for simplicity and performance. Turning off all logging is not recommended. It is

strongly recommended that you at least keep the ExceptionLogger turned on. However, if you want to turn logging off, perform the following steps:

- Set the rootLogger to `OFF`.
- To turn off the com.ibm.atlas logger, set its level to `OFF` and its **additivity** parameter to `false` .
- To turn off the com.ibm.atlas.exception.ExceptionLogger, set its level to `OFF` and its **additivity** parameter to `false`.

For more information on how to configure logging, consult the log4j-documentation available at: http://logging.apache.org/log4j/docs/documentation.html

Gathering logs

1. Collect the following log files (for example, as .zip files):
   - For WebSphere Application Server:
     - *WAS_PROFILE_HOME*\logs\General.log
     - *WAS_PROFILE_HOME*\logs\Atlas.log
     - *WAS_PROFILE_HOME*\logs\AtlasException.log

     Additional logs are found in the *WAS_PROFILE_HOME*\logs\server1directory.
   - For the Spatial Management Client: *IHS_HOME*\htdocs\en_US\Tracking GUI\logs
2. Send the files to your IBM services representative.

Handling alerts for Location Awareness Services for WebSphere Premises Server event providers and receivers

This topic describes how to set up Location Awareness Services for WebSphere Premises Server to handle alerts.

About this task

When alerts are generated for third-party Location Awareness Services for WebSphere Premises Server event providers and devices, D packet messages are generated, which in turn generate events that are sent to the CEI event database. These messages are classified as type `AtlasAloeInfraStructure`.

To set up Location Awareness Services for WebSphere Premises Server to handle this type of alert, do the following:

1. Define a notification channel that refers to the messages of type `AtlasAloeInfraStructure`.
2. Define a notification program to handle these messages.
3. Define it to use the notification channel and to call the e-mail program, but define a specific e-mail receiver to handle these diagnostic messages by selecting the type `AtlasAloeInfraStructure` as the alert type.
4. Filter on the details related to the messages of type `AtlasAloeInfraStructure`. All other D packet messages are ignored.

General troubleshooting tips

This topic describes problems that might occur and provides possible solutions.

- "Something is wrong with Location Awareness Services for WebSphere Premises Server and I do not understand the problem" on page 337

- "Exceptions in the WAS_PROFILE_HOME\logs directory"
- "My system did not automatically reconnect after a network failure and I did not receive a fatal error telling me to restart my browser" on page 338
- "The browser window hangs up and then the browser crashes" on page 338
- "I had a browser error, but refreshing the page did not correct the problem" on page 338
- "I had a browser error message, and I selected the attempt to recover option. But it did not correct the problem, and I got the error message again." on page 338
- "I cannot stop server1 using the GUI menu" on page 338
- "Tag processing does not seem to stop" on page 339
- "Chinese characters are not displayed properly on English Windows 2003 Server operating system" on page 339
- "Event information might contain inconsistent times in event date and message" on page 339
- "Rule violation detected with some delay" on page 339

Something is wrong with Location Awareness Services for WebSphere Premises Server and I do not understand the problem

Verify that all of the path settings in the System Properties portlet are correct.

Exceptions in the *WAS_PROFILE_HOME*\logs directory

Multiple log4j-1.2.13.jar files

If you see an exception in the *WAS_PROFILE_HOME*\logs file that looks similar to this example, then a possible cause for this exception is that there is more than one copy of the log4j-1.2.13.jar file:

```
[31.10.06 16:43:25:246 CET] 0000000a SystemErr
    R log4j:WARN custom level class [com.ibm.atlas.logging.AtlasLevel]
    does not have a constructor which takes one string parameter
[31.10.06 16:43:25:246 CET] 0000000a SystemErr
    R java.lang.NoSuchMethodException: com.ibm.atlas.logging.AtlasLevel.toLevel
    (java.lang.String, org.apache.log4j.Level)
 at java.lang.Class.getMethod(Class.java:1078)
 at org.apache.log4j.helpers.OptionConverter.toLevel(OptionConverter.java:209)
 at org.apache.log4j.PropertyConfigurator.parseCategory(PropertyConfigurator.java:588)
 at org.apache.log4j.PropertyConfigurator.parseCatsAndRenderers
    (PropertyConfigurator.java:524)
 at org.apache.log4j.PropertyConfigurator.doConfigure(PropertyConfigurator.java:408)
 at org.apache.log4j.PropertyConfigurator.doConfigure(PropertyConfigurator.java:432)
 at org.apache.log4j.helpers.OptionConverter.selectAndConfigure
    (OptionConverter.java:460)
 at org.apache.log4j.LogManager.<clinit>(LogManager.java:113)
 at org.apache.log4j.xml.DOMConfigurator.configure(DOMConfigurator.java:543)
 at com.screamingmedia.openportlet.common.log.Log4jSvr.init(Log4jSvr.java:52)
 at javax.servlet.GenericServlet.init(GenericServlet.java:256)
 at com.ibm.ws.webcontainer.servlet.ServletWrapper.init(ServletWrapper.java:275)
 at com.ibm.ws.webcontainer.servlet.ServletWrapper.initialize(ServletWrapper.java:1400)
 at com.ibm.wsspi.webcontainer.extension.WebExtensionProcessor.createServletWrapper(
    WebExtensionProcessor.java:86)
 at com.ibm.ws.webcontainer.webapp.WebApp.getServletWrapper(WebApp.java:793)
 at com.ibm.ws.webcontainer.webapp.WebApp.initializeTargetMappings(WebApp.java:520)
 at com.ibm.ws.webcontainer.webapp.WebApp.initialize(WebApp.java:409)
 at com.ibm.ws.webcontainer.webapp.WebGroup.addWebApplication(WebGroup.java:115)
 at com.ibm.ws.webcontainer.VirtualHost.addWebApplication(VirtualHost.java:128)
 at com.ibm.ws.webcontainer.WebContainer.addWebApp(WebContainer.java:939)
 at com.ibm.ws.webcontainer.WebContainer.addWebApplication(WebContainer.java:892)
 at com.ibm.ws.runtime.component.WebContainerImpl.install(WebContainerImpl.java:167)
 at com.ibm.ws.runtime.component.WebContainerImpl.start(WebContainerImpl.java:391)
 at com.ibm.ws.runtime.component.ApplicationMgrImpl.start(ApplicationMgrImpl.java:1228)
 at com.ibm.ws.runtime.component.DeployedApplicationImpl.fireDeployedObjectStart
    (DeployedApplicationImpl.java:1067)
```

My system did not automatically reconnect after a network failure and I did not receive a fatal error telling me to restart my browser

It is possible that the network retry values are set for an excessively long period of time. In theory, there are no maximum values for networkRetryInterval, maxNetworkRetries, or maxNoResponseDisplayManager; however, if you set the at numbers that are too high, the recovery system tries for a long time. The values are used in two formulae:

- networkRetryInterval x maxNetworkRetries = The time spent trying to reconnect to the network before giving up.
- maxNoResponseDisplayManager = The number of times the software attempts to read tag data from the server before giving up and sending a fatal error.

  This value should be no greater than 60,000 ms (the number of seconds to wait).

Open the *IHS_HOME*\htdocs\en_us\Tracking GUI\xml\prefsV3.xml file with a text editor and reduce the values for the following parameters:

- **networkRetryInterval ms=** - The frequency of retry attempts if the network connection fails. The default is 30,000 ms.
- **maxNetworkRetries attempts=** - The maximum number of attempts before a fatal error displays. The default is 4.
- **maxNoResponseDisplayManager attempts=** - The maximum number of "no response" attempts that the Display Manager will tolerate before checking for a network connection failure. The default is 15.

The browser window hangs up and then the browser crashes

Location Awareness Services for WebSphere Premises Server may have crashed. Restart the browser.

I had a browser error, but refreshing the page did not correct the problem

The application attempts to perform error recovery but it is not always possible to recover from an error. Restart the browser.

I had a browser error message, and I selected the attempt to recover option. But it did not correct the problem, and I got the error message again.

The application attempts to perform error recovery but it is not always possible to recover from an error. Restart the browser.

I cannot stop server1 using the GUI menu

Try using the command line interface:

1. Navigate to the *was_profile*\bin directory.
2. From a command prompt, issue the following command to stop WebSphere Application Server:

   Note: Keep in mind that the user IDs and passwords could be different on your system. You do not have to specify user and password, if WebSphere Application Server security is not enabled.

   ```
   stopServer server1 -username wpsbind -password wpsbind
   ```

Tag processing does not seem to stop

If you stopped tag processing on the Control Processing portlet in the WebSphere Application Server administrative console and the tags are still moving on the Spatial Management Client or you can see that Location Awareness Services for WebSphere Premises Server is still retrieving events from the dispatcher, do the following:

1. Stop the dispatcher, if you are using it.
2. Stop tag processing again.
3. To restart tag processing with the dispatcher, start the dispatcher before starting tag processing.

If necessary, repeat the steps.

Chinese characters are not displayed properly on English Windows 2003 Server operating system

Chinese characters (or any other non-standard ASCII characters) can be displayed after installing the corresponding languages.

Event information might contain inconsistent times in event date and message

If the location event information contains inconsistent times in the event date and message, the problem might occur because the DB2 server time and the WebSphere Application Server time are not synchronized. In order to solve this problem, prior to running your configuration, it is recommended that you synchronize these server times because location events use the DB2 server time for event creation, but CEI (Common Event Infrastructure) events use the WebSphere Application Server time for event creation.

The following is an example of event information that contains inconsistent times in the event date and message:

```
Event Date
Fri Feb 22 14:12:41 CET 2008

Event Type
LasZoneEntry

Event Message
Tag [00000007] with label [] entered zone
[abc1234567d] at [Fri Feb 22 11:12:41 CET 2008]
inadmittedly. Details: Classes: [New Class?], Groups:
[Printer?]
```

Rule violation detected with some delay

If **Duration of Stay in Zone** or **Visitor Escorting** rule violations are detected with some delay, check whether their respective **Maximum duration of stay** or **Maximum tolerated rule violation time** values are less than 30 seconds. If either of these timeout values are less than 30 seconds, change the settings of the scheduler for the **Business Rules** engine. To change the settings of the scheduler for the **Business Rules** engine:

1. From the WebSphere Application Server administrative console, navigate to **Resources** → **Schedulers** → **AMITSCHEDULER**.

2. Set the **Poll interval** parameter to the minimum value for the **Maximum duration of stay** and the **Maximum tolerated rule violation time** parameters in your rule instances.

Troubleshooting the Spatial Management Client

This topic describes problems that might occur with the Spatial Management Client and provides possible solutions.

- "The Spatial Management Client does not completely start"
- "Search results are not saved"
- "Personal preferences are not saved"
- "Tags are still visible when they have already left the area, but the tag counts seem to be correct" on page 341

The Spatial Management Client does not completely start

If you cannot see the map of the current area, and you cannot see Zones in the Zones list (the Zones list basically is empty), then make sure that the Adobe Scalable Vector Graphics (SVG) Viewer plug-in for your browser is installed.

Search results are not saved

If you are using the Spatial Management Client on a Windows operating system and your search results are not properly saving as HTML, enable ActiveX in Internet Explorer:

1. In the browser, navigate to **Tools** → **Internet Options**.
2. Select the **Security** tab.
3. Click **Custom Level**.
4. Scroll down to **ActiveX controls and plug-ins** → **Initialize and script ActiveX controls not marked as safe**, and click **Enable** or click **Prompt** if you would like to be prompted with a confirmation window in order to save the search results.
5. Click **Ok**, and then click **Ok** again.

There are also two workarounds you can use if you do not choose to enable ActiveX:

- Use the Search portlet in the WebSphere Application Server administrative console and save the results as HTML.
- Use the Spatial Management Client and save the results in XML format.

Personal preferences are not saved

There are limitations in saving your personal preferences for the Spatial Management Client:

- Selected areas are not saved to your user preference. Instead, the Spatial Management Client always shows the area in the sequence defined in the prefsv3.xml file.
- The selected tag filter is not saved as your user preference. Logging in with the same user ID always starts with a tag filter of **All**.

Tags are still visible when they have already left the area, but the tag counts seem to be correct

If you have this issue, you need to add or modify the value of the `<DisplayRefreshCounter>` parameter in the prefsV3.xml file. The `<DisplayRefreshCounter>` parameter forces a repainting of all the tags in the Spatial Management Client every *nth* poll interval (`<pollInterval ms="">`).

For example, a setting of `<DisplayRefreshCounter>50</DisplayRefreshCounter>` means that the Spatial Management Client repaints every 50th poll. If you have a poll interval of 3000 (`<pollInterval ms="3000">`), then the Spatial Management Client repaints every 150th second.

If you have a lot of tags on the Spatial Management Client, repainting too often increases the load on your system. To avoid overloading, set the parameters to update every 120 seconds, or less often than that.

Messages

This section explains each element in the message line of messages. It also describes the troubleshooting components of message descriptions and presents a list of messages, each of which includes the following descriptive information:

* Message
* Explanation
* Response

The messages are arranged in numeric order, according to the message number.

Message text components

This topic explains the text components of a message.

`ATL000E DD MISSING. TERMINATING.`

Number/Severity

* `ATL0000` is the unique number for this message.
* `E` is the severity level code for the message.

    See "Severity code levels for messages" on page 342.

Message text

> `DD MISSING. TERMINATING.`The text explains the reason for the message. It might also include possible causes and system or user actions. In this example, the system is taking the action to terminate the process.

Troubleshooting components of messages

This topic describes the troubleshooting components of a message.

Message

> Example: `ATL000E CONFIGURATION MISSING. TERMINATING.`

Explanation:

> Describes what caused the message.
> * Examples of an explanation for this message:
>   Mail host configuration is missing. E-mails cannot be sent.
>   To send emails, a mail host configuration must be defined. Processing terminates.

- Examples of possible explanations for other messages:
- The name in the field member is not valid. The naming conventions are: The name must be 1 to 8 alphanumeric characters. Correct for the next run.
- A number parsing exception occurred. This happens if, for example, a letter was entered in a number field. The intended action was not performed.

System action:
> Describes what the system does.
>
> System action for this message: Processing terminates.
>
> Examples of system action include:
> - Processing terminates.
> - Processing continues.

Response:
> Describes what you must do to proceed, to recover from the error, or to avoid a problem
> - Example of the User Response for this message:
>   Either delete the notification channel pointing to the email program or configure the mail host.
> - Examples of a possible User Response for other messages:
>   - Either delete the notification channel pointing to the email program or define a mail receiver. If you do not need email notification for this time and event, ignore the message.
>   - Ask if one of your colleagues accidently deleted this record or look to see if a record that was referenced by this record was deleted

Severity code levels for messages

This topic explains severity code levels used in messages.

Severity code indicators are:
- I (informational)
- W (warning)
- E (error)

I   Informational. Provides users with information or feedback about typical events that have occurred or are occurring or requests information from users in situations where the outcome will not be negative, regardless of the response.

> **Examples:**
> - The status request is processing.
> - The files were successfully transferred.
> - Do you want to save the output in file log.txt or in file error.txt?

W   Warning. Indicates that potential problem conditions have occurred or could occur, but the program can continue. Warning messages often ask you to make decisions before processing continues.

> **Examples:**
> - The resource tahiti.com was not found. Processing will continue.
> - A file already exists with the name logfile.txt. Do you want to overwrite this file?

E   Error. Indicates problems that require intervention or correction before the program can continue. The typical result of Error messages is that processing terminates.

Examples:
- The file logfile.txt was not found and is required for processing.
- There is no space on the C drive. The file logfile.txt cannot be saved to this drive.

ATL01001E   NumberParsingException {0} occurred.

Explanation:
A number parsing exception occurred. This happens if, for example, a letter was entered in a number field. The intended action was not performed.

System action:
Processing terminates

User response:
Verify and correct the values. Then retry the operation.

ATL08001E   A RuntimeException {0} occurred.

Explanation:
A RuntimeException occurred in the Database Access Layer. The intended action was not performed. This is an internal error.

User response:
Retry the operation. If the error persists, report it to your IBM representative.

ATL08002E   A general database exception occurred. SQLcode: {0}, SQLstate {1}

Explanation:
An unhandled database exception occurred. The intended action was not performed. Review the log files for more detailed information.

User response:
Contact your database administrator.

ATL08003E   A lock, deadlock, or timeout exception occurred. SQLcode: {0}, SQLstate: {1}, cause: {2}

Explanation:
The intended action was not performed due to a lock, deadlock, or timeout. Review the log files for detailed information.

User response:
Retry the operation.

ATL08004E   Update of an entry on table {0} with key values {1} was based on an outdated version.

Explanation:

The performed update operation failed due to an outdated data record. This happened because another process had already updated the same data record.

User response:
Reload the data. Then retry the operation.

ATL08005E   The insert or update operation violated the foreign key constraint {0}. SQLcode: {1}, SQLstate: {2}

Explanation:
The value of the foreign key, which was passed to the abortive insert or update operation, did not match any parent key of the parent table. This happened because another process updated or deleted the referenced data record of the parent table before.

User response:
Correct the value and try again.

ATL08006E   The insert or update operation violated a primary key, unique constraint, or unique index for column(s) {0} of table {1}. SQLcode: {2}, SQLstate: {3} .

Explanation:
The value of the primary key, which was passed to the abortive insert or update operation, violated a primary key, unique constraint, or unique index constraint. This happened either because another process updated or inserted a data row using the values or because an update operation was performed by using values that are already in the database.

User response:
Correct the value and try again.

ATL08007E   The insert or update operation violated the check constraint {0}. SQLcode: {1}, SQLstate: {2}

Explanation:
The performed insert or update operation violated a defined check constraint.

User response:
Correct the value and try again.

ATL08008E   Assigning a 'NULL' value to a 'NOT NULL' column {0} is not allowed. SQLcode: {1}, SQLstate: {2}

Explanation:
The value, which was passed to the abortive insert or update operation, was 'NULL', but the object column was declared as 'NOT NULL' in the table definition.

User response:
Correct the value and try again.

ATL08009E   Assgined value is too long or too large. SQLcode: {0}, SQLstate: {1}

Explanation:
A value, which was passed to the abortive select, insert or update operation, was too long or too large.

User response:
Correct the value(s) and try again.

GENERAL   A general exception has occurred.

Explanation:
An exception has occurred. No additional information is available.

User response:
Contact the System Administrator for further information.

DBEXCEPTIONINPORTLET   A database exception has occurred {0}.

Explanation:
The system tried to access the database and an error occurred.

User response:
Contact the System Administrator for further information.

SQLEXCEPTION   A SQL exception has occurred.

Explanation:
A SQL exception has occurred and is wrapped by an Atlas data base exception.

User response:
Contact your database administrator.

RUNTIMEDBEXCEPTION   A Runtime Exception has occurred.

Explanation:
A Runtime Exception has occurred within the Database Access Layer.

User response:
Contact your Database Administrator.

JMSEXCEPTION   A JMS Exception has occurred ({0}).

Explanation:
Communication with the remote legacy system has failed.

User response:
Verify the configuration for the service bus.

GENERALDBEXCEPTION   A general database exception has occurred: {0}.

Explanation:
A general database exception has occurred. No additional information is available.

User response:
Contact the System Administrator or the Database Administrator for further information.

IMPORTEXCEPTION   Error in an ATLAS import operation.

Explanation:
See message.

User response:
Correct errors and try again.

INVALIDINPUTEXCEPTION   Invalid input: {0}

Explanation:
You have specified a value that is not valid.

User response:
Enter the correct value and try again.

REGUNITCONNECTIONEXCEPTION   An exception occurred when working with the registration-unit. {0}

Explanation:
See message.

User response:
Verify that:
- Your registration-unit is running
- The correct ip-address and port are specified in the RegistrationUnits-Portlet.

GENERALCEIEXC   An exception related to the Common Event Infrastructure has occurred. It is not possible to send, get or update events.

Explanation:
Communication with the event database or the event emitter failed.

User response:
Ask your System Administrator to review the Common Event Infrastructure configuration.

CEIEVENTNOSND

Explanation:
CEI events cannot be sent.

System action:
This can be due to configuration errors in the event database, the CEI server application, or the underlying service bus.

User response:
Ask your System Administrator to verify the Common Event Infrastructure configuration.

CEIEVENTNOGET   CEI events cannot be retrieved.

Explanation:
This can be due to configuration errors in the event database or in the CEI server application.

User response:
Ask your System Administrator to verify the Common Event Infrastructure configuration.

CEIEVENTNOCHG   CEI events cannot be updated to reflect alert handling.

Explanation:
This can be due to configuration errors in the event database, the CEI server application, or the underlying service bus.

User response:
Ask your System Administrator to verify the Common Event Infrastructure configuration.

XPATHSELECTOR   The channel selector to determine the events of interest is not usable. The notification channel will be ignored.

Explanation:
This might be due to a version inconsistency or an incorrect manual edit of the selector.

User response:
Delete the notification channel and add it again, using the dialog.

FILEIOEXCEPTION   An exception occurred when writing file '{0}'.

Explanation:
See message.

User response:
Contact your System Administrator.

INTERNAL   An internal error has occurred ({0}).

Explanation:
The intended action was not performed because of an internal error that is not covered.

User response:
Try the operation again. If the error persists, report it to your IBM representative.

KEYPROPERTYNOTDELETABLE   You cannot delete key-property {0} because {1} are existing.

Explanation:
Objects exist that depend on the key property you want to delete.

User response:
First delete the corresponding objects. Then delete the key property.

UPDATEABLERECORDDELETED   Your update on {0} could not be saved because {0} was deleted by someone else.

Explanation:
While you were editing the record, someone else deleted it.

User response:
Speak with your colleagues and ask if someone accidently deleted your record.

FILENOTFOUND   The specified file or path {0} could not be found.

Explanation:
Either the entered file or path does not exist or access is denied because of missing authorizations.

User response:
Verify that you entered the correct file or path and that you have the required access authorizations.

ZIPEXCEPTION   Either the .zip file {0} could not be opened or the specified path {1} could not be found.

Explanation:
The entered file path does not exist. Either the .zip file is damaged or access is denied because of missing authorizations.

User response:
Verify that you entered the correct file path and retry the operation.

DUPLICATEKEYPROPERTIES   An item already exists with the same values in its key properties.

Explanation:

ATL01002W • CANTEDITBECAUSEDELETED

An item is already defined that has same values in all of its key properties.

User response:
Verify that all key property values for this item are correct.

ATL01002W   None of the search criteria were selected.

Explanation:
None of the required selection criteria were selected. One of the search criteria checkboxes, Class Properties, Group Properties, or Tag Properties must be selected. .

User response:
Select at least one of the search criteria and try the operation again.

ATL15001E   Sender address {0} is not a valid internet address.

Explanation:
The address must be in the xxx@yyy format.

User response:
Correct the email address in the configuration for the mail host.

ATL15002E   Mail host configuration is missing. E-mails cannot be sent.

Explanation:
To send mails, a mail host configuration must be defined.

User response:
Either delete the notification channel pointing to the email program or configure the mail host.

ATL15003E

Explanation:
Mail host configuration data not accessible.

System action:
The table for the mail host configuration was not accessible.

User response:
Inform the System Administrator.

ATL15004E   Mail receiver data not accessible.

Explanation:
The table for mail receivers was not accessible.

