



June 2007

This edition applies to IBM WebSphere RFID version 6, release 0, modification 0. This edition applies to all subsequent releases and modifications until otherwise indicated in new editions.

A form for readers' comments appears at the back of this publication. If the form has been removed, address your comments to:

International Business Machines Corporation
Department 6R4A
P.O. Box 12195
Research Triangle Park, North Carolina
27709-2195

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© Copyright International Business Machines Corporation 2007. All rights reserved.

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

Contents

Chapter 1. Welcome to the

documentation 1

Intended audience	1
Conventions	1
Publications terms of use	2

Chapter 2. System overview 5

What is RFID?	5
RFID components.	5
WebSphere RFID Premises Server	5
Data Capture and Delivery	6
Example usage scenarios	11
Print, Verify, and Ship example usage scenario.	11
Standard dock door receiving example usage scenario	13
Enhanced dock door receiving example usage scenario	14

Chapter 3. Installing and configuring 19

Installing the product	19
Planning your server topology	19
Packaging	20
Identifying hardware and software requirements	21
Prerequisites	22
Installing WebSphere RFID Premises Server	25
Installing Device Manager server for WebSphere RFID Premises Server	30
Installing silently	39
Installing using Tivoli Configuration Manager.	39
Installing and enabling IBM Tivoli License Compliance Manager	42
Installing the toolkits	43
Toolkit prerequisites	43
Installing WebSphere RFID Premises Server Toolkit	44
Installing IBM RFID Data Transformation Toolkit for WebSphere RFID Premises Server.	44
Installing IBM Data Capture and Delivery Toolkit for WebSphere RFID Premises Server	45
Configuring the IBM Data Capture and Delivery Toolkit for WebSphere RFID Premises Server	46
Installing the fix pack for WebSphere RFID Premises Server	49
Verifying the installation	50
Creating a cluster for WebSphere RFID Premises Server	51
Planning your cluster topology	51
Installing a cluster	52
Installing the WebSphere Application Server log file adapters	58
Installing the edge controller heartbeat log file adapters	59
Uninstalling the product	60
Uninstalling the fix pack for WebSphere RFID Premises Server	61

Uninstalling the toolkits	61
Uninstalling the WebSphere RFID Premises Server Toolkit.	61
Uninstalling the IBM RFID Data Transformation Toolkit for WebSphere RFID Premises Server	62
Uninstalling the IBM Data Capture and Delivery Toolkit for WebSphere RFID Premises Server	62
Migrating to WebSphere RFID Premises Server 6.0.x from a previous version	63
Enabling security with WebSphere Application Server	64

Chapter 4. Administering 73

WebSphere RFID Premises Server Administrative Console overview	73
Opening the WebSphere RFID Premises Server Administrative Console	74
Managing your Data Capture and Delivery configuration	75
Working with Data Capture and Delivery agents	76
Working with Data Capture and Delivery devices	87
Working with Data Capture and Delivery locations	91
Working with Data Capture and Delivery contacts	96
Working with Data Capture and Delivery controllers	98
Understanding Data Capture and Delivery PIDs and Factory PIDS	102
Importing the Data Capture and Delivery configuration file	102
Working with Data Capture and Delivery print templates	113
Working with Data Capture and Delivery update sites	115
Managing your WebSphere RFID Device Infrastructure configuration.	116
Modifying the property values of agents	116
Working with readers	125
Working with printers	128
Working with print templates	133
Working with locations	136
Working with location contacts	139
Working with controllers	140
Managing event processing.	143
Working with event templates.	143
Working with output channels.	145
Working with tasks	147
Managing the EPC configuration	149
Working with pack types	149
Working with profiles	155
Working with serial numbers	157
Working with the EPCglobal company prefix index	160
Reporting	162

Viewing tags	162
Viewing configuration variables	163
Disabling tag aggregation	164
Disabling tag persistence	164
Understanding Application Ping	165
Setting the delete filter for Data Capture and Delivery	165
Verifying the WebSphere RFID Premises Server installation and setup.	166
Starting a simulated reader	167
Stopping a simulated reader	167
Resetting a simulated reader	167
Running the simulated reader and simulated WebSphere RFID Premises Server	168

Chapter 5. Developing an IBM RFID solution.	169
WebSphere RFID Premises Server API	169

Chapter 6. Tuning	171
Changing MQ settings to improve performance	171
Disabling ALE messages.	172
Increasing memory used by RFID Data Transformation	172
Tuning the databases to improve performance	172
Tuning Oracle	173
Tuning the timeout value for a tag printer.	176

Chapter 7. Print, Verify, and Ship . . .	179
Configuring printers	180
Adding and configuring a logical printer	181
Configuring physical printers	183
Creating print templates.	184
Creating custom templates	185
Creating properties files for print templates	186
Configuring EPC commissioning details	188
Configuring EPC conversions	188
Substitution variables for template properties files	191
Using the Print, Verify, and Ship Reference User Interface	192

Opening the user interface	193
Printing RFID tag labels.	193
Associating labels with containers	199
Validating outgoing shipments	202
Generating reports	203

Chapter 8. Troubleshooting	205
Debugging and troubleshooting Data Capture and Delivery	205
Verifying that the WebSphere RFID Premises Server is generating correct XML	205
Enabling tracing for your Equinox or Eclipse launch configuration	205
Suspecting that MicroBroker is the problem	206
Suspecting a problem within your WebSphere MQ environment	207
Monitoring messages using the Edge Event Monitor tool.	207
Using Notification Service to troubleshoot.	207
Using IBM Support Assistant	207
Installing IBM Support Assistant	208
Gathering information	208
Error messages and logging	208
What is QOS?	209
What are heartbeats?	210
Log file locations and settings	210
How to modify logging levels and output.	212
Error messages	214
Troubleshooting tips	219
Troubleshooting techniques.	225
MQ queues	225
Troubleshooting MicroBroker issues	227

Chapter 9. Reference information . . .	229
Accessibility features for WebSphere RFID Premises Server	229
Additional information	229
Copyright notice and trademarks.	230

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® RFID Premises Server solution.

This information center assumes that users have prior knowledge of or proficiency with WebSphere Application Server, WebSphere MQ, and DB2 Universal Database™. 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 229 section.

Conventions

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

These conventions have the following meanings.



Bold	Boldface type indicates commands or graphical user interface (GUI) controls such as names of fields, buttons, or menu choices.
<i>Italic</i>	<i>Italic type</i> 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. In WebSphere RFID Premises Server 6.0 and later, this functionality can run as part of the WebSphere RFID 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 WebSphere RFID Device Infrastructure, the term edge controller is used primarily in this document.

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 RFID Premises Server. On Windows, typing `echo %IBM_RFID_HOME%` at a command prompt shows you the path where WebSphere RFID 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 RFID Premises Server is installed, such as `/opt/IBM/RFID`.
- *DEVICE_MANAGER_HOME* is a variable for Windows and Linux that is defined during the installation of Device Manager server when using the WebSphere RFID Premises Server installation wizard. On Windows, typing `echo %DEVICE_MANAGER_HOME%` at a command prompt shows you the path where Device Manager server is installed, such as `C:\Program Files\IBM\RFID\DeviceManager`. On Linux, typing `echo $DEVICE_MANAGER_HOME` at a command prompt shows you the path where Device Manager server is installed, such as `/opt/IBM/RFID/DeviceManager`.
- *IHS_HOME* is a variable representing the installation path of IBM HTTP Server.
- *WAS_PROFILE_HOME* is a variable representing the installation path of WebSphere Application Server.

For reference, the WebSphere RFID 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 RFID Premises Server and its related products to implement RFID-based solutions for business problems. RFID stands for Radio Frequency Identification. To learn more about this technology, refer to “What is RFID?”

A RFID solution consists of I/O devices including RFID devices, such as tag readers, edge controllers, and WebSphere RFID Premises Server. For more descriptions of supported scenarios in which these devices and servers are used, refer to “Example usage scenarios” on page 11.

WebSphere RFID 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 RFID 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 RFID devices, edge controllers, and WebSphere RFID Premises Server, refer to the topics under “RFID components.”

What is RFID?

RFID stands for Radio Frequency Identification. This technology can be used to track goods in the supply chain, track the pedigree of pharmaceuticals, manage business assets such as cars or computers, and many other potential business applications.

RFID is based on “smart tags.” An RFID tag contains a microscopic chip that stores information about an item to which it is attached. The tag also contains a small, flat antenna. When the RFID tag is activated by a tag reader, the antenna sends out information as radio waves from the chip to the tag reader. Tag information varies by manufacturer, but most likely consists of a unique identification number with the make, manufacturer, and model of the item.

RFID components

WebSphere RFID Premises Server

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

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

WebSphere RFID Premises Server consists of WebSphere Application Server, DB2 Universal Database (or Oracle), WebSphere MQ, MicroBroker, RFID Data Transformation, Data Capture and Delivery, and a Web application for the administrative console.

The RFID Data Transformation is the bridge between MicroBroker and WebSphere MQ. The IBM RFID Data Transformation Toolkit for WebSphere RFID Premises Server, which runs in the Eclipse Equinox environment, allows you to create OSGi bundles like those shipped with WebSphere RFID Premises Server.

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 RFID Premises Server allows you to customize the sample agents shipped with the product.

WebSphere RFID Premises Server also includes Tivoli® Resource Models for WebSphere Application Server and WebSphere MQ that monitor WebSphere RFID Premises Server. Software Package Definition (SPD) files are also provided for the WebSphere RFID Premises Server components, for optional installation using Tivoli Configuration Manager. WebSphere RFID Premises Server also includes several example applications, including the Print, Verify, and Ship Reference User Interface, Standard Dock Door Receiving, and Enhanced Dock Door Receiving example applications.

Data Capture and Delivery

Data Capture and Delivery communicates with RFID devices and then communicates that information to WebSphere RFID 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 RFID 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 RFID 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. In WebSphere RFID Premises Server 6.0 and later, this functionality can run as part of the WebSphere RFID 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 WebSphere RFID Device Infrastructure, the term edge controller is used primarily in this document.

Data Capture and Delivery controllers control I/O devices, filter tag information, and send tag information to the WebSphere RFID 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 RFID Premises Server through the MicroBroker.

WebSphere RFID Premises Server supports several Data Capture and Delivery controllers. For information on the IBM RFID device validation program, supported devices, readers, and RFID device manufacturers, refer to: <http://www.ibm.com/solutions/sensors>

The components include:

- Device Adapters - Interface to RFID device functions.
- I/O Adapters - Interface to I/O device functions.
- Filter Agents - Modules that filter and aggregate tag data before passing the data to the MicroBroker and up to the WebSphere RFID Premises Server.
- Controller Agents - Modules that 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 Technology 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 RFID device validation program, supported devices, readers, and RFID device manufacturers, refer to: <http://www.ibm.com/solutions/sensors>

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 9 for more information about these profiles.

I/O Agents

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

Printer Agents

Agents for each printer adapter, connecting the adapter to the messaging service.

Note: Printer agents and adapters are not shipped with WebSphere RFID Premises Server 6.0 and later; however, if you are using a WebSphere RFID Premises Server 1.1 edge controller, they are still supported.

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:

- Simple: Once the portal is activated, this matrix will cycle the reader on and off.
- sDDR or Simple 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 13.
- eDDR or 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 14.

Filter Agents

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

For information on the IBM RFID device validation program, supported devices, readers, and RFID device manufacturers, refer to: <http://www.ibm.com/solutions/sensors>

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.

Printer Adapters

Interface with the printers and supported only with WebSphere RFID Device Infrastructure version 1.1.1. This module is the API-level interface to a specific make and model of a tag printer. It enables complete access to the capabilities of the printer. There is a printer adapter for each printer model.

Note: Printer adapters are not shipped with WebSphere RFID Premises Server 6.0 and later; however, if you are using a WebSphere RFID Premises Server 1.1 edge controller, they are still supported.

For information on the IBM RFID device validation program, supported devices, readers, and RFID device manufacturers, refer to: <http://www.ibm.com/solutions/sensors>

MicroBroker

MicroBroker is a publication and subscription engine for the RFID system.

Note: The term, "topic," here means any message that is sent through the MicroBroker. Topics can include commands, I/O events, or status messages.

RFID agents publish and subscribe to topics through the MicroBroker. For example, the controller agent subscribes to I/O topics and publishes topics that correspond to those subscribed topics. For instance, when the motion sensor is triggered, a "motion-detected" topic is published. The controller agent receives this topic and, as a result, publishes a topic to activate the tag reader antennae.

The WebSphere RFID Premises Server solution provides a set of example agents. You can use the set of example agents or customize them to fit your specific business needs. The example agents are written using the MicroBroker Application Framework. For more information about the example RFID agents and how to customize them using the MicroBroker Application Framework, refer to the help documentation installed with the IBM Data Capture and Delivery Toolkit for WebSphere RFID Premises Server.

For more information about the usage scenarios implemented by the example RFID agents, refer to the section entitled "Example usage scenarios" on page 11.

Device Kit

The Device Kit is a core component of IBM Data Capture and Delivery Toolkit for WebSphere RFID 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/>

Example usage scenarios

This topic provides links to the included product usage scenarios. Usage scenarios provide an outline of the events that occur when a user or the application performs a particular action.

Print, Verify, and Ship example usage scenario

The IBM WebSphere RFID 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.

Note: Print, Verify, and Ship is not shipped with WebSphere RFID Premises Server 6.0. However, if you are using WebSphere RFID Device Infrastructure 1.1.1, it is still supported.

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 RFID 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*. 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*.

Tag labels are printed based on print templates created in the WebSphere RFID Premises Server Administrative Console. You can print tag labels using either a logical or a physical tag printer. A logical tag printer is connected to Print, Verify,

and Ship through a third-party software labeling system, such as BarTender or Software Labeling System. However, you can develop and add adapters for other logical printers. A physical tag printer is connected to Print, Verify, and Ship through an edge controller. For additional information about logical and physical tag printers, see *Working with printers*.

WebSphere RFID 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.

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 RFID 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. The printer can be a logical or a physical printer.
 - 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 drop-down 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, a EPC URN for an sgtin 64 tag would be: urn:epc:tag:sgtin-64:0.1234567.10050.1
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 RFID 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.

Standard dock door receiving example usage scenario

IBM WebSphere RFID 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 RFID Premises Server or in RFID 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. In WebSphere RFID Premises Server 6.0 and later, this functionality can run as part of the WebSphere RFID 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 WebSphere RFID Device Infrastructure, the term edge controller is used primarily in this document.

The following steps describe the usage scenario. The 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 RFID Premises Server.

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 RFID 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 filter agent receives the tag information from the messaging service.
8. The filter 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 RFID Premises Server.
10. The tag information is received by the Event server application running on the WebSphere RFID 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 expected 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 RFID 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

IBM WebSphere RFID 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. In WebSphere RFID Premises Server 6.0 and later, this functionality can run as part of the WebSphere RFID 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 WebSphere RFID Device Infrastructure, the term edge controller is used primarily in this document.

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 RFID 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.

To begin and throughout the process, the HealthCheckAgent checks the availability of the RFID hardware and software for readiness, specifically, the reader and the status of the sensors, and it checks the availability of WebSphere RFID Premises Server and the back-end system. The ApplicationPingAgent is responsible for checking WebSphere RFID Premises Server and the back end. The Data Capture and Delivery controller passes a token item (a message with a timestamp) to WebSphere RFID Premises Server and from there it might be forwarded to the integration domain; 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 RFID 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 residing 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 RFID Premises Server
 - a back-end system
- The system is active, and the portal is 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 RFID 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 RFID 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 RFID 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 "Aked" 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 RFID Premises Server.
11. The aggregation 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 RFID Premises Server, and then clears the list.
17. The WebSphere RFID 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 "Aked" 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 RFID 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 RFID 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.

Chapter 3. Installing and configuring

These topics describe how to install WebSphere RFID Premises Server.

Installing the product

This topic contains an overview of the steps required for installing and configuring WebSphere RFID Premises Server.

Before you begin

Remember: If your WebSphere RFID Premises Server is running on a Linux platform, you must be a root user to install, uninstall, and back up your system.

Read through this topic, and its related topics, to prepare for installation and to make yourself familiar with installation options, before you use the installation tools.

- “Planning your server topology”
- “Identifying hardware and software requirements” on page 21 and the WebSphere RFID Premises Server system requirements page
- Installation prerequisites
- “Installing WebSphere RFID Premises Server” on page 25
- “Installing Device Manager server for WebSphere RFID Premises Server” on page 30
- “Installing silently” on page 39

Installing

Follow these high-level steps to install a WebSphere RFID Premises Server solution. Follow the links for more details on how to perform each step.

1. Install the product. Or, optionally, install the product using Tivoli Configuration Manager.
2. Verify the installation.

Uninstalling

If you need to uninstall WebSphere RFID Premises Server, refer to “Uninstalling the product” on page 60.

Planning your server topology

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

Installation scenarios

During the product installation, you are prompted for a **Typical** or **Custom** installation. A **Typical** installation installs both WebSphere RFID Premises Server

and an embedded Device Manager server. If you choose a **Custom** installation, then you have the choice of installing either WebSphere RFID Premises Server or Device Manager server.

When planning your server topology, you have the option of installing both the WebSphere RFID Premises Server and the Device Manager server on the same server in your environment, or you can install the Device Manager server on a separate server.

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

Important: If you want to install Device Manager server on a server separate from WebSphere RFID Premises Server, be sure to install Device Manager server before installing WebSphere RFID Premises Server.

Packaging

WebSphere RFID Premises Server includes the following software products.

- CD 1 - Quick Start, including product documentation
- CD 2 - WebSphere Application Server 6.0 for Windows
- CD 3 - WebSphere Application Server 6.0 Refresh Pack 2 for Windows
- CD 4 - WebSphere Application Server 6.0.2 Fix Pack 15 and interim fix PK32968 for Windows
- CD 5 - WebSphere Application Server 6.0 Edge Components for Windows (optional)
- CD 6 - WebSphere Application Server 6.0 Edge Components Refresh Pack 2 for Windows (optional)
- CD 7- DB2 Universal Database 8.2.4 (Workgroup Server Unlimited Edition) for Windows
- CD 8 - WebSphere MQ 6.0 for Windows
- CD 9 - WebSphere MQ 6.0 Refresh Pack 1 and Fix Pack 1 for Windows
- CD 10 - WebSphere Application Server 6.0 for Linux
- CD 11 - WebSphere Application Server 6.0 Refresh Pack 2 for Linux
- CD 12 - WebSphere Application Server 6.0.2 Fix Pack 15 and interim fix PK32968 for Linux
- CD 13 - WebSphere Application Server 6.0 Edge Components for Linux (optional)
- CD 14 - WebSphere Application Server 6.0 Edge Components Refresh Pack 2 for Linux (optional)
- CD 15 - DB2 Universal Database 8.2.4 (Workgroup Server Unlimited Edition) for Linux
- CD 16 - WebSphere MQ 6.0 for Linux
- CD 17 - WebSphere MQ 6.0 Refresh Pack 1 for Linux
- CD 18 - WebSphere MQ 6.0.1 Fix Pack 1 for Linux
- CD 19 - WebSphere RFID Premises Server SPDs for installing with Tivoli Configuration Manager on Windows

- CD 20- WebSphere RFID Premises Server 6.0 for Windows
- CD 21- WebSphere RFID Premises Server 6.0 for Linux
- CD 22- WebSphere RFID Premises Server Toolkit and IBM RFID Data Transformation Toolkit for WebSphere RFID Premises Server
- CD 23 - IBM Data Capture and Delivery Toolkit for WebSphere RFID Premises Server
- CD 24 - WebSphere RFID Premises Server v6.0.0.1 Upgrade Installer for Windows Server 2003 and for SUSE Linux Enterprise Server

Note: The InstallShield wizard for WebSphere RFID Premises Server also installs MicroBroker for the Data Capture and Delivery component.

Identifying hardware and software requirements

Hardware requirements



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

Table 1. Minimum supported hardware

Processor	Memory (RAM)	Free Disk Space	Temporary disk space during installation
3 GHz Pentium® 4	2 GB	8 GB	500 MB

Software requirements

WebSphere RFID Premises Server supports the following operating systems:

-  Windows Server 2003 with Service Pack 1 or Service Pack 2 or Windows Server 2003 R2
-  SUSE LINUX Enterprise Server (SLES) V9.3 (Kernel 2.6)

See the WebSphere RFID Premises Server system requirements page for the latest information about supported operating systems.

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

The following software is required to install the WebSphere RFID Premises Server software. These software packages are included with WebSphere RFID Premises Server, with the exception of Oracle. See “Packaging” on page 20 for more details on exactly what products and versions are included with WebSphere RFID Premises Server, and then see “Prerequisites” on page 22 for details on installing these products.