User response:
Inform the System Administrator.

ATL15005E

Explanation:
One of the receiver addresses is not a valid internet address: {0}

System action:
The address must be in the xxx@yyy format.

User response:
Correct the receiver email address in the configuration.

ATL15006E   Mail could not be sent.

Explanation:
The email could not be sent because of the reason specified.

User response:
Correct the receiver email address in the configuration.

ATL15007W   Mail cannot be sent since no receiver addresses defined.

Explanation:
To send mails a mail receiver must be defined for this time and event type.

User response:
Either delete the notification channel pointing to the email program or define a mail receiver. If you do not need email notification for this time and event, ignore the message.

ATL15008W   No mail receivers available.

Explanation:
To send mails, a mail receiver must be defined for this time and event type.

User response:
Either delete the notification channel pointing to the email program or define a mail receiver. If you do not need email notification for this time and event, ignore the message.

CANTEDITBECAUSEDELETED   You cannot edit the {0} because it was already deleted.

Explanation:
The record you want to edit has already been deleted. Either this was done by someone else or it was done indirectly because something was deleted that is referenced by this record; and therefore, this record was also deleted. .

User response:
Ask if one of your colleagues accidently deleted this record or look to see if a record that was referenced by this record was deleted

Glossary

This topic lists terms that are used in this documentation.

Alarm zone

Zone where access restriction rules or similar rules can be triggered when an item (usually person or asset) enters this type of zone. Restriction rules can also be set for other zone types, but they have additional semantics.

Area A representation of the real physical space within the location to be monitored. Areas have a flat lower and an optionally flat upper boundary and are the container for all zones.

Boundary zone

Zone used to monitor tags entering and leaving another zone.

Container

Items that can contain other items. Tags that are added to a container inherit the position of the container. Also you can define the size of a container using the EDGELENGTH system property, which assumes the container is a cube.

Device

A device is used for an event provider to provide location, notification, or telemetry data. Devices always belong to a hub and can be grouped in device groups.

Event converter

Applications that convert external events into a format that Location Awareness Services for WebSphere Premises Server can process. Event converters are specific to each location event provider and can be provided as plugins.

Event database

A database that stores all events that are sent by Location Awareness Services for WebSphere Premises Server.

Event group

A group of related messages. A filter is defined to route certain types of alert messages to the related message queue.

Exit zone

Zone used to determine whether a tag has exited the area. If the tag passed and no signals can be received thereafter, the item has left the area and there is no reason to be concerned about not receiving a signal.

Gate An entry or exit to or from a zone that is monitored by one device.

Group A container that allows grouping of items from different classes for common rules, searches, or so forth.

Item Entities within a location that can be equipped with tags and whose positions can therefore be tracked. An example is an asset or person.

Item class

Class of items with common attributes. You can define sets of attributes and rules for each item class. For example, you might have the following classes: Person and Asset. Within these classes, you can also have subclasses with extended attributes.

Location

A real physical space that is made up of many areas.

Location event provider

A third party that monitors areas and feeds Location Awareness Services for WebSphere Premises Server tag location data. Location event providers are not part of Location Awareness Services for WebSphere Premises Server, so they must be defined within Location Awareness Services for WebSphere Premises Server. They must be configured for an existing area so that Location Awareness Services for WebSphere Premises Server can track tags within that area.

Location event device

A third party that receives the tag signal and transmits the data to the location event provider.

Notification channel

A channel definition that defines for a given subscriber the program or web service that should be called for an event, and the filter criteria under which the program or web service should be called.

Notification program

A program or web service that can be triggered when an event occurs.

Privacy zones

Currently, privacy zones behaves like alarm zones.

Registration unit

A location event provider that, as a whole or with a special part of its infrastructure, reads tag IDs into the Location Awareness Services for WebSphere Premises Server system for the purpose of defining an item for the first time.

Rule   Criteria or circumstances that are defined to trigger an event. For example, rules can be triggered during entry to or exit from a zone and can be specified for a tag ID, class, or group. You can set the following types of rules in Location Awareness Services for WebSphere Premises Server:

- Zone entry and exit rules
- Tag not responsive rule
- Tag battery low rule
- Proximity rule
- Unknown tag rule

Shadow zone

Zone where the tags might not be visible temporarily because they are out of reach of the tag reader infrastructure or the signals are shielded. Location Awareness Services for WebSphere Premises Server assumes that a tag continues to be in the shadow zone at the last reported position after it has been seen. No alert is generated if the tag is no longer visible.

Smoothing algorithm

Algorithm used to smooth position estimates, so that tag icons do not move abruptly in the Spatial Management Client.

Subarea

An area that is nested within another area.

Subscriber program

A program that subscribes all, or a defined subset of, events arriving for a given event group. It dispatches the arriving events to the Location Awareness Services for WebSphere Premises Server notification programs.

Zone   Logical section within an area for which rules can be defined. A zone can

span multiple subareas of the area to which it is related. It is the unit on which rules can be performed, and on which counts and statistics for a tag entering or leaving can be calculated. Rules can be defined for entering and exiting a zone.

Chapter 8. Use cases and samples

This section contains use cases and samples for WebSphere Premises Server.

Standard dock door receiving example usage scenario

In this scenario, a dock door is enabled to read tags, tags move through the doorway and trip the sensor, and messages are sent, received, and handled by WebSphere Premises Server.

IBM WebSphere Premises Server provides example code for the following usage scenario. It also provides code for other usage scenarios, including enhanced dock door receiving. You can also develop your own agents or modify the example agents, in which case, you might also need to develop other business logic on WebSphere Premises Server or in Data Transformation.

Note: The term, *portal*, here is used to indicate a dock door and its associated I/O devices. A portal is the physical installation that enables the reading of information when pallets move through it. A portal consists of a reader, antennas, sensor devices, and feedback devices, such as a light tree. In a retail dock door receiving scenario, the portal is directly behind a dock door of a retail store or retail distribution center.

Note: The terms *edge controller*, *Data Capture and Delivery*, *remote Data Capture and Delivery*, and *local Data Capture and Delivery* all refer to the same functional concept, and can be used interchangeably most of the time. These terms refer to the portion of the RFID system that interfaces directly with the physical readers, collecting the raw data and performing some basic processing. Starting with the WebSphere RFID Premises Server 6.0 release, this functionality can run as part of the WebSphere Premises Server (local Data Capture and Delivery), or on a separate processor (remote Data Capture and Delivery) to distribute load. In previous versions of WebSphere RFID Premises Server, this functionality running on a remote processor was referred to as an edge controller. For simplicity and compatibility with previous versions of the product, the term edge controller is still used in the product documentation.

The following steps describe the usage scenario:
1. By default, the portal is enabled (`portal.initial` is set to `on` in the PortalControllerAgent file). The I/O agent publishes an event message to the messaging service. The controller agent that is subscribed to the switch topic registers the event and publishes a "dock door enabled message" to the messaging service and then to WebSphere Premises Server.

   Note: If the portal property, `portal.initial`, is set to `off` in the PortalControllerAgent file, or the switch is ever used, then the switch is required to set the portal back on. At that point, you would press a switch to enable the portal, and an I/O agent connected to the switch through an I/O adapter senses the change.
2. A motion sensor is tripped by the movement of an item through a reader portal.

3. The I/O agent connected to this motion sensor notes the change and publishes a sensor event message to the messaging service.
4. The controller agent, also subscribed to the motion sensor topic, registers the event and publishes a message to the portal reader to begin reading tags.
5. The reader agent receives the message to begin reading, starts reading, and publishes the found tags to the messaging service.
6. After a period of motion sensor inactivity, the controller agent publishes a message to the reader to stop reading.
7. The reader agent receives the tag information from the messaging service.
8. The reader agent removes duplicate reads and any non-pallet tags from the data.
9. A filtered set of tags is published to the messaging service and then to the WebSphere Premises Server.
10. The tag information is received by the Event server application running on the WebSphere Premises Server.
11. The list of tags and the tag reader from which they were retrieved are sent to the enterprise system to be verified against an excepted list in the warehouse management system.
12. The enterprise responds with an "accept" or "reject" message for the items in the list.
13. The WebSphere Premises Server formats the response and forwards it to the correct Data Capture and Delivery controller.
14. The message is published to the messaging service and is received by the controller agent.
15. If the item was expected, a green light message is published through the messaging service. If the item was not expected, a red light message is published.

Enhanced dock door receiving example usage scenario

This scenario is a behavior enhancement to the standard dock door receiving example usage scenario.

IBM WebSphere Premises Server provides example code for the following usage scenario. To support other usage scenarios, you must develop your own agents or modify the example agents.

Note: The term, *portal*, here is used to indicate a dock door and its associated I/O devices. A portal is the physical installation that enables the reading of information when pallets move through it. A portal consists of a reader, antennas, sensor devices, and feedback devices, such as a light tree. In a retail dock door receiving scenario, the portal is directly behind a dock door of a retail store or retail distribution center.

Note: The terms *edge controller*, *Data Capture and Delivery*, *remote Data Capture and Delivery*, and *local Data Capture and Delivery* all refer to the same functional concept, and can be used interchangeably most of the time. These terms refer to the portion of the RFID system that interfaces directly with the physical readers, collecting the raw data and performing some basic processing. Starting with the WebSphere RFID Premises Server 6.0 release, this functionality can run as part of the WebSphere Premises Server (local Data Capture and Delivery), or on a separate processor (remote Data Capture and Delivery) to distribute load. In previous versions of WebSphere

RFID Premises Server, this functionality running on a remote processor was referred to as an edge controller. For simplicity and compatibility with previous versions of the product, the term edge controller is still used in the product documentation.

Overview

Goods tagged with case or pallet tags are brought through a portal that is controlled by a motion sensor (an entrance) and a light barrier (the exit). These tags are read and reported to the back-end system. The back-end system returns a validation by way of the light tree.

Note: The enhanced dock door receiving usage scenario behaves differently than the standard dock door receiving usage scenario. Any error (such as a sensor error, a reader that is down, or application ping) terminates the current pallet movement cycle. Regardless of the sensor signals, an aggregated tag message is sent to WebSphere Premises Server and the yellow light signals that the portal is no longer active. So when the error condition is resolved, a motion sensor signal is required to start a new portal read cycle. In addition, the sequence sensor signals are different for the enhanced dock door receiving usage scenario. When the operator is inside the portal, the motion sensor goes off even when there is movement inside the portal. When the reader reconnects after a short connection drop, in most cases, the motion sensor status is "off." The operator must leave the portal, and wait until the yellow light signals that the portal is active again before moving the next pallet through.

The HealthCheckAgent checks the availability of the RFID hardware and software for readiness. Specifically, the HealthCheckAgent checks the reader and the status of the sensors, and it checks the availability of WebSphere Premises Server and the back-end system. The ApplicationPingAgent is responsible for checking WebSphere Premises Server and the back end. The Data Capture and Delivery controller passes a token item (a message with a timestamp) to WebSphere Premises Server and from there it might be forwarded to the integration domain (a back-end system with which WebSphere Premises Server can integrate through WebSphere MQ, for example). Then, the integration domain passes the token to the back-end system. The back-end system returns the token to the integration domain where it passes the token by way of WebSphere Premises Server back to the Data Capture and Delivery controller. The termination outcome is "successful." If the token is not returned within a configurable time frame (a system malfunction), the ApplicationPingAgent returns a negative result (the termination outcome is "failure") to all HealthCheckAgents that are on the Data Capture and Delivery controller. The HealthCheckAgent informs the PortalControllerAgent about changes in the portal health. The PortalControllerAgent might signal either the portal health or reader activity using the yellow light on the light tree.

Four additional agents that play an important role in the enhanced dock door receiving usage scenario are listed below:
- HealthCheckAgent
- ApplicationPingAgent
- PortalControllerAgent

This usage scenario assumes the following preconditions:
- The system consists of
  - a dock door with a RFID reader

- a motion sensor
- a light barrier
- a light tree with red, yellow, and green lights
- an audio device
- a Data Capture and Delivery controller
- WebSphere Premises Server
- a back-end system

- The system is active, and the portal is operable ("healthy") and working.
- The portal is activated.
- The reader is not reading.
- The red and green lights are off.
- All sensors are inactive.
- A yellow light signals that the portal is operable ("healthy").

Note: You can configure how the yellow light signals the portal health status. By default, the light "on" signals that the portal is operable. The light "off" means that there is a problem with one of the sensors or the reader, or that the WebSphere Premises Server or back end is not available. To avoid the yellow light being on throughout the day, configure the light tree agent to signal error conditions by the light being on.

Usage Scenario

1. An attendant moves the pallet toward the portal.
2. A motion sensor connected to the reader, which is connected to the Data Capture and Delivery controller, is tripped by the movement of an item through the portal and triggers the start of the new aggregation cycle.
3. The portal controller agent, also subscribed to the motion sensor topic, registers the event and publishes a message to the reader to begin reading tags.
4. During the aggregation cycle, the Data Capture and Delivery controller filters duplicates and stores the gathered EPC codes in a list. For tag read events from pallet tags (containing SSCC codes), the system immediately converts them into EPC-ID format (configurable) and forwards the read event to the Integration Domain.
5. By way of the Integration Domain, the back-end system validates each tag-read event with a response code of Accept, Reject, or Acked (acknowledged). This response appears in the Tag History on WebSphere Premises Server. Depending on the validation result, the light tree shows:
   - green - accept
   - red - reject
   - no change to the light tree - acked
6. When the pallet is inside the portal, the motion sensor goes off, but the reader is still reading tags. When the pallet leaves the portal, the light barrier's light beam is, at first, interrupted by the pallet. The light barrier sensor reports "blocked" to the Data Capture and Delivery controller. When the pallet completely leaves the portal, the light barrier signals "unblocked" again. This signal is the trigger that indicates the end of the aggregation cycle.
7. The PortalControllerAgent issues a message to stop the reader and tells the aggregation agent to terminate the cycle.
8. A list of all tags read is sent to WebSphere Premises Server. The back end sends a validation response in response to the aggregation list. If the back end

identifies this shipment as incomplete (for example, a pallet is missing on a stacked pallet), the back end might return a validation of "Reject" and the light tree would show a red light. Under normal conditions, the validation would be "Acked" and nothing changes on the light tree. In any case, this ends the enhanced dock door receiving usage scenario.

Agent logic

This section describes how the agents work together in the enhanced dock door receiving usage scenario.

1. The portal read cycle starts when the sensor detects motion.
2. Because portal sensors are mostly connected to I/O ports of the reader, the I/O agent processing this signal is usually part of the reader agent. The I/O agent publishes an I/O event message on the messaging service inside of the Data Capture and Delivery controller.
3. The UniversalSensorAgent has several instances, such as Motion or Barrier for one portal. These instances, called sensor agents, are identified by their alias names. These alias names and the portal ID of the UniversalSensorAgent configuration make up a unique ID on the messaging service, such as Motion-P1 and Barrier-P1. The I/O event is received by the corresponding sensor agent, which performs some processing, such as inverting input to output, delaying the change to inactivity (inactivity timeout), and checking for sensor error situations, such as a blocked light barrier.
4. After processing, the sensor agent publishes a sensor topic (not an I/O topic) with a defined meaning of its values "On" and "Off." (Barrier = On means that the barrier is interrupted and Motion = On means that motion is detected.)
5. The PortalControllerAgent receives a sensor topic and reacts on it.
6. Back to the scenario, Motion = On starts the reader and the aggregation cycle begins.
7. Tags might be read.
8. The reader publishes a reader tag read topic to the filter agent and the aggregation agent.
9. The reader agent filters out duplicates and all tags except SSCC tags (pallet tags).
10. For new SSCC tags, the reader agent publishes a tag read event to the WebSphere Premises Server.
11. The reader agent puts the tag reads in a list, indexed by EPC code.
12. During the aggregation cycle, the motion sensor might go off, but the reader continues reading tags.
13. To end an aggregation cycle, motion must be off and the light barrier must have transitioned from the "unblocked" state to "blocked" and back to "unblocked" to signal the end of the pallet.
14. There might be a delay in the blocked to unblocked transition by the sensor agent to make sure that every tag at the end of the pallet has been read.
15. The PortalControllerAgent turns off the reader and terminates the aggregation cycle.
16. When the TagAggregatorAgent receives the "end of aggregation" message from the PortalControllerAgent, it sends the complete list of received tags to the WebSphere Premises Server, and then clears the list.
17. The WebSphere Premises Server sends each single tag read event and the aggregated list to the Integration Domain.

18. The back end responds with "Accept," "Reject," or "Acked" and sends these responses back to the Data Capture and Delivery controller.

19. The light tree signals an "accept" message with a green light and a "reject" message with a red light.

Independent of the portal read cycle, the Data Capture and Delivery controller constantly monitors the portal status for error conditions (health) and actively checks the availability of the WebSphere Premises Server by way of the Integration Domain up to the back-end system:

1. In a normal health check situation, the reader is up and no sensor error messages are received.

2. Initially, the HealthCheckAgent assumes that application ping is up and that the ApplicationPingAgent pings the WebSphere Premises Server periodically to identify connectivity problems.

3. The HealthCheckAgent listens to sensor error messages, reader up and down messages, and application ping up and down messages.

4. When an error message arrives, the HealthCheckAgent publishes a message on the messaging service to tell the PortalControllerAgent that the portal health status is currently "down."

5. Sensor agents signal an error condition if the sensor is active for too long. The error condition is cleared with a sensor state change.

6. The ApplicationPingAgent signals an error when no response to an application ping message is received within a specified time period (response timeout). Receiving a response to a ping message (called a pong message), in time, clears the error condition.

7. When all errors are cleared for this portal, the HealthCheckAgent sends a message that the portal health status is "up" again.

Print, Verify, and Ship example usage scenario

The IBM WebSphere Premises Server Print, Verify, and Ship Reference User Interface enables users to print RFID tag labels, associate case tags with containers, validate outgoing containers, and run a variety of reports. This topic defines terms and describes the Print, Verify, and Ship processes.

Overview

You can use the Print, Verify, and Ship Reference User Interface in both integrated and non-integrated environments. In an integrated environment, the RFID network retrieves information from the back-end enterprise system; therefore, product and catalog information display directly in the Print, Verify, and Ship Reference User Interface. In a non-integrated environment, the RFID network is not connected to the back-end enterprise system and does not have access to product and catalog information.

Before using the Print, Verify, and Ship Reference User Interface, your administrator must create pack types and profiles using the WebSphere Premises Server Administrative Console. A pack type represents a type of container, such as a case or pallet. Each pack type is associated with various pieces of information that are required for converting customer-specific product codes to EPC format. For additional information about pack types, see "Working with pack types" on page 185. A profile is an association of a particular customer's pack types into a single record. Profiles simplify the process of printing tag labels. For additional information about profiles, see "Working with profiles" on page 191.

Tag labels are printed based on print templates defined in the WebSphere Premises Server Administrative Console. You can print tag labels using a device adapter for a tag printer. You can use adapters for printer software vendors, such as Loftware or BarTender, or you can develop and add adapters that can be used for other printer vendors. For additional information about tag printers, see "Configuring printers" on page 359.

WebSphere Premises Server provides example code for the following usage scenario. To support other usage scenarios, you must develop your own agents or modify the example agents.

Scenario steps

1. Open the Print, Verify, and Ship Reference User Interface.
2. Click **Print** on the menu bar.
3. Click the **Setup** tab:
   - In an integrated environment, select a profile and purchase order for the print job. The interface retrieves the purchase order and catalog information from your enterprise system.
   - In a non-integrated environment, select the profile and enter the purchase order number. The purchase order number and any associated products you add for printing are saved in a record in the WebSphere Premises Server database. You can retrieve this information later for verification and shipping.
4. Click one of the following tabs to determine the products for which you are printing tag labels:
   - Click **Select** to select the products from a purchase order or catalog.
   - Click **Search** to search for products by description keyword.
   - Click **Enter** to scan GID (Global ID/UPC) codes with a hand-held reader or enter the codes manually.
5. Ensure that the customer profile, purchase order information, and details are correct.
6. Click the **Print** tab to set up the print job:
   a. Select the printer to which you are sending the print job.
   b. Enter a description of the print job.
   c. Click **Submit** to send the job to the printer.

   Note: To view the status of the print job, select it from the menu and click **Status**.
7. If a tag label is damaged, you can reprint it from the **Reprint** tab by entering the EPC URN that is printed on the label, selecting the encoding type for the tag label, and entering the serial number. For example, an EPC URN for an sgtin 69 tag would be: urn:epc:tag:sgtin-96:2.1234567.100150.11
8. Click **Verify** on the menu bar to associate existing tagged items with containers so that the items being shipped are tracked accurately:
   - Click **Manual** to retrieve all the EPC URN tag values printed for a purchase order, and store the relative associations in a database. You do this without a reader. For example, you can associate case tags with a particular pallet tag. You can define any selected tag as a container. When a tag is made a container, you can associate other tags as subordinates. When an association is stored, the total number of items decrements from the number of items required for a purchase order.

- Click **Automatic** to retrieve a list of tags printed for a purchase order. A reader reads a set of tags. The tags are filtered based on what previously printed for a purchase order. If the tags read by the reader have printed for a purchase order, they display in the Expected Tags list. If the tags read were not associated with a purchase order, they display in the Unexpected Tags list. Tags in the Associated Tags list can be associated.

9. Save the association. The Verification Report displays the status of the associated cases.

  - In an integrated environment, the system saves the association to your back-end enterprise system database and updates the Verification Report to reflect the status of the items on the purchase order.

  - In a non-integrated environment, the system saves the association to the WebSphere Premises Server database for validation later but does not display the Verification Report.

10. When outgoing shipments are ready to exit the dock door, click **Ship** on the menu bar to match the container tag with a purchase order.

  - If the container tag matches the purchase order, a green light displays on the light tree and the shipment proceeds.

  - If the container tag does not match the purchase order, a red light displays on the light tree and the shipment is stopped.

Configuring Print, Verify, and Ship

The Print, Verify, and Ship application enables you to print RFID tag labels, associate case tags with containers, validate outgoing containers, and run a variety of reports.

This document uses the generic term *container* to include any kind of container that stores cases of items. For example, a *pallet* is one example of a container.

When you installed WebSphere Premises Server, you installed the software components required for running the Print, Verify, and Ship application, including the following:

- Print, Verify, and Ship Reference User Interface, which is the Web-based application used to manage the print, verify, and ship processes. You can access the Print, Verify, and Ship application from any computer connected to the RFID network by typing `http:/premises_server_hostname:9080/RFIDPrintWeb/ RFIDPrintWeb` in the **Address** field of your Web browser. If WebSphere Premises Server is installed on your local server (Windows platforms only), you can access the interface by selecting **Start** → **All Programs** → **IBM WebSphere Premises Server** → **Premises Server** *version* → **PVS Reference User Interface**.

- The WebSphere Premises Server Administrative Console, which contains functions required for configuring the Print, Verify, and Ship Reference User Interface. You can access the WebSphere Premises Server Administrative Console by typing `http:/premises_server_hostname:9080/ibmrfidadmin` in the **Address** field of your Web browser. If WebSphere Premises Server is installed on your local server, you can access the administrative console by selecting **Start** → **All Programs** → **IBM WebSphere Premises Server** → **Premises Server** *version* → **Administrative Console**.