- WebSphere Application Server 6.0.2.15 plus Interim Fix PK32968
- WebSphere MQ 6.0.1.1
- DB2 Universal Database 8.2.4 (Workgroup Server Edition) or Oracle 9i Standard/Enterprise Release 2 (9.2.0.8)

Note: Oracle 10g 10.1.0.2 JDBC driver is recommended if using Oracle.

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

- Tivoli Enterprise Console® 3.9 Fix Pack 4 (optional)
- Tivoli Configuration Manager 4.2.3 Fix Pack 1 (optional)
- IBM Tivoli Monitoring 6.0 Fix Pack 1 (optional)
- IBM Tivoli Monitoring for Databases 6.0 (optional)
- IBM Tivoli Monitoring for Web Infrastructure 6.0 (optional)

Tivoli Configuration Manager Software Package Definition (SPD) files:

WebSphere RFID Premises Server provides Tivoli Configuration Manager SPD files for WebSphere Application Server, DB2 Universal Database and WebSphere MQ running on Windows platforms only. You can use Tivoli Configuration Manager to install and configure these prerequisites on WebSphere RFID Premises Server. For instructions on how to do this, refer to “Installing using Tivoli Configuration Manager” on page 39.

Prerequisites

This topic contains prerequisite information for installing WebSphere RFID Premises Server.

Before installing WebSphere RFID 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”
- “Configuring Internet Explorer”
- “Installing the prerequisite software”

Configuring Linux for the prerequisite software

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 9 operating system for WebSphere Application Server.

Configuring Internet Explorer

By default, Internet Explorer has scripting disabled when it is installed. You must enable scripting in order to use the WebSphere RFID 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.

Installing the prerequisite software

1. Install either the DB2 Universal Database or the Oracle database. Refer to the DB2® information center or Oracle documentation for further details on installing the databases.

For a local DB2 database:

- a. Perform a standard DB2 installation on the local machine.
- b. Leave the domain name text field blank and defer adding a contact.

- c. Take note of the DB2 administrative user name and password that you create.
- d. Check the DB2 installation logs to make sure that the installation was successful.
- e. Take note of the DB2 installation location.

For a remote DB2 database:

- a. Install the DB2 server on a remote machine.
- b. Start the DB2 server.
- c. Install the DB2 client on the local machine.

For a local Oracle database:

- a. Install Oracle on the local machine, taking note of the SYS and SYSDBA passwords.
- b. When prompted for the Oracle SID, type in the name of your RFID database.

Note: Linux commands are case-sensitive.

For a remote Oracle database:

- a. Install Oracle server on a remote machine.
- b. When prompted for the Oracle SID, type in the name of your RFID database.

Note: Linux commands are case-sensitive.

- c. Start the Oracle server.
 - d. Install the Oracle client on the local machine.
 - e. Set up Oracle Net Services to connect to the remote database.
2. Check the following for your database:
- If you are using DB2, your primary DNS suffix must be set.
- If you are using Oracle:
- The sqlnet.ora file must exist in the *ORACLE_HOME/network/admin* directory.
 - Your primary DNS suffix must be set.
 - If you plan to configure the Device Manager server database on a port that is different from the WebSphere RFID Premises Server database, make sure that the database and port are configured in the tnsnames.ora file.
3. Manually create the RFID database for DB2. 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.
- You are given the option to create tables and populate the data for the database when installing WebSphere RFID Premises Server.

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

For a local DB2 database:

- a. Open the DB2 Control Center.
- b. Right-click **All Databases** and select **Create Database** → **Standard**.
- c. Enter IBMRFID as the database name. Do not fine tune the database when it is created.

Note: If you are storing characters from double-byte character sets, you must use the UTF-8 codeset to create the database.

Note: Linux commands are case-sensitive.

- d. Exit the DB2 Control Center.

For a remote DB2 database:

- a. Open the DB2 Control Center.
- b. Right-click **All Databases** and select **Create Database → Standard**.
- c. Enter IBMRFID as the database name. Do not fine tune the database when it is created.

Note: If you are storing characters from double-byte character sets, you must use the UTF-8 codeset to create the database.

Note: Linux commands are case-sensitive.

- d. Exit the DB2 Control Center.
 - e. (Optional) Catalog the remote database, IBMRFID, to the local machine.
4. Install WebSphere Application Server 6.0 and its components. Refer to the WebSphere Application Server information center for complete installation details.
 - a. In the launchpad window, choose to install WebSphere Application Server first. Choose a full installation of WebSphere Application Server.
 - b. If you are planning to install Device Manager server and WebSphere RFID Premises Server on the same server, choose to install IBM HTTP Server.

Note: Use an administrator password for IBM HTTP Server so it can run as a service.

- c. If you are planning to install Device Manager server and WebSphere RFID Premises Server on the same server, choose to install IBM HTTP Server, choose to install the Web server plug-ins from the launchpad window. Select to install the plug-ins on IBM HTTP Server on the local WebSphere Application Server machine. Browse to the existing httpd.conf file in the IBM HTTP Server conf directory when prompted. Keep the default Web server name (webserver1) and the default configuration file (plugin-cfg.xml).
 - d. (Optional) Start WebSphere Application Server if it is not already started and remove the sample Enterprise Applications (PlantsbyWebSphere, SamplesGallery, ivtApp, and query) by stopping the EARs, and then uninstalling them. Removing the samples is recommended for a production environment.
 - e. Stop and restart WebSphere Application Server.
 - f. Apply the necessary WebSphere Application Server refresh pack and fixes. You might need to browse to and select multiple fixes to install. They might not be selected by default.
5. Install WebSphere MQ. For complete details on how to install WebSphere MQ, refer to the WebSphere MQ information center.
 - a. Navigate to Software Requirements in the launchpad and choose to install WebSphere Eclipse Platform Version 3.0.1, if it is not installed.
 - b. Navigate to Network Configuration in the launchpad, and select the radio button for **No** on the **Configuring WebSphere MQ for Windows domain users** page.

- c. Start the WebSphere MQ installation and select the option to perform a custom installation.
- d. When prompted, select **Windows Client** and its subfeatures (Client Extended Transaction Support and Client File Transfer) for installation.
- e. In the Prepare WebSphere MQ Wizard, select the radio button for **No** when asked if any of the network controllers in your domain are running Windows 2000 or later.
- f. In the Prepare WebSphere MQ Wizard, click **Setup the Default Configuration**. A new wizard opens.
- g. In the Default Configuration Wizard, unselect **Allow remote administration of the queue manager** and **Join the queue manager to the default cluster**.
- h. When the Default Configuration Wizard finishes, click **Close** to exit the wizard.
- i. In the Prepare WebSphere MQ Wizard, click **Next** to finish installing the product.
- j. Apply the necessary WebSphere MQ refresh pack and fix pack.

Note: Be sure to stop WebSphere MQ before installing any updates.

- k. Start WebSphere MQ.



Installing WebSphere RFID Premises Server

Follow the steps in this topic to install WebSphere RFID 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.
3. Verify that you have properly installed WebSphere Application Server and that webserver1 is running before installing WebSphere RFID Premises Server, if you are planning to also install Device Manager server on the server. If webserver1 is running, then IBM HTTP Server is properly installed as well.

Note: Names for the Web server, other than webserver1, are supported.

4. Run the installation program located in the root directory of the CD.

	setupwin32.exe
	setupLinux.bin

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

You can also run the installation program in silent mode. Refer to “Installing silently” on page 39 for further instructions.

5. Choose the language for your installation.
6. In the InstallShield Welcome panel, click **Next** to continue.
7. Click the radio button beside the **I accept the terms in the license agreement** message 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.
8. Select the installation directory for WebSphere RFID Premises Server.

Important: If you are installing the Device Manager server on the same machine as WebSphere RFID Premises Server, make sure the installation directory name contains only English ASCII characters.

9. InstallShield prompts you to select either a **Typical** or **Custom** installation.
 - Select the **Typical** radio button if you are installing both WebSphere RFID Premises Server and Device Manager server. Click **Next** to continue.

Important: If you are installing both WebSphere RFID Premises Server and Device Manager 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 RFID Premises Server or Device Manager server. Click **Next** to continue.

Important: If you want to install Device Manager server on a server separate from WebSphere RFID Premises Server, install Device Manager server before installing WebSphere RFID Premises Server.


The rest of this procedure assumes you are installing WebSphere RFID Premises Server. If you are installing Device Manager server only, refer to “Installing Device Manager server for WebSphere RFID Premises Server” on page 30.

If you are installing WebSphere RFID Premises Server only, then the installer prompts you to provide the host name, user name, and password for your existing Device Manager server.

10. Choose a database type, either DB2 or Oracle, and click **Next**.
11. 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**.
12. Enter your database information for Device Manager server.

For DB2:



- **Administrator username** is the instance owner, such as

	db2admin
	db2inst1

- **Administrator group** is the Administrator username’s group name. This is only required for Linux operating systems.

For Oracle:

- **Administrator username:**

	system
	system oracle user

- **Administrator group** is the Administrator username’s group name. This is only required for Linux operating systems.

For more detailed information on the configuration options for Device Manager server, refer to Preparing a properties file for the Device Manager configuration.

Click **Next** to continue.

Note: The installer will not validate the database username and password for Device Manager server.

Restriction: If you are installing WebSphere RFID Premises Server and Device Manager server on the same server, then Device Manager server must use the same type of database as your WebSphere RFID Premises Server installation. For example, if you are using WebSphere RFID Premises Server with DB2, then Device Manager server must also use DB2.

Also, Device Manager server only supports a local database. A remote database is not supported.

13. 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 RFID Premises Server APIs or the Print, Verify, and Ship application, set the **HTTP transport port** to 9080 when you create the profile.

14. 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 RFID 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.


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

16. Browse to your WebSphere MQ installation directory and click **Next**.

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

18. 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

dms_config_trace.log

 **Windows** IBM_RFID_HOME\DeviceManager\log\dms_config_trace.log

 **Linux** IBM_RFID_HOME/DeviceManager/log/dms_config_trace.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 and dms_config_trace.log files. If you are still seeing errors after reinstalling WebSphere RFID Premises Server, contact IBM Support.

The resulting installation includes:

- The creation of a WebSphere RFID Premises Server directory at:

 **Windows** C:\Program Files\IBM\RFID

 **Linux** /opt/IBM/RFID

- If you have installed both WebSphere RFID Premises Server and Device Manager server, then the installation also creates a Device Manager server directory at:

Windows C:\Program Files\IBM\RFID\DeviceManager

Linux /opt/IBM/RFID/DeviceManager

- The creation of 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 Device Manager servers.

Post-installation steps

1. Make sure that the IVEHOME 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

2. Make sure that the correct file paths are specified for the edge alerts and heartbeat log files in the premises.properties file.
The premises.properties file is located in the *IBM_RFID_HOME*/premises/properties/ directory. See “Log file locations and settings” on page 65 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 premises.properties file. See “Setting the delete filter for Data Capture and Delivery” on page 71.
4. Make sure that the IBM RFID Queue Manager is running.
 - **Windows** Open the WebSphere MQ explorer and look for IBM.RFID.QM in the Queue Managers folder. If there is a green arrow next to IBM.RFID.QM, it is running.
 - **Linux** Run the command dspmq in /opt/mqm/bin. This command tells you the current status of the queue manager.

If the Queue Manager is not running, refer to the WebSphere MQ information center for troubleshooting topics.

5. If you have installed Device Manager server, change directory to %IVEHOME%\bin or \$IVEHOME/bin and start the DMS_AppServer:

Windows startServer.bat DMS_AppServer

Linux startServer.sh DMS_AppServer

6. 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:

- Premises_Admin_Console
- Premises_DockDoorApp
- Premises_EventServer
- Premises_PVSConsole
- Premises_Services
- Premises_SupplyChain

The following Enterprise applications are part of Device Manager server and you should see a red cross next to them:

- DMS_BundlesMgmtApp
- DMS_WebApp



7. Open the WebSphere RFID Premises Server Administrative Console to verify that it is accessible.
8. Check for errors in the WebSphere Application Server and WebSphere RFID Premises Server log files. Refer to “Log file locations and settings” on page 65 for information about where to find the log files.
9. Edit the `config.ini` file in the `IBM_RFID_HOME\dts\configuration` directory and update the following code with the host name and port number of your server.

The default port number is 9081. This port number is defined when you create your WebSphere Application Server profile.

`com.ibm.rfid.bundle.list.url=host_name:port_number/bundleadmin/GetBundle?name=http://IBM_HTTP_Server_name/bundles/bundlelists/rfid_test.txt`



10. Edit the `rfid_test.txt` file and provide the correct host name of your server for the following:
PREFIX `http://host_name/bundles/`
11. (Optional) If you will be using WebSphere RFID Device Infrastructure 1.1 devices or remote Data Capture and Delivery, in the `bridge.properties` file in the `IBM_RFID_HOME/dts` directory, modify the value of the `flow.4.transformation.0.input.topic.reload.config` property to `restart/+`.
12. Start the RFID Data Transformation service manually.
 - a. Check to see if RFID Data Transformation was started as a service, and if so, stop it.

Note: If the RFID Data Transformation test bundle (`com.ibm.rfid.dts.test_version`) is running, RFID Data Transformation fails to properly shut down. Stop the test bundle before stopping the RFID Data Transformation service.

-  **Windows** Stop the service by going to **Start → Control Panel → Administrative tools → Services**. Select **IBM WebSphere RFID Premises Server DT Service** and click **Stop**.
 -  **Linux** Run the `ibm_dts_service stop` command in the `IBM_RFID_HOME/dts` directory.
- b. Start RFID Data Transformation using the script file.
 - For Windows, run the `dts.bat` file in the `IBM_RFID_HOME/dts` directory.
 - For Linux, run the `dts.sh` file in the `IBM_RFID_HOME/dts` directory.

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

13. Start the `com.ibm.rfid.bundle.loader_version` bundle.
 - a. From the RFID Data Transformation command prompt in the window where you started RFID Data Transformation, type `ss` to list the installed bundles.
A list of bundles displays, including the ID number, state, and name of each bundle.
 - b. Identify the ID number of the `com.ibm.rfid.bundle.loader_version` bundle and type `start ID_number`.
14. Check the log files for any failures in loading the bundles.
15. Tune your database to improve performance.
16. (Optional) If you will be using WebSphere RFID Device Infrastructure 1.1 or remote Data Capture and Delivery, in the `bridge.properties` file in the `IBM_RFID_HOME/dts` directory, modify the value of the `flow.4.transformation.0.input.topic.reload.config` property to `restart/+`.

17. (Optional) 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`.
18. (Optional) If you will be configuring WebSphere RFID Device Infrastructure 1.1 devices, you need to run the SQL files `rfid_1.1.1_standard_ddr.sql` and `wrdi_default_config_db2.sql` or `wrdi_default_config_oracle.sql`, which are located in the `IBM_RFID_HOME\premises\install\db\wrdi` directory:
 - For DB2:
 -  **Windows**
`db2cmd`
`db2 connect to rfid_database`
`db2 tvf-sql_file_name`
 -  **Linux**
`su db2_user_name`
`db2 connect to rfid_database`
`db2 tvf-sql_file_name`
 - For Oracle, use SQL Plus to run the commands.After running the SQL files, WebSphere RFID Premises Server will be configured to use the Standard Dock Door Receiving use case with the SamSys reader. Other device SQL files are located in the `IBM_RFID_HOME\premises\install\db\wrdi\devices` directory.
19. Verify the installation.

If you need to uninstall the WebSphere RFID Premises Server software, refer to “Uninstalling the product” on page 60.

Installing Device Manager server for WebSphere RFID Premises Server

Follow the steps in this topic to install Device Manager server on a server separate from WebSphere RFID Premises Server.

Remember: If you want to install Device Manager server on a server separate from WebSphere RFID Premises Server, install Device Manager server before installing WebSphere RFID Premises Server.

Also, Device Manager server only supports a local database. A remote database is not supported.

WebSphere Application Server, IBM HTTP Server, and the Web server plug-in are required on the server before installing Device Manager server.

The Device Manager server included with WebSphere RFID Premises Server supports only OSGi devices and can only be installed on Windows or Linux operating systems. This installation of Device Manager server supports a local database only.

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.
3. Run the installation program located in the root directory of the CD.

 **Windows** `setupwin32.exe`

 `setupLinux.bin`

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

You can also run the installation program in silent mode. Refer to “Installing silently” on page 39 for further instructions.

4. Choose the language for your installation.
5. In the InstallShield Welcome panel, click **Next** to continue.
6. Click the radio button beside the **I accept the terms in the license agreement** message 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.
7. Select the installation directory for WebSphere RFID Premises Server.

Important: Make sure the installation directory name contains only English ASCII characters.

8. Choose a **Custom** installation.
9. Select only the Device Manager server feature when prompted, and click **Next**.
10. Choose a database type, either DB2 or Oracle, and click **Next**.
11. Choose your database installation location.
12. Enter your database information for Device Manager server. Click **Next** to continue.

Note: The installer will not validate the database username and password for Device Manager server.

13. Enter your Web server information and click **Next**.
14. Enter your database information and click **Next**.
15. A summary panel displays your installation selections. Click **Install** to continue the installation process.

Note: If you are installing on Linux, you need to supply the DB2 user group name when the installation begins.

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

dms_config_trace.log

 `DEVICE_MANAGER_HOME\log\dms_config_trace.log`

 `DEVICE_MANAGER_HOME/log/dms_config_trace.log`

If you do see errors or exceptions in the installation log file, also check the `DEVICE_MANAGER_HOME\config\DMSconfig.properties` file and try reinstalling the product by changing the installer’s input fields according to the `dms_config_trace.log` file. If you are still seeing errors after reinstalling Device Manager server or editing the properties file, contact IBM Support.

17. To verify that your Device Manager server installation was successful, check the end of your `dms_config_trace.log`. You should see a message similar to the following:

`dms-return-code:`

```
[copy] Copying 1 file to C:\Program Files\IBM\RFID\DeviceManager\config\work
[copy] Copying 1 file to C:\Program Files\IBM\RFID\DeviceManager\etc
[logmsg] 2007.02.05 11:01:02.438 dms-components-install
[logmsg] DYM8400I DMS Components installation has completed successfully.
```

`dms-cleanup:`



```

BUILD SUCCESSFUL
Total time: 9 minutes 15 seconds
ANT return code is 0

##### End Install #####
Mon 02/05/2007 11:01 AM
#####

```

The resulting installation includes:

- The creation of a Device Manager server directory at:
 -  C:\Program Files\IBM\RFID\DeviceManager
 -  /opt/IBM/RFID/DeviceManager
- The creation of 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 Device Manager servers.
- The creation of tables and population of data for Device Manager server.
- The deployment of the Device Manager server application to WebSphere Application Server. The installer creates a server called DMS_AppServer in your existing WebSphere Application Server node and deploys an application called DMS_WebApp under that server. The names of this server and application are not configurable.
- The deployment of a bundle management application to WebSphere Application Server called DMS_BundlesMgmtApp under the DMS_AppServer server.

Now, complete the “Post installation steps on Device Manager server.”

If you need to uninstall the Device Manager server software, refer to “Uninstalling the product” on page 60.

Post installation steps on Device Manager server

After installing WebSphere RFID Premises Server and Device Manager server, complete the following post installation steps on Device Manager server.

Enabling WebSphere Application Server security:

Before you enable WebSphere Application Server security, make sure that users are defined for the following roles:

- WebSphere Application Server administrator (for example, wasadmin)
- WebSphere RFID Premises Server administrator (for example, ibmrfdadmin)

Note: The standard WebSphere RFID Premises Server installation already creates this user.

- Device owner for Data Capture and Delivery controllers (for example, dmsuser)

Make sure that you know the passwords that are set for these users so that you can login to the system running the Device Manager server using these user IDs and passwords. You might want to use a single operating system user for more than one role. For example, you can also use the user “ibmrfdadmin” for the WebSphere Application Server administration user.

Note: The standard WebSphere RFID Premises Server installation does not set a password for the user "ibmrfidadmin". Set the password now in order to be able to access the WebSphere RFID Premises Server administrative console later.


1. Create two operating system users if they are not already created: one for WebSphere Application Server administration (wasadmin) and one for device owners (dmsuser).
2. Enable WebSphere Application Server security using the script provided with WebSphere RFID Premises Server. The script sets security to the local operating system user registry and defines the WebSphere Application Server administrative console user.


- a. Navigate to the security directory:

 `IBM_RFID_HOME\premises\install\security`

 `IBM_RFID_HOME/premises/install/security`

- b. Run the following command:

 `ws_security.bat enable wasadmin password`

 `./ws_security.sh enable wasadmin password`

Note: If WebSphere Application Server is not running, it will be started automatically. Ignore the exception in the log if WebSphere Application Server is already running.

- c. Verify that the command ran successfully. Also check the WebSphere Application Server SystemOut.log file for exception or errors.
3. Stop Device Manager server and WebSphere Application Server.
 4. Start WebSphere Application Server.