Before you can use the Print, Verify, and Ship application, complete the steps in the following sections:

1. "Configuring printers" - refer to this section to use the WebSphere Premises Server Administrative Console to configure the necessary tag printers and print templates used for printing tag labels.
2. "Configuring EPC commissioning details" on page 198 - refer to this section to use the WebSphere Premises Server Administrative Console to configure the information required for converting suppliers' product codes to Electronic Product Code (EPC) format.

After you configure the items mentioned above, you can use the Print, Verify, and Ship Reference User Interface to print RFID tag labels. See the "Using the Print, Verify, and Ship Reference User Interface" on page 362 for more information.

Configuring printers

You can use any of the supported printers with the Print, Verify, and Ship scenario.

Using the WebSphere Premises Server Administrative Console, you can define devices as printers and then set up print templates for those printers to use.

There are two ways to handle print jobs with WebSphere Premises Server:
- Logical printers - These are predefined printer devices, such as Loftware Labeling System by Loftware, Inc. or BarTender by Seagull Scientific, Inc, that allow tag printing through a third-party software system.
- Inbound and outbound printing using print profiles - This feature uses a publish/subscribe method to send and receive messages through the WebSphere Application Server service integration bus (SIBus).

Creating print templates

Use the **Print Templates** link in the WebSphere Premises Server Administrative Console to create a template to use for printing tag labels in the Print, Verify, and Ship Reference User Interface.
1. Follow the steps in "Adding print templates" on page 205
2. Create the properties file for the print template to submit print jobs from the Print, Verify, and Ship Reference User Interface. See "Creating properties files for print templates" on page 360 for more information.

Creating custom templates

This section describes how to create a custom template for both a logical and a physical tag printer. Creating a custom template enables you to specify what information prints on the label and how it appears.

Basically, there are three functions that you must complete before you can use a custom template:
1. Define the data and appearance of the information that prints on the tag
2. Create a .zip file that contains all the files for the template
3. Define the template using the WebSphere Premises Server Administrative Console

You can use a sample print template and customize it to meet your specific label requirements. Sample print templates are provided in the following directories:

> **Windows** *IBM_RFID_HOME*\premises\pvs\templates
> **Linux** *IBM_RFID_HOME*/premises/pvs/templates

When you create a custom print template, the information is stored in the WebSphere Premises Server database. A custom print template for a logical printer

must be stored on the file system of the logical printer software. For example, the .lwl Loftware print template must be on the Loftware server to access it.

To submit custom print jobs from the Print, Verify, and Ship Reference User Interface, you must create a corresponding properties file after you define the print template. The properties file contains static information such as customer name and address, and dynamic information like product name and description. During the printing process, the application uses the data in the properties file to construct the contents of the label.

Creating properties files for print templates:

To submit print jobs from the Print, Verify, and Ship Reference User Interface, you must create a corresponding properties file on WebSphere Premises Server after you create a new print template.

About this task

Most print templates contain static information for the label stored in template properties files. However, you can create properties files using substitution variables. These properties files are stored on the premises server, and the information contained within them is retrieved when you submit a print job from the Print, Verify, and Ship Reference User Interface. For a list of substitution variables, see "Substitution variables for template properties files" on page 361.

The easiest way to create a new properties file is to modify one of the existing files located in the following directory:

> **Windows** *WAS_PROFILE_HOME*\installedApps*node_name*\\ IBM_Premises_PVS_Console.ear\ibmrfid_premises_pvsapp.war\config

> **Linux** *WAS_PROFILE_HOME*/installedApps/*node_name*/ IBM_Premises_PVS_Console.ear/ibmrfid_premises_pvsapp.war/config

This is the default directory for your properties files unless another directory is specified in the pvsapp.properties file.

Note: You can change the location of these files by modifying the pvsapp.properties file, which is located in the default properties file directory.

If you modify the pvsapp.properties file, you must stop and then restart either WebSphere Application Server server 1 or the IBM_Premises_PVSConsole enterprise application from the WebSphere Application Server administrative console. Use the following steps to stop and restart the IBM_Premises_PVSConsole enterprise application:

1. Log on to the WebSphere Application Server administrative console.
2. Click **Applications → Enterprise Applications**.
3. Stop and restart IBM_Premises_PVSConsole.

Use the following steps to create properties files for print templates:

1. Open one of the existing template properties files from the premises\pvs\templates directory.
2. Modify the static properties in the file to match the information needed for your print template:

- If you are using a Loftware print template, use the Loftware software to examine the .lwl template file to see what properties it is expecting.
- If you are using a Bartender print template, use the Bartender software to examine the .btw template file to see what properties it is expecting.
- If you are using a physical print template, open the *template_name*.csv file located in the template .zip file. For example:

```
0,TEMPLATE,$TEMPLATE_NAME
1,RFID,$TAG
3,STRING,productname
4,STRING,productdescription
5,STRING,productquantity
6,STRING,manufactureid
7,STRING,manufacturename
```

  Variables with a "$" are dynamically inserted by the Print, Verify, and Ship Reference User Interface application during printing.

  Note: When printing tag labels that use substitution variables, be sure to limit the amount of data you enter in the Print, Verify, and Ship Reference User Interface to prevent printing more characters than can fit on the tag label.

  You must include the string variables in the properties file. For example:

```
productname=Widgets
productdescription=steel widgets
productquantity=50
manufacturerid=123456
manufacturername=Widget Company
```

3. Save the properties file in the templates directory, using the same name as the print template file. For example, if the print template file is called zebra-SIMPLE-template.zip or Simple.lwl, name the properties file SIMPLE.properties.
4. Restart the Data Transformation service on both the WebSphere Premises Server and the edge controller.

What to do next

Note: You must restart WebSphere Premises Server each time you make changes to these properties files.

  To stop and restart the WebSphere Premises Server:
- Run *WAS_HOME*\bin\stopServer server1 to stop.
- Run *WAS_HOME*\bin\startServer server1 to start.

    > Windows   stopServer.bat and startServer.bat
    > Linux   stopServer.sh and startServer.sh

Important: When using a properties file in the Print, Verify, and Ship Reference User Interface that contains non-English-language characters, be sure to run the J2SE utility, native2ascii, against the properties file to convert the non-English-language characters to their Unicode ASCII equivalent. The properties files are required when adding print templates to the WebSphere Premises Server Administrative Console.

Substitution variables for template properties files:

When creating properties files for printer templates, you can substitute information for the following variables.

Note: When printing tag labels that use substitution variables, be sure to limit the amount of data you enter in the Print, Verify, and Ship Reference User Interface to prevent printing more characters than can fit on the tag label.

Variable	Description
$BUSINESSREFERENCEID	Synonym for $PURCHASEORDERID
$CASESPERPALLET	Value in PVS.PRODUCTDATA.CASESPERPALLET
$DESCRIPTION	Value in PVS.PRODUCTDATA.DESCRIPTION
$GID	Value in PVS.PRODUCTDATA.GID
$ITEMSPERCASE	Value in PVS.PRODUCTDATA.ITMSPERCASE
$MANUFACTURERID	Value in PVS.PRODUCTDATA.MANUFACTURE
$MANUFACTURERNAME	Value in PVS.MANUFACTURER.MANUFACTURERNAME
$PARTNUMBER	Value in PVS.PRODUCTDATA.PARTNUMB
$PRODUCTNAME	Value in PVS.PRODUCTDATA.PRODUCTNAME
$PRODUCTQUANTITY	For cases: Value in PVS.PRODUCTDATA.ITEMSPERCASE. For pallets: Value in PVS.PRODUCTDATA.ITEMSPERCASE multiplied by the value in PVS.PRODUCTDATA.CASESPERPALLET. For other pack types: defaults to "1."
$PURCHASEORDERID	The current purchase order number
$SHIPFROMCITY	Value in PVS.PODATA.SHIPFROMCITY
$SHIPFROMCOMPANY	Value in PVS.PODATA.SHIPFROMCOMPANY
$SHIPFROMCOUNTRY	Value in PVS.PODATA.SHIPFROMCOUNTRY
$SHIPFROMNAME	Value in PVS.PODATA.SHIPFROMNAME
$SHIPFROMSTATE	Value in PVS.PODATA.SHIPFROMSTATE
$SHIPFROMSTREET	Value in PVS.PODATA.SHIPFROMSTREET
$SHIPFROMZIP	Value in PVS.PODATA.SHIPFROMZIP
$SHIPTOCITY	Value in PVS.PODATA.SHIPTOCITY
$SHIPTOCOMPANY	Value in PVS.PODATA.SHIPTOCOMPANY
$SHIPTOCOUNTRY	Value in PVS.PODATA.SHIPTOCOUNTRY
$SHIPTONAME	Value in PVS.PODATA.SHIPTONAME
$SHIPTOSTATE	Value in PVS.PODATA.SHIPTOSTATE
$SHIPTOSTREET	Value in PVS.PODATA.SHIPTOSTREET
$SHIPTOZIP	Value in PVS.PODATA.SHIPTOZIP
$TRANSPORTCO	Value in PVS.PODATA.TRANSPORTCO
$UNITOFMASS	Value in PVS.PRODUCTDATA.UOM
$UPC	Value in PVS.PRODUCTDATA.UPC

Using the Print, Verify, and Ship Reference User Interface

The Print, Verify, and Ship Reference User Interface is an easy-to-use, Web-based software application that is used to manage the print, verify, and ship processes for the WebSphere Premises Server solution.

It contains the following main functions:
- **Print** - use the Print panel to determine the products for which you need to print RFID tag labels. The labels print with information stored in properties files,

such as *SampleCaseTag.properties* and *SamplePalletTag.properties*. Some properties file information are hard-coded; however, you can create a properties file that substitutes information that is specific to your shipment for many of the properties file variables. This functionality eliminates the need to create a properties file for each label item. After the properties file is created using the substitution variables, you can use the same properties file for multiple labels. For a list of substitution variables, see "Substitution variables for template properties files" on page 361.

You can load all products from a particular purchase order or catalog, scan or enter Global Identifier (GID codes), or search the database by keyword. After you select the products, you can print the tag labels based on existing print templates created in WebSphere Premises Server Administrative Console.

The process for printing tag labels depends on whether your system is installed in an *integrated* or a *non-integrated* environment. In an integrated environment, the RFID network retrieves information from the back-end enterprise system, so that product and catalog information displays directly in the Print, Verify, and Ship Reference User Interface. In a non-integrated environment, the RFID network is not connected to the back-end enterprise system and, therefore, does not have access to product and catalog information. See "Printing RFID tag labels" on page 364 for more information.

- **Verify** - use the Verify panel to create associations in the database between cases and containers, either manually or automatically. After you select the items to associated with a container, save the association in the database for reference purposes. See "Associating labels with containers" on page 369 for more information.

  Note: This document uses the generic term *container* to include any kind of container that stores cases of items. For example, a *pallet* is one example of a container.
- **Ship** - use the Ship panel to match scanned items against the database for outgoing containers. See "Validating outgoing shipments" on page 373 for more information.
- **Report** - use the Report panel to run reports on items that have been printed and verified. See "Generating reports" on page 374 for more information.

See "Printing RFID tag labels" on page 364 to get started.

Opening the user interface

This topic describes how to open the Print, Verify, and Ship Reference User Interface.

About this task

If WebSphere Premises Server is installed on your local server, you can access the Print, Verify, and Ship Reference User Interface by selecting **Start** → **All Programs** → **IBM WebSphere Premises Server** → **Premises Server** *version* → **PVS Reference User Interface**.

If WebSphere Premises Server is on a remote server, follow these instructions.
1. Open a new Web browser.

   Note: Use Mozilla Firefox or Internet Explorer 6.0 or later to open the Print, Verify, and Ship Reference User Interface. Ensure that JavaScript is enabled.

2. Type `http://`*`premises_server_host_name`*`:9080/RFIDPrintWeb/` in the **Address** field of your Web browser.

Printing RFID tag labels

After you install the Print, Verify, and Ship Reference User Interface and configure your tag printer, you can begin printing tag labels.

The Print, Verify, and Ship application supports two kinds of environments for printing: integrated and nonintegrated.

Printing in an integrated environment

In an integrated environment, your backend enterprise database is connected to the Print, Verify, and Ship Reference User Interface to allow the purchase order and catalog information from your enterprise system to display in the application. Follow this process to print tag labels:

1. **Set up the print job** - in an integrated environment, select a purchase order and customer profile before selecting the products. See "Setting up the print job" on page 365 for more information.
2. **Select products** - select the products for which you want to print tag labels. There are three methods. See "Selecting products from a purchase order or catalog" on page 366, "Searching for products" on page 367, or "Scanning or entering GID codes" on page 367 for more information.
3. **Select a printer** - determine the tag printer to which you are sending the print job. See "Printing tag labels" on page 368 for more information.
4. **Print the tag labels** - when the correct information is loaded, click the **Submit** button from the Print Labels panel. See "Printing tag labels" on page 368 for more information.

Printing in a nonintegrated environment

In a nonintegrated environment, there is no backend database connected to the Print, Verify, and Ship Reference User Interface. In this scenario, only the non-item pack types section on the **Select** tab is applicable. The **Search** tab is disabled, but you can still enter case or container tags on the **Enter** tab. You must still select a customer profile and enter the purchase order on the **Setup** tab. You must also enter the shipping information.

For example, you might do the following:

1. **Set up the print job** - select a customer profile and enter a purchase order from the **Setup** tab. See "Setting up the print job" on page 365 for more information.
2. **Select products** - select a non-item pack type to print a container tag label for a heterogeneous container. See "Selecting products from a purchase order or catalog" on page 366 to select non-item pack types.
3. **Scan or enter products** - scan your product codes on the **Enter** tab using a reader or enter the GID codes manually to print a case or container tag label for those products. See "Scanning or entering GID codes" on page 367 for more information.
4. **Print the tag labels** - when the correct information is loaded, click the **Submit** button from the Print Labels panel. See "Printing tag labels" on page 368 for more information.

Note: In a non-integrated environment, make sure that the `enterprise.data.interface` attribute in the pvsapp.properties file is blank. The file is located in this directory:

> **Windows** *WAS_PROFILE_HOME*\installedApps*node_name*\ IBM_Premises_PVS_Console.ear\ibmrfid_premises_pvsapp.war\config

> **Linux** *WAS_PROFILE_HOME*/installedApps/*node_name*/ IBM_Premises_PVS_Console.ear/ibmrfid_premises_pvsapp.war/config

If you plan to verify items, you must print at least one case tag label and one container tag label, and this requirement can span multiple print jobs. For example, you might print all of your case tag labels for a particular shipment, and then print the container tag labels at a later time.

Setting up the print job:

Use the **Setup** tab to select or enter purchase orders and to determine a customer profile.

About this task

Before you begin printing tag labels in either an integrated or non-integrated environment, you must select a customer profile and purchase order for the print job.

Purchase orders contain the products that require RFID tag labels for shipping. They automatically display in the Print, Verify, and Ship Reference User Interface from your back-end enterprise database when working in an integrated environment.

The profile contains a list of associated pack types for a particular customer. Use the EPC Commissioning Configuration module in the WebSphere Premises Server Administrative Console to create profiles.

1. Log onto the Print, Verify, and Ship Reference User Interface by opening a Web browser and typing `http://premises_server_hostname:9080/RFIDPrintWeb/ RFIDPrintWeb` in the **Address** field. If WebSphere Premises Server is installed on your local machine and it is running on Windows, you can access the interface by selecting **Start** → **All Programs** → **IBM WebSphere Premises Server** → **Premises Server** *version* → **PVS Reference User Interface**.
2. Click **Print**, and then click the Setup tab. The Setup panel displays.
3. In the **Profile** field, select a profile to apply to this print job.

   Note: Do not select a profile for 64-bit tags. 64-bit tags are not supported in this release.
4. In the **Existing Purchase Order** field, select the purchase order that contains the items for which you are printing labels.

   Note: If you are using Print, Verify, and Ship in a non-integrated environment, you must manually enter the purchase order number and click **Set**. The purchase order number and any products you add for printing are saved in a record in the WebSphere Premises Server database. You can retrieve this information later for verification and shipping, if desired.
5. When finished, click the **Select** tab to select items from the purchase order or catalog, click the **Enter** tab to scan or enter product codes, or click the **Search** tab to search for products by keyword.

Selecting products:

After you set up your print job, you must select the products to be included in the shipments.

About this task

You can do this in one of three ways:
- Use the **Select** tab to choose products directly from the purchase order you selected, choose products from a product catalog, or choose a pack type without items. See "Selecting products from a purchase order or catalog."
- Use the **Search** tab to search the product database.
- Use the **Enter** tab to enter or scan a product's Global Identifier (GID) code.

Selecting products from a purchase order or catalog:

About this task

Use the **Select** tab in the Print, Verify, and Ship Reference User Interface to select products for shipping in one of three ways:
- In an integrated environment, choose products directly from the purchase order you selected in "Setting up the print job" on page 365.
- In an integrated environment, choose products from a catalog loaded from your back-end enterprise database.
- In both integrated and non-integrated environments, choose a pack type without items. For example, you might need to print a tag label for a heterogeneous container.

You can also search for a product name by keyword or enter a GID code for a specific product. See "Searching for products" on page 367 and "Scanning or entering GID codes" on page 367 for more information.

1. Click **Print**, and then click the **Select** tab. The Select panel displays.
2. To include items from a purchase order:
   a. Under **Select products from purchase order**, select the product from the **Item** field.
   b. Select a pack type from the drop list.
   c. Click **Add**.

      Note: Click **Add all items** to print tag labels for all products on the purchase order.
   d. Repeat this process until you have included all of the required items. The items display in the *Review selections* panel at the bottom of the window.
3. To include items from a catalog:
   a. Select a catalog from the **Catalog** field and click **Load**. A list of items available in that catalog displays in the **Item** field.
   b. Select a product from the **Item** field.
   c. Select a pack type from the drop-down list.
   d. Click **Add**.
   e. Repeat this process until you have included all of the required items. The items display in the Review selections panel at the bottom of the window.

4. To include a pack type without items, select a pack type from the **Pack type** field and click **Add**. The item displays in the Review selections panel at the bottom of the window.

5. Verify that the details in the Review selections panel are accurate and change the quantity or label, if necessary.

   Note: The label is the print template applied to the print job. All print templates that were created in the WebSphere Premises Server Administrative Console display in this field. See "Creating print templates" on page 359 for more information.

6. When you finish making the changes, click **Update** or click **Reset** to start over from the beginning.

Searching for products:

If you do not have specific information about a product, such as a purchase order number or GID code, and you are using Print, Verify, and Ship in an integrated environment, you can search the database by product keyword.

About this task

Use the **Search** tab to do a keyword search for products, as described below. To search by GID codes, see "Scanning or entering GID codes." To select products from an existing purchase order or catalog, see "Selecting products from a purchase order or catalog" on page 366.

1. Click **Print**, and then click the **Search** tab. The Search panel displays.

2. Type your search criteria in the **Description keyword** field and click **Search**.

   Note: You can enter either an entire word or phrase, or partial words or phrases. For example, searching on **c** might yield the following results: *CD Player* and *Projection TV*, while searching on **cd** would yield only *CD Player*.

   You can also enter the wildcard characters, "_" (to match any one character) and "%" (to match zero or more characters).
   The search results display in the **Print labels for** field.

3. From the **Print labels for** drop-down list, select the product for which you want to print tag labels

4. Select a pack type.

5. Click **Add**. The selected item displays in the Review selections panel.

6. Search for and select any additional products, as necessary.

7. Verify that the details in the Review selections panel are accurate and change the quantity or label, if necessary.

8. Click **Update** when you finish making changes, or click **Reset** to start over from the beginning.

Scanning or entering GID codes:

Before printing tag labels for containers and cases, you must select the products that need labels.

About this task

Use the **Enter** tab on the Print, Verify, and Ship Reference User Interface to select products by Global Identifier (GID code), either by scanning the code with an attached hand-held reader or by manually entering the code into the application. Use this feature in both integrated and non-integrated Print, Verify, and Ship environments.

1. Click the **Enter** tab from the Print, Verify, and Ship Reference User Interface. The Scan or Enter Products panel displays.
2. Enter the GID code:

   Note: GID codes in the Print, Verify, and Ship Reference User Interface must contain English alphanumeric characters only.

   a. To manually enter the code, type the code in the **GID** field. You can enter multiple values in this field, separated by semi-colons, but you must configure your barcode scanner for semi-colons. Click **Enter** when ready. The product displays in the list below. If the product does not exist in the database and you are in a non-integrated environment, the Scan or Enter Products panel displays prompting you to complete the fields.

   b. To scan the code, scan one or more products with a tag reader. When you finish scanning, click **Enter**. The products display in the list below.
3. If the product does not exist in the database and you are in a non-integrated environment, the Scan or Enter Products panel displays with the products. Complete all the fields on this panel. Then go to step 5.
4. From the drop-down list, select the pack type for each product.
5. When you finish, click **Add**. The selected items display on the **Review selections** panel.
6. On the **Review selections** panel, verify the accuracy of the details and change the quantity or label, if necessary.
7. Click **Update** when finished making changes, or click **Reset** to start over from the beginning.

Printing tag labels:

After you select the products for shipment, you can print the RFID tag labels for these products.

About this task

Use the **Print** tab to send the print job to the appropriate tag printer. Remember that you must have already selected a purchase order and profile to successfully print tag labels. See "Setting up the print job" on page 365 for more information.

1. Click **Print**, and then click the **Print** tab. The Print panel displays.
2. In the **Printer** field, select the tag printer to which you are sending the print job.

   Note: If you changed the printer when you set up the print job, you might also need to change it here.
3. In the **Description** field, type a brief description of this print job.
4. Ensure that the customer profile and purchase order information is correct, and make any necessary changes. See "Setting up the print job" on page 365 for more information.

5. Verify that the details in the Review selections panel are accurate and change the quantity or label, if necessary.

   Note: The Print, Verify, and Ship Reference User Interface lists all labels, or print templates, created in the WebSphere Premises Server Administrative Console. Labels that are incompatible with the selected printer are not excluded; therefore, make sure that you select the appropriate label before continuing.

6. Click **Update** when finished making changes, or click **Reset** to start over from the beginning.
7. After reviewing the print job, click **Submit**. The job is sent to the printer.

What to do next

To check the status of an existing print job, select the job from the **Print job** field and click **Status**. The status displays directly below the **Print job** field.

Reprinting tag labels:

If a tag label is damaged, you can reprint that label by entering its serial number.

About this task

Use the **Reprint** tab in the Print, Verify, and Ship Reference User Interface to enter the EPCglobal Tag URI and code of the tag label that you want to reprint. You can reprint a tag only if no items are selected for printing.

1. Click **Print**, and then click the **Reprint** tab. The Reprint panel displays.
2. From the EPCglobal Tag URI field drop-down list, select the encoding type that is associated with the tag label that you want to reprint; then type the code. You can find this information on the damaged tag.

   Note: The format of the serialized GID depends on the encoding type that you select. For example, encoding type `sgtin96` requires four entry fields: an indicator digit, the manufacturer ID or company prefix, the item reference or object class, and the item serial number.

3. Click **Search** to validate the selected type and number. If the data that you entered is not found, an error message displays. If the system validates the information, the selected items display in the Review selections panel.
4. Enter additional items, as necessary.
5. Verify that the details in the Review selections panel are accurate.
6. Click **Update** or click **Reset** to start over from the beginning.
7. When you are ready to print, go to the Print panel and submit the print job. See "Printing tag labels" on page 368 for more information.

Associating labels with containers

After you print the tag labels, use the Verify function in the Print, Verify, and Ship Reference User Interface to associate existing labels with containers so that the items being shipped can be accurately tracked. To verify, you must have printed at least one label tag and one container tag for the shipment.

There are two ways to associate labels with containers: *manual* and *automatic*.
- Use the manual method to load items from a purchase order and associate them with a container on the Verify panel.

- Use the automatic method to scan the label tags into the application. After the tags are scanned, they display on the Verify panel where you associate them with a container.

Note: DOD tags (CAGE and DoDAAC) cannot be verified because they are not associated with products.

When you save the association, a Verification Report displays the status of the associated labels. After you accept the verification report in an integrated environment, the purchase order status in the Enterprise system changes to *partially filled* until the entire purchase order is associated and verified.

See "Manually associating labels with containers" or "Automatically associating labels with containers" on page 371 for more information.

Manually associating labels with containers:

There are two ways to associate labels with containers in the Print, Verify, and Ship Reference User Interface: manual and automatic. This section contains the instructions for manually making these associations.

About this task

Use the Manual tab on the Verify panel to associate labels with containers when you do not have a reader to automatically scan tag values.

Note: You can also use the Manual Verify function to disassociate an item from a pallet. For example, if you mistakenly associate the wrong items with a container using the Auto Verify function, you can go to the Manual tab, select the appropriate purchase order and container, and remove those items.

The manual association process involves selecting the items from a purchase order, and then associating the items with a container. After the labels are associated with containers, you can validate the containers against the database records for outgoing shipments. To verify, you must have printed at least one case tag label and one container tag label.

Note: DOD tags (CAGE and DoDAAC) cannot be verified because they are not associated with products.

1. Open the Verify panel in the Print, Verify, and Ship Reference User Interface.
2. Click the **Manual** tab. The Manual panel displays.
3. Select the profile from the **Profile** field.
4. In an integrated environment, select a purchase order from the **Purchase Order** field and click **Select**. In a non-integrated environment, manually enter the purchase order number and click **Load**. The **Shipping container** field displays a list of containers for which you have already printed tag labels. The **Unassociated labels** column displays a list of all items from the purchase order that are currently not associated with a container; these items may include labels and other containers.
5. From the **Shipping container** field, select the container with which you want to associate the labels and click **Load**. A list of the labels that are currently associated with the selected container display in the **Labels associated with container** column.

Note: In the **Unassociated labels** column, you can also select an item with children in its pack type containment hierarchy and click **Make container**. The selected item then displays in the **Shipping container** field, and now you can associate additional labels with this new container.

6. From the **Unassociated labels** column, select the items that you want to associate with this container and click **->**. The selected items display in the **Labels associated with container** column.

   Note: To remove an item from the **Labels associated with container** column, click **<-**.

7. When you are finished, click **Save container**. In an integrated environment, the association is saved to the Premises server database and the Verification Report is updated to reflect the status of the items on the purchase order. In a non-integrated environment, the association is saved to the Premises server database, but no Verification Report displays.

8. In an integrated environment, click **Accept** when you are satisfied with the results on the Verification Report. The symbols that display in the **Status** column are:

   - ? - indicates that these items are not yet loaded.
   - < - indicates that there are fewer items loaded onto the shipping container than there were on the purchase order.
   - > - indicates that there are more items loaded onto the shipping container than there were on the purchase order.
   - check mark - indicates that there are the same number of items on the purchase order as there were on the shipping container.

   The purchase order status in the enterprise system changes to *partially filled* until all items are associated.

Automatically associating labels with containers:

After you print the tag labels, use the second function, *Verify*, in the Print, Verify, and Ship Reference User Interface to associate the labels with containers.

Use the Automatic tab on the Verify panel to scan your tags with a reader, rather than manually enter them into the application. If the tags are expected -- that is, printed using the specified purchase order -- *and* at least one expected container tag has been read, these tags are automatically associated when you click **Save Associations**.

These associations are saved to your back-end enterprise system in an integrated environment or to the WebSphere Premises Server database in a non-integrated environment so that outgoing shipments can be validated against the database.

Note: DOD tags (CAGE and DoDAAC) cannot be verified because they are not associated with products.

Prerequisites

Before beginning this process, be sure that you have printed at least one case tag label and one container tag label.

Automatically associating cases with containers:

1. Open the Verify panel in the Print, Verify, and Ship Reference User Interface.

2. Click the **Automatic** tab. The Automatic panel displays.
3. From the **Profile** field, select a profile.
4. In an integrated environment, select the purchase order that contains the items that you want to verify from the **Purchase Order** field and click **Select**. In a non-integrated environment, manually enter the purchase order number. The available readers defined in the WebSphere Premises Server Administrative Console display in the **Reader ID** field.
5. From the **Reader ID** field, select the reader to use for scanning the tag values.

   The following icons represent the status of the reader:

   - - The reader is off, but available.

   - - The reader status is unavailable.

   - - The reader is on and ready to read tags.

   Note: The ″ready″ icon means that the reader is ready to read tags, but it does not necessarily mean that it is reading tags currently. If the portal state is already on, the status may show as reading, but you still need to click the **Start** button to start reading tags in the console.
6. Click **Start** to turn on the motion sensor and begin reading tags. The reader turns on when the motion sensor detects movement.
7. Scan the tags, ensuring that you scan only one container tag. If you scan more than one, you cannot make the association because the system always uses the label that was read last. Labels that follow the pack type containment hierarchy appear in the Expected labels column.

   Note: Labels that do not follow the pack type containment hierarchy appear in the Unexpected labels column. However, note that overages and underages do not display in that column. In an integrated environment, they display in the Status column of the Verification Report; in a non-integrated environment, they do not display.
8. When the reader finishes reading the tags, click **Stop** to turn off the motion sensor.
9. Click **Save Associations** to associate the case tag labels with the container tag label. In an integrated environment, the association is saved to the Premises server database and the Verification Report is updated to reflect the status of the items on the purchase order. In a non-integrated environment, the association is saved to the Premises server database, but no Verification Report displays.
10. In an integrated environment, click **Accept** when you are satisfied with the results on the Verification Report. The symbols that display in the **Status** column are:
    - ? - indicates that these items are not yet loaded.
    - < - indicates that there are fewer items loaded onto the shipping container than there were on the purchase order.
    - > - indicates that there are more items loaded onto the shipping container than there were on the purchase order.

- check mark - indicates that there are the same number of items on the purchase order as on the shipping container.

  The purchase order status in the enterprise system changes to *partially filled* until all items are associated.
11. Click **Reset** to clear the existing screen and re-scan your tag labels.

Validating outgoing shipments

After you print tag labels and associate cases with containers, you can validate that the outgoing containers are associated with the correct purchase order.

When the outgoing shipments are ready to exit the dock door, use the **Ship** feature in the Print, Verify, and Ship Reference User Interface to check the tag labels on the containers against the data that you registered in the WebSphere Premises Server database during the **Verify** phase. When the containers are scanned, the system attempts to match the container tag with a purchase order in the database. If the scanned tag matches the association with the purchase order in the database, a green light displays on the light tree and the shipment can proceed. If the scanned container tag does not match the purchase order, a red light displays on the light tree.

Prerequisites

Before beginning this process, ensure that you have completed the following prerequisites:
1. You must have printed at least one case tag label and one container tag label, and made an association using the Verify function.
2. You must have disabled the CaseFilter property from the WebSphere Premises Server Administrative Console. If filtering is set, there are two places where you must turn off filtering: *externally* as described directly below in steps 2a through 2g and *internally* (inside the reader agent) as described below step 2g.
   a. Log on to the WebSphere Premises Server Administrative Console.
   b. Depending on the version of the Data Capture and Delivery that you are running, navigate to **Data Capture Configuration** → **Agent Configuration** from the left pane.
   c. Select **FilterAgent** from the **Reader Agent** field.
   d. Select **Filters** from the **Agent Properties** field.
   e. Change the **Property Value** field to display only **Duplicates**.
   f. Click **Update**. The changes are saved.
   g. Restart theData Capture and Delivery environment using the /dts/dts.bat or /dts/dts.sh command.

   To turn off filtering and aggregation inside the reader, clear the following fields:
   - RfidInventory/AggregationMaskSetting value=""
   - RfidInventory/DuplicateFilteringExpression" value=""
   - RfidInventory/TagAggregatingExpression" value=""
   - RfidInventory/TagMaskSetting" value=""

Validating outgoing shipments:
1. Open the Ship panel in the Print, Verify, and Ship Reference User Interface.
2. In an integrated environment, select a purchase order from the **Purchase Order** field and click **Select**. In a non-integrated environment, manually enter the

purchase order number. The available readers defined in the WebSphere Premises Server Administrative Console display in the **Reader ID** field.

3. Select the reader to use for scanning the RFID tags from the **Reader ID** field.

   Note: If you create a new reader in the WebSphere Premises Server Administrative Console and want to use that reader for automatic verification, you must either restart WebSphere Application Server or restart the Common Services application in the WebSphere Application Server administrative console before continuing.

   The following icons represent the status of the reader:

   - - The reader is off, but available.

   - - The reader status is unavailable.

   - - The reader is on and ready to read tags.

   Note: The "ready" icon means that the reader is ready to read tags, but it does not necessarily mean that it is reading tags currently. If the portal state is already on, the status may show as reading, but you still need to click the **Start** button to start reading tags in the console.

4. Click **Start** to turn on your motion sensor and begin reading tags. As the container moves through the dock door, the motion detector senses movement, the reader begins reading, and the scanned items display in the Expected tags column.

   Note: If you scan a container tag that is not associated with the purchase order, then an exception displays in the Unexpected tags column and the red light on the light tree displays.

5. Click **Stop** when finished reading tags to turn off your motion sensor. The green light on the light tree displays after each successful container scan, and the database is updated to reflect the shipment. In an integrated environment, the purchase order status is changed to *Shipped* after the containers are scanned.

Generating reports

The reporting feature in the Print, Verify, and Ship Reference User Interface enables you to run reports on items that have been printed and verified.

About this task

Generating a report in the Print, Verify, and Ship Reference User Interface involves two steps:

1. Selecting the items that you want to display on the report, based on a verify date and, optionally, a ship date.
2. Determining the format of the report.

The default report type installed with Print, Verify, and Ship is .csv.

After you generate the report, the selected report displays in a new window on your computer and a copy of the report is saved to the directory that was set up

when you installed Print, Verify, and Ship. You set the directory using the *report.location.csv* attribute in the pvsapp.properties file, which is located in the directory:

> **Windows** *WAS_PROFILE_HOME*\installedApps*node_name*\
> IBM_Premises_PVS_Console.ear\ibmrfid_premises_pvsapp.war\config

> **Linux** *WAS_PROFILE_HOME*/installedApps/*node_name*/
> IBM_Premises_PVS_Console.ear/ibmrfid_premises_pvsapp.war/config

1. Open the Report function in the Print, Verify, and Ship Reference User Interface.
2. In the **Purchase Order** field, select the purchase order that contains the items on which you want to report.
3. In the **Verification Date** field, enter the date the items were verified using the mm/dd/yyyy format, or click on the calendar to select a date.
4. Optionally, in the **Customer** field, enter the customer number to use as search criteria.
5. Click **Load**. The items matching the selected criteria display in the Review report panel.
6. From the **Report File Type** field, select the file format in which you want the report to display.
7. Click **Generate Report File**. The report displays, and a copy is saved to the report location specified in the pvsapp.properties file.

EPCIS Connector sample application

Use this application to persist events to an Electronic Product Code Information System (EPCIS).

EPCIS is a standard for storing and sharing RFID data. It is based on a standard maintained by the EPC Global organization. The EPCIS standard includes schemas for XML messages to deliver and query for RFID data. IBM has implemented the EPCIS standard in a product named WebSphere RFID Information Center.

One industry that has taken advantage of the EPCIS standard is pharmaceuticals. EPCIS is used to persist each read of a particular tagged pharmaceutical. The tag read histories can then be queried and used to build a document, called a pedigree, for the tagged item. The pedigree is used to verify the integrity of the pharmaceutical and prevent counterfeiting. The use of EPCIS is not limited to the pharmaceutical space; however, and is applicable to any RFID solution that uses persisted data, such as track and trace or asset monitoring.

For details on how to use the sample application, refer to WebSphere Premises Server Toolkit documentation that is installed with the toolkit.

Reusable Event Monitor component and sample user interface

The Reusable Event Monitor component enables WebSphere Premises Server applications to include dynamic event information.

The Reusable Event Monitor provides the following functions:

SIBus event message caching
> The event monitor component caches SIBus messages to a JMS queue on the SIBus. Each event placed into the queue is given a time to live (TTL). When the TTL expires, the event is automatically deleted from the queue.

The SystemAgent property, `com.ibm.premises.eventmonitor.TTL`, can be set to override the default TTL value of 600000 milliseconds (which is 10 minutes).

Message retrieval

A session EJB provides access to the cached messages, which are returned in descending event header dateTime order. The format of the returned events is JavaScript Object Notification (JSON) text.

Filtered message retrieval

Client code can also provide a message selector to filter which messages are retrieved by the session EJB. If a message selector is given, only those messages where the message selector evaluates to true are retrieved. For example, to retrieve all alert events use a message selector of: `ibmse like 'dccontroller/report/diagnostic/alert/%'`. If no message selector is given, all messages are received. See the WebSphere Premises Server gateway documentation for a list of properties available in the message selector.

JavaScript libraries

JavaScript libraries provide the underlying AJAX request and JSON event processing functions.

Sample user interface

The sample event monitor user interface illustrates how you can build a dynamic user interface using the deployed event monitor EAR and the JavaScript libraries. For details on how to create your own user interface, refer to the WebSphere Premises Server Toolkit documentation that is installed with the toolkit.

Using the sample Reusable Event Monitor user interface

This topic provides information on running the sample user interface from a browser.

Running the sample user interface

To run the sample user interface, enter the following URL into a Web browser:
http://*servername*:9080/ibmseeventmonitor/index.jsp

The browser view displays all events currently in the queue, refreshing automatically every 1000 milliseconds.

Changing the message selector

To change the message selector, enter a new value in the **Message Selector** field and click **Update**. If a syntax error occurs in the message selector, a message displays and the user interface does not refresh. To fix the error, type in a new message selector and click **Update**. The user interface will refresh automatically once the error is fixed.

Chapter 9. Troubleshooting and support

To help you understand, isolate, and resolve problems with your IBM software, the troubleshooting and support information contains instructions for using the problem-determination resources that are provided with your IBM products.

To resolve a problem on your own, you can find out how to identify the source of a problem, how to gather diagnostic information, where to get fixes, and which knowledge bases to search. If you need to contact IBM Support, you can find out what diagnostic information the service technicians need to help you address a problem.

Troubleshooting a problem

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and explain 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 Support person 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, and that is the best way to start down the path of 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 might seem like a straightforward question; 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?
* What is the business impact of the problem?

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?

Remember that 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 do this 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; however, this is not always easy to do and takes practice. Knowing when to stop looking is especially difficult when multiple layers of technology are involved, and when each has its own diagnostic information.

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 questions like this helps to provide you with 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, problems that can be reproduced 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 recreated on a test system?
- Are multiple users or applications encountering the same type of problem?
- Can the problem be recreated by running a single command, a set of commands, or a particular application, or a stand-alone application?

Gathering information

Record the following values and have them available for reference when troubleshooting a problem.

__ • WebSphere Premises Server version. See "Checking the server version" on page 99 for details on how to do this.

__ • Location of the WebSphere Premises Server installation directory

__ • Location of the WebSphere Application Server installation directory

__ • Location of the log files.

__ • WebSphere Premises Server name and port number

__ • Configuration of the Data Capture and Delivery controller. See "Verifying that the WebSphere Premises Server is generating correct XML" on page 396 for how to get this information.

Searching knowledge bases

You can often find solutions to problems by searching IBM knowledge bases. Learn how to optimize your results by using available resources, support tools, and search methods and how to receive automatic updates.

Available technical resources

In addition to this information center, the following technical resources are available to help you answer questions and resolve problems:

- WebSphere Premises Server version 6.1.x technotes and APARs (problem reports)
- WebSphere Premises Server all versions technotes and APARs
- WebSphere Premises Server Support Web site
- WebSphere Redbooks® Domain
- You can find a complete list of online references relevant to the product and its components in "Additional information" on page 413.

Searching with support tools

The following tools are available to help you search IBM knowledge bases:

- **IBM Support Assistant (ISA)** is a free software serviceability workbench that helps you resolve questions and problems with IBM software products. Instructions for downloading and installing the ISA can be found on the ISA Web site: www.ibm.com/software/support/isa/
- **IBM Software Support Toolbar** is a browser plug-in that provides you with a mechanism to easily search IBM support sites. You can download the toolbar at: www.ibm.com/software/support/toolbar/.

Search tips

The following resources describe how to optimize your search results:
- Searching the IBM Support Web site
- Using the Google search engine

Receiving automatic updates

You can receive automatic updates in the following ways:
- **My support**. To receive weekly e-mail notifications regarding fixes and other support news, follow these steps:
  1. Go to the IBM Software Support Web site at www.ibm.com/software/support/.
  2. Click **My support** in the upper-right corner of the page under **Personalized support**.
  3. If you have already registered for My support, sign in and skip to the next step. If you have not registered, click **Register now**. Complete the registration form using your e-mail address as your IBM ID and click **Submit**.
  4. Click **Edit profile**.
  5. Click **Add products** and choose a product category; for example, **Software**. A second list is displayed.
  6. In the second list, select a product segment; for example, **Data & Information Management**. A third list is displayed.
  7. In the third list, select a product subsegment, for example, **Databases**. A list of applicable products is displayed.
  8. Select the products for which you want to receive updates.
  9. Click **Add products**.
  10. After selecting all products that are of interest to you, click **Subscribe to email** on the **Edit profile** tab.
  11. Select **Please send these documents by weekly email**.
  12. Update your e-mail address as needed.
  13. In the **Documents list**, select the product category; for example, **Software**.
  14. Select the types of documents for which you want to receive information.
  15. Click **Update**.
- **RSS feeds**. For information about RSS, including steps for getting started and a list of RSS-enabled IBM Web pages, visit www.ibm.com/software/support/rss/

Using IBM Support Assistant

IBM Support Assistant (ISA) is part of the WebSphere Premises Server installation package. ISA enables you to search the product documentation, create product management reports (PMRs), and package log files.

Specifically, ISA collects logs for WebSphere Premises Server, WebSphere Application Server, WebSphere MQ, and your DB2 for Linux, UNIX, and Windows systems or Oracle server.

ISA is a standalone application that you can install on any workstation, and then enhance it by installing plug-in modules for the IBM products you use. For more information about ISA and its features, refer to the ISA Support page.

Installing IBM Support Assistant

WebSphere Premises Server supports version 3.0.2 and later versions of IBM Support Assistant (ISA). You can install more than one version of ISA on the same system.

About this task

ISA can be installed locally with WebSphere Premises Server and WebSphere Application Server, or you can install it on a remote system.

1. Install WebSphere Premises Server.

2. Install ISA.

3. Locate the ISA plug-in files:

   > **Windows** *IBM_RFID_HOME*\premises\isa\plugin\
   com.ibm.esupport.client.product.SSAN9K61

   > **Linux** *IBM_RFID_HOME*/premises/isa/plugin/
   com.ibm.esupport.client.product.SSAN9K61

4. Use the ISA updater to install the WebSphere Premises Server plug-in. Alternatively, you can download and install the WebSphere Premises Server plug-in, and any additional product plug-ins, from the list of supported ISA plug-ins.

5. Use the links on the ISA Support page for detailed instructions on using ISA.

Gathering data with the Data Capture and Delivery debug export utility

The debug export utility allows you to gather and analyze data used in the Data Capture and Delivery component of WebSphere Premises Server.

The debug export utility gathers data by using exports that collect specific data. The following table includes a description of the data that is gathered:

Table 74. Data gathered by debug export utility

Data	Description
OSGi short status (ss)	The contents of the OSGi `ss` command are displayed.
OSGi status	The contents of the OSGi `status` command are displayed.
System properties	A list of system properties is displayed in alphabetical order. This list can help you find specific properties more quickly.
VM information	Various data can be gathered from the VM such as free memory and maximum memory.
config.ini	The contents of the config.ini file are displayed from the location given by the `osgi.configuration.area` system property plus /config.ini.
EdgeXML	The contents of the Data Capture and Delivery XML file are displayed from the URL given by the `com.ibm.rfid.edge.config.url` system property.