Note: From now on you can only stop WebSphere Application Server instances using the command line. You must provide the WebSphere Application Server user ID (as configured above, for example, wasadmin) and password.

5. Open the Snoop servlet (http://fully_qualified_host_name/snoop) and verify that you can access the servlet with the dmsuser user ID and password.
6. Open the WebSphere Application Server administration console verify that you can successfully login using the wasadmin user ID and password.
7. Start Device Manager server.
8. Verify that you can open http://fully_qualified_host_name/dmservlet/SyncMLDMServletAuthRequired and access the URL with the dmsuser user ID and password. You are successful if you can access the URL or if you receive an HTTP 400 error.

If you are running WebSphere RFID Premises Server on the same machine as Device Manager server, you need to login to the WebSphere Application Server administrative console to access the WebSphere RFID Premises Server administrative console. By default, any user ID registered for the operating system can access the console but only the user ibmrfidadmin can change the configuration, for example, to create locations. You can change this in the WebSphere Application Server administrative console by configuring the mapping of the security roles to users and groups for the enterprise application **Premises AdminConsole**:

1. Open the WebSphere Application Server administrative console and login with your wasadmin account.
2. Click **Applications** → **Enterprise Applications** → **Premises AdminConsole**.

3. Under **Additional Properties**, select **Map security roles to users/groups**.
4. Select **rfidadmin** and then click **Look up users** or **Look up groups**.
5. Move an existing operating system user or group to the selected list and click **OK**.
6. Save the configuration.
7. Log in to the WebSphere RFID Premises Server administrative console with a user ID that is part of the rfidadmin group and verify that you can create locations.

Verify that you can access the WebSphere RFID Premises Server administrative console with the correct privileges.

Configuring Device Manager server tools:

Besides the Device Management Console there are two tools to support Device Manager server. The first tool is a set of programs that build the Device Manager server command line interface, which enables the use of the Web services APIs for Device Manager server in a command shell or command script. The second tool is called XMLConfig and it supports creating Device Manager jobs based on an XML file. Both tools need to be configured before use.

1. Set up the Device Manager server command line interface:
 - a. Open the file `admcli.properties`, which is located in the `IBM_RFID_HOME\DeviceManager\dmadmcli\bin` directory.
 - b. Modify the file with your host name and the Device Manager server user ID and password.

Note: Any valid operating system user can be entered because the Device Manager server Web Service API can be accessed by any authenticated user.

- c. Verify that the Device Manager server administration command line interface works:
 - 1) Open a command prompt.
 - 2) Change directory to `IBM_RFID_HOME\DeviceManager\dmadmcli\bin`.
 - 3) Run the following command to list all jobs for the sample OSGi device category:

```
dm lsjob -dc OSGi
```

The command might not generate results, but there should not be any errors.

2. Configure the Java environment so that the XMLConfig tool that is provided with WebSphere RFID Premises Server works. For example, configure Java to use the WebSphere Application Server JRE:

```
set JAVA_HOME=C:\Program Files\IBM\WebSphere\AppServer\java
set WAS_HOME=C:\Program Files\IBM\WebSphere\AppServer\
```

Preparing for remote deployment of the Device Manager client on a remote Data Capture and Delivery controller:

As described in “Installing the Device Manager client on a remote Data Capture and Delivery controller” on page 35, 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. Make sure the latest version of the `rfid_dms_osgiclient.zip` file is located in the `http_root/htdocs/locale/bundles/DMS` directory.
2. Unzip the file 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:

```
// Normally the bundles reside on a local directory
//PREFIX file:./bundlefiles/

// In case the bundles reside 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

After you have completed the post-installation steps on Device Manager server, install the Device Manager client on the Data Capture and Delivery controller.

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.

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.agenttext.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.agenttext.config.manufacturer=Unknown
com.ibm.rfid.dms.agenttext.config.modelextension=Edge
#the following line should remain commented out unless
#you want to define the DMS device name here
#com.ibm.rfid.dms.agenttext.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.

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.

1. 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:

```
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.agenttext.config.manufacturer=Unknown
com.ibm.rfid.dms.agenttext.config.modelextension=Edge
#the following line should remain commented out unless you want
#to define the DMS device name here
#com.ibm.rfid.dms.agenttext.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. 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.

The Device Manager client should now connect to the Device Manager server.

Creating Data Capture and Delivery configuration jobs

Use the XMLConfig tool to create Data Capture and Delivery configuration jobs.

The XMLConfig tool is installed with WebSphere RFID Premises Server and can be found under `IBM_RFID_HOME\premises\tools\dms`. 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\dmadmccli\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:

```
dmjsjob -dc OSGi
```

- Check job progress for an individual device:

```
dm\sprogress -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/dmsserver/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/ibmrfdiadmin/premises.sl?action=
getConfig&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 RFID 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 silently



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

Note: Silent uninstallation is not supported.

A silent installation uses the `-options responsefile` parameter, which causes the Installation wizard to read your responses from the options response file, instead of from the interactive user interface. You must customize the sample response file for your environment before installing silently. Detailed instructions on how to customize the file are included in the sample file. After customizing the file, you must 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. Open the `rfidSilent.rsp` file, which is located on the root of the WebSphere RFID Premises Server CD (CD 20 for Windows and CD 21 for Linux), in a text editor.
2. Uncomment the command, `# -silent` by removing the `#`.
3. Follow the instructions in the file and update the response values to reflect your system settings.
4. Save your changes.
5. Run the command:

	<code>setupwin32.exe -options rfidSilent.rsp</code>
	<code>setupLinux.bin -options rfidSilent.rsp</code>

Installing using Tivoli Configuration Manager

This topic describes how to install WebSphere RFID Premises Server and its prerequisite software using Tivoli Configuration Manager.

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

Tivoli Configuration Manager 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 Configuration Manager using the instructions in the Tivoli Configuration Manager documentation.
3. Register your Tivoli endpoints (one for each WebSphere RFID Premises Server) for Tivoli Configuration Manager. You can register a Tivoli endpoint from either a Tivoli Configuration Manager server or from WebSphere RFID Premises Server.
 - To register from a Tivoli Configuration Manager server, run the following command:

```
winstlcf -j -n endpoint_host_name -g server_host_name
```

Make sure that the host name is defined in the endpoint's `/etc/hosts` file.
 - Register using Tivoli Management Framework version 4.1.1 on the target WebSphere RFID Premises Server.
4. Verify that your endpoints registered properly.

- a. Run the tivoli command.
 - b. In the Tivoli Desktop, double-click **EndpointManager**. The gateway list displays.
 - c. Double-click a gateway item to get the endpoint list and then double-click an endpoint to display its properties.
5. Create a profile manager.
 - a. Run the tivoli command.
 - b. In the Tivoli Desktop, double-click *host_name-region* and navigate to **Create → Profile Manager**.
 - c. Add the profile manager name to the **Name/Icon Label** box, and select the **Dataless Endpoint Mode** check box.
 - d. Click **Create & Close**.
 - e. Double-click the newly created **Profile Manager** icon.
 - f. In the Profile Manager window, navigate to **Edit → Profile Manager** and select the **Dataless Endpoint Mode** check box.
 - g. Click **Create & Close**.
 - h. Navigate to **Profile Manager → Subscribers** and add the desired endpoints to the current subscribers.
 - i. Click **Set Subscriptions & Close**.
6. Set up Tivoli Configuration Manager to install the prerequisite software for WebSphere RFID Premises Server.
 - a. Copy WebSphere RFID Premises Server CD 19 to the Tivoli Configuration Manager server's C: drive.
 - b. Copy WebSphere RFID Premises Server CD 2 to C:\IBM\SIF\isp\windows\cdimages\WASND6.
 - c. Copy WebSphere RFID Premises Server CD 3 to C:\IBM\SIF\isp\windows\cdimages\WAS60RP2.
 - d. Copy WebSphere RFID Premises Server CD 4 to C:\IBM\SIF\isp\windows\cdimages\WAS602FP15.
 - e. Copy WebSphere RFID Premises Server CD 5 to C:\IBM\SIF\isp\windows\cdimages\WASEC6.
 - f. Copy WebSphere RFID Premises Server CD 6 to C:\IBM\SIF\isp\windows\cdimages\WASEC6RP2.
 - g. Copy WebSphere RFID Premises Server CD 7 to C:\IBM\SIF\isp\windows\cdimages\DB2WSE824.
 - h. Copy WebSphere RFID Premises Server CD 8 to C:\IBM\SIF\isp\windows\cdimages\MQ6.
 - i. Copy the WebSphere RFID Premises Server CD 9 MQ6RP1 directory to C:\IBM\SIF\isp\windows\cdimages\MQ6RP1.
 - j. Copy the WebSphere RFID Premises Server CD 9 MQ601FP1 directory to C:\IBM\SIF\isp\windows\cdimages\MQ601FP1.
7. Import the software packages into Tivoli Management Region.
 - a. Open a command line prompt.
 - b. Run the following command:


```
%TISDIR%\setup_env.cmd
sh
. /IBM/SIF/bin/sifImport.sh profile_manager_name
C:/IBM/SIF/isp/windows/packages C:/IBM/SIF/isp/windows/packages
```
8. Verify that the software packages were created properly.

- a. Run the tivoli command.
- b. In the Tivoli Desktop, double-click *host_name-region* and navigate to **Create → Profile Manager**.
- c. Double-click the **Profile Manager** icon you created in step 5 on page 40. You should see 17 profiles created in this profile manager. Each profile associates with a package list below.

Table 2. Data packages for Windows

Package name	Package description
AcceleratorsBase60WinD	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
Mq6Rp1WinD	Contains WebSphere MQ 6.0 Refresh Pack 1, which brings the product level to 6.0.1
Mq601FP1WinD	Contains WebSphere MQ 6.0.1 Fix Pack 1, which brings the product level to 6.0.1.1
Db2Wse824WinD	Contains the installable image of DB2 Universal Database (Workgroup Server Edition) 8.2.4
Was6WinD	Contains the installable image of WebSphere Application Server 6.0
WasEc6WinD	Contains the installable image of WebSphere Application Server 6.0 Edge Components
Was60Rp2WinD	Contains the installable image of WebSphere Application Server 6.0 Refresh Pack 2.
Was602Fp15WinD	Contains the installable image of WebSphere Application Server 6.0.1 Fix Pack 15 and interim fix PK32968

Table 3. Installation packages for Windows

Package name	Package description
Mq6WinI	Installs WebSphere MQ 6.0
Mq6Rp1WinI	Installs WebSphere MQ 6.0 Refresh Pack 1, which brings the product level to 6.0.1
Mq601FP1WinI	Installs WebSphere MQ 6.0.1 Fix Pack 1, which brings the product level to 6.0.1.1
Db2Wse824WinI	Installs DB2 Universal Database (Workgroup Server Edition) 8.2.4
Was6WinI	Installs WebSphere Application Server 6.0
WasEc6WinI	Installs WebSphere Application Server 6.0 Edge Components
Was60Rp2WinI	Installs WebSphere Application Server 6.0 Refresh Pack 2
Was602Fp15WinI	Installs WebSphere Application Server 6.0.1 Fix Pack 15 and interim fix PK32968

9. Install the AcceleratorsBase60WinD package first. Distribute all "D" packages to the endpoints before distributing the "I" packages.

For example, if you want to install WebSphere MQ 6.0.1.1 remotely, distribute the packages in the following sequence.

- a. AcceleratorsBase60WinD
- b. Mq6WinD
- c. Mq6Rp1WinD
- d. Mq601FP1WinD
- e. Mq6WinI
- f. Mq6Rp1WinI
- g. Mq601FP1WinI

To install WebSphere Application Server 6.0.2.15 plus interim fix PK32968 remotely, distribute the packages in the following sequence.

- a. AcceleratorsBase60WinD
- b. Was6WinD
- c. Was60Rp2WinD
- d. Was602Fp15WinD
- e. Was6WinI
- f. Was60Rp2WinI
- g. Was602Fp15WinI

To install DB2 Universal Database 8.2.4 remotely, distribute the packages in the following sequence:

- a. AcceleratorsBase60WinD
- b. Db2Wse824WinD
- c. Db2Wse824WinI

- 10. Follow the steps provided in “Installing WebSphere RFID Premises Server” on page 25.

If you need to uninstall the WebSphere RFID Premises Server software, refer to “Uninstalling the product” on page 60.


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 RFID 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 RFID Premises Server. Instructions for downloading the Tivoli License Compliance Manager are documented in the Tivoli License Compliance Manager information center.

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

 `IBM_RFID_HOME\premises\itlm\WRPSRV0600.SYS2`

Installing the toolkits

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

Toolkit prerequisites

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

Prerequisites for WebSphere RFID Premises Server Toolkit

WebSphere RFID Premises Server Toolkit requires the following software.

-  Windows XP

Note: WebSphere RFID Premises Server Toolkit is not supported on Linux.

- Rational® Application Developer for WebSphere Software 6.0.1.1 plus Interim Fix 001, Interim Fix 002, Interim Fix 003a, WebSphere Application Server V6.0 Test Environment Update 6.0.2.5, and Java SDK Update for WebSphere Application Server V6.0.2.5 Integrated Test Environment V1.0.0
- DB2 Universal Database 8.2.4 (Workgroup Server Edition) or Oracle 9i Standard/Enterprise Release 2 (9.2.0.8)

Note: Oracle 10g 10.1.0.2 JDBC driver is recommended if using Oracle.

- WebSphere MQ 6.0.1.1

Prerequisites for IBM RFID Data Transformation Toolkit for WebSphere RFID Premises Server

This toolkit requires the following software:

-  Windows XP
- WebSphere RFID Premises Server Toolkit

In addition, the following software is required and is available on the CD containing the toolkits.

- Eclipse 3.2.2
- Equinox 3.2.2

Unzip Eclipse 3.2.2. Then unzip Equinox 3.2.2 into the Eclipse 3.2.2. directory, making sure that the feature and plugins directories overwrite the same directories in the Eclipse directory.

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

This toolkit requires the following software:

-  Windows XP

In addition, the following software is required and is available on the CD containing the Data Capture and Delivery toolkit.

- Eclipse 3.2.2

Unzip Eclipse 3.2.2.

Installing WebSphere RFID Premises Server Toolkit

Use these steps to install the WebSphere RFID 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 containing the toolkit update site for WebSphere RFID Premises Server Toolkit. The update site is located on CD 22.
6. Expand the new local site and select **IBM WebSphere RFID Premises Server Toolkit**.
7. Click **Next**.
8. Select to install the **IBM WebSphere RFID Premises Server Toolkit Feature**, and click **Next**.
9. Accept the license agreement and click **Next**.
10. Select an installation location and click **Finish**.

Note: If you choose to create a new WebSphere Application Server profile and you are going to use any WebSphere RFID 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.

Tip: The panel may list your computer's Free Space as "0KB". This is a known issue that you can ignore during installation.

11. On the Jar Verification (feature verification) panel, review your choices and click **Install**.
12. When the installation completes, click **Yes** to restart the workbench.
13. When Rational Application Developer for WebSphere Software has restarted, import the projects for WebSphere RFID Premises Server Toolkit by selecting **File** → **New** → **Project** → **IBM WebSphere RFID** → **Premises Server Toolkit** and click **Next**.
14. Click **Finish** to install the toolkit project in the current workspace.

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

If you need to uninstall the WebSphere RFID Premises Server Toolkit software, refer to "Uninstalling the WebSphere RFID Premises Server Toolkit" on page 61.

Installing IBM RFID Data Transformation Toolkit for WebSphere RFID Premises Server

Use these steps to install the IBM RFID Data Transformation Toolkit for WebSphere RFID Premises Server.

1. Check your hardware and operating system to make sure they meet the necessary requirements. Refer to “Toolkit prerequisites” on page 43 for information.
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 RFID Data Transformation Toolkit for WebSphere RFID Premises Server. Then click **OK**. The update site is located on the CD containing the toolkits in the DTS_Toolkit directory.
6. If desired, enter a more descriptive name for the local site and click **OK**.
7. Click **Finish**.
8. In the Updates window, expand the new local site and select **IBM WebSphere RFID Premises Server Data Transformation 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 projects for IBM RFID Data Transformation Toolkit for WebSphere RFID Premises Server by selecting **File → New → Project → IBM WebSphere RFID → Premises Server Data Transformation Toolkit** and click **Next**.
15. Select **IBM WebSphere RFID Premises Server Data Transformation**.
16. Click **Finish** to install the toolkit project in the current workspace.
17. Restart the Eclipse SDK.

To import the test project for IBM RFID Data Transformation Toolkit for WebSphere RFID Premises Server, complete the following steps:

1. Create a Java project named `com.ibm.rfid.dts.test`.
2. Right-click the new project and click **Import → General → Archive File**.
3. Click **Next**.
4. Browse to the DTS_Toolkit\examples folder on the CD containing the toolkits and click **Finish**.

If you need to uninstall the IBM RFID Data Transformation Toolkit for WebSphere RFID Premises Server software, refer to “Uninstalling the IBM RFID Data Transformation Toolkit for WebSphere RFID Premises Server” on page 62.

Installing IBM Data Capture and Delivery Toolkit for WebSphere RFID Premises Server

Use these steps to install the IBM Data Capture and Delivery Toolkit for WebSphere RFID 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 RFID 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 **RFID Data Capture 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 projects for IBM Data Capture and Delivery Toolkit for WebSphere RFID Premises Server by selecting **File** → **New** → **Project** → **IBM WebSphere RFID** → **RFID Data Capture Toolkit** and click **Next**.
15. Select **Data Capture**.
16. Click **Finish** to install the toolkit project in the current workspace.

If you need to uninstall the IBM Data Capture and Delivery Toolkit for WebSphere RFID Premises Server software, refer to “Uninstalling the IBM Data Capture and Delivery Toolkit for WebSphere RFID Premises Server” on page 62.

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

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

When using the IBM Data Capture and Delivery Toolkit for WebSphere RFID Premises Server, make sure the Java compiler is at the same compliance level as the Java Runtime Environment (JRE) installed on your system. For example, a JRE base level 1.4.2 requires that the classes are compliance level 1.4 or lower. 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 RFID Premises Server on one machine. This configuration works immediately after installation and no other machine or WebSphere RFID Premises Server is required. You can use this launch configuration to verify the installation.

DataCapture-RdrSim

Launches a remote Data Capture and Delivery device and the Simulated Reader. This configuration simulates a remote Data Capture and Delivery device that has a Simulated Reader and is connected to a WebSphere RFID Premises Server (real or simulated) that is running on a separate machine. This launch configuration requires another machine and also requires additional configuration.

DataCapture-PremSim

Launches a simulated WebSphere RFID Premises Server. The simulated server must be run on a separate machine from the Simulated Reader and requires additional configuration.

Configuring the toolkit to use the Simulated Reader and simulated WebSphere RFID Premises Server on the local system

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

Before launching the configuration, if you previously launched a configuration other than **DataCapture-FullSim**, remove all MicroBroker residue. Delete the *eclipse_runtime_root*/MicroBroker directory, as well as the *eclipse_runtime_root*/workspace/.metadata/.plugins/org.eclipse.core.runtime/.settings/com.ibm.micro.prefs file (or, if you are not using it for projects, you can delete the entire workspace directory).

Run launches/DataCapture-FullSim.launch to launch the Simulated Reader, I/O simulator, and WebSphere RFID Premises Server simulator on the local machine.

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

Configuring the toolkit to use the Simulated Reader connecting to a remote WebSphere RFID Premises Server or Premises Simulator

This section describes how to configure the Simulated Reader when you are connecting it to a WebSphere RFID 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 RFID 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.xml` file, modify the `matrix.properties` property of the `PortalControllerAgent` and replace *put_premises_hostname_here* with the IP address of the WebSphere RFID Premises Server.
3. On Linux, add the bundle `org.eclipse.swt.gtk.linux.x86` to the launch configuration in order to start the simulator windows for the Simulated Reader.
 - a. Make sure the projects for IBM Data Capture and Delivery Toolkit for WebSphere RFID Premises Server have been created on the Eclipse workspace.
 - b. On the Eclipse workspace, click **Run** → **Run...**
 - c. Expand **Equinox OSGi Framework** and select **DataCapture-PremSim**.
 - d. In the **Plug-ins** list under **Target Platform**, select **org.eclipse.swt.gtk.linux.x86**.
 - e. Click **Apply**.

4. Run launches/DataCapture-RdrSim.launch, which is located within the com.ibm.rfid.resource.toolkit project.
 - a. From within Eclipse, click **Run** → **Run....**
 - b. Browse to and select **DataCapture-RdrSim**. It is located under **Equinox OSGi Framework**.
 - c. Click **Run**.

You will see errors in the console indicating that the MicroBroker could not connect to the remote server. For example: [ERROR] *date time* - PremisesSim: (MBAF-200.306) An MqttException was thrown while starting. However, the Data Capture and Delivery controller can run locally without problems. 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.

Configuring the toolkit to use the Premises Simulator

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

Run launches/DataCapture-PremSim.launch, which is located within the com.ibm.rfid.resource.toolkit project.

1. From within Eclipse, click **Run** → **Run....**
2. Browse to and select **DataCapture-PremSim**. It is located under **Equinox 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 RFID 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 an Data Capture and Delivery controller ID. For example, E2=edge-samsys.xml.
3. Restart the Premises Simulator.

Installing the fix pack for WebSphere RFID Premises Server


This section describes how to install WebSphere RFID Premises Server 6.0.0.1.

Only follow these instructions if WebSphere RFID Premises Server 6.0 is already installed. Otherwise, if this is a new installation, follow the instructions in “Installing WebSphere RFID Premises Server” on page 25 to install version 6.0.0.1.

Before you install the fix pack, make sure that you meet the following prerequisites:

- You must have administrative access on Windows or root access on Linux.
- WebSphere RFID Premises Server 6.0 must already be installed.

Complete the following steps to install the fix pack:

1. Copy the Premises_v6.0.0.1 directory to *IBM_RFID_HOME*.
2.  Make sure the permissions are set correctly in the directory. Run the following commands:

```
cd $IBM_RFID_HOME/Premises_v6.0.0.1
dos2unix db_scripts/db2/*.sh
dos2unix db_scripts/oracle/*.sh
dos2unix db_scripts/migration/*.sh
dos2unix db_scripts/migration/6.0.0.1/*.sql
chmod 755 db_scripts/db2/*.sh
chmod 755 db_scripts/oracle/*.sh
chmod 755 db_scripts/migration/*.sh
chmod 755 ./*.sh
```

3. Create database entries for the fix pack. If you want to migrate existing databases, run the migration scripts located in the *db_script\migration* directory. If you want to create a new default database for WebSphere RFID Premises Server 6.0.0.1, run the create scripts located in the *db_script* directory.
4. Set the following environment variables:
 - *WAS_PROFILE_NAME* - The WebSphere Application Server profile name that was used to install WebSphere RFID Premises Server.
 - *BUNDLE_REPOSITORY_DIR* - The Device Manager server bundle directory. This environment variable is not necessary if you only plan to update WebSphere RFID Premises Server.

Open a command prompt or shell console and run the following command:

 `set environment_variable_name=value`

 `export environment_variable_name=value`

5. Run the fix pack installation script from *IBM_RFID_HOME/Premises_v6.0.0.1*:
 - If WebSphere Application Server security is *not* enabled, run the following command:

 `updateinstall.bat`

 `./updateinstall.sh`

- If WebSphere Application Server security is enabled, run the following command:

 `updateinstall.bat user_ID password`

 `./updateinstall.sh user_ID password`

When prompted, choose to install WebSphere RFID Premises Server, Device Manager server, or both. Then follow the prompts to install the fix pack.

After installing the fix pack, make sure you set the delete filter correctly for your installation in the `premises.properties` file. See “Setting the delete filter for Data Capture and Delivery” on page 71.

Verifying the installation

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

You can verify that WebSphere RFID 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 RFID 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 `premises.properties` file. 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 `matrix_simple.properties` file. 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 28.
2. Open the `premises.properties` file and modify the value of the `com.ibm.rfid.applping.shortcut` property to `true`.
3. Restart WebSphere Application Server.
4. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
5. Select **Simulated Reader** from the left navigation pane.
6. On the Simulated Reader console page, select a reader from the menu.

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

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

The following icons represent the status of the reader:

-  - The reader is turned on, but not yet ready.
-  - The reader status is unavailable.



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

You should see tag information appear in the output box.

8. Click **Stop Reader** to end simulating tag reads.
9. (Optional) Click **Reset Reader** to cancel the current start or stop request and reset the reader to its original state.
10. Click **Clear Output** to clear the displayed tag data.

After the installation has been successfully verified, system administrators may wish to disable the edge bundle or the Simulated Reader for performance reasons. Disabling both results in optimal performance.

To disable the edge bundle, access the edge controller and stop the bundle.

To disable the Simulated Reader, complete the following steps:

1. Select **Event Templates** from the left navigation pane in the WebSphere RFID Premises Server Administrative Console.
2. Click **View Template Properties** for the tag_read_external event template.
3. Remove tagmonitor.out.channel from the list of selected channels.
4. Click **Update Event Template**.
5. Open the premises.properties file and modify the value of the com.ibm.rfid.applping.shortcut property to false.
6. Restart WebSphere Application Server.

To re-enable the Simulated Reader and edge bundle, restart the bundle on the edge controller and add the output channel for the Simulated Reader back to the event template.

Creating a cluster for WebSphere RFID Premises Server

Creating a WebSphere RFID Premises Server cluster provides several benefits, including load balancing and failover.

Planning your cluster topology

The following topic helps you plan the topology of your WebSphere RFID Premises Server cluster.

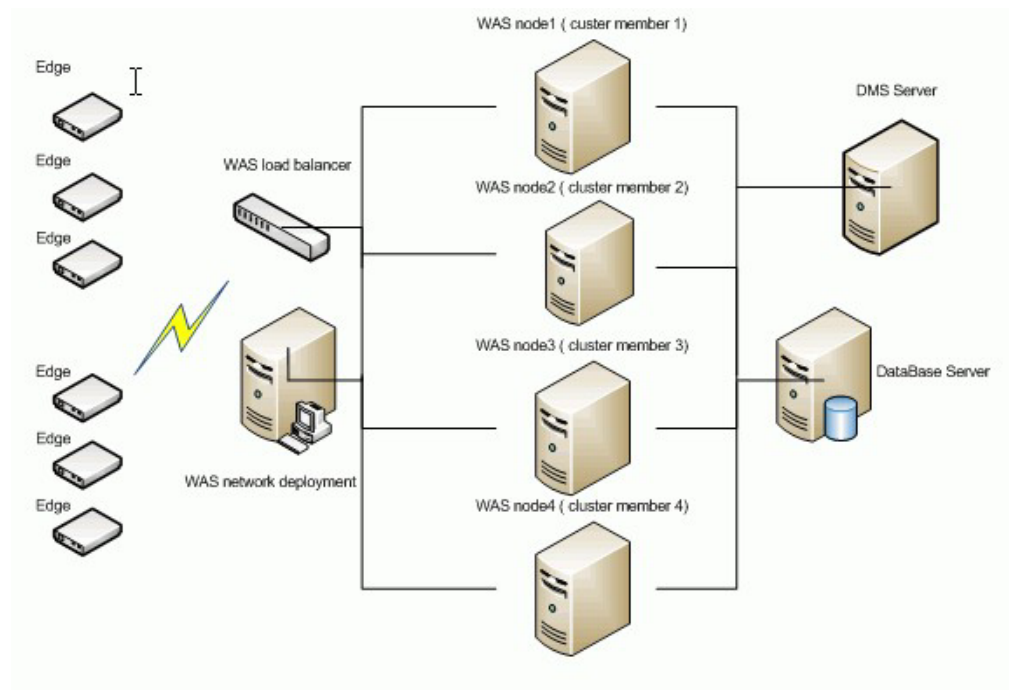
A WebSphere RFID Premises Server cluster consists of the following cluster members:

- WebSphere RFID Premises Server applications
- A centralized database
- A Device Manager server
- WebSphere Application Server Network Deployment components, which are installed on a machine called the *cluster controller*.

In a production environment these components might be installed on multiple machines.

When you configure the WebSphere Application Server Network Deployment dispatcher, it is necessary to create an additional host name and IP address on the

cluster controller for the cluster. Requests that are sent to this IP address are handled by the Load Balancer and, if configured, dispatched to the cluster nodes. The same address must be used for the loopback devices on the cluster nodes.



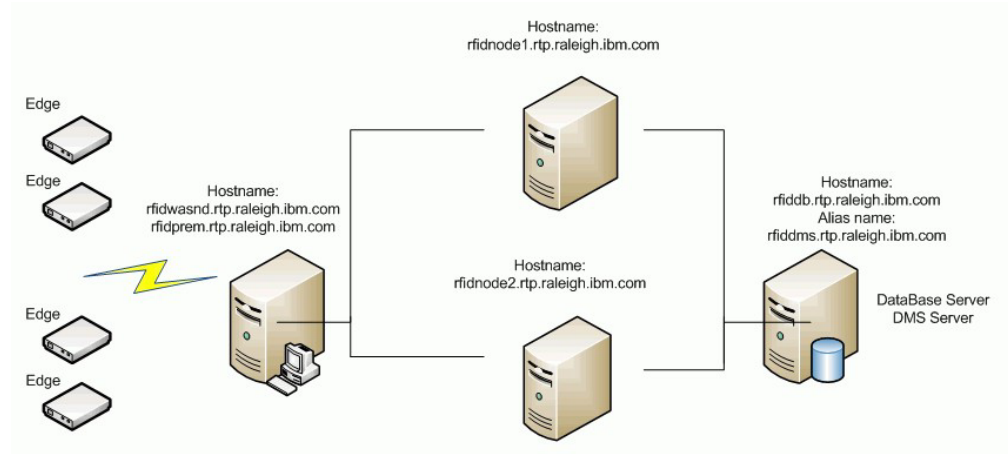
Installing a cluster

The following installation scenario describes how to install a WebSphere RFID Premises Server cluster.

This scenario uses the following machines in the cluster environment:

- Machine A - WebSphere Application Server Network Deployment and Load Balancer. This machine has two IP addresses and `rifdwasnd.rtp.raleigh.ibm.com` is the host name and `rfidprem.rtp.raleigh.ibm.com` is the cluster host name for load balancing.
- Machine B - WebSphere Application Server Network Deployment base for WebSphere RFID Premises Server. This machine has one IP address and `rfidnode1.rtp.raleigh.ibm.com` is the host name.
- Machine C - WebSphere Application Server Network Deployment base for WebSphere RFID Premises Server. This machine has one IP address and `rfidnode2.rtp.raleigh.ibm.com` is the host name.
- Machine D - The database server and the Device Manager server. This machine has one IP address and `rfiddb.rtp.raleigh.ibm.com` is the host name. The alias name is `rfiddms.rtp.raleigh.ibm.com`.

Note: Machine B and C must use the same operating system and WebSphere RFID Premises Server must be installed in the same directory on both machines. Also, the time difference between the machines that make up the cluster can be no more than 5 minutes.



1. Setup the WebSphere RFID Premises Server database on the database server (rfiddb).
 - a. Install the database server on a remote machine.
 - b. Create a local database.
 - c. Use the database scripts provided on the WebSphere RFID Premises Server CD 20 (Windows) or CD 21 (Linux) to create and populate tables.
2. Install Device Manager server on the database server (rfiddb). See “Installing Device Manager server for WebSphere RFID Premises Server” on page 30.
3. Install WebSphere RFID Premises Server on the cluster nodes (rfidnode1 and rfidnode2). Follow the instructions in “Installing WebSphere RFID Premises Server” on page 25, with the following exceptions:
 - In step 9 on page 26, make sure to select the **Custom** radio button and then select to install WebSphere RFID Premises Server only.
 - In step 11 on page 26, uncheck **Create and populate tables**. Also, change the database host name to the remote database server host name (rfiddb.rtp.raleigh.ibm.com).
4. Install WebSphere Application Server Network Deployment on the cluster controller (rfidwasnd) from CDs 2, 3, and 4.
5. Install the Load Balancer for the WebSphere Application Server Network Deployment Edge Components on the cluster controller (rfidwasnd) from CDs 5 and 6.

Note: When you install Load Balancer 6.0 refresh pack 2, you need to back up the license file at \servers\conf\lb60Full.LIC before you uninstall Load Balancer 6.0. After you finish installing Load Balancer 6.0 refresh pack 2, copy lb60Full.LIC to \servers\conf.

Creating the cluster

Before adding any nodes to Deployment Manager make sure that the Deployment Manager on the cluster controller (rfidwasnd) and WebSphere Application Server Network Deployment on the cluster nodes (rfidnode1 and rfidnode2) is started and running correctly. Also, if WebSphere Application Server security is enabled, disable security before you add nodes to the Deployment Manager.

1. Run the following command from a command prompt on the first node machine (rfidnode01):

```
cd was_home\bin
addnode deployment_manager_host_name -includeapps
```

You should see a message that the node has been successfully federated.

2. Run the following command at command line window on second node machine (rfidnode02) and any subsequent node machines:

```
cd was_home\bin  
addnode deployment_manager_host_name
```

Note: If WebSphere Application Server Network Deployment is not running on default port 8879, run the command and specify the port number:

```
addnode deployment_manager_host_name deployment_manager_port_number
```

3. Log in to the Administrative Console for the Deployment Manager:
<http://rfidwasnd.rtp.raleigh.ibm.com:9060/ibm/console>
4. Click **System Administrative** → **Nodes** and verify that the new nodes are displayed.
5. Delete **server1** from the second and any subsequent nodes:
 - a. Click **Servers** → **Application Servers**.
 - b. Select **server1** for the second node and click **Stop**.
 - c. Then click **Delete**.
 - d. Repeat this step for any subsequent nodes.

Note: Make sure you do not delete **server1** from the first node. It must be deleted from the second node and any subsequent nodes so that the default WebSphere TCP ports are released, meaning that the cluster members on each node can have the same TCP ports.

6. Create the cluster:
 - a. Click **Servers** → **Cluster** and click **New**.
 - b. Enter an appropriate name for the cluster.
 - c. Select **Prefer local**.
 - d. Select **Select an existing server to add to this cluster** and choose **server1** for the first node (rfidnode01Node01) to be the first cluster member.
 - e. Click **Next**.
 - f. On the next panel, enter an appropriate member name. This name is the server name that is created on the node machine.
 - g. For **Select node**, choose the second node (rfidnode02Node01).
 - h. Uncheck **Generate Unique Http Ports** and click **Apply** to add the cluster member to the cluster.
 - i. On the Summary panel, click **Finish** to create the cluster.
 - j. Save and synchronize the changes with the nodes of your cell.
7. Verify that the cluster was created correctly.
 - a. Select **Servers** → **Cluster** and click the name of the cluster you created. The cluster properties panel will display.
 - b. In the cluster properties panel, verify that all cluster members are running.
 - c. Verify that the WebSphere RFID Premises Server application is mapped to the cluster and not to any dedicated server.
 - d. You also can check the SystemOut.log file on every node machine and verify that there are no exceptions.

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.

Configuring the Load Balancer

Two IP addresses are necessary for the load-balanced dispatcher machine. One is for host name and the other is for the cluster. In this scenario, the first IP address will map to `rifdwasnd.rtp.raleigh.ibm.com`, which is the host name. The second IP address will map to `rfidprem.rtp.raleigh.ibm.com`, which is the cluster IP address for load balancing. You can have two network interface cards in one machine and can set up one IP address for each network card. If you only have one network interface card, you need to set up two IP addresses in one network interface.

1. Set up two IP addresses in one network interface:

Note: You can also use the load balancer command, `dscontrol` executor `configure`, to set up the cluster IP address. Refer to the *Load Balancer Administration Guide* for more information about this command.

- **Windows** Complete the following steps to set up the IP addresses:
 - a. Click **Start** → **Settings** → **Network Connections**.
 - b. Open your local area connection properties.
 - c. Select **Internet Protocol (TCP/IP)** and click **Properties**.
 - d. Click **Advanced**.
 - e. Click **Add** in the IP addresses section.
 - f. Add the second IP address and subnet mask, which is the same as the first IP address.


- **Linux** Run the following command, where `eth0:0` is the network interface ID:



```
ifconfig eth0:0 cluster_IP_address netmask 255.255.255.255
```

2. Set up the loopback device for the cluster node machines. You must alias the loopback device (often called `lo0`) to the cluster address.

Note: In this installation scenario, Load Balancer and WebSphere Application Server Network Deployment are installed on the same machine. The cluster IP address (`rfidprem.rtp.raleigh.ibm.com`) is used for all load balancer configuration steps.

- **Windows** Complete the following steps:
 - a. Click **Start** → **Settings** → **Control Panel**.
 - b. Add the MS Loopback Adapter Driver if you have not already done so:
 - 1) Click **Add Hardware** to launch the Add Hardware Wizard.
 - 2) Click **Next**.
 - 3) Select **Yes, I have already connected the hardware**, then click **Next**.
 - 4) If the MS Loopback Adapter is in the list, it is already installed. Click **Cancel** to exit.
 - 5) If the MS Loopback Adapter is not in the list, select **Add a New Device** and click **Next**.
 - 6) To select the hardware from a list, click **No** and then click **Next**.
 - 7) Select **Network Adapters** and click **Next**.
 - 8) On the Select Network Adapter panel, select **Microsoft** from the **Manufacturers** list and then select **Microsoft Loopback Adapter**.
 - 9) Click **Next**. Then click **Next** again to install the default settings.
 - 10) Click **Finish** to complete the installation.
 - c. From the Control Panel, double-click **Network and Dial-up Connections**.

- d. Select the connection with the **Device Name** of “Microsoft Loopback Adapter”.
 - e. Select **Properties**.
 - f. Select **Internet Protocol (TCP/IP)** and then click **Properties**.
 - g. Click **Use the following IP address**. Fill in **IP address** with the cluster address and **Subnet mask** with the subnet mask of the server.
- Note:** Do not enter a router address. Use the local host as the default DNS server.
- h. Make sure the loopback adapter is listed in the correct order:
 - 1) Click **Start** → **Settings** → **Network Connections**.
 - 2) On the **Advanced** tab, click **Advanced Settings**.
 - 3) In the **Connections** box on the **Adapters and Bindings** tab, make sure **Loopback adapter** is listed *after* **Local Area Connection**. Move **Loopback adapter** if the order is not correct.
-  Run the following command:

```
ifconfig lo:1 cluster_IP_address netmask 255.255.255.255 up
```
3. Create the edge cluster for the Load Balancer:
 - a. Start the Load Balancer GUI:
 -  Click **Start** → **Programs** → **IBM WebSphere** → **Edge Components** → **IBM Load Balancer** → **Load Balancer**.
 -  Run the following command as root:
 dsserver
 - b. In the Dispatcher Login, connect to the cluster controller host (rfidwasnd.rtp.raleigh.ibm.com).
 - c. In the left navigation pane, expand **Dispatcher** → **Host: host_name** and right-click **Executor: port_number**.
 - d. Click **Add cluster** and provide the following information:
 - Enter DTSCluster as the **Cluster**.
 - Provide the cluster IP address and the host name IP address for the cluster controller.
 - Make sure to select **Configure this cluster?**
 - Click **OK**.
 - e. Right-click **Executor: port_number** and click **Add port**.
 Add port 1883 and choose **MAC Based Forwarding** as the forwarding method. Click **OK**.
 Repeat this step to add port 9080. Also, only for port 9080, make sure that the **Sticky time (seconds)** setting on the **Configuration Settings** tab is set to 1800.
 - f. Right-click **Executor: port_number** and click **Add server**.
 Add both cluster nodes as servers for both port numbers.
 Add the cluster node host name (rfidnode01.rtp.raleigh.ibm.com and rfidnode02.rtp.raleigh.ibm.com) as the server and the port number (1883 and 9080) as the server address. Click **OK**.
 Repeat this step forth both host names and port numbers.
 - g. In the left navigation pane, expand **Dispatcher** → **Host: host_name** → **Manager** and right-click **Advisor: port_number**. Click **Start**.
 - h. Save your configuration file.

- i. Reload the configuration from the Load Balancer GUI. Expand **Dispatcher** and right-click **Host: *host_name***. Then click **Load New Configuration**

Here is the sample configuration:

```
dscontrol set loglevel 1
dscontrol executor start
dscontrol cluster add DTSCluster address 9.42.139.131 primaryhost 9.42.139.183
dscontrol cluster set DTSCluster proportions 49 50 1 0
dscontrol executor configure 9.42.139.131 en0 255.255.255.128
dscontrol port add DTSCluster:9080 reset no
dscontrol server add DTSCluster:9080:rfidnode02.rtp.raleigh.ibm.com address 9.42.139.184
dscontrol server add DTSCluster:9080:rfidnode01.rtp.raleigh.ibm.com address 9.42.139.185
dscontrol port add DTSCluster:1883 reset no
dscontrol server add DTSCluster:1883:rfidnode02.rtp.raleigh.ibm.com address 9.42.139.184
dscontrol server add DTSCluster:1883:rfidnode01.rtp.raleigh.ibm.com address 9.42.139.185
dscontrol manager start manager.log 10004
dscontrol advisor start Connect 9080 Connect_9080.log
dscontrol advisor start Connect 1883 Connect_1883.log
```

4. To enable load balancing for the cluster, you need to set the MicroBroker address to the cluster address of the load balancer. You can update the MicroBroker server IP address from the WebSphere RFID Premises Server Administrative Console or using the SQL command line tools.
 - From WebSphere RFID Premises Server Administrative Console:
 - a. Click **Data Capture Configuration** → **Controllers**. The Controllers panel displays.
 - b. Click the configuration group your controller belongs to. For example, Distribution Center. The Edit Controller Configuration Group panel displays.
 - c. Click **MicroBrokerConfigurationAgent**.
 - d. In the **Property** field, select **server.ip** from the dropdown list.
 - e. In the **Value** field, enter your cluster IP address.
 - f. Click **Update**.
 - From a DB2 command line window or the using the sqlplus command on Oracle, enter the following SQL statement to update the `server.ip` property value:

```
update SAGE.DCCONTROLLERAGENT
set PROP_VALUE = 'cluster_IP_address'
where AGENT_NAME = 'MicroBrokerConfigurationAgent'
and PROP_NAME = 'server.ip';
```

Note: You can tune several parameters to increase load balancer performance. Refer to the product documentation for Edge Components to find out what parameters and values are best for your environment.

Verifying the cluster

Verify the cluster by using the TagEventMonitor to simulate tag reads, application ping, or heartbeat. From a separate Windows machine that is not part of the cluster, perform the following steps:

1. Download the TagEventMonitor.zip file from the bundles\tools directory on CD 2.
2. Unzip the file to a temporary directory and run the **EdgeEventMonitor** script.
3. In the **MQTT server** field, enter the load balancer cluster host name. In this example, it will be `rfidprem.rtp.raleigh.ibm.com`. Click **Connect** to see the TagEventMonitor client connect to RFID Data Transformation on the first node.
4. Start another instance of TagEventMonitor by running the **EdgeEventMonitor** script in a second command window.
5. Input the same server name in **MQTT server** field. It will connect to RFID Data Transformation on the second node.

6. In each TagEventManager window, you can simulate different events by sending different topics and data.

Installing the WebSphere Application Server log file adapters

Follow the instructions below to install the WebSphere Application Server log file adapters on one or more WebSphere RFID Premises Server using the Tivoli Enterprise Console.

The WebSphere Application Server log file adapters enable you to view exceptions that occur on WebSphere RFID 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 RFID 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 **Identifier**. 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 RFID 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 RFID 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.

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 RFID Premises Server using the Tivoli Enterprise Console.

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 RFID 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-heartbeats.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 **Identifier**. 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 RFID 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 RFID 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.

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.

Uninstalling the product

This task describes how to uninstall WebSphere RFID Premises Server and its related products.

The uninstaller file removes the WebSphere Application Server code relative to WebSphere RFID Premises Server, such as Enterprise Java Beans (EJBs), servlets, and Java Server Pages (JSPs). It also removes the WebSphere MQ code relative to WebSphere RFID Premises Server, including queues and queue managers. It does not remove the WebSphere RFID Premises Server database, but it does change the WebSphere Application Server configuration and settings for the WebSphere RFID Premises Server applications.


Remember: To perform this task using a Linux platform, log in as a root user.

1. Ensure that WebSphere Application Server and WebSphere MQ are running, and that the RFID Data Transformation service is not running.
2. Start the uninstallation wizard, and follow the instructions on the panels.

-  `IBM_RFID_HOME\uninst\uninstaller.exe`

You can also use one of the following options:

- Click **Start** → **Programs** → **IBM WebSphere RFID** → **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**.
 -  `IBM_RFID_HOME/_uninst/uninstaller.bin`
3. If you have Device Manager server installed, choose to either remove or keep it and click **Next** when prompted.
If you choose to remove Device Manager server later, refer to the instructions in the Information Center for Device Manager.
 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.

Uninstalling the fix pack for WebSphere RFID Premises Server



This section describes how to uninstall WebSphere RFID Premises Server 6.0.0.1. After running the uninstallation script, your installation will be at version 6.0.

1. Make sure the following environment variables are set:
 - `WAS_PROFILE_NAME` - The WebSphere Application Server profile name that was used to install WebSphere RFID Premises Server.
 - `BUNDLE_REPOSITORY_DIR` - The Device Manager server bundle directory. This environment variable is not necessary if you only plan to update WebSphere RFID Premises Server.

If not, open a command prompt or shell console and run the following command:

```
 set environment_variable_name=value
 export environment_variable_name=value
```

2. Run the fix pack uninstallation script from `IBM_RFID_HOME/Premises_v6.0.0.1`:
 - If WebSphere Application Server security is *not* enabled, run the following command:


```
 updateuninstall.bat
 ./updateuninstall.sh
```
 - If WebSphere Application Server security is enabled, run the following command:

```
 updateuninstall.bat user_ID password
 ./updateuninstall.sh user_ID password
```

When prompted, choose to uninstall WebSphere RFID Premises Server, Device Manager server, or both. Then follow the prompts to uninstall the fix pack.

Uninstalling the toolkits

Use the topics below to uninstall the toolkits.

Uninstalling the WebSphere RFID Premises Server Toolkit

This task describes how to uninstall the WebSphere RFID Premises Server Toolkit.

1. Start Rational Application Developer for WebSphere Software.
2. Navigate to **Help → Software Updates → Manage Configuration**.
3. Expand the `RAD_INSTALL_DIR\eclipse` directory in the left navigation pane.

4. Select **IBM WebSphere RFID Premises Server Toolkit Feature *version*** and then click **Uninstall**.
5. Restart Rational Application Developer for WebSphere Software.

To uninstall any of the Rational Application Developer for WebSphere Software features and WebSphere MQ, follow the instructions in the product documentation:

- Rational Application Developer for WebSphere Software v6.0.1 Information Center
- WebSphere MQ v6.0 Information Center

Uninstalling the IBM RFID Data Transformation Toolkit for WebSphere RFID Premises Server

This task describes how to uninstall IBM RFID Data Transformation Toolkit for WebSphere RFID Premises Server.

1. Start Eclipse.
2. Navigate to **Help** → **Software Updates** → **Manage Configuration**.
3. Select **IBM WebSphere RFID Premises Server Data Transformation *version*** and click **Disable**.
4. Delete the `com.ibm.rfid.toolkit.feature_version` directory from the `Eclipse_home/feature` directory. *Eclipse_home* is the installation location of Eclipse 3.2.2.
5. Delete the following files from the `Eclipse_home/plugins` directory:
 - `com.ibm.micro.bridge.mq.jms_version.jar`
 - `com.ibm.micro.utils_version.jar`
 - `com.ibm.micro_version.jar`
 - `com.ibm.mqttclient_version.jar`
 - `com.ibm.mqttlocalclient_version.jar`
 - `com.ibm.rfid.bundle.loader_version.jar`
 - `com.ibm.rfid.dt.toolkit.doc_version.jar`
 - `com.ibm.rfid.mbafe.admin_version.jar`
 - `com.ibm.rfid.mbafe_version.jar`
 - `com.ibm.rfid.toolkit.plugin_version.jar`
 - `com.ibm.rfid.toolkit.ui_version.jar`
 - `Rfid.jar`
6. Restart Eclipse.

Uninstalling the IBM Data Capture and Delivery Toolkit for WebSphere RFID Premises Server

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

1. Start Eclipse.
2. Navigate to **Help** → **Software Updates** → **Manage Configuration**.
3. Expand the tree in the left navigation pane. Right click **RFID Data Capture Toolkit *version*** and click **Uninstall**.
4. Restart Eclipse.

Migrating to WebSphere RFID Premises Server 6.0.x from a previous version

When you migrate from a previous version of WebSphere RFID Premises Server to version 6.0 or later, keep the following information in mind.

Migrating WebSphere RFID Premises Server

- Data migration
 - Migrate the topology.
 - If you migrate your topology from WebSphere RFID Device Infrastructure to WebSphere RFID Device Infrastructure, no changes are necessary. However, you can begin scripting.
 - If you migrate your topology from WebSphere RFID Device Infrastructure to Data Capture and Delivery, significant changes are necessary.
 - Migrate tagging. Most tags remain the same.
- Bundle transformation
 - Convert your bundle projects using the Eclipse 3.2.2 PDE tool.
 - Rename the bundle to follow the Eclipse 3.2.2 naming standards (optional).
 - Recompile the bundle using IBM RFID Data Transformation Toolkit for WebSphere RFID Premises Server and then test it.
- WebSphere Application Server J2EE custom applications
 - Upgrade the WebSphere Application Server J2EE custom applications to run on WebSphere Application Server 6.0, including applications that use event server processing (tasks, channels, and templates)
 - Migrate your databases.

What has changed?

- The product is based on Eclipse 3.2.
 - All bundles must be converted to Eclipse 3.2.
 - The edge controller (remote Data Capture and Delivery) runs on Equinox.
- The configuration is different.
 - Agents are no longer involved in parsing the edge configuration XML. They operate directly from ConfigAdmin.
 - The EdgeConfigAgent parses the edge XML, and puts it straight into ConfigAdmin.
- The Device Kit is open source.
 - Package names have changed.
 - Readers implement a new open source API that is based on API subsets called *profiles*.
 - A new open source data format is used to report tags.
 - Configuration is different.
 - Topic names are fixed
- Edge agent code.
 - MicroBroker is now only used to transmit data to and from a remote WebSphere RFID Premises Server.
 - Data Capture and Delivery uses the open source NotificationService, which is based on the Equinox EventAdmin.

- NotificationService and EventAdmin require a dictionary, rather than single-value native data, use a different wildcard character, and only allow a wildcard character at the end of a subscription topic.
- There is a new NotificationService<->Microbroker Bridge agent that bridges topics across the two publish and subscribe buses.
- AbstractAgent has changed to support NotificationService, but also helps abstract the publish interface for agents.
- Controllers and sensors.
 - The PortalControllerAgent is used as the Controller/State machine. This is defined in a properties file (matrix.properties), which describes the states, triggers, transitions, and associated actions.
 - Instead of MotionSensorAgent and SwitchAgent, a configurable UniversalSensorAgent is used. I/O pins can be mapped to different logical names.

Enabling security with WebSphere Application Server

Use the scripts provided to enable and disable security for WebSphere Application Server with the local operating system, or local OS, user registry.

Before running the **ws_security** script, ensure that a local user (for example, ibmrfidadmin) exists or that a local user group (for example, ibmrfid) exists and has users in it. After WebSphere Application Server security is enabled, you can sign on to the WebSphere RFID Premises Server administrative console using only the local user or a user ID that belongs to the local user group.

1. Navigate to the security directory:

Windows	<code>IBM_RFID_HOME\premises\install\security\</code>
Linux	<code>IBM_RFID_HOME/premises/install/security/</code>

2. Run the following command:

```
ws_security action userid password
```

- *action* = enable or disable
- *userid* = Local OS user ID, which must be ibmrfidadmin or belong to the group called ibmrfid
- *password* = Local OS password

Opening the WebSphere RFID Premises Server Administrative Console

Use the WebSphere RFID Premises Server Administrative Console to define and edit the components, and the relationships between these components, in your RFID network topology.

1. Open a new Web browser.

Note: Use Internet Explorer 6.0 to open the WebSphere RFID Premises Server Administrative Console. Ensure that JavaScript is enabled.

2. In the **Address** field of your Web browser, type `http://premises_server_hostname:9080/ibmrfidadmin`.

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 Enabling WebSphere Application Server security.

3. If WebSphere Application Server security is enabled, enter the default user name, `ibmrfidadmin`, and password, `ibmrfidadmin`. Or you can use any user ID that belongs to the group, **ibmrfid**. A Welcome page displays.
4. Click **About** to view the version of the console that you are running.

Note: If WebSphere RFID Premises Server is installed on your local server, you can access the console by clicking **Start** → **Programs** → **IBM WebSphere RFID** → **Premises Server version** → **Administrative Console**.

Troubleshooting techniques

Use these instructions to help you troubleshoot your problem.

Checking the depth of MQ Queues

1. Open MQ Explorer.
2. Select **Start** → **Programs** → **IBM WebSphere MQ** → **WebSphere MQ Explorer**.
3. Check the depths of the RFID queues. Queues usually process and go to zero quickly. If the depth of any queue is greater than zero, it indicates a problem.

Enabling WebSphere RFID Premises Server trace with WebSphere Application Server



1. Open a Web browser.
2. Go to `http://premises_IP_address:9060/ibm/console`.
3. Go to **Troubleshooting** → **Logs and Trace** → **server1** → **Diagnostic Trace** → **Change Log Detail Levels** → **Groups**.
4. Modify the Trace Specification to `RFIDALE=all: com.ibm.rfid.*=all: com.ibm.kimono.*=all`.
5. Click **Apply** → **OK** → **Save** and **Save** again.

Log file locations and settings

This topic lists the locations and settings of the log files.

Installation log files for WebSphere RFID Premises Server and Device Manager server



`install.log`

 Windows	<code>IBM_RFID_HOME\logs\install.log</code>
 Linux	<code>IBM_RFID_HOME/logs/install.log</code>

`dms_config_trace.log`



 Windows	<code>IBM_RFID_HOME\DeviceManager\log\dms_config_trace.log</code>
 Linux	<code>IBM_RFID_HOME/DeviceManager/log/dms_config_trace.log</code>

Alert error log for the edge controller

- **File name:** There can be up to 10 alert log files. The log file name is `edge-alert.x.log` where `x` is a number from 0 to 9.
- **Default location:**
 -  **Windows** `IBM_RFID_HOME\logs`
 -  **Linux** `IBM_RFID_HOME/logs`
- **Format:**



- TimeStamp -- Time error issued from edge controller
- Alerttype -- information, warning, error
- Edge ID -- logical ID of the edge device
- Message -- java exception or a message with the format of:
 Reader *readerid* is *ON/OFF*

Heartbeat log for the edge controller

- **File name:** edge-heartbeats.log
- **Default location:**
 -  *IBM_RFID_HOME\logs*
 -  *IBM_RFID_HOME/logs*
- **Format:**
 - TimeStamp -- Heartbeat time
 - Location ID -- location ID (for now this is the portal ID of the tag reader)
 - EdgeID -- logical ID of the edge device reporting heartbeat
 - ReaderID -- logical tag Reader ID
 - Message -- heartbeat messages of the format:
 ON/OFF
 edgeid=UP/DOWN
 readerid=UP/DOWN

WebSphere Application Server and WebSphere RFID Premises Server log files

The WebSphere Application Server log files also contain information for WebSphere RFID Premises Server.


- **File names:** SystemOut.log, SystemErr.log, and trace.log
- **Location:**
 -  *WAS_PROFILE_HOME\logs\server1*
 -  *WAS_PROFILE_HOME/logs/server1*

Note: The default installation directory for WebSphere Application Server is C:\Program Files\IBM\WebSphere\AppServer on Windows and /opt/IBM/WebSphere/AppServer on Linux. 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 “Troubleshooting techniques” on page 65 for details on how to enable tracing on WebSphere Application Server for WebSphere RFID Premises Server.

DB2 Universal Database log files

- **File names:** db2diag.log and jdbcerr.log
- **Default location:**
 -  *C:\Program Files\IBM\SQLLIB\DB2*
 -  */opt/IBM/SQLLIB/DB2*

RFID Data Transformation service

- **File name:** DTSruntime.log
- **Default location:**

-  `IBM_RFID_HOME\logs`
-  `IBM_RFID_HOME/logs`

Note: `IBM_RFID_HOME` is an environment variable created when you installed WebSphere RFID Premises Server. If you modified the installation directory for WebSphere RFID Premises Server, be sure to use the modified installation path.

Tuning the databases to improve performance



Use the steps in this topic to improve your database performance.

Tuning DB2 Universal Database



To tune your 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 CDs and when you install the product. The scripts are located in these paths:

Before installation:

-  On CD 20 in `db_script\performance_tuning_db2.bat`
-  On CD 21 in `db_script/performance_tuning_db2.sh`

After installation:

-  `IBM_RFID_HOME\premises\install\db\performance_tuning_db2.bat`
-  `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
```

Tuning Oracle

Important: In order to use these performance tuning steps, you must have the Oracle 10g 10.1.0.2 JDBC driver.

- Apply all Oracle configuration changes to a default Oracle installation.
- Do not run any configuration scripts after Oracle installation.
- Only apply the configuration changes listed in the following steps.
- Enter all commands using the Oracle `sqlplus` utility.
- For all commands, be sure to use the directory paths and database instance name that are correct for the server.

1. Create a new table space for indices using this command:

```

CREATE TABLESPACE "USERS_IDX"
noLOGGING
DATAFILE 'c:\oracle\ORADATA\ibmrfd\USERS_IDX_1.dbf'
SIZE 500M REUSE AUTOEXTEND
ON NEXT 200K MAXSIZE 3000M EXTENT MANAGEMENT
LOCAL SEGMENT SPACE MANAGEMENT MANUAL;

```

2. Allow the user SAGE access to the USERS_IDX table space using this command:

```
ALTER USER "SAGE" QUOTA UNLIMITED ON "USERS_IDX";
```

3. Move indices to a new table space using these commands:

```

alter index SAGE.CC1119257758767 rebuild tablespace users_idx;
alter index SAGE.CC1119257886811 rebuild tablespace users_idx;
alter index SAGE.PK_ADDRESS rebuild tablespace users_idx;
alter index SAGE.PK_AGGREGATETAGEXTENSION rebuild tablespace users_idx;
alter index SAGE.PK_BASECHANNELCONFIG rebuild tablespace users_idx;
alter index SAGE.PK_CHANNELPARAMETER rebuild tablespace users_idx;
alter index SAGE.PK_CHANNELTEMPLATE rebuild tablespace users_idx;
alter index SAGE.PK_CNT_AGENTS rebuild tablespace users_idx;
alter index SAGE.PK_CNT_AGTS_ENT rebuild tablespace users_idx;
alter index SAGE.PK_CNT_AGTS_PROPS rebuild tablespace users_idx;
alter index SAGE.PK_CONTACT rebuild tablespace users_idx;
alter index SAGE.PK_CONTROLLER rebuild tablespace users_idx;
alter index SAGE.PK_CONTROLLER_TASK rebuild tablespace users_idx;
alter index SAGE.PK_DCAGENT rebuild tablespace users_idx;
alter index SAGE.PK_DCAGENTPROP rebuild tablespace users_idx;
alter index SAGE.PK_DCCONTROLLERAGENT rebuild tablespace users_idx;
alter index SAGE.PK_DCCTRLAGENTS rebuild tablespace users_idx;
alter index SAGE.PK_DCCTRLAGENT rebuild tablespace users_idx;
alter index SAGE.PK_DCCTRLAGTPROPS rebuild tablespace users_idx;
alter index SAGE.PK_DEVICE rebuild tablespace users_idx;
alter index SAGE.PK_DEVICEYPE rebuild tablespace users_idx;
alter index SAGE.PK_EMAILCHANNELCONFIG rebuild tablespace users_idx;
alter index SAGE.PK_ENTCATMETA rebuild tablespace users_idx;
alter index SAGE.PK_ENTITYCATEGORY rebuild tablespace users_idx;
alter index SAGE.PK_ENTITYTYPE rebuild tablespace users_idx;
alter index SAGE.PK_ENTITYTYPEINSTANCE rebuild tablespace users_idx;
alter index SAGE.PK_ENTTYPINSMETA rebuild tablespace users_idx;
alter index SAGE.PK_ENTTYPMETA rebuild tablespace users_idx;
alter index SAGE.PK_EPCCOMPANYPREFIXINDEX rebuild tablespace users_idx;
alter index SAGE.PK_EPCENCODINGTYPE rebuild tablespace users_idx;
alter index SAGE.PK_EPCINPUTTYPE rebuild tablespace users_idx;
alter index SAGE.PK_EPCSERIALNUMBER rebuild tablespace users_idx;
alter index SAGE.PK_EVENTPARAMETER rebuild tablespace users_idx;
alter index SAGE.PK_EVENTPARAMETER_EVENTTEMPLA3 rebuild tablespace users_idx;
alter index SAGE.PK_EVENTTEMPLATE rebuild tablespace users_idx;
alter index SAGE.PK_EVENTTEMPLATE_TASK rebuild tablespace users_idx;
alter index SAGE.PK_HTTPCHANNELCONFIG rebuild tablespace users_idx;
alter index SAGE.PK_JMSCHANNELCONFIG rebuild tablespace users_idx;
alter index SAGE.PK_JMSTOPICCONFIG rebuild tablespace users_idx;
alter index SAGE.PK_LOCATION rebuild tablespace users_idx;
alter index SAGE.PK_LOGICALPRINTERPROPERTY rebuild tablespace users_idx;
alter index SAGE.PK_MQCHANNELCONFIG rebuild tablespace users_idx;
alter index SAGE.PK_OBJECTLINK rebuild tablespace users_idx;
alter index SAGE.PK_PRINTDATA rebuild tablespace users_idx;
alter index SAGE.PK_PRINTER rebuild tablespace users_idx;
alter index SAGE.PK_PRINTERTYPE rebuild tablespace users_idx;
alter index SAGE.PK_PRINTJOBS rebuild tablespace users_idx;
alter index SAGE.PK_PRINTSTATISTICS rebuild tablespace users_idx;
alter index SAGE.PK_PRINTTEMPLATE rebuild tablespace users_idx;
alter index SAGE.PK_RDR_AGENTS rebuild tablespace users_idx;
alter index SAGE.PK_RDR_AGTS_LOCS rebuild tablespace users_idx;
alter index SAGE.PK_RDR_AGTS_PROPS rebuild tablespace users_idx;
alter index SAGE.PK_READER rebuild tablespace users_idx;
alter index SAGE.PK_READERTYPE rebuild tablespace users_idx;
alter index SAGE.PK_RFIDANTENNA rebuild tablespace users_idx;