Table 74. Data gathered by debug export utility (continued)

Data	Description
| OSGi ConfigAdmin | The contents of the OSGi `ConfigurationAdmin` (ConfigAdmin) data structure are displayed in the following format for each configuration:<br><br>```
PID:
Factory PID:
Bundle Location:
Properties:
    [property...0]
        .
        .
        .
    [property...n]
``` |
| matrix properties file | The contents of the matrix file are displayed from the location given by the `matrix.properties` property in the Portal Controller Configuration in `ConfigurationAdmin`. |
| Data Capture and Delivery log entries | The previous n log entries made will display with n being the current value of the `LogService` `log.size` property. The most recent entry is at the bottom. |

The utility ships as a set of bundles that allows you to view the data through a servlet (`com.ibm.rfid.support.debug.servlet`), in a file (`com.ibm.rfid.support.debug.file`), or through a socket (`com.ibm.rfid.support.debug.socket`). The bundles are installed with the IBM Data Capture and Delivery Toolkit for WebSphere Premises Server and are also installed in the Data Capture and Delivery bundles directory on WebSphere Premises Server. In the toolkit, the bundles will be loaded and started as part of the launch configurations. In the bundle lists on WebSphere Premises Server, the file and server socket export bundles will be loaded and started by default. The servlet view bundle is installed and started automatically with Data Capture and Delivery. Regardless of which view is being used, the `com.ibm.rfid.support.debug.model` bundle must always be installed since the other bundles depend on it.

Viewing data through a servlet

You can view data through a servlet. The servlet presents the data in an organized way that can be easily viewed in a Web browser. Each export of specific data has its own section in the servlet that can be expanded or collapsed to easily view the data. Exports that encounter an error will identify where the error occurred with an icon next to the title of the section. Each time the Web browser is refreshed the most current debug data will be displayed.

The servlet view bundle is installed and started automatically with Data Capture and Delivery.

To use the servlet export functionality, access the following URL in a Web browser: `http://ip_address:8777/datacapture/debug`

You can also access the servlet by accessing the following URL and then clicking **debug**: `http://ip_address:8777/device`

Note: In a production environment, Data Capture and Delivery servlets are available on port 8777, to avoid conflict with the WebSphere Application Server servlet engine. In the IBM Data Capture and Delivery Toolkit for

WebSphere Premises Server environment (for example, using the launch configurations), these servlets default to port 80, the standard HTTP server port.

Viewing data in a file

You can view data in a file. Debug data is gathered and exported to a time-stamped text file in the directory specified by the `com.ibm.rfid.support.debug.file.path` property, which defaults to the path specified by the `osgi.install.area` system property. The format of the file name is DataCaptureDebugLogs_*yyyy-mm-dd_hh-mm-ss-xxx*, where the timestamp consists of year, month, day, hour, minute, second, and milliseconds. The text file is organized with a section at the top that displays the names of the exports that encountered errors. The rest of the text file consists of clearly labeled sections that contain data from the various exports.

The file view bundle is installed with Data Capture and Delivery, but is not started by default. Once you start the bundle, it gathers the data, exports it to the file, and then stops itself. Permissions must be set to allow the bundle to write to the hard drive.

To use the file export functionality, start the bundle. Then view the *debug_file_path*/DataCaptureDebugLogs_*yyyy-mm-dd_hh-mm-ss-xxx* file.

Viewing data through a server socket

If you cannot run a full JRE (allowing use of the servlet) or cannot write to the hard drive, you can export the data through a server socket and then decide what to do with the data.

The socket view bundle is installed with Data Capture and Delivery, and it is started by default. Once you start the bundle, it opens a server socket using the default port number 12345; however, this port number is configurable.

The port number is configurable through the `com.ibm.rfid.support.debug.socket.port` system property which defaults to 12345 at start. To change this port number, stop the bundle, update the property to the new port number, and restart the bundle. The socket will now use the new port number assigned to the `com.ibm.rfid.support.debug.socket.port` property.

The bundle waits until a client connects to it through the port and then gathers the debug data and exports it through the client-server connection. The data is transferred in the same format as that sent to the file. You can choose where to have the data sent. After the data is transferred, the client-server connection is closed and the server socket waits until another connection is made. The bundle remains active until you stop it.

To use the socket export functionality, start the bundle if it is not already started. Then connect to it through a client (for example, using Telnet) and export the data to the location of your choice.

Monitoring messages using the Edge Event Monitor tool

You can monitor messages on Data Capture and Delivery devices using the Edge Event Monitor tool.

The Edge Event Monitor is a standalone Java tool that runs on the same server as the WebSphere Premises Server and connects to the MicroBroker on the edge controller as a MicroBroker client.

The Edge Event Monitor tool is located in the tools directory on the CD that contains the IBM Data Capture and Delivery Toolkit for WebSphere Premises Server. For more information on how to use the Edge Event Monitor, refer to the PDF document, edge_event_monitor.pdf, in the compressed EdgeEventMonitor.zip file.

Logging, tracing, and error messages

If you are experiencing a problem, check the error messages and log information.

There are various levels of logging available in WebSphere Premises Server and its components. You can set logging on tracing on WebSphere Application Server for WebSphere Premises Server. You can also set logging at a system level for Data Capture and Delivery, or you can set it at an agent level.

For information on the general concepts of logging and tracing, refer to Log and trace settings in the WebSphere Application Server Information Center.

Use these topics to help you with these tasks:

What is QoS?

QoS stands for Quality of Service. It consists of several parameters that control message communication behavior between the Data Capture and Delivery controller and WebSphere Premises Server.

QoS for messages from the Data Capture and Delivery controller

The default configuration for the Data Capture and Delivery controller is QoS level: **QOS 1** and QoS persistence: **memory only**. This means that messages, including tag reads, are assured to flow from the Data Capture and Delivery controller to WebSphere Premises Server, except when the Data Capture and Delivery controller has been turned off, the Data Transformation has been stopped during network outages, or WebSphere Premises Server is down.

Reasons for these default settings:
- The tags must be delivered to the WebSphere Premises Server, regardless of the condition of the network. If the network is down, the delivery of tags must be retried until they can be delivered.
- Memory-only persistence was used because space is minimal on the Data Capture and Delivery controller.
- Storing tags in a file or database might fill up the device file system and cause operating system problems.

Tag reads eventually flow to the back end, as long as the Data Capture and Delivery controller is not rebooted or restarted, regardless of network communications between the Data Capture and Delivery controller and WebSphere Premises Server. Tags cannot be read or queued at all when the network between the tag reader and the Data Capture and Delivery controller is down because there is no quality of service supported by the tag reader protocols.

QoS levels

At the Data Capture and Delivery controller, there are three QoS levels at which messages can be configured to be delivered from the Data Capture and Delivery controller to WebSphere Premises Server:

QOS 0
> Messages are delivered at most once. If there is a disruption in the network or on the Data Capture and Delivery controller software, the message may not be delivered.

QOS 1
> Messages are delivered at least once. It is possible that a message could be delivered more than once, but they are always delivered at least once.

QOS 2
> Messages are delivered once and only once.

QoS persistence

Persistence is configured through the `persistence` property key in the "MicroBroker agent" on page 134. The values for the `persistence` property align with the QoS levels 0, 1, and 2.

There are two ways to configure persistence on the Data Capture and Delivery controller:

Memory only
> Messages are stored in memory until they can be delivered at the above quality of service.

File Persistence
> Messages are persisted in a file until they can be delivered at the above quality of service. The file is saved only when there is a clean "shutdown" of the Data Transformation service.

Setting the QoS level

The configurations for each individual agent are set in the Data Capture and Delivery configuration XML file, which is generated from the agent settings in the WebSphere Premises Server database. Use the WebSphere Premises Server Administrative Console to modify the QoS values. The `qos` value defines what QoS level a particular agent will use for publication. For example:

```
<property key="qos" value="1" required="false" default="1" name="QoS"
description="Messaging Quality of Service: 0-at most once, 1-at least once,
2-exactly once."/>
```

In addition, a `qos.cutoff` value can be set that is specific to the Alert agent. This value sets the lowest alert level that will be published for QoS. Any level that is below the value specified for `qos.cutoff` publishes at `qos=0`. For example:

```
<property key="qos.cutoff" value="warning" default="warning" name="QoS Threshold Cutoff"
description="Lowest threshold level before assuming QoS=0. Threshold levels that are equal
to or higher than this value will be published at the agent-defined QOS level."/>
```

Since the value is set to `warning`, all alerts of level warning and above (for example, warning and error alerts) will be published at the QoS level defined for the alert agent. Levels below `warning` (for example, info and debug alerts) will be published at the `qos=0` level.

What are heartbeats?

A heartbeat is a signal (like a ping) that one component sends to another at a regular interval, so that the other component knows that the sender of the signal is still out there.

If the entity listening for the heartbeat does not hear it within a set amount of time, it knows that the sender of the signal might be in trouble.

In the RFID system, the Data Capture and Delivery controller has a heartbeat to the reader to make sure that the reader is still there. The controller also heartbeats back to the WebSphere Premises Server. If WebSphere Premises Server does not hear the heartbeat from the Data Capture and Delivery controller within the timeout period, it assumes that the controller is down or disconnected.

The heartbeat from the Data Capture and Delivery controller to the WebSphere Premises Server contains the current status of the heartbeats from the controller to the tag reader. The WebSphere Premises Server can tell from the Data Capture and Delivery controller heartbeat if the tag readers are down.

Log file locations and settings

This topic lists the locations and settings of the log files for the product.

Installation log files for WebSphere Premises Server

File name	Default location
install.log	**Windows** *IBM_RFID_HOME*\logs **Linux** *IBM_RFID_HOME*/logs

Note: *IBM_RFID_HOME* is an environment variable created when you installed WebSphere Premises Server. If you modified the installation directory for WebSphere Premises Server, be sure to use the modified installation path.

Alert error log for the edge controller

File name	Default location
edge-alerts.*x*.log, where *x* is an integer	**Windows** *IBM_RFID_HOME*\logs **Linux** *IBM_RFID_HOME*/logs
edge-alerts-.*x*.log, where *x* is an integer	

Format of the log:
- TimeStamp - Time error issued from an edge controller
- Alerttype - Information, warning, error, or debug
- Edge ID - Logical ID of the edge device
- Message - Java exception or a message in this format:

  ```
  Reader readerid  is ON/OFF
  ```

Heartbeat log for the edge controller

File name	Default location
edge-heartbeats.*x*.log, where *x* is an integer	**Windows** *IBM_RFID_HOME*\logs **Linux** *IBM_RFID_HOME*/logs

Format of the log:
- TimeStamp - Heartbeat time
- Location ID - Location ID (currently the portal ID of the tag reader)
- EdgeID - Logical ID of the edge device reporting the heartbeat
- ReaderID - Logical tag reader ID
- Message - Heartbeat messages in this format:
    ```
    edgeid=UP/DOWN
    readerid=UP/DOWN
    ```

WebSphere Application Server and WebSphere Premises Server log files

The WebSphere Application Server log files also contain information for WebSphere Premises Server.

File name	Default location
SystemOut.log SystemErr.log trace.log	**Windows** *WAS_PROFILE_HOME*\logs\server1 **Linux** *WAS_PROFILE_HOME*/logs/server1

Note: The default installation directories for WebSphere Application Server are:

> **Windows** C:\Program Files\IBM\WebSphere\AppServer
>
> **Linux** /opt/IBM/WebSphere/AppServer

If you modified the installation directory, use the modified installation path.

Backup: When these logs reach a pre-configured size (usually 1 MB), they are copied to a dated backup file, for example, SystemOut_05.01.27_13.24.49.log.

See "Modifying the logging levels of WebSphere Premises Server using WebSphere Application Server" on page 390 for details on how to enable tracing on WebSphere Application Server for WebSphere Premises Server.

DB2 for Linux, UNIX, and Windows log files

File name	Default location
db2diag.log jdbcerr.log	**Windows** C:\Program Files\IBM\SQLLIB\DB2 **Linux** /opt/IBM/SQLLIB/DB2

Data Transformation service log files

File name	Default location
edge_controller_name_x.log, where *x* is an integer	**Windows** *IBM_RFID_HOME*\logs
	Linux *IBM_RFID_HOME*/logs
For example, E1_1.log	

Data Capture and Delivery log files

A Log File agent listens to messages and directs all OSGi log output to a configurable set of rotating files.

When one of these log file fills up, the system then creates a new file and writes to it. Each log file name is the Data Capture and Delivery controller name plus *_number*. For example, if the first log file is E1_0.txt, then the next file will be E1_1.txt. If the maximum number of files is reached, then the oldest log file will be deleted.

To configure the settings for these files, see the "Log File agent" on page 129 properties.

Modifying logging levels and output

These topics describe how to turn logging on and off and how to modify logging levels, files names, and paths.

Modifying the logging levels of the Data Capture and Delivery controller

Use these steps to modify which kinds of messages are sent to WebSphere Premises Server.

About this task

This procedure does not modify the level of logging actually running on the system. To modify the system-level logging, see "Enabling logging and tracing for your Equinox or Eclipse launch configuration."

1. Open the WebSphere Premises Server Administrative Console. The Welcome page displays.
2. Click **Controllers** in the left navigation pane. The Controllers panel displays.
3. Click the controller you wish to modify. The Edit Controller Details panel displays.
4. Modify the **Alert Threshold** value. Valid levels are **Error**, **Warning**, and **Info**.
5. Click the **Reload Configuration** button to apply the new value.

Enabling logging and tracing for your Equinox or Eclipse launch configuration

This topic describes how to enable logging and tracing at the agent level or at the system level.

Logging and tracing is controlled by setting properties on the Alert agent.

System-level logging and tracing

By default, logging is set to DEBUG at the system level. When the Alert agent starts, it uses the configuration of the org.eclipse.soda.sat.core.util.logLevel and org.eclipse.soda.sat.core.util.trace properties for system-level logging and tracing.

Table 75. Alert agent logging and tracing properties

Property	Description
org.eclipse.soda.sat.core.util.logLevel	Indicates which level of logging to enable for the Service Activation Toolkit. This level should be the same level as specified for the `edge.log.threshold` property.
org.eclipse.soda.sat.core.util.trace	Displays system level trace output. Values can be true or false.

The Alert agent is also responsible for forwarding log messages to the WebSphere Premises Server. To change the level of messages that are forwarded, change the `threshold` property in Alert agent. The alert threshold can be set to `INFO`, `WARNING`, or `ERROR`.

Agent-level tracing and logging

Every agent has a `tracing` property. To enable tracing on an agent, the system trace level, `org.eclipse.soda.sat.core.util.trace`, must be set to true. Also, set the system log level to `DEBUG` or no trace will be displayed.

To modify the `tracing` property for all agents, you can enter something similar to the following example. This configuration disables tracing for all P1/E1 configurations.

```
<?xml version="1.0"?>
<configurationAdmin>
 <requests>
  <request type="update">
   <configurations>
    <configuration filter="(|(portal.id=P1)(edge.id=E1))">
     <properties>
      <property key="tracing" value="false"/>
     </properties>
    </configuration>
   </configurations>
  </request>
 </requests>
</configurationAdmin>
```

Many agents also have a `log.level` property. Setting this property allows you to control logging each agent. See the "Agent details" on page 111 for more information on the properties available for each agent.

In addition, the following Console Log agent properties can be used to configure the level of messages displayed to the OSGi console without modifying the system log level:

Table 76. Console log agent properties and descriptions

Property	Description
errorLogThreshold	Minimum level of messages that are written to stderr. Valid values are none, error, warning, info, or debug.
logThreshold	Minimum level of messages that are written to stdout. Valid values are none, error, warning, info, or debug. If the value is empty then the system log level is used.

Viewing messages and collecting logs

Install the `com.ibm.rfid.console.log` bundle into your runtime environment and start it to enable log messages from the agents to be seen on the OSGi console. When collecting a log to send with a problem report, be sure to retrieve the system properties by issuing the `setprop` command at the OSGI prompt. Also retrieve the list of installed bundles by issuing the `ss` command at the OSGI prompt.

Modifying the logging levels of WebSphere Premises Server using WebSphere Application Server

Use these steps to change the WebSphere Premises Server using the WebSphere Application Server administrative console.

1. Open the WebSphere Application Server administrative console.
2. Browse to **Troubleshooting** → **Logs and Trace** → **server1** → **Diagnostic Trace**.
3. Use the Configuration panel to apply new tracing values to the next restart of the application server. Use the Runtime page to make changes to the tracing values and apply them to the configuration immediately.
4. Click **Change Log Details Levels** on either panel. A window appears where all of the currently registered logging groups can be enabled.
5. Scroll to one of the following groups related to WebSphere Premises Server in `*=info`:
   - com.ibm.sensorevent.*
   - com.ibm.rfid.*
   - com.ibm.kimono.*
   - com.ibm.rfid.epcg.log.premises.*
   - com.ibm.ebo.rfid.*
   - com.ibm.wireless.ebo.rfid.*
   - com.ibm.internal.premises.*
6. Select the group to enable or modify tracing for and select the **all** setting.
7. Click **Apply**.
8. On the Configuration/Runtime panel, click **Apply** and then click **OK**.
9. Click **Save** if you wish to save this change to the master configuration.

   Note: If you made these changes using the Configuration panel, you must restart WebSphere Application Server for these changes to take effect.

Modifying log file names and paths for IBM Tivoli Monitoring

By default, IBM Tivoli Monitoring monitors the edge-heartbeats.log and edge-alerts.log files. IBM Tivoli Monitoring looks for these files in the *IBM_RFID_HOME*\logs directory.

If you have changed the log file path, modify the LogSources variable in the tecad_win.conf file so that IBM Tivoli Monitoring can find the files. LogSources is equal to the fully-qualified path and name of the files to be watched.

The tecad_win.conf file is located in the following directories:

> **Windows** *IBM_RFID_HOME*\monitoring
> **Linux** *IBM_RFID_HOME*/monitoring

The IBM Tivoli Enterprise Console v3.9 Adapter's Guide describes the LogSources variable in the following terms.

LogSources: Specifies the ASCII log files to poll for messages. The complete path to each file must be specified, and file names must be separated by commas. Within each file name, you can also use an asterisk to represent any sequence of characters or a question mark to represent any single character. For example, mylog* results in polling all log files with names that begin with mylog, while mylog??? results in polling all log files with names that consist of mylog followed by exactly three characters. These wildcard characters are supported only within the file name; the path must be explicitly specified.

A log file source does not have to exist when the adapter is started; it is polled when it is created. Each line in the file must end with a newline character. If a file truncates while the adapter is active, the adapter automatically resets its internal pointer to the beginning of the file. If during the polling interval the file is overwritten, removed, or recreated with more lines than the previous poll, only the number of lines greater than the previous line count is read. For example, the file has one line. After the poll interval elapses, the file is overwritten with two lines. Only the second line is read on the next polling.

For more details on LogSources and editing the tecad_win.conf file, refer to the online version of the IBM Tivoli Enterprise Console v3.9 Adapter's Guide.

Enabling logging for your WebSphere MQ environment

If you are using WebSphere MQ in your environment and suspect a problem with it, you can enable logging specific to WebSphere MQ.

For information about enabling logging, refer to the tracing topic in the WebSphere MQ information center: http://publib.boulder.ibm.com/infocenter/wmqv6/v6r0/index.jsp?topic=/com.ibm.mq.amqzag.doc/fa15270_.htm

Error messages

This topic contains lists of messages that display for the Data Capture and Delivery controller and WebSphere Premises Server, and is intended for reference purposes only. Some of these messages are generated automatically, while others require tracing to be enabled.

WebSphere Premises Server error messages

WebSphere Premises Server tracing events

The following table contains informational messages generated by WebSphere Premises Server. These business-level event messages display in the WebSphere Application Server trace file when tracing is turned on for **Event** messages.

Class Name	ID	Message
StartStopReadingHandlerBean	StartStopReadingHandlerBean	Received Start/Stop event: {event} {alias} {location}
TagReadEventTaskBean	TagReadEventTaskBean	Received Tag Read event: {event} {alias} {location} {reader} {tag}
ExternalValidationHandlerBean	ExternalValidationHandlerBean	Received validation message: {message} {alias} {location} {tag}

Class Name	ID	Message
StartStopReadingHandlerBean	StartStopReadingHandlerBean	Received Start/Stop eventReceived Start/Stop command: {event} {alias} {location}

WebSphere Premises Server J2EE application messages

The following list contains externalized messages that can be logged by the WebSphere Premises Server J2EE applications that run in WebSphere Application Server.

- An input message could not be parsed into the XML format expected by WebSphere Premises Server. Make sure the message is in XML format and conforms with the XML schema IBMPremisesUnifiedMessageFormat.xsd. The message was \"{0}\".
- Unable to send message \"{0}\" to channel \"{1}\". Reason given was \"{2}\".
- Unable to send message \"{0}\" to task \"{1}\" using filter \"{2}\". Reason given was \"{3}\".
- Unsupported message type received: \"{0}\"
- Undeliverable external validation response message. A location having alias \"{0}\" could not be found. Ensure that a location with this alias exists within the database.
- Undeliverable dock door receiving message. Unrecognized format in message \"{0}\". Ensure that the message source delivers messages in the required format.
- Undeliverable dock door receiving message. Missing location information in message \"{0}\". (1) Ensure that the appropriate location exists within the database and has been assigned the proper alias. (2) Ensure that the message source has been configured to provide the location alias.
- Unsupported JMS message received. The message type was \"{0}\". Supported message types are \"{1}\".
- An input message could not be parsed into the XML format expected by the Premises server. Make sure that the message is in XML format and conforms with the XML schema IBMPremisesUnifiedMessageFormat.xsd. The message was \"{0}\".
- The input XML message did not contain the required information. This component requires the \"{0}\" complex type in order to function. Review the IBMPremisesUnifiedMessageFormat.xsd schema for more information.
- Unable to extract the contents of the JMS message. Reason given was \"{0}\".
- Unable to convert location \"{0}\" into the internal format. Reason given was \"{1}\". Make sure \ that the location value is a valid location, location alias, or location hierarchy.
- Unable to publish event \"{0}\" with message \"{1}\" and location \"{2}\".

Data Capture and Delivery error messages

Informational messages

The following table contains informational messages generated by the Data Capture and Delivery controller. These business-level event messages display when the **Alert Threshold** field on the Controller Details panel is set to **info**.

Agent Name	ID	Message
AbstractAgent	getOptionalBooleanProperty(String, boolean) getOptionalByteProperty(String, byte) getOptionalDictionaryProperty(String, Dictionary) getOptionalDoubleProperty(String, double) getOptionalFloatProperty(String, float) getOptionalIntegerProperty(String, int) getOptionalLongProperty(String, long) getOptionalShortProperty(String, short) getOptionalStringProperty(String, String)	*data_format_exception_message* default value assumed: *default_value.*
ApplicationPingAgent	doApplicationPing()	Edge *ID* - Application Ping after timeout - received pong sequence number (*receive_sequence_number*) was greater than the ping sent (*send_sequence_number*).
	handleTopicToEdge(String)	Edge *ID* - Application Ping - received pong sequence number (*receive_sequence_number*) was not equal to the ping sent (*send_sequence_number*).
	logPingPongInfo(String)	Edge *ID* - Application Ping/Pong sequence = *sequence_number.*
FilterAgent	filtersChanged()	Stopping to wait for filter(s): *unavailable_filters.*
	handleTopicReaderTags(Object)	Allowing tag through: *tag.*
	tryToStart()	Starting. Waiting for filter(s): *unavailable_filters.*
HealthCheckAgent	handleTopicPortalStatus(Object)	Portal *ID* - HealthCheck status *up_or_down* - while portal is enabled.
PortalControllerAgent	handleTopicControllerCommand(Object)	The current sensor matrix state: *state.*
	handleTopicPalletFeedback(Object)	Portal enabled. Tag rejected. Tag acknowledged.
	handleTopicTimeout(int, Object)	*Portal_ID* - Timeout occurred at timer *ID.*
	processMatrix()	*Portal_ID* - State transition: *current_state_name* –> *next_state_name.*
	setPortal(Boolean)	Portal enabled Portal disabled
RestartAgent	handleRestartTopic(String)	Restart request received, Edge *ID* about to restart.
RFIDMapAgent	handlePublishArrived_content(String, Object)	*tag_count_log*
	handlePublishArrived(String, Object)	Self test: received unknown format data.
TagAggregatorAgent	handleTopicDumpTags()	Sending tag aggregation to Premises. Collection count: *aggregated_tag_count.*
UniversalSensorAgent	logWithLevel(int, String)	*log_message*

Warning messages

The following table contains warning messages generated by the Data Capture and Delivery controller. These business-level event messages display when the **Alert Threshold** field on the Controller Details panel is set to **warning**.

Agent Name	ID	Message
ApplicationPingAgent	logWarning(String, String)	Edge *get_description* - ApplicationPing *message* - Application Ping/Pong sequence = *sequence_number:reason*.
HealthCheckAgent	handleTopicAppPingSignalStatus(Object)	Portal *ID* - HealthCheck status changed to UP - application ping is OK. Portal *ID* - HealthCheck status changed to DOWN - application ping timeout.
	handleTopicDeviceSignalHealth(int)	Portal *ID* - HealthCheck status changed to *up_or_down* - reader signaled health *up_or_down*.
	handleTopicDevicesSignalStatus(String, String)	Portal *ID* - HealthCheck status changed to UP - sensor *topic* is *on_or_off*. Portal *get_description* - HealthCheck status changed to DOWN - sensor has error.
PortalControllerAgent	handleTopicHealthSignal(Object)	System health down. Performing a reset...
	handleTopicReaderSignalStatus(Object	Reader error detected. Performing a reset...
	handleTopicSensor(int, Object)	Error at sensor *ID* detected. Performing a reset...
	initMatrix()	Waiting for service com.ibm.rfid.agent.portalcontroller.service. Portal ControllerPropertiesService interrupted.
	processMatrix()	Did not find a match in the matrix with these input states: *states*.
	setDataExtension(SensorMatrixRow)	Got reply with correct topic: *topic*, but different data: *data*.
	setError(SensorMatrixRow)	Cannot publish error message, topic is null.
	setGatheringCycle(int)	Action not changing state: Start gathering cycle although already started. Action not changing state: Stop gathering cycle although already stopped.
	setTimer(int, int)	Action not changing state: Starting timer although already started. Action not changing state: Stopping timer although already stopped.
RFIDMapAgent	handlePublishArrived_content(String, Object)	*tag_count_log*
TagAggregatorAgent	checkCollectionSizeAndWarn()	Tag Aggregator collection list has grown to *size* elements.
UniversalSensorAgent	logWithLevel(int, String)	*log_message*

Error messages

The following table contains error messages generated by the Data Capture and Delivery controller. These business-level event messages display when the **Alert Threshold** field on the Controller Details panel is set to **error**.

Agent Name	ID	Message
FilterAgent	handlePublishArrived(String, Object)	Message received before all filters loaded. Verify configuration for unavailable filter(s): *unavailable_filters*.

Agent Name	ID	Message
PortalControllerAgent	handleTopicHealthSignal(Object)	Unexpected health signal value: *value*.
	handleTopicPalletFeedback(Object)	Unexpected pallet feedback value: *value*.
	handleTopicPortalCommand(Object)	Unexpected portal command value: *value*.
	handleTopicReaderSignalStatus(Object)	Unexpected reader signal value: *value*.
	handleTopicSensor(int, Object)	Unexpected sensor topic value: *value*.
	handleTopicSwitchSignal(Object)	Unexpected switch signal value: *value*.
	handleTopicTimeout(int, Object)	Unexpected timeout topic value from timer *ID*: *value*.
	loadPropertiesFromURL(String)	Cannot load properties. URL *URL* is malformed (*error*)
	processMatrix()	Processing matrix failed: *illegal_argument_exception*. Performing a reset...
	setDataExtension(SensorMatrixRow)	Timeout while waiting for *notification_topic*.
RFIDMapAgent	handlePuglishArrived_content(String, Object)	Sending tag aggregation to Premises. Collection count: *tag_count*.
TagAggregatorAgent	getSubscriptions()	Tag aggregator agent has topics and values that are not valid for Start and Stop triggers. Configure separate topics or values for stop and start events.
UniversalActorAgent	handleControlAllTopic(Object)	Expected Boolean value with topic *topic*, but got object of class: *class*.
	handleControlTopic(Actor, String, Object)	Expected Boolean value with topic *topic*, but got object of class *class*.
UniversalSensorAgent	logWithLevel(int, String)	*log_message*
	setLogLevel(String)	Unknown value *log_level* in configuration property sensor.statelogging - using DEBUG as default value.
Publication	publish	*message*

MicroBroker Application Framework error messages

The following list contains error messages that display for the MicroBroker
Application Framework.
- Error occurred while starting the MicroBroker
- Error occurred while creating bridge
- Failed to start agent { 0 }
- Failed to create bridge { 0 }
- Failed to delete bridge { 0 }
- Failed to stop agent { 0 }
- ClassNotFoundException while decoding data
- StreamCorruptedException while decoding data
- Exception while decoding data
- Error occurred while deleting bridge { 0 }
- Failed to logon to Broker { 0 }
- Failed to subscribe to topics
- Failed when topic {0} was published with the value { 1 }
- Exception while encoding data
- The property { O } does not exist in micro.cfg

- Failed to publish topic { 0 } because the agent is not connected to the MicroBroker
- The PublicationManager is not started.
- Unable to published: { 0 }
- Failed to encode data for topic { 0 }
- Failed to start broker { 0 }
- Failed to delete broker { 0 }
- Failed to subscribe to topics
- Failed to reconnect
- An MqttException was thrown while trying to start
- Failed to unsubscribe to topics

Verifying that the WebSphere Premises Server is generating correct XML

This topic describes how to verify that WebSphere Premises Server is generating the correct XML for Data Capture and Delivery.

Open the following URL in a Web browser:

http://*premises_server_hostname*:9080/ibmrfidadmin/premises.sl?action=getconfig &edge=*edge_ID*&version=6.1

The "Portal Controller agent" on page 138 gets the `matrix.properties` value from the location specified in the edge.xml file:

```
<configuration
  factoryPid="com.ibm.rfid.agent.protalcontroller.bundle.PortalController
      AgentManagedServiceFactoryActivator">
<properties>
   <property key="matrix.properties"
         value="http://premises_server_hostname/BDDR.properties"/>
```

You can also see the `matrix.properties` value in the WebSphere Premises Server Administrative Console by going to **Agent Configuration** → **PortalControllerAgent**.

Troubleshooting problems with MicroBroker

Use these tips to resolve errors caused by MicroBroker.

Enabling trace

If you suspect that MicroBroker is the source of a problem, you can modify the MicroBroker trace level to receive more information.

To do this, set the `trace.level` property in the "MicroBroker agent" on page 134. Possible values for the `trace.level` property are min, 1, 2, 3, 4, 5, or max.

Increasing the queue size

Increase the MicroBroker queue size if you are receiving MicroBroker warnings, such as the following:

```
[WARNING] FMBM1009 MicroBroker Client 'BridgeMicro' - queue 'bridge:E1-prem' is full. Depth: 1000
```

You can increase the MicroBroker queue size by editing the `queueSize` parameter in the "MicroBroker agent" on page 134.

Increasing the maximum message size

Increase the MicroBroker queue size if you are receiving MicroBroker errors similar to the following examples.

Note: In all of these examples, the number of tags is 300.

XML with additional EPC URI data

```
[ERROR] FMBT1761 MicroBroker Client 'BridgeMicro' - PUBLISH MQTT protocol flow
exceeds the maximum message size. Max size:51200 bytes, Message size:241047
```

XML without additional EPC URI data

```
[ERROR] FMBT1761 MicroBroker Client 'BridgeMicro' - PUBLISH MQTT protocol flow
exceeds the maximum message size. Max size:51200 bytes, Message size:136139
```

Serialized object with additional EPC URI data

```
[ERROR] FMBT1761 MicroBroker Client 'BridgeMicro' - PUBLISH MQTT protocol flow
exceeds the maximum message size. Max size:51200 bytes, Message size:154454
```

Serialized object without additional EPC URI data

```
[ERROR] FMBT1761 MicroBroker Client 'BridgeMicro' - PUBLISH MQTT protocol flow
exceeds the maximum message size. Max size:51200 bytes, Message size:94374
```

You can increase the MicroBroker maximum message size by editing the `maxMessageSize` parameter in the "MicroBroker agent" on page 134.

Troubleshooting using queues

Queues can be used for troubleshooting because they usually process and go to zero quickly. If any of the queues are not zero, it indicates a problem. WebSphere Premises Server uses WebSphere MQ queues and WebSphere Application Server SIBus queues.

WebSphere Application Server SIBus queues

You can view all of the queues, including the SIBus queues, by navigating to **Resources** ▸ **JMS** ▸ **Queues** in the WebSphere Application Server administrative console.

ALE.Report.Bus.Queue
JNDI name is jms/ale.report.bus.q. This SIBus queue is used by the Application Level Events (ALE) engine to put reports that are generated by ALE into the system.

EVENT.MONITOR.QUEUE
JNDI name is jms/event.monitor.q. This SIBus queue monitors events as they occur in real-time.

Enterprise.In.Bus.Queue
JNDI name is jms/enterprise.in.bus.q. Enterprise applications send messages to this queue.

Enterprise.Out.Bus.Queue
JNDI name is jms/enterprise.out.bus.q. Messages are sent to this queue from WebSphere Premises Server to be processed by enterprise applications.

WebSphere MQ queues

WebSphere MQ queues for WebSphere Premises Server are named from the premises server point-of-view. "IN" queues are coming "in" to WebSphere Premises Server. "OUT" queues are going "out" from WebSphere Premises Server to the MicroBroker (for the Data Capture and Delivery controller) and the back-end adapters.

Tip: For an advanced troubleshooting technique, you can stop individual queues from processing to help isolate where the problem is occurring.

Queues in IBM.DC.QM

DC.IN.Q
> This queue receives messages from Data Capture and Delivery and sends them to the sensor gateway to publish to the SIBus.

DC.OUT.Q
> Messages flow from message-driven beans (MDBs) through this queue to the Data Capture and Delivery controllers.

DEAD.MESSAGE.Q
> This queue keeps messages that cannot be processed due to some internal error. IBM Support may ask administrators to report the contents of this queue when troubleshooting a problem.

ENTERPRISE.IN.Q
> Enterprise applications send messages to the ENTERPRISE.IN.Q queue, where they are sent to the SIBus.

ENTERPRISE.OUT.Q
> Messages are sent to the ENTERPRISE.OUT.Q queue from WebSphere Premises Server to be processed by enterprise applications.

fmb.sync.q
> An internal queue used for communication.

Queues in IBM.RFID.QM

ALE.REPORT.Q
> This queue is used by the Application Level Events (ALE) engine to put reports that are generated by ALE into the system.

ALE.TAG.INPUT.Q
> The ALE engine uses this queue to retrieve tag read events so that it can filter them.

CONTROL.IN.Q
> Messages come to the CONTROL.IN.Q queue from adapters and are processed into task messages and sent to the TASK.Q queue.

CONTROL.OUT.Q
> Messages come to the CONTROL.OUT.Q queue from the TASK.Q queue and are sent to the appropriate adapters for implementation.

DEAD.MESSAGE.Q
> This queue keeps messages that cannot be processed due to some internal error. IBM Support may ask administrators to report the contents of this queue when troubleshooting a problem.

EDGE.IN.Q
> Messages flow from the MicroBroker bridge into the EDGE.IN.Q queue.

They can be command, event, or tag messages. The messages are processed into task messages and sent to the TASK.Q queue.

EDGE.OUT.Q

Task messages are sent from the TASK.Q queue to the EDGE.OUT.Q queue where they are converted into MicroBroker messages and sent to the edge controller.

EDGE.OUTBYTES.Q

This queue is used to send serialized objects instead of XML to the edge controller. It requires no transforms. It is used by WebSphere Premises Server to send print jobs to the edge controller.

EDGE.PRINT.IN.Q

This queue is a status queue that is used to get the status of a print job.

fmb.sync.q

An internal queue used for communication.

KIMONO.RESPONSE.Q

This queue gets a response to an event from the back end.

MANAGEMENT.Q

This queue processes messages specific to system management, such heartbeats and alerts.

PERSISTENCE.Q

This queue processes tag persistence messages when tag persistence is enabled in the SystemAgent.

TAGMONITOR.OUT.Q

This queue monitors tag reads as they occur in real-time.

TASK.Q

Messages come to the TASK.Q queue from the EDGE.IN.Q queue and are sent to the CONTROL.OUT.Q queue. Messages also come to the TASK.Q queue from the CONTROL.IN.Q queue and are sent to the EDGE.OUT.Q queue.

Checking the depth of WebSphere MQ queues

Queues usually process and go to zero quickly. If the depth of any queue is greater than zero, it indicates a problem.

About this task

Windows For Windows operating systems:

1. Open MQ Explorer by selecting **Start** → **Programs** → **IBM WebSphere MQ** → **WebSphere MQ Explorer**.
2. Check the depths of the WebSphere Premises Server queues.

Linux For Linux operating systems, run this command:

```
export AMQECLIPSE=/opt/mqm/ies30/eclipse
/opt/mqm/bin/runmqcfg
```

Troubleshooting tips

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

This list is not an all-inclusive list of problems. These steps are not guaranteed to solve your problems. If you attempted these steps and the problem persists, capture the WebSphere Application Server logs, traces, and Data Transformation logs and contact your IBM representative for further assistance.

- "Installation issues"
- "Communication and connectivity issues" on page 401
- "Queue issues" on page 403
- "Other issues" on page 404
- "Exceptions and errors" on page 405

Installation issues

- "Installation fails on Linux"
- "Installer cannot find WebSphere Application Server installation directory "
- "URI length exceptions in the install.log file"
- "Error in the IRU_DeploymentWizard.log file after silent installation" on page 401
- "A "Microsoft Visual C++ ..." window appears after installing DB2" on page 401

Installation fails on Linux

The installation of WebSphere Premises Server on Linux fails. The installation fails if the installation script was not run from a shell window. Try running the installation script again, making sure to run the command from a shell window.

Installer cannot find WebSphere Application Server installation directory

During the installation of WebSphere Premises Server on Windows 2003, the installation might not be able to find the WebSphere Application Server installation directory. See the topic about starting the installation in the Microsoft Windows Server TechCenter.

To resolve this problem, complete the following steps:
1. Exit the installation.
2. Open a command prompt and run the following command:
   ```
   change /user install
   ```
3. Restart the WebSphere Premises Server installation.

URI length exceptions in the install.log file

If you are installing on a Windows operating system, and you see exceptions in *IBM_RFID_HOME*\logs\install.log file similar to the following, then there is a path character limitation on the operating system:

```
com.ibm.websphere.management.exception.ConfigServiceException
com.ibm.ws.sm.workspace.WorkSpaceException
java.io.IOException: java.io.IOException: The URI length is greater than the Windows
limit of 259 characters.
```

To resolve this issue, use a shorter profile name when you install WebSphere Premises Server, or use a shorter WebSphere Application Server installation path.

Error in the IRU_DeploymentWizard.log file after silent installation

If you have installed WebSphere Premises Server silently, and you see a message similar to the following example, you can safely ignore it.

```
2008-01-28 16:56:49, , exception: java.lang.NullPointerException
java.lang.NullPointerException
at com.ibm.jsdt.rxa.RxaRemoteAccessSelector.populateRxaCredentials(RxaRemoteAccessSelector.java:184)
at com.ibm.jsdt.main.InstallDriver.pushIia(InstallDriver.java:88)
at com.ibm.jsdt.main.AbstractInstallDriver.runInstalls(AbstractInstallDriver.java:179)
at com.ibm.jsdt.main.AbstractInstallDriver.installGroup(AbstractInstallDriver.java:108)
at com.ibm.jsdt.task.InstallTask.execute(InstallTask.java:448)
at com.ibm.jsdt.task.JsdtTask.launch(JsdtTask.java:151)
at com.ibm.jsdt.task.TaskManager.launchTheseTasks(TaskManager.java:205)
at com.ibm.jsdt.factory.task.TaskWorker.launchTasks(TaskWorker.java:86)
at com.ibm.jsdt.factory.task.TaskWorker.doWork(TaskWorker.java:72)
at com.ibm.jsdt.factory.base.Factory.startWorkers(Factory.java:224)
at com.ibm.jsdt.factory.task.TaskFactory.generate(TaskFactory.java:59)
at com.ibm.jsdt.factory.base.Builder.parseURI(Builder.java:192)
at com.ibm.jsdt.task.TaskManager.createTasks(TaskManager.java:138)
at com.ibm.jsdt.main.MainManager.createTasks(MainManager.java:856)
at com.ibm.jsdt.main.MainManager.<init>(MainManager.java:328)
at com.ibm.jsdt.main.MainManager.main(MainManager.java:447)
```

A ″Microsoft Visual C++ ...″ window appears after installing DB2

If you use the installation wizard to install DB2 for Linux, UNIX, and Windows, you could see an ″Microsoft Visual C++ ...″ window that appears as a blue or gray bar on the server desktop. You can ignore this window. Restarting the DB2 server will remove this window.

Communication and connectivity issues

- "The back-end system does not receive messages"
- "The edge controller cannot connect to WebSphere Premises Server" on page 402
- "Connection between the tag reader and edge controller is interrupted" on page 402
- "The edge controller is unable to obtain configuration from WebSphere Premises Server" on page 402
- "The edge controller is unable to communicate with the tag reader" on page 402
- "Unable to start the device agent on WebSphere Premises Server" on page 403

The back-end system does not receive messages

Perform the following actions to try and resolve the problem:
- Check that WebSphere MQ is running. Start WebSphere MQ if it is not running.
- Use the MQ Explorer to view the IBM.DC.QM queue manager and check that the depth of the ENTERPRISE.OUT queue is zero.
- Check that WebSphere Application Server is running. Using a Web browser, go to: http://*premises_server_ip*:9060/ibm/console and log in with any user name. Start WebSphere Application Server if it is not running. Start any stopped listeners, and restart WebSphere Application Server if they cannot be started.
- On the WebSphere Application Server administrative console, go to **Servers → Application Servers → server1 → Messaging → Messaging Listener service → Listener Ports**. Check that all listeners are running. A listener is running if it has a green arrow next to it.
- Check that the Data Transformation service is running. Check the runtime log:

  > **Windows** C:\Program Files\IBM\RFID\logs\DTSRuntime.log
  > **Linux** /opt/IBM/RFID/logs/DTSruntime.log

Stop and start the Data Transformation service if the log shows errors or exceptions.

The edge controller cannot connect to WebSphere Premises Server

Use the following actions to try and resolve the problem:
- Check that WebSphere Application Server is running. Use the Windows Services panel. If WebSphere Application Server is down, start it.
- Check that the Data Transformation service is running. Use the Windows Services panel to locate **IBM WebSphere Premises Server DT Service**. If the service is down, start it.
- Try to access the configuration from a browser at: http://*premises_server_ip*:9080/ ibmrfidadmin/premises.sl?action=getconfig&edge=*EdgeID*. If you cannot "ping" WebSphere Premises Server from the edge controller, check cables and hardware connections.
- Check the network connection between the edge controller and WebSphere Premises Server. Try to Telnet into the edge controller and "ping" WebSphere Premises Server. If you cannot Telnet into the edge controller, make sure that the edge controller is running.

Connection between the tag reader and edge controller is interrupted

If the connection between the tag reader and the edge controller is interrupted due to power failure or network outage, the edge controller might not immediately connect to the tag reader. If the edge controller does not reconnect to the tag reader within the specified reconnection time out, use the following two steps.
1. Switch the power off and back on again on the tag reader. In many cases, turning the power off and on solves the problem.
2. Restart the edge controller.

The edge controller is unable to obtain configuration from WebSphere Premises Server

- Try to access the configuration from a browser at: http://*premises_server_ip*:9080/ ibmrfidadmin/premises.sl?action=getconfig&edge=*EdgeID*
- Once the connection from the edge controller to WebSphere Premises Server is fixed, you do not need to perform any additional steps. You do not need to restart the edge controller. It automatically tries to restart approximately every two minutes to obtain the configuration from the premises server.
- Verify that the network topology is correct. If it is not, fix the network topology and restart the edge controller.
- Verify that the correct EDGEID, PREMISES_IP, and PORT_NUMBER were delivered from DMS UpdateParameters.xml job. If they were not, reissue the DMS UpdateParameters.xml job.

The edge controller is unable to communicate with the tag reader

- Check the Data Transformation log.
- Check the tag reader. If you cannot Telnet to the tag reader using the reader port, it might already be controlled by another edge controller. Ensure that no other edge controller is configured to use that tag reader and no other machine has a Telnet session open to that tag reader through the reader port.

- Check the network connection between the edge controller and the tag reader. Try to Telnet into the edge controller and "ping" the tag reader. If you cannot "ping" the reader, check the cables and hardware connections.
- If the problem persists, restart the tag reader.
- If the problem persists, capture the Data Transformation log and contact your IBM representative for additional assistance.

Unable to start the device agent on WebSphere Premises Server

If you are unable to configure the device adapter with WebSphere Premises Server, update the core bundle list copy it to the bundle repository.

To resolve this problem, copy the following bundle loader files to the bundlelists directory in the bundle repository (for example, C:\Program Files\IBM HTTP Server\htdocs\en_US\bundles\bundlelists):
- The dc_core4dts.txt file is for running Data Capture and Delivery bundles inside the Data Transformation service on WebSphere Premises Server.
- The dc_core.txt file is for running Data Capture and Delivery bundles that are remote to the Data Transformation service (on the remote Data Capture and Delivery controller, which is running in an Equinox environment).

To install the bundles on the local machine or on the remote Data Capture and Delivery controller:
1. Copy the device agent bundles to the bundle repository.
2. Edit the bundle loader file (dc_core4dts.txt or dc_core.txt) and add the bundle name to it (for example, START bundle.jar) and update *host_name* with the correct host name or IP address.
3. Update the config.ini file that is located in the configuration folder (for RFID Data Transformation Service, the file is located under *IBM_RFID_HOME*/dts/configuration) with the correct bundle file name:
   com.ibm.rfid.bundle.list.url=http://*host_name:port*/bundleadmin/
   GetBundle?name=http://*host_name*/bundles/bundlelists/*bundle_loader_file*
4. Reset the bundle list on the local Data Transformation service by running the **resetDTS** script, which is located in the *IBM_RFID_HOME*/dts directory. On the remote Data Capture and Delivery controller, reset the bundle list to the default settings.
5. Restart the Data Transformation service or the remote Data Capture and Delivery controller.
6. Start the bundle loader bundle (com.ibm.rfid.bundle.loader_*version*.jar).

Queue issues

- "Queues filled to maximum depth in the queue managers"
- "Queue managers are not removed after uninstallation of WebSphere Premises Server" on page 404

Queues filled to maximum depth in the queue managers

Check to see if the maximum queue depth has been reached. See "Checking the depth of WebSphere MQ queues" on page 399.

If you have reached the maximum queue depth, perform the following workaround steps:

1. Stop WebSphere Application Server.
2. Stop the Data Transformation on all edge controllers.
3. Extend the maximum queue depth for all queues that are saturated.

   Note: The default queue depth is 5,000.
4. Restart WebSphere Application Server.
5. Restart the Data Transformation on the WebSphere Premises Server.
6. Monitor the affected queue depths until they fall to zero.
7. Restart the Data Transformation on all edge controllers.

Queue managers are not removed after uninstallation of WebSphere Premises Server

If you are using a Linux operating system and you have uninstalled WebSphere Premises Server, but the WebSphere MQ queue managers, IBM.RFID.QM and IBM.DC.QM, have not been deleted, you need to check your group membership and delete the queue managers manually.

If you have this problem, you should see an MQ error message in the uninstall.log file that states:

```
AMQ7077: You are not authorized to perform the requested operation.
```

This error message indicates that the terminal session root user running the uninstallation program has not inherited the mqm group; therefore, the MQ commands in the uninstallation program, endmqm and dltmqm do not work. The terminal session root user must be a member of the mqm group to delete the queue managers.

To find out if this is the cause of the problem, use the id -a command to see if the current terminal session root user is a member of the mqm group and make any necessary changes.

Then, use the following commands to stop and delete the queue managers:

```
/opt/mqm/bin/endmqm -i IBM.RFID.QM
/opt/mqm/bin/dltmqm IBM.RFID.QM
/opt/mqm/bin/endmqm -i IBM.DC.QM
/opt/mqm/bin/dltmqm IBM.DC.QM
```

Other issues
- "WebSphere Premises Server does not work after stopping and restarting"
- "WebSphere Premises Server does not work in general" on page 405
- "Usage of direct JNDI lookup of resources has been deprecated" on page 405
- "WebSphere Premises Server Administrative Console password on Linux can be shorter than required" on page 405
- "The WAS_HOME environment variable is not applied in a remote deployment" on page 405

WebSphere Premises Server does not work after stopping and restarting
- Check that WebSphere MQ is running. If not, start WebSphere MQ from the Services panel.
- Check that DB2 for Linux, UNIX, and Windows (DB2) or Oracle is running. If not, start DB2 or Oracle from the Services panel.

- Check that WebSphere Application Server is running. If not, start WebSphere Application Server from the Services panel.
- Check that the Data Transformation is running. If not, start **IBM WebSphere Premises Server DT Service** from the Services panel.

WebSphere Premises Server does not work in general

- Check the WebSphere Application Server server1 logs in the *WAS_PROFILE_HOME*\logs\server1 directory. Check the SystemOut.log and the SystemErr.log files. Send the log files to the IBM support team.
- Check that trace is enabled. Enable trace and send the trace.log file to the IBM support team.

Usage of direct JNDI lookup of resources has been deprecated

See J2CA0294W: Deprecated usage of direct JNDI lookup of resource for details.

WebSphere Premises Server Administrative Console password on Linux can be shorter than required

If you use the default encryption method on SUSE LINUX 9.3, the WebSphere Premises Server Administrative Console may accept passwords that are eight characters or shorter in length.

To resolve this issue, change the password encryption from DES to MD5:
1. Navigate to **YAST → Security and Users → Edit and Create Users**.
2. Select **Password Encryption** in the **Expert options** menu.
3. Change the value from DES to MD5.

The WAS_HOME environment variable is not applied in a remote deployment

If you have installed WebSphere Premises Server remotely, you may see an error about the WAS_HOME environment variable not being applicable when you try to run the dts.bat file, even though it appears that the environment variable has been set correctly.

This problem can occur if you have logged into the target server before starting the remote installation of WebSphere Premises Server.

To resolve this issue, log out of the target server you used for your remote deployment (the server where you installed WebSphere Premises Server). Then log back in to the server and try running the dts.bat file again.

Exceptions and errors
- "Incorrectly labeled ALE information messages in the WebSphere Application Server logs" on page 406
- "A NullPointerException occurs when OSGi starts" on page 406
- ""Failed to resolve plug-in" error in the WebSphere Application Server SystemOut.log file" on page 407
- "Print job fails with a rollback exception" on page 407
- "Oracle 11g exceptions in SystemOut.log file" on page 408
- "JMSResource exceptions in the SystemOut.log files on the central server and node servers" on page 409

Incorrectly labeled ALE information messages in the WebSphere Application Server logs

The WebSphere Application Server SystemOut.log file shows informational log messages for ALE that are incorrectly labeled as error messages. These messages are not error messages.

A NullPointerException occurs when OSGi starts

An org.eclipse.osgi.framework.internal.core.BundleHost.getLoaderProxy error, such as the following, might occur when starting OSGi. This error will *not* affect the operation of the system.

```
java.lang.NullPointerException
at org.eclipse.osgi.framework.internal.core.BundleHost.getLoaderProxy(BundleHost.java:534)
at org.eclipse.osgi.framework.internal.core.BundleHost.getBundleLoader(BundleHost.java:526)
at org.eclipse.osgi.framework.internal.core.ExportedPackageImpl.getImportingBundles
(ExportedPackageImpl.java:56)
at org.eclipse.soda.sat.core.internal.framework.bundle.BundleDependencyManager.register
ImportedPackageDependency(BundleDependencyManager.java:470)
at org.eclipse.soda.sat.core.internal.framework.bundle.BundleDependencyManager.register
ImportedPackageDependencies(BundleDependencyManager.java:445)
at org.eclipse.soda.sat.core.internal.framework.bundle.BundleDependencyManager.handleBundle
Installed(BundleDependencyManager.java:293)
at org.eclipse.soda.sat.core.internal.framework.bundle.BundleDependencyManager.populateDependency
Tracker(BundleDependencyManager.java:360)
at org.eclipse.soda.sat.core.internal.framework.bundle.BundleDependencyManager.handleManager
Started(BundleDependencyManager.java:324)
at org.eclipse.soda.sat.core.internal.framework.bundle.BundleManager.startup
(BundleManager.java:366)
at org.eclipse.soda.sat.core.internal.framework.bundle.Activator.startupBundleDependencyManager
(Activator.java:310)
at org.eclipse.soda.sat.core.internal.framework.bundle.Activator.addExportedBundleDependencyService
(Activator.java:93)
at org.eclipse.soda.sat.core.internal.framework.bundle.Activator.activate
(Activator.java:85
at org.eclipse.soda.sat.core.framework.BaseBundleActivator$1.activate
(BaseBundleActivator.java:280
at org.eclipse.soda.sat.core.internal.framework.bundle.BundleActivationManager.activate
(BundleActivationManager.java:150)
at org.eclipse.soda.sat.core.internal.framework.bundle.BundleActivationManager.performActivation
(BundleActivationManager.java:1262)
at org.eclipse.soda.sat.core.internal.framework.bundle.BundleActivationManager.access$0
(BundleActivationManager.java:1248)
at org.eclipse.soda.sat.core.internal.framework.bundle.BundleActivationManager$1.acquired
(BundleActivationManager.java:391)
at org.eclipse.soda.sat.core.internal.record.container.ImportServiceRecordContainer.serviceAcquired
(ImportServiceRecordContainer.java:470)
at org.eclipse.soda.sat.core.internal.record.container.ImportServiceRecordContainer.access$0
(ImportServiceRecordContainer.java:458)
at org.eclipse.soda.sat.core.internal.record.container.ImportServiceRecordContainer$4.serviceAcquired
(ImportServiceRecordContainer.java:282)
at org.eclipse.soda.sat.core.internal.record.ImportServiceRecord.acquire
(ImportServiceRecord.java:115)
at org.eclipse.soda.sat.core.internal.record.ImportServiceRecord.acquire
(ImportServiceRecord.java:124)
at org.eclipse.soda.sat.core.internal.record.container.ImportServiceRecordContainer$1.execute
(ImportServiceRecordContainer.java:58)
at org.eclipse.soda.sat.core.internal.record.container.ServiceRecordContainer.doForService
(ServiceRecordContainer.java:353)
at org.eclipse.soda.sat.core.internal.record.container.ServiceRecordContainer.doForEach
(ServiceRecordContainer.java:321)
at org.eclipse.soda.sat.core.internal.record.container.ImportServiceRecordContainer.acquire
(ImportServiceRecordContainer.java:237)
at org.eclipse.soda.sat.core.internal.framework.bundle.BundleActivationManager.acquireImportedServices
(BundleActivationManager.java:125)
at org.eclipse.soda.sat.core.internal.framework.bundle.BundleActivationManager.startSync
(BundleActivationManager.java:1663)
at org.eclipse.soda.sat.core.internal.framework.bundle.BundleActivationManager.start
(BundleActivationManager.java:1632)
at org.eclipse.soda.sat.core.framework.BaseBundleActivator.start
(BaseBundleActivator.java:1073)
at org.eclipse.osgi.framework.internal.core.BundleContextImpl$2.run
(BundleContextImpl.java:991)
at java.security.AccessController.doPrivileged(AccessController.java:220)
at org.eclipse.osgi.framework.internal.core.BundleContextImpl.startActivator
(BundleContextImpl.java:985)
at org.eclipse.osgi.framework.internal.core.BundleContextImpl.start
(BundleContextImpl.java:966)
at org.eclipse.osgi.framework.internal.core.BundleHost.startWorker
(BundleHost.java:317)
at org.eclipse.osgi.framework.internal.core.AbstractBundle.start
(AbstractBundle.java:256)
at com.ibm.rfid.bundle.loader.BundleLoader.startBundles(Unknown Source)
at com.ibm.rfid.bundle.loader.BundleLoader.loadBundles(Unknown Source)
at com.ibm.rfid.bundle.loader.Activator.doStart(Unknown Source)
at com.ibm.rfid.bundle.loader.Activator$2.run(Unknown Source)
at java.lang.Thread.run(Thread.java:719)
Exception when starting bundle: org.eclipse.soda.sat.core
org.osgi.framework.BundleException:
Exception in org.eclipse.soda.sat.core.internal.framework.bundle.Activator.start()
of bundle org.eclipse.soda.sat.core.
```

To prevent this problem from occurring, set the following property to false in the config.ini file on your system: `-Dorg.eclipse.soda.sat.core.bds.status=false`.

Setting this property disables the SAT BundleDependencyManager and prevents SAT from collecting dependency data. The SAT BundleDependencyManager is used by tooling for development and debugging. Disabling it does not impact normal production systems.

If you need the SAT BundleDependencyManager for debugging or development, you can turn this option on again. If this problem reoccurs, restart the system since the problem only occurs approximately one out of 50 times OSGi starts.

"Failed to resolve plug-in" error in the WebSphere Application Server SystemOut.log file

If you see this error, it may appear similar to the following example:

```
[11/19/07 11:15:08:703 CST] 0000001d ApplicationMg A  WSVR0200I: Starting application:
IBM_Premises_Server_BIRT
[11/19/07 11:15:08:703 CST] 0000001d ApplicationMg A  WSVR0204I: Application:
IBM_Premises_Server_BIRT  Application build level: Unknown
[11/19/07 11:15:08:921 CST] 0000001d ExtensionRegi E  CWXRS0004E: Failed to resolve plug-in
[11/19/07 11:15:08:937 CST] 0000001d ExtensionRegi E  CWXRS0004E: Failed to resolve plug-in
[11/19/07 11:15:08:953 CST] 0000001d ExtensionRegi E  CWXRS0004E: Failed to resolve plug-in
[11/19/07 11:15:08:968 CST] 0000001d ExtensionRegi E  CWXRS0004E: Failed to resolve plug-in
[11/19/07 11:15:09:187 CST] 0000001d WebGroup      A  SRVE0169I: Loading Web Module: Eclipse
BIRT Report Viewer.
[11/19/07 11:15:11:625 CST] 00000027 SampledbPlugi I  Sampledb plugin starts up. Current
startCount=0
[11/19/07 11:15:11:625 CST] 00000027 SampledbPlugi I  Creating Sampledb database at location
C:\WINDOWS\TEMP\/BIRTSampleDB_1195442111625_15d815d8
[11/19/07 11:15:13:109 CST] 0000001d VirtualHost   I  SRVE0250I: Web Module Eclipse BIRT
Report Viewer has been bound to default_host[*:9080,*:80,*:9443,*:5060,*:5061,*:443].
[11/19/07 11:15:13:109 CST] 0000001d ApplicationMg A  WSVR0221I: Application started:
IBM_Premises_Server_BIRT
```

You can safely ignore these messages. They are from Business Intelligence and Reporting Tools (BIRT), which WebSphere Premises Server uses for reports.

Print job fails with a rollback exception

The maximum number of tags that can be printed in a single print request varies and is dependent on a number of factors, including the label design, the amount of data per tag, your server size, and your network. If you submit a print job and the job fails, check for an error similar to the following in your WebSphere Application Server SystemOut.log file that indicates that you have too many tags in your print job:

```
[10/25/07 14:14:06:750 CST] 0000002f ExceptionUtil E  CNTR0019E:
EJB threw an unexpected (non-declared) exception during invocation of
method "getPrintTemplateDetails". Exception data:
com.ibm.websphere.csi.CSITransactionRolledbackException: Transaction rolled back;
nested exception is:
 javax.transaction.TransactionRolledbackException: Transaction is ended due to timeout
 at com.ibm.ejs.csi.TransactionControlImpl.completeTxTimeout(TransactionControlImpl.java:1403)
 at com.ibm.ejs.csi.TransactionControlImpl.preInvoke(TransactionControlImpl.java:295)
 at com.ibm.ejs.container.EJSContainer.preInvokeActivate(EJSContainer.java:3402)
 at com.ibm.ejs.container.EJSContainer.preInvoke(EJSContainer.java:2874)
 at com.ibm.rfid.admin.model.ejb.session.EJSRemoteStatelessPrinterAdmin_84bad528.getPrintTemplateDetails
(EJSRemoteStatelessPrinterAdmin_84bad528.java:425)
 at com.ibm.rfid.admin.model.ejb.session._PrinterAdmin_Stub.getPrintTemplateDetails(
_PrinterAdmin_Stub.java:1245)
 at com.ibm.rfid.premises.supplychain.data.GenericPrintProfile.getTemplateName
(GenericPrintProfile.java:274)
 at com.ibm.rfid.premises.supplychain.data.GenericPrintProfile.createGenericXML
(GenericPrintProfile.java:236)
 at com.ibm.rfid.premises.supplychain.data.GenericPrintProfile.print
(GenericPrintProfile.java:80)
 at com.ibm.rfid.premises.supplychain.data.PrintRequestHandler.handleRequest
(PrintRequestHandler.java:135)
 at com.ibm.rfid.premises.supplychain.task.command.ejb.PrintRFIDTagCommandTaskBean.onMessage
(PrintRFIDTagCommandTaskBean.java:118)
 at com.ibm.ejs.jms.listener.MDBWrapper$PrivilegedOnMessage.run(MDBWrapper.java:302)
 at com.ibm.ws.security.util.AccessController.doPrivileged(AccessController.java:63)
 at com.ibm.ejs.jms.listener.MDBWrapper.callOnMessage(MDBWrapper.java:271)
 at com.ibm.ejs.jms.listener.MDBWrapper.onMessage(MDBWrapper.java:240)
 at com.ibm.mq.jms.MQSession.run(MQSession.java:1592)
 at com.ibm.ejs.jms.JMSSessionHandle.run(JMSSessionHandle.java:970)
 at com.ibm.ejs.jms.listener.ServerSession.connectionConsumerOnMessage(ServerSession.java:891)
 at com.ibm.ejs.jms.listener.ServerSession.onMessage(ServerSession.java:656)
 at com.ibm.ejs.jms.listener.ServerSession.dispatch(ServerSession.java:623)
 at sun.reflect.GeneratedMethodAccessor61.invoke(Unknown Source)
 at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
 at java.lang.reflect.Method.invoke(Method.java:615)
 at com.ibm.ejs.jms.listener.ServerSessionDispatcher.dispatch(ServerSessionDispatcher.java:37)
 at com.ibm.ejs.container.MDBWrapper.onMessage(MDBWrapper.java:96)
 at com.ibm.ejs.container.MDBWrapper.onMessage(MDBWrapper.java:132)
 at com.ibm.ejs.jms.listener.ServerSession.run(ServerSession.java:481)
 at com.ibm.ws.util.ThreadPool$Worker.run(ThreadPool.java:1469)
```

```
Caused by: javax.transaction.TransactionRolledbackException: Transaction is ended due to timeout
    at com.ibm.ws.Transaction.JTA.TranManagerImpl.completeTxTimeout(TranManagerImpl.java:576)
    at com.ibm.ws.Transaction.JTA.TranManagerSet.completeTxTimeout(TranManagerSet.java:625)
    at com.ibm.ejs.csi.TransactionControlImpl.completeTxTimeout(TransactionControlImpl.java:1395)
    ...
```

If you find this error, reduce the number of tags in your print job and submit the job again. If it still fails, continue reducing your tag count until the print job succeeds.

Oracle 11g exceptions in SystemOut.log file

If you use Oracle 11g, you may see the following exceptions in the WebSphere Application Server SystemOut.log file during WebSphere Premises Server startup:

```
[6/13/08 9:30:31:125 EDT] 0000001d jdbc E    Error while registering Oracle JDBC Diagnosability MBean.
 javax.management.MalformedObjectNameException: Invalid character '
 ' in value part of property
 at javax.management.ObjectName.construct(ObjectName.java:544)
    at javax.management.ObjectName.<init>(ObjectName.java:1312)
    at oracle.jdbc.driver.OracleDriver.registerMBeans(OracleDriver.java:303)
    at oracle.jdbc.driver.OracleDriver$1.run(OracleDriver.java:213)
    at java.security.AccessController.doPrivileged(AccessController.java:197)
    at oracle.jdbc.driver.OracleDriver.<clinit>(OracleDriver.java:209)
    at java.lang.J9VMInternals.initializeImpl(Native Method)
    at java.lang.J9VMInternals.initialize(J9VMInternals.java:194)
    at oracle.jdbc.pool.OracleDataSource.<clinit>(OracleDataSource.java:94)
    at java.lang.J9VMInternals.initializeImpl(Native Method)
    at java.lang.J9VMInternals.initialize(J9VMInternals.java:194)
    at java.lang.J9VMInternals.initialize(J9VMInternals.java:159)
    at java.lang.J9VMInternals.initialize(J9VMInternals.java:159)
    at java.lang.J9VMInternals.initialize(J9VMInternals.java:159)
    at java.lang.Class.newInstanceImpl(Native Method)
    at java.lang.Class.newInstance(Class.java:1328)
    at com.ibm.ws.rsadapter.DSConfigurationHelper.createDataSource(DSConfigurationHelper.java:1078)
    at com.ibm.ws.rsadapter.spi.WSRdbDataSource$6.run(WSRdbDataSource.java:1975)
    at com.ibm.ws.security.util.AccessController.doPrivileged(AccessController.java:118)
    at com.ibm.ws.rsadapter.spi.WSRdbDataSource.createNewDataSource(WSRdbDataSource.java:1971)
    at com.ibm.ws.rsadapter.spi.WSRdbDataSource.<init>(WSRdbDataSource.java:902)
    at com.ibm.ws.rsadapter.spi.WSManagedConnectionFactoryImpl.setDataSourceProperties(WSManagedConnectionFactoryImpl.java:1947)
    at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
    at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:79)
    at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
    at java.lang.reflect.Method.invoke(Method.java:618)
    at com.ibm.ejs.j2c.J2CUtilityClass.createMCFEntry(J2CUtilityClass.java:389)
    at com.ibm.ejs.j2c.ConnectionFactoryBuilderServerImpl.createMCFandPM(ConnectionFactoryBuilderServerImpl.java:551)
    at com.ibm.ejs.j2c.ConnectionFactoryBuilderServerImpl.processObjectInstance(ConnectionFactoryBuilderServerImpl.java:922)
    at com.ibm.ejs.j2c.ConnectionFactoryBuilderImpl.getObjectInstance(ConnectionFactoryBuilderImpl.java:618)
    at javax.naming.spi.NamingManager.getObjectInstance(NamingManager.java:316)
    at com.ibm.ws.naming.util.Helpers.processSerializedObjectForLookupExt(Helpers.java:896)
    at com.ibm.ws.naming.util.Helpers.processSerializedObjectForLookup(Helpers.java:705)
    at com.ibm.ws.naming.jndicos.CNContextImpl.processResolveResults(CNContextImpl.java:2093)
    at com.ibm.ws.naming.jndicos.CNContextImpl.doLookup(CNContextImpl.java:1947)
    at com.ibm.ws.naming.jndicos.CNContextImpl.doLookup(CNContextImpl.java:1862)
    at com.ibm.ws.naming.jndicos.CNContextImpl.lookupExt(CNContextImpl.java:1552)
    at com.ibm.ws.naming.util.IndirectJndiLookupObjectFactory$1.run(IndirectJndiLookupObjectFactory.java:372)
    at com.ibm.ws.security.util.AccessController.doPrivileged(AccessController.java:118)
    at com.ibm.ws.naming.util.IndirectJndiLookupObjectFactory.getObjectInstanceExt(IndirectJndiLookupObjectFactory.java:221)
    at com.ibm.ws.naming.util.IndirectJndiLookupObjectFactory.getObjectInstance(IndirectJndiLookupObjectFactory.java:149)
    at com.ibm.ws.naming.util.ResRefJndiLookupObjectFactory.getObjectInstance(ResRefJndiLookupObjectFactory.java:144)
    at javax.naming.spi.NamingManager.getObjectInstance(NamingManager.java:316)
    at com.ibm.ws.naming.util.Helpers.processSerializedObjectForLookupExt(Helpers.java:896)
    at com.ibm.ws.naming.urlbase.UrlContextHelper.processBoundObjectForLookup(UrlContextHelper.java:191)
    at com.ibm.ws.naming.java.javaURLContextRoot.processBoundObjectForLookup(javaURLContextRoot.java:406)
    at com.ibm.ws.naming.urlbase.UrlContextImpl.lookup(UrlContextImpl.java:1280)
    at com.ibm.ws.naming.java.javaURLContextImpl.lookup(javaURLContextImpl.java:384)
    at com.ibm.ws.naming.java.javaURLContextRoot.lookup(javaURLContextRoot.java:204)
    at com.ibm.ws.naming.java.javaURLContextRoot.lookup(javaURLContextRoot.java:144)
    at javax.naming.InitialContext.lookup(InitialContext.java:363)
    at com.ibm.ejs.container.BeanMetaData.doConnectionHandlePerformanceSettings(BeanMetaData.java:4719)
    at com.ibm.ws.runtime.component.EJBContainerImpl.processBean(EJBContainerImpl.java:1852)
    at com.ibm.ws.runtime.component.EJBContainerImpl.install(EJBContainerImpl.java:2860)
    at com.ibm.ws.runtime.component.EJBContainerImpl.start(EJBContainerImpl.java:3720)
    at com.ibm.ws.runtime.component.ApplicationMgrImpl.start(ApplicationMgrImpl.java:1303)
    at com.ibm.ws.runtime.component.DeployedApplicationImpl.fireDeployedObjectStart(DeployedApplicationImpl.java:1138)
    at com.ibm.ws.runtime.component.DeployedModuleImpl.start(DeployedModuleImpl.java:569)
    at com.ibm.ws.runtime.component.DeployedApplicationImpl.start(DeployedApplicationImpl.java:817)
    at com.ibm.ws.runtime.component.ApplicationMgrImpl.startApplication(ApplicationMgrImpl.java:949)
    at com.ibm.ws.runtime.component.ApplicationMgrImpl$AppInitializer.run(ApplicationMgrImpl.java:2122)
    at com.ibm.wsspi.runtime.component.WsComponentImpl$_AsynchInitializer.run(WsComponentImpl.java:342)
    at com.ibm.ws.util.ThreadPool$Worker.run(ThreadPool.java:1473)
```

If you see the following string in the SystemOut.log file, you need to download the patched ojdbc.jar file:

```
InternalOracl I DSRA8206I: JDBC driver version : 11.1.0.6.0-Production
```

Note: If there is a plus sign (+) at the end of the string, you are already running the patched file.

The patched ojdbc.jar file can be downloaded from Oracle:http://www.oracle.com/technology/software/tech/java/sqlj_jdbc/htdocs/jdbc_111060.html.

JMSResource exceptions in the SystemOut.log files on the central server and node servers

You may see the following exceptions in the WebSphere Application Server SystemOut.log files on the central server and on the cluster node servers after running the high availability installer:

```
[8/7/08 12:50:23:531 CST] 0000000a JMSResourceRe E   WMSG0902E: The WebSphere MQ JMS Binders have been disabled as either
the WebSphere MQ Client has not been installed, or the MQ_INSTALL_ROOT variable has not been set.
[8/7/08 12:50:23:531 CST] 0000000a ResourceMgrIm I   WSVR0049I: Binding IBMRFIDQM as jms/ibm.rfid.qm
[8/7/08 12:50:23:546 CST] 0000000a JMSResourceRe E   WMSG0902E: The WebSphere MQ JMS Binders have been disabled as either
the WebSphere MQ Client has not been installed, or the MQ_INSTALL_ROOT variable has not been set.
[8/7/08 12:50:23:546 CST] 0000000a ResourceMgrIm I   WSVR0049I: Binding EDGE.IN.QUEUE as jms/edge.in.q
[8/7/08 12:50:23:546 CST] 0000000a JMSResourceRe E   WMSG0902E: The WebSphere MQ JMS Binders have been disabled as either
the WebSphere MQ Client has not been installed, or the MQ_INSTALL_ROOT variable has not been set.
[8/7/08 12:50:23:562 CST] 0000000a ResourceMgrIm I   WSVR0049I: Binding EDGE.OUT.QUEUE as jms/edge.out.q
[8/7/08 12:50:23:562 CST] 0000000a JMSResourceRe E   WMSG0902E: The WebSphere MQ JMS Binders have been disabled as either
the WebSphere MQ Client has not been installed, or the MQ_INSTALL_ROOT variable has not been set.
[8/7/08 12:50:23:562 CST] 0000000a ResourceMgrIm I   WSVR0049I: Binding CONTROL.IN.QUEUE as jms/control.in.q
[8/7/08 12:50:23:578 CST] 0000000a JMSResourceRe E   WMSG0902E: The WebSphere MQ JMS Binders have been disabled as either
the WebSphere MQ Client has not been installed, or the MQ_INSTALL_ROOT variable has not been set.
[8/7/08 12:50:23:578 CST] 0000000a ResourceMgrIm I   WSVR0049I: Binding CONTROL.OUT.QUEUE as jms/control.out.q
[8/7/08 12:50:23:578 CST] 0000000a JMSResourceRe E   WMSG0902E: The WebSphere MQ JMS Binders have been disabled as either
the WebSphere MQ Client has not been installed, or the MQ_INSTALL_ROOT variable has not been set.
[8/7/08 12:50:23:593 CST] 0000000a ResourceMgrIm I   WSVR0049I: Binding TASK.QUEUE as jms/task.q
[8/7/08 12:50:23:593 CST] 0000000a JMSResourceRe E   WMSG0902E: The WebSphere MQ JMS Binders have been disabled as either
the WebSphere MQ Client has not been installed, or the MQ_INSTALL_ROOT variable has not been set.
[8/7/08 12:50:23:593 CST] 0000000a ResourceMgrIm I   WSVR0049I: Binding MANAGEMENT.QUEUE as jms/management.q
[8/7/08 12:50:23:609 CST] 0000000a JMSResourceRe E   WMSG0902E: The WebSphere MQ JMS Binders have been disabled as either
the WebSphere MQ Client has not been installed, or the MQ_INSTALL_ROOT variable has not been set.
[8/7/08 12:50:23:609 CST] 0000000a ResourceMgrIm I   WSVR0049I: Binding PERSISTENCE.QUEUE as jms/persistence.q
[8/7/08 12:50:23:609 CST] 0000000a JMSResourceRe E   WMSG0902E: The WebSphere MQ JMS Binders have been disabled as either
the WebSphere MQ Client has not been installed, or the MQ_INSTALL_ROOT variable has not been set.
[8/7/08 12:50:23:625 CST] 0000000a ResourceMgrIm I   WSVR0049I: Binding DEAD.MESSAGE.QUEUE as jms/dead.message.q
[8/7/08 12:50:23:625 CST] 0000000a JMSResourceRe E   WMSG0902E: The WebSphere MQ JMS Binders have been disabled as either
the WebSphere MQ Client has not been installed, or the MQ_INSTALL_ROOT variable has not been set.
[8/7/08 12:50:23:625 CST] 0000000a ResourceMgrIm I   WSVR0049I: Binding TAGMONITOR.OUT.QUEUE as jms/tagmonitor.out.q
[8/7/08 12:50:23:640 CST] 0000000a JMSResourceRe E   WMSG0902E: The WebSphere MQ JMS Binders have been disabled as either
the WebSphere MQ Client has not been installed, or the MQ_INSTALL_ROOT variable has not been set.
[8/7/08 12:50:23:640 CST] 0000000a ResourceMgrIm I   WSVR0049I: Binding ALE.TAG.INPUT.Q as jms/ale.tag.input.q
[8/7/08 12:50:23:640 CST] 0000000a JMSResourceRe E   WMSG0902E: The WebSphere MQ JMS Binders have been disabled as either
the WebSphere MQ Client has not been installed, or the MQ_INSTALL_ROOT variable has not been set.
[8/7/08 12:50:23:656 CST] 0000000a ResourceMgrIm I   WSVR0049I: Binding EDGE.PRINT.IN.Q as jms/edge.print.in.q
[8/7/08 12:50:23:656 CST] 0000000a JMSResourceRe E   WMSG0902E: The WebSphere MQ JMS Binders have been disabled as either
the WebSphere MQ Client has not been installed, or the MQ_INSTALL_ROOT variable has not been set.
[8/7/08 12:50:23:656 CST] 0000000a ResourceMgrIm I   WSVR0049I: Binding EDGE.OUTBYTES.Q as jms/edge.outbytes.q
[8/7/08 12:50:23:671 CST] 0000000a JMSResourceRe E   WMSG0902E: The WebSphere MQ JMS Binders have been disabled as either
the WebSphere MQ Client has not been installed, or the MQ_INSTALL_ROOT variable has not been set.
[8/7/08 12:50:23:671 CST] 0000000a ResourceMgrIm I   WSVR0049I: Binding ALE.REPORT.Q as jms/ale.report.q
[8/7/08 12:50:23:671 CST] 0000000a JMSResourceRe E   WMSG0902E: The WebSphere MQ JMS Binders have been disabled as either
the WebSphere MQ Client has not been installed, or the MQ_INSTALL_ROOT variable has not been set.
[8/7/08 12:50:23:687 CST] 0000000a ResourceMgrIm I   WSVR0049I: Binding IBMDCQM as jms/ibm.dc.qm
[8/7/08 12:50:23:687 CST] 0000000a JMSResourceRe E   WMSG0902E: The WebSphere MQ JMS Binders have been disabled as either
the WebSphere MQ Client has not been installed, or the MQ_INSTALL_ROOT variable has not been set.
[8/7/08 12:50:23:687 CST] 0000000a ResourceMgrIm I   WSVR0049I: Binding DC.IN.QUEUE as jms/dc.in.q
[8/7/08 12:50:23:703 CST] 0000000a JMSResourceRe E   WMSG0902E: The WebSphere MQ JMS Binders have been disabled as either
the WebSphere MQ Client has not been installed, or the MQ_INSTALL_ROOT variable has not been set.
[8/7/08 12:50:23:703 CST] 0000000a ResourceMgrIm I   WSVR0049I: Binding DC.OUT.QUEUE as jms/dc.out.q
[8/7/08 12:50:23:703 CST] 0000000a JMSResourceRe E   WMSG0902E: The WebSphere MQ JMS Binders have been disabled as either
the WebSphere MQ Client has not been installed, or the MQ_INSTALL_ROOT variable has not been set.
[8/7/08 12:50:23:718 CST] 0000000a ResourceMgrIm I   WSVR0049I: Binding ENTERPRISE.IN.QUEUE as jms/enterprise.in.q
[8/7/08 12:50:23:718 CST] 0000000a JMSResourceRe E   WMSG0902E: The WebSphere MQ JMS Binders have been disabled as either
the WebSphere MQ Client has not been installed, or the MQ_INSTALL_ROOT variable has not been set.
[8/7/08 12:50:23:718 CST] 0000000a ResourceMgrIm I   WSVR0049I: Binding ENTERPRISE.OUT.QUEUE as jms/enterprise.out.q
[8/7/08 12:50:23:734 CST] 0000000a JMSResourceRe E   WMSG0902E: The WebSphere MQ JMS Binders have been disabled as either
the WebSphere MQ Client has not been installed, or the MQ_INSTALL_ROOT variable has not been set.
[8/7/08 12:50:23:734 CST] 0000000a ResourceMgrIm I   WSVR0049I: Binding KIMONO.RESPONSE.Q as jms/kimono.response.q
```

To resolve these errors, restart the central server and the cluster.

Scheduler exception in the SystemOut.log file when migrating

You may see the following exception in the WebSphere Application Server SystemOut.log files when you migrate from WebSphere Premises Server 6.1 to version 6.1.0.1:

```
[8/30/08 15:40:24:984 CST] 00000041 SchedulerDaem E   SCHD0104E: The Scheduler poll daemon
AMITSCHEDULER (sched/Amit) failed to load tasks from the database due to an exception:
com.ibm.websphere.scheduler.SchedulerNotAvailableException: com.ibm.db2.jcc.c.SqlException:
DB2 SQL error: SQLCODE: -727, SQLSTATE: 56098, SQLERRMC: 2;-204;42704;DB2ADMIN.SCHEDTASK
 at com.ibm.ws.scheduler.TaskStoreImpl.findTasksBeforeNotComplete(TaskStoreImpl.java:1161)
 at com.ibm.ws.scheduler.SchedulerDaemonImpl.poll(SchedulerDaemonImpl.java:653)
 at com.ibm.ws.scheduler.SchedulerDaemonImpl.run(SchedulerDaemonImpl.java:451)
 at com.ibm.ws.asynchbeans.J2EEContext.run(J2EEContext.java:761)
 at com.ibm.ws.asynchbeans.WorkWithExecutionContextImpl.go(WorkWithExecutionContextImpl.java:218)
 at com.ibm.ws.asynchbeans.ABWorkItemImpl.run(ABWorkItemImpl.java:158)
 at java.lang.Thread.run(Thread.java:810)
Caused by: com.ibm.db2.jcc.c.SqlException: DB2 SQL error: SQLCODE: -727, SQLSTATE: 56098,
SQLERRMC: 2;-204;42704;DB2ADMIN.SCHEDTASK
 at com.ibm.db2.jcc.c.kh.c(kh.java:1660)
 at com.ibm.db2.jcc.c.kh.a(kh.java:1224)
 at com.ibm.db2.jcc.b.db.n(db.java:737)
 at com.ibm.db2.jcc.b.db.i(db.java:257)
 at com.ibm.db2.jcc.b.db.c(db.java:53)
 at com.ibm.db2.jcc.b.t.c(t.java:46)
 at com.ibm.db2.jcc.b.sb.g(sb.java:154)
 at com.ibm.db2.jcc.c.kh.o(kh.java:1219)
 at com.ibm.db2.jcc.c.lh.d(lh.java:2436)
 at com.ibm.db2.jcc.c.lh.S(lh.java:432)
 at com.ibm.db2.jcc.c.lh.executeQuery(lh.java:415)
 at com.ibm.ws.rsadapter.jdbc.WSJdbcPreparedStatement.pmiExecuteQuery(WSJdbcPreparedStatement.java:878)
 at com.ibm.ws.rsadapter.jdbc.WSJdbcPreparedStatement.executeQuery(WSJdbcPreparedStatement.java:559)
 at com.ibm.ws.scheduler.TaskStoreImpl.executeQueryWithRetry(TaskStoreImpl.java:1729)
 at com.ibm.ws.scheduler.TaskStoreImpl$ExecuteQueryPriviledged.run(TaskStoreImpl.java:1616)
```

```
    at java.security.AccessController.doPrivileged(AccessController.java:246)
    at com.ibm.ws.scheduler.TaskStoreImpl.executePrivilegedQueryWithRetry(TaskStoreImpl.java:1785)
    at com.ibm.ws.scheduler.TaskStoreImpl.findTasksBeforeNotComplete(TaskStoreImpl.java:1154)
    ... 6 more
```

This error occurs during the uninstallation of WebSphere Premises Server 6.1 when you are migrating and can be safely ignored.

Shared library exception in SystemOut.log files on cluster members

You may see the following exception in the cluster member SystemOut.log files when running a high availability topology:

```
[8/12/08 9:08:00:765 EDT] 0000000a ModuleManifes E   UTLS0002E:
The shared library PremisesClientAPI contains a classpath entry which does
not resolve to a valid jar file, the library jar file is expected to be found at
C:\Program Files\IBM\RFID\premises\api\lib\Rfid.jar.
[8/12/08 9:08:00:781 EDT] 0000000a ModuleManifes E   UTLS0002E:
The shared library PremisesClientAPI contains a classpath entry which does
not resolve to a valid jar file, the library jar file is expected to be found at
C:\Program Files\IBM\RFID\premises\api\lib\xsdbeans.jar.
[8/12/08 9:08:00:781 EDT] 0000000a ModuleManifes E   UTLS0002E:
The shared library PremisesClientAPI contains a classpath entry which does
not resolve to a valid jar file, the library jar file is expected to be found at
C:\Program Files\IBM\RFID\premises\api\lib\ibmrfid_premises_api_client.jar.
[8/12/08 9:08:00:796 EDT] 0000000a ModuleManifes E   UTLS0002E:
The shared library PremisesClientAPI contains a classpath entry which does
not resolve to a valid jar file, the library jar file is expected to be found at
C:\Program Files\IBM\RFID\premises\api\lib\ibmrfid_premises_api_ejbClient.jar.
[8/12/08 9:08:00:796 EDT] 0000000a ModuleManifes E   UTLS0002E:
The shared library PremisesClientAPI contains a classpath entry which does
not resolve to a valid jar file, the library jar file is expected to be found at
C:\Program Files\IBM\RFID\premises\api\lib\ibmrfid_premises_api_ws.jar.
[8/12/08 9:08:00:812 EDT] 0000000a ModuleManifes E   UTLS0002E:
The shared library PremisesClientAPI contains a classpath entry which does
not resolve to a valid jar file, the library jar file is expected to be found at
C:\Program Files\IBM\RFID\premises\api\lib\ibmrfid_premises_util.jar.
[8/12/08 9:08:00:812 EDT] 0000000a ModuleManifes E   UTLS0002E:
The shared library PremisesClientAPI contains a classpath entry which does
not resolve to a valid jar file, the library jar file is expected to be found at
C:\Program Files\IBM\RFID\premises\api\lib\com.ibm.rfid.epcg.tds.jar.
[8/12/08 9:08:00:828 EDT] 0000000a ModuleManifes E   UTLS0002E:
The shared library PremisesClientAPI contains a classpath entry which does
not resolve to a valid jar file, the library jar file is expected to be found at
C:\Program Files\IBM\RFID\premises\api\lib\org.apache.regexp.jar.
[8/12/08 9:08:00:828 EDT] 0000000a ModuleManifes E   UTLS0002E:
The shared library PremisesClientAPI contains a classpath entry which does
not resolve to a valid jar file, the library jar file is expected to be found at
C:\Program Files\IBM\RFID\premises\api\lib\ibmrfid_common_utils.jar.
[8/12/08 9:08:00:843 EDT] 0000000a ModuleManifes E   UTLS0002E:
The shared library TaskAgentRuntime contains a classpath entry which does
not resolve to a valid jar file, the library jar file is expected to be found at
C:\Program Files\IBM\RFID\premises\api\lib\Amit3.0Common.jar.
[8/12/08 9:08:00:843 EDT] 0000000a ModuleManifes E   UTLS0002E:
The shared library TaskAgentRuntime contains a classpath entry which does
not resolve to a valid jar file, the library jar file is expected to be found at
C:\Program Files\IBM\RFID\premises\api\lib\com.ibm.rfid.epcg.tds.jar.
[8/12/08 9:08:00:843 EDT] 0000000a ModuleManifes E   UTLS0002E:
The shared library TaskAgentRuntime contains a classpath entry which does
not resolve to a valid jar file, the library jar file is expected to be found at
C:\Program Files\IBM\RFID\premises\api\lib\org.apache.regexp.jar.
[8/12/08 9:08:00:859 EDT] 0000000a ModuleManifes E   UTLS0002E:
The shared library TaskAgentRuntime contains a classpath entry which does
not resolve to a valid jar file, the library jar file is expected to be found at
C:\Program Files\IBM\RFID\premises\api\lib\ibmse_common_util.jar.
[8/12/08 9:08:00:859 EDT] 0000000a ModuleManifes E   UTLS0002E:
The shared library TaskAgentRuntime contains a classpath entry which does
not resolve to a valid jar file, the library jar file is expected to be found at
C:\Program Files\IBM\RFID\premises\api\lib\ibmse_taskagent_runtime.jar.
[8/12/08 9:08:00:875 EDT] 0000000a ModuleManifes E   UTLS0002E:
The shared library TaskAgentRuntime contains a classpath entry which does
not resolve to a valid jar file, the library jar file is expected to be found at
C:\Program Files\IBM\RFID\premises\api\lib\ibmse_event_model_uuid.jar.
[8/12/08 9:08:00:875 EDT] 0000000a ModuleManifes E   UTLS0002E:
The shared library TaskAgentRuntime contains a classpath entry which does
not resolve to a valid jar file, the library jar file is expected to be found at
C:\Program Files\IBM\RFID\premises\api\lib\ibmse_event_model_converter.jar.
[8/12/08 9:08:00:890 EDT] 0000000a ModuleManifes E   UTLS0002E:
The shared library TaskAgentRuntime contains a classpath entry which does
not resolve to a valid jar file, the library jar file is expected to be found at
C:\Program Files\IBM\RFID\premises\api\lib\ibmse_event_model.jar.
[8/12/08 9:08:00:890 EDT] 0000000a ModuleManifes E   UTLS0002E:
The shared library TaskAgentRuntime contains a classpath entry which does
not resolve to a valid jar file, the library jar file is expected to be found at
C:\Program Files\IBM\RFID\premises\api\lib\ibmrfid_common_utils.jar.
```

This error can be safely ignored; however, to remove these messages from the file, copy all JAR files from the central server *IBM_RFID_HOME*\premises\api\lib to the same director structure. The shared libraries PremisesClientAPI and TaskAgentRuntime are intended to customize applications using WebSphere Premises Server.

Contacting IBM Support

IBM Support provides assistance with product defects.

Before you begin

Before contacting IBM Support, your company must have an active IBM software maintenance contract, and you must be authorized to submit problems to IBM. For information about the types of maintenance contracts available, see "Enhanced Support" in the *Software Support Handbook* at: http://techsupport.services.ibm.com/ guides/services.html

About this task

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 help, see the "Contacting IBM" in the *Software Support Handbook*: http://techsupport.services.ibm.com/guides/beforecontacting.html
2. Gather diagnostic information.
3. Submit your problem to IBM Support in one of the following ways:
   - Using IBM Support Assistant (ISA):
   - Online: Click the **Report problems** tab on the IBM Software Support site: http://www.ibm.com/software/support/probsub.html
   - By phone: For the phone number to call in your country, go to the Contacts page of the *Software Support Handbook*: http://techsupport.services.ibm.com/ guides/contacts.html

What to do next

If the problem 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 Software 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 web site daily, so that other users who experience the same problem can benefit from the same resolution.

Chapter 10. Reference information

These topics are provided as additional reference information to help you.

Accessibility features for WebSphere Premises Server

Accessibility features help users who have a physical disability, such as restricted mobility or limited vision, to use information technology products successfully.

Accessibility features

The following list includes the major accessibility features in WebSphere Premises Server. These features support:

- Keyboard-only operation.
- Interfaces that are commonly used by screen readers.

Tip: The WebSphere Premises Server Information Center and its related publications are accessibility-enabled for screen readers. You can operate all features using the keyboard instead of the mouse.

Keyboard navigation

This product and its components uses standard Microsoft Windows navigation keys.

IBM and accessibility

See the *Human Ability and Accessibility Center* for more information about the commitment that IBM has to accessibility.

Additional information

The following additional resources are available online.

IBM Support Assistant

WebSphere Premises Server provides a plug-in to the IBM Support Assistant. The IBM Support Assistant is a collection of pointers to various IBM support resources online. The WebSphere Premises Server plug-in for IBM Support Assistant contains pointers to additional support resources that are specific to WebSphere Premises Server. For more information on how to download and install the IBM Support Assistant and the corresponding WebSphere Premises Server plug-in, refer to "Using IBM Support Assistant" on page 380.

WebSphere software

- WebSphere courses, training, and certification: http://www.ibm.com/software/ info1/websphere/index.jsp?tab=education/index
- WebSphere education: http://www.ibm.com/developerworks/websphere/ education/enablement/

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 6.1 Information Center: http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp

WebSphere MQ

- WebSphere MQ product support page: http://www.ibm.com/software/integration/wmq/support/
- WebSphere MQ information library: http://www.ibm.com/software/integration/wmq/library/

DB2 for Linux, UNIX, and Windows systems

- DB2 for Linux, UNIX, and Windows (DB2) product support page: http://www.ibm.com/software/data/db2/support/db2_9/
- Information management training and certification: http://www.ibm.com/software/data/education
- Information management information library: http://www.ibm.com/software/data/sw-library/
- DB2 for Linux, UNIX, and Windows 9.1 Information Center:http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp

Redbooks

- WebSphere Redbooks Domain: http://publib-b.boulder.ibm.com/Redbooks.nsf/portals/WebSphere
- WebSphere RFID Redbooks query: http://publib-b.boulder.ibm.com/cgi-bin/searchsite.cgi?query=websphere+rfid

Tivoli software

- Tivoli training and certification: http://www.ibm.com/software/tivoli/education/

Tivoli Enterprise Console

- Tivoli Enterprise Console product support page: http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliEnterpriseConsole.html
- Tivoli Enterprise Console 3.9 Information Center: http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp?toc=/com.ibm.itec.doc_3.9/toc.xml

Tivoli Provisioning Manager for Software

- Tivoli Provisioning Manager for Software product support page: http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliProvisioningManagerforSoftware.html
- Tivoli Provisioning Manager for Software 5.1.0.2 Information Center: http://publib.boulder.ibm.com/infocenter/tivihelp/v17r1/index.jsp?topic=/com.ibm.tivoli.tpm.doc_5.1.0.2/welcome/tpmsofthome.htm

IBM Tivoli Monitoring

- IBM Tivoli Monitoring product support page: http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliMonitoring.html

- IBM Tivoli Monitoring 6.1 Information Center: http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/index.jsp

IBM Tivoli Monitoring for Databases

- IBM Tivoli Monitoring for Databases product support page: http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliMonitoringforDatabases.html
- IBM Tivoli Monitoring for Databases 6.1 Information Center: http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/index.jsp?toc=/com.ibm.itmfd.doc/toc.xml

Copyright notice and trademarks

Copyright notice

Trademarks

Alien is a trademark or registered trademark of Alien Technology Corporation in the U.S and other countries.

Zebra is a registered trademark of ZIH Corporation.

Intermec is a registered trademark of Intermec Technologies Corporation.

Symbol is a registered trademarks of Symbol Technologies Corporation.

SAMSys is a product of SAMSys Technologies Inc.

OSGi is a registered trademark of OSGi Alliance.

Loftware is a registered trademark of Loftware, Inc.

Bartender is a registered trademark of Seagull Scientific, Inc.

Electronic Product Code (EPC) is a trademark of EPCglobal.

Application Level Events (ALE) is a product of EPCglobal.

Other company, product, and service names may be trademarks or service marks of others.

Readers' Comments — We'd Like to Hear from You

Premises Server
WebSphere Premises Server Information Center
Version 6.1.0.1

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.   E-mail address

IBM®

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 Corporation
Information Development
Department 9BSA
P.O. Box 12195
Research Triangle Park, NC   27709-9990

Fold and Tape   **Please do not staple**   Fold and Tape