```

```

alter index SAGE.PK_SC_PACKTYPE rebuild tablespace users_idx;
alter index SAGE.PK_SC_PROFILE rebuild tablespace users_idx;
alter index SAGE.PK_SC_PROFILE_PROPERTIES rebuild tablespace users_idx;
alter index SAGE.PK_STATUS rebuild tablespace users_idx;
alter index SAGE.PK_TAG rebuild tablespace users_idx;
alter index SAGE.PK_TAGEXTENSION rebuild tablespace users_idx;
alter index SAGE.PK_TAGHISTORY rebuild tablespace users_idx;
alter index SAGE.PK_TASK rebuild tablespace users_idx;
alter index SAGE.PK_TASK_LOCATION rebuild tablespace users_idx;
alter index SAGE.PK_USERACCTEJB rebuild tablespace users_idx;
alter index SAGE.PK_CNT_AGENTS rebuild tablespace users_idx;
alter index SAGE.PK_CNT_AGTS_ENT rebuild tablespace users_idx;
alter index SAGE.PK_CNT_AGTS_PROPS rebuild tablespace users_idx;
alter index SAGE.PK_RDR_AGENTS rebuild tablespace users_idx;
alter index SAGE.PK_RDR_AGTS_LOCS rebuild tablespace users_idx;
alter index SAGE.PK_RDR_AGTS_PROPS rebuild tablespace users_idx;
alter index SAGE.PK_SUBLOCATION rebuild tablespace users_idx;
alter index SAGE.PK_OBJINSMETA rebuild tablespace users_idx;
alter index SAGE.PK_UPDATESITE rebuild tablespace users_idx;

```

4. Disable logging for the USERS table space using the Oracle Enterprise Manager Console (OEM).
 - a. In the OEM, select **Network** → **Databases** → **IBMRFID** → **Storage** → **Tablespaces** → **Users**.
 - b. On the Storage tab in the Enable Logging section, select **No**.
5. Using the OEM, increase the size of the redo logs to 100 MB and use only one log in each group (this step should already be done by the default Oracle installation). In the OEM, select **Network** → **Databases** → **IBMRFID** → **Storage** → **Redo Log Groups** to verify the settings.
6. Using the OEM, select **Network** → **Databases** → **IBMRFID** → **Storage** → **Tablespaces** → **Users** → **Datafiles**.
 There should only be one data file listed in the tree on the left. Select the data file and change the following properties:
 - On the General tab set the size to 500 MB
 - On the Storage tab set the following:
 - automatically extend datafile when full
 - increment = 100 MB
 - maximum value = 32767 MB
7. Exit the OEM.
8. For Oracle, use a new init.ora file based upon the following settings.
 - a. Be sure to check that all paths, *db_name*, *instance_name*, *service_names*, and *undo_tablespace* are the correct values for the current Oracle system.
 - b. Put this init.ora file in the *ORACLE_HOME*\database directory.
 - c. Name the file *initDB_NAME.ora* where *DB_NAME* is the name of the database. For example, *initIBMRFID.ora* for the IBMRFID database.

```

background_dump_dest = C:\oracle\admin\ibmrfid\bdump
backup_tape_io_slaves = TRUE
compatible = 9.2.0
control_files = ('C:\oracle\oradata\ibmrfid\control01.ctl',
'C:\oracle\oradata\ibmrfid\control02.ctl', 'C:\oracle\oradata\ibmrfid\control03.ctl')
cursor_space_for_time = TRUE
db_block_buffers = 76800
db_block_size = 8192
db_file_multiblock_read_count = 8
db_files = 1024
db_name = IBMRFID
event = '10126 trace name context forever, level 1'
global_names = FALSE
instance_name = IBMRFID
java_pool_size = 25165824
job_queue_processes = 4
large_pool_size = 8388608
log_archive_dest_1 = 'LOCATION=C:\ORACLE\ORA92\RDBMS'
log_buffer = 32768

```

```

log_checkpoint_interval = 10000
log_checkpoint_timeout = 1800
max_dump_file_size = 10240
max_enabled_roles = 30
open_cursors = 300
open_links = 4
oracle_trace_collection_name = ''
os_authent_prefix = ''
parallel_max_servers = 5
processes = 150
remote_login_passwordfile = EXCLUSIVE
service_names = IBMRFD
shared_pool_size = 201326592
sort_area_retained_size = 65536
sort_area_size = 500536
undo_management = AUTO
undo_retention = 1800
undo_suppress_errors = TRUE
undo_tablespace = UNDOTBS1
user_dump_dest = C:\oracle\admin\ibmrfd\udump

```

9. Use sqlplus and run the following Oracle scripts while logged in as sysdba. These scripts are found in the *ORACLE_HOME\rdbms\admin* directory.
 - a. To log in to sqlplus as sysdba, enter sqlplus without any parameters.
 - b. When prompted for the user name, enter *ID/PASSWORD@DB_NAME* as sysdba.
 - initxa.sql
 - initjvm2.sql
 - initjvm4.sql
 - initjvm5.sql
10. While still logged into sqlplus as sysdba, enter the following commands:


```

shutdown immediate
create spfile from pfile;
startup

```

Note: To make future changes, modify the *initDB_NAME.ora* file then run these commands to update the spfile.
11. While still logged into sqlplus as sysdba, reanalyze the table statistics by entering the command:


```

exec dbms_stats.gather_schema_stats('SAGE');

```
12. Exit sqlplus.

Configuring WebSphere Application Server for Oracle

Update WebSphere Application Server to use the Oracle 10g 10.1.0.2 JDBC driver.

1. Download the Oracle 10g 10.1.0.2 JDBC driver from metalink.oracle.com or from another Oracle download site.
2. Place the 10g JDBC driver JAR file in the *ORACLE_HOME\jdbc\lib* directory.
3. Start WebSphere Application Server if it is not already running.
4. Open a Web browser and go to the WebSphere Application Server Administrative Console.
5. Navigate to **Resources** → **JDBC Providers**.
6. Select the Node scope and click **Apply**.
7. In the JDBC Providers list, click **OracleJDBCThinDriver** to see the configuration properties.
8. Modify the classpath to point to the 10g JDBC driver JAR file and click **OK**.
9. Follow the same process to change the classpath for the OracleJDBCThinDriverXA JDBC provider.
10. Click **OracleJDBCThinDriver**:
 - a. Then, click **Data Sources** → **IBMSESSION**.
 - b. For the Data Store helper class name, select **Oracle10g data store helper** and click **OK**.

11. Click **OracleJDBCThinDriverXA**:
 - a. Then, click **Data Sources** → **IBMRFID**.

Note: IBMRFID should be the database name.
 - b. For the Data Store helper class name, select **Oracle10g data store helper** and click **OK**.
12. Click **Save** on the WebSphere Application Server Administrative Console tool bar.
13. Click **Save** to save the master configuration.
14. Restart WebSphere Application Server.

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 Data Capture and Delivery 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.

Delete filter configuration settings

The setting for the delete filter is configurable in the `premises.properties` file.

- 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 as follows:

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.

```
com.ibm.rfid.premises.edgeconfig.delete.filter=!(|(service.pid=com.ibm.rfid.bundle.loader)
(service.pid=com.ibm.rfid.edge.config)))
```

- 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 as follows:

```
com.ibm.rfid.premises.edgeconfig.delete.filter=(&(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 as follows:

```
com.ibm.rfid.premises.edgeconfig.delete.filter=(|(|(|(|(|(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))))
```

To view the delete filter configuration settings in the WebSphere RFID Premises Server Administrative Console, use the instructions in “Viewing configuration variables” on page 72. Look for `com.ibm.rfid.premises.edgeconfig.delete.filter` in the Name column. The current set value for each configuration variable is in the **Value** column.

Viewing configuration variables

Use the WebSphere RFID Premises Server Administrative Console to view the configuration variables for the WebSphere RFID Premises Server.

The Configuration Variables panel is a read-only panel that displays the parameters from your `premises.properties` file. This file is located on the WebSphere RFID Premises Server in these directories:

 Windows	C:\Program Files\IBM\RFID\premises\properties
 Linux	/opt/ibm/rfid/premises/properties

You can examine the current settings on the WebSphere RFID Premises Server from the WebSphere RFID Premises Server Administrative Console without actually locating the `properties` file on the WebSphere RFID Premises Server. Although modifying the behavior of the server requires making changes to the `properties` file on the server and then stopping and restarting the server, the Configuration Variables panel allows you to view the current settings without accessing the actual file.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **Reporting** → **Configuration Variables** from the left navigation pane. The Configuration Variables panel displays.

Chapter 4. Administering

This section describes how to perform administrative tasks for WebSphere RFID Premises Server.

Administering WebSphere RFID Premises Server includes managing edge controllers, store locations, output channels and tag readers. It also includes viewing configuration variables, tags, and tasks. You can perform these functions using the WebSphere RFID Premises Server Administrative Console.

WebSphere RFID Premises Server Administrative Console overview

The WebSphere RFID Premises Server Administrative Console is a Web-based application for defining the critical resources comprising your RFID network, as well as the relationships among these various components.

This information is stored in a network topology database on the WebSphere RFID 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 RFID Premises Server Administrative Console to immediately implement the changes.

Note: Use Internet Explorer 6.0 to open the WebSphere RFID Premises Server Administrative Console. Ensure that JavaScript is enabled.

Attention: To prevent someone from overwriting your changes, be sure that when using the WebSphere RFID 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 RFID Premises Server Administrative Console with links to corresponding topics:

- Data Capture Configuration - for information about this topic, refer to “Managing your Data Capture and Delivery configuration” on page 75.
 - Agent Configuration - see “Working with Data Capture and Delivery agents” on page 76
 - Devices - see “Working with Data Capture and Delivery devices” on page 87
 - Locations - see “Working with Data Capture and Delivery locations” on page 91
 - Controllers - see “Working with Data Capture and Delivery controllers” on page 98
 - Import Configurations - see “Importing the Data Capture and Delivery configuration file” on page 102
 - Print Templates - see “Working with Data Capture and Delivery print templates” on page 113
 - Update Sites - see “Working with Data Capture and Delivery update sites” on page 115

- WRDI Configuration - for information about this topic, refer to “Managing your WebSphere RFID Device Infrastructure configuration” on page 116.
 - Agent Configuration see “Modifying the property values of agents” on page 116
 - Readers - see “Working with readers” on page 125
 - Printers - see “Working with printers” on page 128
 - Locations - see “Working with locations” on page 136
 - Controllers - see “Working with controllers” on page 140
 - Print Templates - see “Working with print templates” on page 133
- Event Processing - for information about this topic, refer to “Managing event processing” on page 143.
 - Event Templates - see “Working with event templates” on page 143
 - Output Channels - see “Working with output channels” on page 145
 - Tasks - see “Working with tasks” on page 147
- EPC Configuration - for information about this topic, refer to “Managing the EPC configuration” on page 149.
 - Profile Configuration - see “Working with profiles” on page 155
 - Serial Number Configuration - see “Working with serial numbers” on page 157
 - Company Prefix Index Translation - see “Working with the EPCglobal company prefix index” on page 160
- Reporting - for information about this topic, refer to “Reporting” on page 162.
 - Tags - see “Viewing tags” on page 162
 - Configuration Variables - see “Viewing configuration variables” on page 72
- Verification - for information about this topic, refer to “Verifying the WebSphere RFID Premises Server installation and setup” on page 166.
 - Simulated Reader - see “Starting a simulated reader” on page 167, “Stopping a simulated reader” on page 167, and “Resetting a simulated reader” on page 167

See “Opening the WebSphere RFID Premises Server Administrative Console” on page 64 to get started.

Opening the WebSphere RFID Premises Server Administrative Console

Use the WebSphere RFID Premises Server Administrative Console to define and edit the components, and the relationships between these components, in your RFID network topology.

1. Open a new Web browser.

Note: Use Internet Explorer 6.0 to open the WebSphere RFID Premises Server Administrative Console. Ensure that JavaScript is enabled.

2. In the **Address** field of your Web browser, type `http://premises_server_hostname:9080/ibmrfdadmin`.

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 Enabling WebSphere Application Server security.

3. If WebSphere Application Server security is enabled, enter the default user name, `ibmrfidadmin`, and password, `ibmrfidadmin`. Or you can use any user ID that belongs to the group, **ibmrfid**. A Welcome page displays.
4. Click **About** to view the version of the console that you are running.

Note: If WebSphere RFID Premises Server is installed on your local server, you can access the console by clicking **Start** → **Programs** → **IBM WebSphere RFID** → **Premises Server version** → **Administrative Console**.

Managing your Data Capture and Delivery configuration

This section describes how to create and manage configuration groups for controllers, locations, and devices within your WebSphere RFID Premises Server infrastructure using the WebSphere RFID Premises Server Administrative Console and Data Capture and Delivery.

Use the WebSphere RFID 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 RFID 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 RFID Premises Server Administrative Console; however, you define and manage the metadata through the XML configuration file that you import.

Note: The WebSphere RFID 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 a location type configuration group called *Enhanced Dock Door Receiving*. This location configuration group type contains all the agents that are normally part of enhanced dock door 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 RFID Premises Server Administrative Console to implement and manage configuration groups. You can also import an XML document into the WebSphere RFID 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:

- “Data Capture and Delivery device configuration group details” on page 91
- “Data Capture and Delivery location configuration group details” on page 96
- “Data Capture and Delivery controller configuration group details” on page 101

WebSphere RFID Premises Server Administrative Console

The WebSphere RFID Premises Server Administrative Console navigation panel contains both a WRDI Configuration and a Data Capture Configuration section. The information in this section applies only to Data Capture and Delivery configuration. When you create a reader or location, for example, in the WRDI section of the WebSphere RFID Premises Server Administrative Console, it does not appear in the Data Capture and Delivery configuration list of readers or locations. Devices, locations, and controllers are unique throughout the system; for example, you cannot have multiple readers in the system with the same the device identifier.

You can perform the following functions using either the WebSphere RFID 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 (of category reader, logical printer, and simulated reader).
- 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
- 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 Data Capture and Delivery agents

This section explains Data Capture and Delivery agents and how to view and manage them using the WebSphere RFID Premises Server Administrative Console.

From the Agent Configuration panel, you can view and manage Data Capture and Delivery agents. WebSphere RFID Premises Server comes with three agent types: controller type, location type, and device type. This section contains the following topics:

Viewing existing Data Capture and Delivery agents

The Agent Configuration panel on the WebSphere RFID Premises Server Administrative Console shows all of the agents defined for a particular agent type.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **Data Capture Configuration** → **Agent Configuration** from the left navigation pane. The Agent Configuration panel displays.
3. In the **Agent Type** field, click the drop-down arrow and 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.

Adding and configuring a new Data Capture and Delivery agent and PIDs

This topic describes how to add a new agent and configure a PID, persistence ID, using the WebSphere RFID Premises Server Administrative Console.

To define an agent, enter the agent name, a description of the agent, and indicate the agent type. An agent can be a controller type, location type, or device type. After adding an agent, you define properties for PIDs associated with the agent. For information about PIDs, refer to “Understanding Data Capture and Delivery PIDs and Factory PIDS” on page 102.

1. Open the WebSphere RFID 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 **Create Agent**. The New Agent panel displays.
4. Enter a descriptive name for this agent.
5. In the **Agent Type** field, click the drop-down arrow and select the type of agent from the list.
6. Enter a unique description of the agent.
7. Click **Add PIDs to the Agent**. 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 Data Capture and Delivery PIDs and Factory PIDS” on page 102.
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. Click the down arrow and select the type of property from the list.
 - e. Click the down arrow and select the cardinality value from the list.
 - f. Click the down arrow and select **true** to indicate that the property is required and **false** to indicate that it is not required.
 - g. 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 Data Capture and Delivery agent

This topic describes how to add a PID and configuration properties to an existing agent using the WebSphere RFID Premises Server Administrative Console.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. In the left navigation panel, click **Data Capture Configuration** → **Data Capture 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 Data Capture and Delivery PIDs and Factory PIDS” on page 102.
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. Click the down arrow and select the type of property from the list.
 - e. Click the down arrow and select the cardinality value from the list.
 - f. Click the down arrow and select **true** to indicate that the property is required and **false** to indicate that it is not required.
 - g. 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 Data Capture and Delivery 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 RFID Premises Server Administrative Console.

You can define an agent by downloading agent properties from an update site. For information about update sites, refer to “Working with Data Capture and Delivery update sites” on page 115.

1. Open the WebSphere RFID 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 **Download Agent**. The Download Agent Properties panel displays.
4. Select **Create a new agent**.
5. In the **Agent Type** field, click the drop-down arrow and select the type of agent from the list. An agent can be a controller type, location type, or device type. 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.

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 RFID Premises Server. The default XSL file, `IBMRFIDPremisesDefaultMapping.xsl`, is stored in the `lhs_root\bundles\import_mappings` directory. You can override the default XSL transformation by creating a new XSL file and storing it in the `lhs_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 Intermecc BRI Runtime Feature, the XSL file must be named "Intermecc 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 "WebSphere RFID Premises Server sample XML schema and configuration files" on page 103.

Modifying Data Capture and Delivery agent properties for a PID

This topic describes how to add or modify agent properties for a PID using the WebSphere RFID Premises Server Administrative Console.

For an explanation of PIDs and factory PIDs, refer to "Understanding Data Capture and Delivery PIDs and Factory PIDs" on page 102.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. In the left navigation panel, click **Data Capture Configuration** → **Data Capture Agent Configuration**. The Agent Configuration panel displays.
3. Click on 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, click on the agent that you want to update. The Edit Agent panel displays. Modify the information and click **Update**.
 - To delete a property from this PID, click 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.

Modifying a Data Capture and Delivery agent by downloading agent properties

This topic describes how to modify an existing agent by downloading agent details from an update site using the WebSphere RFID Premises Server Administrative Console.

You can modify an existing agent by downloading agent properties from an update site. For information about update sites, refer to "Working with Data Capture and Delivery update sites" on page 115.

1. Open the WebSphere RFID 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 **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.

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 RFID Premises Server. The default XSL file, `IBMRFPIDPremisesDefaultMapping.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 "WebSphere RFID Premises Server sample XML schema and configuration files" on page 103.

Deleting Data Capture and Delivery agent properties from a PID

Use the WebSphere RFID Premises Server Administrative Console to delete Data Capture and Delivery agent properties from a PID.

Complete the following steps to delete agent properties from a PID.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. In the left navigation panel, click **Data Capture Configuration** → **Data Capture Agent Configuration**. The Agent Configuration panel displays.
3. Click on 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 a Data Capture and Delivery agent

This topic describes how to delete a PID from an agent using the WebSphere RFID Premises Server Administrative Console.

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 RFID Premises Server Administrative Console. The Welcome page displays.
2. In the left navigation panel, click **Data Capture Configuration** → **Data Capture 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**.

Data Capture and Delivery agent details

The following table defines the fields on the Edit Agent Properties panel of the WebSphere RFID Premises Server Administrative Console.

Types of agents

Note: This topic applies to Data Capture and Delivery version 6.0 agents only. If you are using WebSphere RFID Device Infrastructure version 1.1.1 agents, refer to “Agent details” on page 116.

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 edge controller installation and configuration process. Agents exist for motion sensors, light trees, and more. The agents that are installed in your network are determined by the bundle parameters you set during the initial installation of Device Manager server or by the bundle parameters set during any subsequent agent deployments.

- **Reader agents** connect the tag reader adapters to a messaging service. Although each reader agent has specific code for interfacing to each tag reader adapter, the output form and commands received from other tag reader agents are identical for all tag reader agents.
- **Light Tree agents** connect the light tree I/O adapters to a messaging service.
- Universal Sensor agents connect sensors such as motion detectors, infrared beams, and switches to a messaging service.
- **Filter agents** filter tag data according to configured filters.
- **Portal Controller agents** coordinate activities on the edge controller, such as listening for events from motion sensors and triggering tag readers for specified periods of time.
- **Self-test agents** coordinate location self-test I/O sequences and durations.
- **Health Check agents** manage the system health-checking activities and coordinate the presentation of the system status at the portal site.

Agent properties and values

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 the section below for details on what variables can be substituted.

Table 4. Agents and property values

Agent	Agent Property/Property Value
Alert agent - forwards local log messages and alerts to a remote server.	<ul style="list-style-type: none"> • Tracing - display trace output. • Edge ID - the edge ID associated with this agent. • Edge Name - the edge name associated with this agent. • Threshold - messages of this severity or higher are forwarded to the remote server. • Edge threshold - messages of this severity or higher are logged to the edge console.

Table 4. Agents and property values (continued)

Agent	Agent Property/Property Value
Application Ping agent - monitors remote server status and responds to remote server status requests.	<ul style="list-style-type: none"> • Tracing - display trace output. • Edge ID - the edge ID associated with this agent. • Edge Name - the edge name associated with this agent. • Error Time Interval - after an error, this value is the check interval in milliseconds. • Response Timeout - the threshold in milliseconds to wait for the response. • Normal Time Interval - the normal health check interval in milliseconds.
Filter agent - applies all configured filters to incoming data.	<ul style="list-style-type: none"> • Tracing - display trace output. • Portal ID - the portal ID associated with this agent. • Portal Name - the portal name associated with this agent. • Filters - a comma-delimited list of filters to be configured. • 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. • Publish Topics - a comma-delimited list of topics for publishing filtered data. • Subscribe Topics - a comma-delimited list of topics for receiving data to be filtered. • Duplicates Decay Limit - how often, in seconds, stored duplicates should remain. • Duplicates Decay Cleanup - how often, in seconds, decayed duplicates should be deleted. • 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. • EPC Filter Strategy - strategy for filtering tags. The value can be set to either <i>KeepOnly</i> or <i>RemoveAll</i>. If the value is set to <i>KeepOnly</i>, the filter keeps only the tags that match the specified EPC filter value. If the value is set to <i>RemoveAll</i>, the filter removes all the tags that match the EPC filter value. • EPC Filter Value - only tags with this EPC filter value make it through. • SelfTestMode - indicates if selftestmode is active.
Health Check agent - monitors the health of the edge.	<ul style="list-style-type: none"> • Tracing - display trace output. Value = false; default = false. • Portal ID - the portal ID associated with this agent. Value = P1; default = P1. • Portal Name - the portal name associated with this agent. • Initial Portal State - The initial portal state that the HealthCheckAgent assumes. With the value off, the agent does not publish the health status until it receives the portal signal topic. • Reader ID - the ID of the corresponding reader. • Device Names - A comma-separated list of the observed sensors.
Heartbeat agent - monitors the reader heartbeats.	<ul style="list-style-type: none"> • Tracing - display trace output. • Edge ID - the edge ID associated with this agent. • Edge Name - the edge name associated with this agent. • Heartbeat Period - how often, in milliseconds, heartbeats are reported. • Portal IDs - a comma-delimited list of portals to be monitored. • Reader IDs - a comma-delimited list of readers to be monitored.

Table 4. Agents and property values (continued)

Agent	Agent Property/Property Value
Light Tree agent - controls a lightstack.	<ul style="list-style-type: none"> • Tracing - display trace output. • Portal ID - the portal ID associated with this agent. • Portal Name - the portal name associated with this agent. • GPIO Adapter Prefix - the prefix used to communicate with the IO-Profile • Refresh Topic - the topic that leads to a republish of the actor's state. • Control All Topics - the topic that turns all actors into the given state. • Pins Logical Names - the logical names list of the actors associated to the pins. • Control Green Topic - when received, the corresponding pin is updated. • Duration Green in ms - the length of time in milliseconds that the corresponding pin is on before it goes off. • Invert Green - if set to true, the actor's pin is driven inversely. • IO Green Pin - the pin associated with the corresponding logical actor name. • Control Amber Topic - when received, the corresponding pin is updated. • Duration Amber in ms - the length of time in milliseconds that the corresponding pin is on before it goes off. • Invert Amber - if set to true, the actor's pin is driven inversely. • IO Amber Pin - the pin associated with the corresponding logical actor name. • Control Red Topic - when received, the corresponding pin is updated. • Duration Red in ms - the length of time in milliseconds that the corresponding pin is on before it goes off. • Invert Red - if true, the actor's pin is driven inversely. • IO Red Pin - the pin associated with the corresponding logical actor name. • Control Aux Topic - when received, the corresponding pin is updated. • Duration Aux in ms - the length of time in milliseconds that the corresponding pin is on before it goes off. • Invert Aux - if set to true, the actor's pin is driven inversely • IO Aux Pin - the pin associated with the corresponding logical actor name. • Agent Name - the name of this agent. • Active Green Overwrites - the logical names list of actors that are overwritten if the corresponding actor is active. • Active Amber Overwrites - the logical names list of actors that are overwritten if the corresponding actor is active. • Active Red Overwrites - the logical names list of actors that are overwritten if the corresponding actor is active. • Active Aux Overwrites - the logical names list of actors that are overwritten if the corresponding actor is active.
MicroBroker Configuration agent - configures the MicroBroker bridge.	<ul style="list-style-type: none"> • Tracing - display trace output. • Edge ID - the edge ID associated with this agent. • Edge Name - the edge name associated with this agent. • Edge on Premises - a flag that indicates if the Data Capture and Delivery application is running on RFID Data Transformation or in standalone mode. • Server IP - the IP address or host name of the WebSphere RFID Premises Server. • Server Port - the remote port number on the WebSphere RFID Premises Server. • Bridge Topics Up - a list of topics with messages that should be propagated to the WebSphere RFID Premises Server. • Bridge Topics Down - a list of topics with messages that should be propagated from the WebSphere RFID Premises Server. • Bridge Clean Session - if set to true, the MicroBroker bridge does not retain pending messages from a previous session. • Portal IDs - a list of portal IDs recognized by the edge.

Table 4. Agents and property values (continued)

Agent	Agent Property/Property Value
Portal Controller agent - controls and facilitates portal activity.	<ul style="list-style-type: none"> • Tracing - display trace output. • Portal ID - the portal ID associated with this agent. • Portal Name - the portal name associated with this agent. • Matrix File - the file with the state transitions descriptions. • Operational Mode - 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. • Matrix Queue Processing - specifies if matrix processing happens per each event (false) or for all available events (true). • Error Message 1 Value - the value of error message 1. • Error Message 2 Value - the value of error message 2. • Error Message 3 Value - the value of error message 3. • Error Message 4 Value - the value of error message 4. • Error Message 1 Topic - matrix action 'stateX.Y.out.error=1' publishes this topic with the corresponding value. • Error Message 2 Topic - matrix action 'stateX.Y.out.error=2' publishes this topic with the corresponding value. • Error Message 3 Topic - matrix action 'stateX.Y.out.error=3' publishes this topic with the corresponding value. • Error Message 4 Topic - matrix action 'stateX.Y.out.error=4' publishes this topic with the corresponding value. • Reader On 1 Parameter - matrix action 'stateX.Y.out.reader=ON.1' sets this metadata before turning the reader on. • Reader On 2 Parameter - matrix action 'stateX.Y.out.reader=ON.2' sets this metadata before turning the reader on. • Portal Initial State - defines the initial portal state. • 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 Activation Command Topic - the topic (without prefix) that is sent to turn on the reader. • Reader Activation Command Value - the value that is sent with the message to turn on the reader. • Reader Deactivation Command Value - the value that is sent with the message to turn the reader off. • Reader Activation Signal Topic - the topic (without prefix) that is sent from the reader adapter to confirm that the reader is on. • SelfTestMode - indicates if selftestmode is active. • Sensor 1 initial value - the initial value of sensor 1. • Sensor 1 topic - the topic of the first sensor in the matrix input vector. • Sensor 2 initial value - the initial value of sensor 2. • Sensor 2 topic - the topic of the second sensor in the matrix input vector. • Sensor 3 initial value - the initial value of sensor 3. • Sensor 3 topic - the topic of the third sensor in the matrix input vector. • Sensor 4 initial value - the initial value of sensor 4. • Sensor 4 topic - the topic of the fourth sensor in the matrix input vector. • Sensor 5 initial value - the initial value of sensor 5. • Sensor 5 topic - the topic of the fifth sensor in the matrix input vector. • Strong Checking - logs potential problem situations with matrix processing. • Timer 1 Delay - duration in milliseconds of timer 1 in the matrix input vector. • Timer 2 Delay - duration in milliseconds of timer 2 in the matrix input vector.
Reload agent - reloads the edge configuration	<ul style="list-style-type: none"> • Tracing - displays trace output. • Edge ID - the edge ID associated with this agent. • Edge Name - the edge name associated with this agent. • Reload Topic - reloads the configuration when data of any value is published across this topic.
Restart agent - restarts the OSGi framework.	<ul style="list-style-type: none"> • Tracing - displays trace output. • Edge ID - the edge ID associated with this agent. • Edge Name - the edge name associated with this agent.

Table 4. Agents and property values (continued)

Agent	Agent Property/Property Value
RFID Map agent - transforms tag read information into RFID map objects	<ul style="list-style-type: none"> • Tracing - displays trace output. • Portal ID - the portal ID associated with this agent. • Portal Name - the portal name associated with this agent. • Publication Topics - a comma-delimited list of topics for publishing RfidMap data. • Subscription Topics - a comma-delimited list of topics for receiving tag read data. • Tag Count log level - log level to log aggregation counts (debug/info/warning/error) • SelfTestMode - indicates whether selftestmode is active. • Self Test Mode Publication Topics - a comma-delimited list of topics for publishing RfidMap data under self test mode. • Self Test Mode Subscription Topics - a comma-delimited list of topics for receiving tag read data under self test mode.
Self Test agent - performs reader selftests.	<ul style="list-style-type: none"> • Agent Name - the name of this agent. • Portal ID - the portal ID associated with this agent. • Portal Name - the portal name associated with this agent. • Initial Delay - duration in milliseconds to wait after startup of the agent until the selftest begins. • Output Count - number of outputs available to cycle through in the output test. • Output Length - length in milliseconds of an output to stay activated. • Input Test Length - duration in milliseconds of one input test phase. • Reader Test Length - duration in milliseconds of one reader test phase. • Reader Test Outputs - comma-separated list of output indices to cycle through in the reader test. • Reader Adapter Prefix - name of the reader this instance of this agent is currently running on. • 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 Deactivation Command Value - value for the Reader Activation Command Topic to deactivate the reader. • Self Test Mode - flag to activate and deactivate the selftest mode for this agent.
Tag aggregator agent - aggregates tags.	<ul style="list-style-type: none"> • Tracing - display trace output. • Portal ID - the portal ID associated with this agent. • Portal Name - the portal name associated with this agent. • 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. • 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. • Aggregation Publish Topic - publish aggregated tags to this topic. • Incoming Tags Topic - receive tags from this topic. • SelfTestMode - indicates if selftestmode is active.
Universal Sensor agent - the agent for the switch sensor.	<ul style="list-style-type: none"> • Agent Name - the name of this agent. • Tracing - display trace output. • Portal ID - the portal ID associated with this agent. • Portal Name - the portal name associated with this agent. • Sensor Activelevel - indicates a positive (HIGH) or inverse (LOW) logic of this sensor. • Sensor Aliasname - the alias of this sensor. • Sensor Blocked Timeout - if the sensor is on longer than this amount of time in milliseconds (for example: active, stuck), it issues an error. • Sensor Inactivity Delay - delay in milliseconds if sensor transitions from active to inactive. • Sensor Listen Topic - input topic relevant for this sensor. • Sensor Publish Topic - output topic used by this sensor. • Sensor State Logging - indicates if state changes were logged with INFO, WARNING or ERROR level. • Sensor Pin - the pin number of the output where this sensor is assigned. • SelfTestMode - indicates if selftestmode is active.

Table 4. Agents and property values (continued)

Agent	Agent Property/Property Value
RFID Simulated Reader - simulates an RFID reader.	<ul style="list-style-type: none"> Reader name - the name of the reader and other static values published in TagReports. Antenna - static antenna value published in TagReports. Count - static count value published in TagReports. Send Tag Delay - the delay between tag write periods in milliseconds. Tag Batch Size - the number of tags to send per tag-write period. Length of tag ID - one of : 64, 96 tag length in number of bits. Tag Mode - one of : RFIDTagsEnum : cycles through enumerated list of tags, RFIDTagPrefix : prepends the prefix with hex timestamp for unique tags. Tag Enumeration - comma-delimited hex values of tags: 16 characters for 64bit, 24 characters for 96bit Tag Prefix - the prefix for timestamp generated tag values Activate reader on start - start publishing tags without being specifically turned on over the service bus Tag Reading Expression - 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. 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. 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

Using variables for property values

For the properties listed above, 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 looks like this: `edge.name = "%CONTROLLER_ID%"`, the value in the edge XML will look like this: `edge.name = "E1"` (for Edge E1). Iterative substitutions enable values to be enumerated with each value for that substitution. For example, if the value in the database looks like this: `topics = "[%LOCATIONS]%LOCATIONS%, [%LOCATIONS]"`, the value in the edge XML will look like this: `topics = "P1, P2, P3,"`.

Substitutions for Location-based agents

%LOCATION_ID%

The location ID for the agent on the edge

%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 RFID Premises Server

%CONTROLLER_ID%

The edge ID of the controller

%LOGGING_THRESHOLD%

The logging threshold of the edge

%LOCATIONS_STR%

The locations associated with the controller, in a format compatible with V1.0.2 edge clients

[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 Data Capture and Delivery devices

This section explains Data Capture and Delivery devices and how to manage them using the WebSphere RFID Premises Server Administrative Console.

Data Capture and Delivery devices include physical printers, Bartender and Software logical printers, readers, and simulated readers. Data Capture and Delivery device agents can exist in the system with different configurations for different device configuration groups. 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 Data Capture and Delivery device

This topic describes how to add a new device to your network topology definition. Supported devices are readers, simulated readers, and logical printers.

Devices are readers, simulated readers, and Software 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 RFID 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 **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 Data Capture and Delivery configuration” on page 75.
7. If you selected a simulated reader as the configuration group, continue now with step 8 on page 88. 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 “Reader details” on page 127 or “Printer details” on page 132.

8. Click **Create**. The Devices panel is displayed with the device you added.

Adding Data Capture and Delivery device configuration groups

Use the WebSphere RFID 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.

Devices in the WebSphere RFID 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 RFID 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 deviceconfiguration group.
8. In the **Category** field, click the drop-down arrow and 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 Data Capture and Delivery device

This topic describes how to modify information about a device in your network topology using the WebSphere RFID Premises Server Administrative Console.

Use the following steps to change information about a simulated reader, a reader, or a logical printer.

1. Open the WebSphere RFID 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 Data Capture and Delivery device configuration group

This topic describes how to modify the Data Capture and Delivery configuration group for a particular device using the WebSphere RFID Premises Server Administrative Console.

Use the following steps to modify the configuration group information for a device.

1. Open the WebSphere RFID 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 Data Capture and Delivery device configuration groups” on page 88.
4. Modify the appropriate fields and click **Update**.

Deleting a Data Capture and Delivery device

This topic describes how to delete a device from your network topology using the WebSphere RFID Premises Server Administrative Console.

Use the following steps to delete a simulated reader, a reader, or a logical printer from your network topology.

1. Open the WebSphere RFID 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 Data Capture and Delivery device configuration group

This topic describes how to delete a Data Capture and Delivery configuration group for a particular device using the WebSphere RFID Premises Server Administrative Console.

Use the following steps to delete a configuration group for a device.

1. Open the WebSphere RFID 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**.

Data Capture and Delivery device details

This topic defines the fields on various device panels. Devices are readers, simulated readers, and logical printers.

Reader details

Table 5. Reader device details

Field	Description
Device ID	Enter a unique identifier 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	Enter a unique, textual description of the reader.
Configuration Group	Select the configuration group for the reader.
Communication Protocol	Indicate how you want to communicate with the tag reader. Select TCPIP or SERIAL.
IP Address	Enter the IP address for this tag reader.
IP Port Number	Enter the IP port number for communication with this tag reader. Some default port numbers are listed below, by tag reader type. 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	Enter the serial port number for communication with this tag reader.

Logical printer details:

Table 6. Logical printer device details

Field	Description
Device ID	Enter the ID of the logical tag printer. Note: The identifier must be 10 digits (0-9) or fewer.
Device Name	Enter a unique, textual description of the logical printer.
Configuration Group	Select the configuration group for the logical printer.
Logical Printer Class Name	Choose either Software 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.

Data Capture and Delivery device configuration group details

This topic provides details about the device configuration groups that come with the product for Data Capture and Delivery.

Table 7. 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 Data Capture and Delivery locations

This section explains Data Capture and Delivery locations and how to manage them using the WebSphere RFID Premises Server Administrative Console.

Data Capture and Delivery locations in the WebSphere RFID 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 Data Capture and Delivery configuration” on page 75.

Adding a Data Capture and Delivery location

Use the WebSphere RFID Premises Server Administrative Console to add new Data Capture and Delivery locations to your network topology definition.

Locations in the WebSphere RFID 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 RFID 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 “Data Capture and Delivery location details” on page 95.
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 RFID 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 RFID 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 Data Capture and Delivery location configuration groups

Use the WebSphere RFID Premises Server Administrative Console to add new location configuration groups to your network topology definition. Then select several agents to associate with the new location configuration group.

A location configuration group consists of a name, description, and category. Locations in the WebSphere RFID 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 RFID 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 RFID 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 RFID 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 Data Capture and Delivery location

Use the WebSphere RFID Premises Server Administrative Console to modify Data Capture and Delivery locations in your network topology.

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 RFID 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 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 Data Capture and Delivery location configuration group

This topic describes how to modify the configuration for a particular location using the WebSphere RFID Premises Server Administrative Console.

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 RFID 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 RFID 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:

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 RFID 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 Data Capture and Delivery location

Use the WebSphere RFID Premises Server Administrative Console to delete Data Capture and Delivery locations in your network topology.

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 RFID 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 Data Capture and Delivery location configuration group

This topic describes how to delete a Data Capture and Delivery configuration group for a particular location using the WebSphere RFID Premises Server Administrative Console.

Use the following steps to delete a configuration group for a location.

1. Open the WebSphere RFID 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**.

Data Capture and Delivery 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.

Field	Description
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 location contacts” on page 139 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 location contacts” on page 139 for more information.
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 locations” on page 136 for more information.
Controller**	Displays the controller associated with this location. See “Adding controllers” on page 140 for more information.
Address	Enter the street, city, state, and zip code 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.

Data Capture and Delivery location configuration group details

This topic lists the location configuration groups that come with the product for Data Capture and Delivery.

Table 8. 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 Data Capture and Delivery contacts

This section describes how to manage Data Capture and Delivery location contact information using the WebSphere RFID 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 Data Capture and Delivery contacts

Use the WebSphere RFID Premises Server Administrative Console to add new Data Capture and Delivery location contacts to your network topology definition.

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 Data Capture and Delivery location” on page 91 for more information.

1. Open the WebSphere RFID 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 **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 Data Capture and Delivery contacts

Use the WebSphere RFID Premises Server Administrative Console to modify existing Data Capture and Delivery location contacts in your network topology definition.

1. Open the WebSphere RFID 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 Data Capture and Delivery contacts

Use the WebSphere RFID Premises Server Administrative Console to delete existing location contacts from your network topology definition.

1. Open the WebSphere RFID 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.

Data Capture and Delivery 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.

Field	Description
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 Locations for more information.

* Required field

** This field only displays on the Contact Details panel.

Working with Data Capture and Delivery controllers

This section explains Data Capture and Delivery controllers and how to manage them using the WebSphere RFID Premises Server Administrative Console.

A controller is the component that interacts with and controls devices. It processes, filters, and communicates with the WebSphere RFID 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 Data Capture and Delivery controller

Use the WebSphere RFID Premises Server Administrative Console to add new Data Capture and Delivery controllers to your network topology definition.

Controllers in the WebSphere RFID Premises Server Administrative Console are logical representations of the physical edge devices in your WebSphere RFID 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 RFID 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 **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 Data Capture and Delivery controller configuration groups" on page 99.
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 Data Capture and Delivery controller configuration groups

Use the WebSphere RFID Premises Server Administrative Console to add new controller configuration groups to your network topology definition. Then select one or more agents to associate with each new controller configuration group.

1. Open the WebSphere RFID 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 Data Capture and Delivery controller

Use the WebSphere RFID Premises Server Administrative Console to modify existing Data Capture and Delivery controllers in your network topology definition.

1. Open the WebSphere RFID 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 RFID Premises Server Administrative Console.

You can modify all information except the controller ID. You can also add a location to a controller configuration group.

1. Open the WebSphere RFID 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 on page 100. 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 Data Capture and Delivery controller

Use the WebSphere RFID Premises Server Administrative Console to delete existing Data Capture and Delivery controllers from your network topology definition.

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 RFID 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 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 Data Capture and Delivery controller configuration group

This topic describes how to delete a Data Capture and Delivery configuration group for a particular controller using the WebSphere RFID Premises Server Administrative Console.

Use the following steps to delete a configuration group for a controller.

1. Open the WebSphere RFID 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**.

Data Capture and Delivery 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.
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.
Alert Threshold	<p>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 RFID Premises Server; the lower the alert level, the higher the number of events that are sent to the log file.</p> <p>Choose from the following alert thresholds, from highest to lowest -- for example, selecting debug generates the greatest number of alerts.</p> <ul style="list-style-type: none">• error (default)• warning• info• debug <p>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.</p>
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.

Data Capture and Delivery controller configuration group details

This topic provides details about the controller configuration groups that come with the product for Data Capture and Delivery.

Table 9. 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

Restarting controllers from the console

Use the Reload Configuration function on the Controllers panel to remotely restart an edge controller from the WebSphere RFID Premises Server Administrative Console.

Each time you change a configuration, you must restart the affected edge 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 an edge controller, the changes are not implemented until you restart the edge controller.

By default, the **Reload Configuration** button is set to reload instead of restart. If you are using Data Capture and Delivery, this setting only works with local Data Capture and Delivery. If you are using remote Data Capture and Delivery, you need to edit this line in flow number 4 of the bridge.properties file:

```
flow.4.transformation.0.input.topic.reload.config=reload/+
```

For remote Data Capture and Delivery, the line should change to:

```
flow.4.transformation.0.input.topic.reload.config=restart/+
```

For an explanation of local and remote Data Capture and Delivery controllers, refer to "Data Capture and Delivery controller" on page 6.

Follow these steps to restart an edge controller from the WebSphere RFID Premises Server Administrative Console.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. Depending on your configuration, navigate to either **WRDI Configuration** → **Controllers** or to **Data Capture Configuration** → **Controllers** from the left navigation pane. The Controllers panel displays.
3. Click on the controller that you want to restart. The Edit Controller Details panel displays.
4. Click **Reload Configuration**. The edge controller restarts.

Note: All locations associated with this edge controller are disabled while the device is restarting.

Understanding Data Capture and Delivery PIDs and Factory PIDS

This topic explains Data Capture and Delivery persistence IDs (PIDs) and factory PIDS.

A persistence ID, PID, is the identifier for an OSGi bundle in the Data Capture and Delivery system. PIDs represent the number of instances running on a controller. There are PIDs and factory PIDs. A PID means that there is one instance of an agent running on a controller. A factory PID means that multiple instances of the agent can run on a controller. For more information about PIDs and factory PIDs, refer to the OSGi R4 specification.

Importing the Data Capture and Delivery configuration file

This section explains the Data Capture and Delivery XML configuration file and how to import it using the WebSphere RFID Premises Server Administrative Console.

This section contains the following topics:

WebSphere RFID Premises Server 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 RFID Premises Server.

You can configure the server using the **Import Configuration** link in the WebSphere RFID Premises Server Administrative Console 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/ibmrfdadmin/XMLConfigAdmin

XML Schema

Below is the XML schema that defines the rules for headless configuration of the WebSphere RFID 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 RFID Premises Server installation and contains the actual rules used on the server.

```
<schema targetNamespace="http://www.ibm.com"
version="0.1" xmlns="http://www.w3.org/2001/XMLSchema"
xmlns:ibmrfdconfigadmin="http://www.ibm.com" xmlns:ati="http://www.w3.org/2001/XMLSchema">
<element name="configurationAdmin" type="ibmrfdconfigadmin:IBMRFDConfigAdmin"/>
<complexType name="IBMRFDConfigAdmin">
<sequence>
<element name="requests" type="ibmrfdconfigadmin: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"/>
</complexType>
<!-- REQUESTS DEFINITION -->
<complexType name="Requests">
<sequence>
<element maxOccurs="unbounded" minOccurs="1" name="request" type="ibmrfdconfigadmin:Request"/>
</sequence>
</complexType>
<!-- REQUEST DEFINITION -->
<complexType name="Request">
<all>
<element maxOccurs="1" minOccurs="0"
name="agentconfigurations" type="ibmrfdconfigadmin:AgentConfigurations"/>
<element maxOccurs="1" minOccurs="0"
name="serverconfigurations" type="ibmrfdconfigadmin:ServerConfigurations"/>
</all>
<attribute name="type" type="ibmrfdconfigadmin: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="ibmrfdconfigadmin:Configuration"/>
</sequence>
</complexType>
<!-- CONFIGURATION DEFINITION -->
<complexType name="Configuration">
<sequence>
<element maxOccurs="1" minOccurs="0"
name="properties" type="ibmrfdconfigadmin: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="ibmrfdconfigadmin: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"/>
</complexType>
<!-- *****SERVER CONFIGURATIONS DEFINITION ***** -->
<complexType name="ServerConfigurations">
    <sequence>
        <element maxOccurs="1" minOccurs="0"
            name="configurationgroup" 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"/>
</attributeGroup>
</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:configgroupmetadata-attrgroup">
  </attributeGroup>
</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">
  </attributeGroup>
</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">
  </attributeGroup>
</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"/>
  </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"/>
  <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="ibmrfdconfigadmin:metadata-attrgroup">
  </attributeGroup>
</complexType>
<!-- CONTROLLER DEFINITION -->
<complexType name="Controller">
  <sequence>
    <element maxOccurs="unbounded" minOccurs="0"
      name="controller-category-metadata"
      type="ibmrfdconfigadmin:ControllerCategoryMetaData"/>
    <element maxOccurs="1" minOccurs="0"
      name="controller-locations" type="ibmrfdconfigadmin:ControllerLocations"/>
  </sequence>
  <attribute name="controllerid" type="integer" use="required"/>
  <attribute name="controllername"
    type="ibmrfdconfigadmin:non-empty-string" use="required"/>
  <attribute name="macaddress" type="string" use="optional"/>
  <attribute name="edgeonpremises" type="string" use="optional"/>
  <attribute name="alertlevel" type="string" use="optional" default="error"/>
  <attribute name="config-group-name"
    type="ibmrfdconfigadmin:non-empty-string" use="required"/>
  <attribute name="controlleridprefix"
    type="ibmrfdconfigadmin:non-empty-string" use="optional" default="C"/>
</complexType>
<!-- CONTROLLER CATEGORY METADATA -->
<complexType name="ControllerCategoryMetaData">
  <attributeGroup ref="ibmrfdconfigadmin:metadata-attrgroup">
  </attributeGroup>
</complexType>
<!-- CONTROLLER LOCATION -->
<complexType name="ControllerLocations">
  <sequence>
    <element maxOccurs="unbounded" minOccurs="0"
      name="locationid" type="ibmrfdconfigadmin:non-empty-string"/>
  </sequence>
</complexType>
<!-- CONTACT DEFINITION -->
<complexType name="Contact">
  <attribute name="name" type="ibmrfdconfigadmin: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="ibmrfdconfigadmin:non-empty-string"
    use="required"/>
  <attribute name="config-group-type"
    type="ibmrfdconfigadmin:agentconfiggroupTypeEnum" use="required"/>
  <attribute name="config-group-name"
    type="ibmrfdconfigadmin:non-empty-string" use="optional"/>
</attributeGroup>
<attributeGroup name="metadata-attrgroup">
  <attribute name="name"
    type="ibmrfdconfigadmin: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="ibmrfdconfigadmin: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"/>
    </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 10. String substitution macros for XML configuration file

ControllerAgent string substitution name (Macros)	Value
%PREMISES_IP%	WebSphere RFID Premises Server IP address

Table 10. String substitution macros for XML configuration file (continued)

ControllerAgent string substitution name (Macros)	Value
%DMS_HOSTNAME%	Device Manager server host name
%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 (WRDI only)
%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 (WRDI only)
%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="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"/>
          </properties>
        </configuration>
        <configuration factoryPid="com.motorola.symbol.bsp.device.factory.SymbolBspDeviceFactory" name="SAMSys CHUMP"
          config-group-type="DeviceType" bundlename="" bundleversion="1.1">
          <properties>

```

```
</properties>
</configurati
```

```

    <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="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="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="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="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>
  </configurationgroup>
</configurationgroups>
  <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>
  </devices>

```

```

    <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"
    edgeonpremises="" macaddress="kjajfkdfd">
      <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"
    edgeonpremises="" macaddress="kjajfkdfd">
      <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 Data Capture and Delivery XML configuration file

This topic describes how to import the Data Capture and Delivery XML configuration file that configures the server.

1. Open the WebSphere RFID 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.

Working with Data Capture and Delivery print templates

This section contains information on managing Data Capture and Delivery print templates using the WebSphere RFID Premises Server Administrative Console.

A print template in the WebSphere RFID 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:

	<i>IBM_RFID_HOME\premises\pvs\templates</i>
	<i>IBM_RFID_HOME/premises/pvs/templates</i>

They can be customized to meet your specific label requirements.

When you create a print template in the WebSphere RFID Premises Server Administrative Console, that information is stored in the WebSphere RFID Premises Server database. When the edge controller is started, it receives the location information for all of the currently defined templates. When you submit a print job from the Print, Verify, and Ship Reference User Interface, the edge controller reads the name of the template from the print request and retrieves the required template from the previously defined location. The edge controller then completes the fields of the template with the appropriate data from the print request.

You can create print templates for two types of printers: logical and physical. A print template for a logical tag 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 and the Bartender print template must be on the Bartender server to access it. A print template for a physical tag printer must be stored on an IBM HTTP Server so that the edge controller can download it during RFID Data Transformation startup. The IBM HTTP Server can reside on either the same server as WebSphere RFID 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 Data Capture and Delivery print templates

Use the WebSphere RFID Premises Server Administrative Console to add new Data Capture and Delivery print templates to your network topology.

Note: In this release, Data Capture and Delivery does not support physical printers. To create a print template for a physical printer in WebSphere RFID Device Infrastructure, refer to “Adding print templates” on page 134.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays. .
2. Navigate to **Data Capture Configuration** → **Print Templates** from the left panel. The Print Templates panel displays.
3. Click **New**. The Create a New Print Template panel displays.
4. In the **Printer Type** field, select **Logical**.
5. In the **Properties Location URL** field, enter the location of the template file.
 - If you are creating a print template for a Loftware logical tag printer, use the following convention: `file://Loftware_label_name`. For example:
`file://Logical1-template.lwl`
 - If you are creating a print template for a Bartender logical tag printer, use this convention: `file://Bartender_label_name`. For example:
`file://Logical1-template.btw`
6. Click **Create**. The print template is saved.
7. 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 186 for more information.

Modifying Data Capture and Delivery print templates

Use the WebSphere RFID Premises Server Administrative Console to modify existing Data Capture and Delivery print templates.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **Data Capture Configuration** → **Print Templates** from the left panel. The Print Templates panel displays.
3. Click on the print template that you want to modify. The Edit Print Template Details panel displays.
4. Make the necessary changes and click **Update**.

Deleting Data Capture and Delivery print templates

Use the WebSphere RFID Premises Server Administrative Console to delete existing Data Capture and Delivery print templates from your network topology.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **Data Capture Configuration** → **Print Templates** from the left 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.

Working with Data Capture and Delivery 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 RFID 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 Data Capture and Delivery update sites

Use the WebSphere RFID Premises Server Administrative Console to add new Data Capture and Delivery update sites to your network topology.

Before accessing device-specific download sites, you must define the updates sites.

1. Open the WebSphere RFID 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 Data Capture and Delivery update sites

This topic describes how to modify information about an update site in your network topology using the WebSphere RFID Premises Server Administrative Console.

Use the following steps to change information about an update site.

1. Open the WebSphere RFID 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 Data Capture and Delivery update sites

This topic describes how to delete an update site from your network topology using the WebSphere RFID Premises Server Administrative Console.

Use the following steps to delete an update site from your network topology.

1. Open the WebSphere RFID 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.

Managing your WebSphere RFID Device Infrastructure configuration

This section describes how to create and manage configuration groups for controllers, locations, and devices within your WebSphere RFID Premises Server infrastructure using the WebSphere RFID Premises Server Administrative Console and WebSphere RFID Device Infrastructure.

Modifying the property values of agents

Use the WebSphere RFID Premises Server Administrative Console to modify the property values of agents that have been defined in the network topology.

These properties and values are used to create XML configuration files -- similar to the static XML configuration files in the edge controller development kit -- that are then used to configure edge controllers. For more information about agents, including a list of possible agents and a description of each, refer to “Agent details.”

There are two types of agents that you can modify from this panel: controller-based agents and reader-based agents. Use the steps below to modify the properties of these agents.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. Navigate to **WRDI Configuration** → **Agent Configuration** from the left navigation pane.
3. Choose the type of agent, either controller or reader, for which you are modifying properties:
 - a. Click **Controller agent** to update controller properties. The WRDI Controller Agents List is displayed.
 - b. Click **Reader agent** to update reader properties. The WRDI Reader Agents List is displayed.
4. Select the agent for which you are modifying the property values. You cannot edit this list. The list of agents is determined at edge controller install time.
5. Select the location (for a reader agent) or the controller (for a controller agent) for which you are modifying the property values. By default, the location is set to all (“”). You cannot edit this field.
6. Select the property for which you are changing the value.
7. Modify the value. For a list of properties and possible values, refer to “Agent details.”
8. Click **Update**. The changes are saved.

Agent details

The following table defines the fields on the Edit Agent Properties panel of the WebSphere RFID Premises Server Administrative Console.

Types of agents

Note: This topic applies to agents for WebSphere RFID Device Infrastructure version 1.1.1 only to support older WebSphere RFID Device Infrastructure version 1.1.1 clients. If you are using Data Capture and Delivery agents for version 6.0 clients, ignore this topic. For Data Capture and Delivery version 6.0 agents, refer to “Data Capture and Delivery agent details” on page 81.

Agents are OSGi bundles that communicate with MicroBroker. These agents are installed during the initial edge controller installation and configuration process. Agents exist for each of the supported devices, including tag readers, motion sensors, light trees, and more. The agents that are installed in your network are determined by the bundle parameters you set during the initial installation of Device Manager server or by the bundle parameters set during any subsequent agent deployments.

- **Reader agents** connect the tag reader adapters to MicroBroker. Although each reader agent has specific code for interfacing to each tag reader adapter, the output form and commands received from other tag reader agents are identical for all tag reader agents.
- **Printer agents** connect the tag printer adapters to MicroBroker.
- **Light Tree agents** connect the light tree I/O adapters to MicroBroker.
- **Duty Cycle agents** monitor duty cycle usage, which indicates the amount of time the tag readers have been active.
- **Motion Sensor agents** connect the motion sensor I/O adapters to MicroBroker.
- **Switch agents** connect the switch I/O adapters to MicroBroker.
- **Filter agents** filter tag data according to configured filters.
- **Controller agents** coordinate activities on the edge controller, such as listening for events from motion sensors and triggering tag readers for specified periods of time.
- **Self-test agents** coordinate location self-test I/O sequences and durations.
- **Universal Sensor agents** support light barrier sensor devices by detecting blocking situations in the enhanced Dock Door Receiving usage scenario.
- **Application Ping agents** report the status of the back-end system back to the edge controller.
- **Health Check agents** manage the system health-checking activities and coordinate the presentation of the system status at the portal site.

Note: Some of these agents (UniversalSensor, ApplicationPing, HealthCheck) are enabled by running additional database scripts.

Agent properties and values

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 the section below for details on what variables can be substituted.

Important: Because the PortalControllerAgent and the UniversalSensorAgent are configurable for sensors and related MicroBroker topics, it might be confusing to understand both agent configurations. The sensor definitions for one agent are completely independent of the other.

Table 11. Agents and property values

Agent	Agent Property/Property Value
All agents	<p>Association Property: This property enables the agent to be designated as being associated with a tag reader or tag printer at that location. The property names are “controller.association” and “location.association.” The value must be specified as one of the following:</p> <ul style="list-style-type: none"> • NONE: Agent is disabled and cannot be included in the XML. • ALL: Agent is always enabled and always included in the XML. • READER: Agent is associated with locations with tag readers. If a location-based agent is associated with tag readers, it is included only if there is a tag reader at that location. If a controller based agent is associated with tag readers, it is included only if there is at least one tag reader associated with that controller. • PRINTER: Agent is associated with locations with tag printers. If a location-based agent is associated with tag printers, it is included only if there is a tag printer at that location. If a controller-based agent is associated with tag printers, it is included only if there is at least one tag printer associated with that controller. • If no value is found, “ALL” is assumed, and the agent is always included.
Reader agents -- general properties	<ul style="list-style-type: none"> • green - the output pin on the Digital I/O board to which the green light is attached: default = 2 • red - the output pin on the Digital I/O board to which the red light is attached: default = 0 • amber - the output pin on the Digital I/O board to which the amber light is attached: default = 1 • motion - the input pin on the Digital I/O board to which the motion sensor is attached: default = 0 • inputpins - indicates the types of inputs connected to the Digital I/O board: default = switch,motion • switch - input pin on the Digital I/O board to which the switch is wired: default = 1 • beep - output pin on the Digital I/O board to which the noise signal is attached: default = 3. To enhance performance, disable beep by setting visualizeReadOccurred to OFF; the default is ON. • transport.connection - Device Kit transport type for connection to the tag reader: default = com.ibm.esc.tcpip.connection.TcpipConnection (determined on the reader setting page) • transport.host - Hostname / IP address of the tag reader (determined on the tag reader setting page) • transport.remoteport - IP port for connection to the tag reader (determined on the tag reader setting page) • transport.comport - Serial port number for the tag reader (determined on the tag reader setting page) • reader.id - the ID for the tag reader • reader.name -- the unique, textual description of the reader • io.id - ID used between agents to identify handler of IO events. Setting this variable to 'NOT_SUPPORTED' disables I/O on the tag reader and any hardware IO updates on the tag reader are subsequently ignored. • portal.id - the location with which the tag reader is associated • portal.name -- the unique, textual description of the portal location • selftestmode - a flag that indicates if the tag reader is in self-test mode • location.association - NONE ALL READER PRINTER as describe at the top of this table • filter.duplicates - indicates if the reader should filter duplicate tags. The default is OFF. Setting this variable to ON enhances performance. • duplicates.reset.topic - a topic that resets the duplicates and clears the duplicates cache. • duplicates.reset.value - the value of the message to reset the duplicates and clear the duplicates cache. • aggregateTags - a flag that indicates if the reader should aggregate tag reads. The default is OFF. Setting this variable to ON enables the reader agent, instead of the TagAggregatorAgent, to aggregate tags which enhances performance. • aggregation.publish.topic - a topic that the reader publishes for the tag aggregation.

Table 11. Agents and property values (continued)

Agent	Agent Property/Property Value
Reader agents (for example, AlienReaderAgent) -- Reader-specific properties	<ul style="list-style-type: none"> • Alien reader-specific properties: <ul style="list-style-type: none"> – alien.pollingreadrate - the rate at which to poll the Alien tag reader: default=666 ms – alien.pollinggpiorate - alien.pollinggpiorate - the rate at which to poll the Alien tag readers' Digital I/O: default=250 ms The special value for all tag reader pollinggpiorate properties is -1. Setting the value to -1 disables the I/O on the tag reader -- any hardware IO updates on the tag reader are subsequently ignored. • Intermec tag reader-specific properties: <ul style="list-style-type: none"> – intermec.pollingreadrate - the rate at which to poll the Intermec reader: default=666 ms – intermec.pollinggpiorate - the rate at which to poll the Intermec tag readers' Digital I/O: default = 250 ms The special value for all tag reader pollinggpiorate properties is -1. Setting the value to -1 disables the I/O on the tag reader -- any hardware IO updates on the tag reader are subsequently ignored. • Matrics tag reader-specific properties: <ul style="list-style-type: none"> – symbol.pollingreadrate - the rate at which to poll the Symbol tag reader: default=666 ms – symbol.pollinggpiorate - the rate at which to poll the Symbol tag readers' digital I/O. The special value for all tag reader pollinggpiorate properties is -1. Setting the value to -1 disables the I/O on the tag reader -- any hardware IO updates on the tag reader are subsequently ignored. • TagSys tag reader-specific properties: <ul style="list-style-type: none"> – tagsys.pollingreadrate - the rate at which to poll the Tagsys tag reader: default=666 ms – tagsys.pollinggpiorate - the rate at which to poll the Tagsys tag readers' Digital I/O: default=250 ms The special value for all tag reader pollinggpiorate properties is -1. Setting the value to -1 disables the I/O on the tag reader -- any hardware IO updates on the tag reader are subsequently ignored. – tagsys.tagtype - the type of tag to read: default="6" (possible values: 0 = C210; 1 = C220 2 = C240; 3 = C270 with anti-collision; 4 = C270 with unselected read; 5 = C270 with EAS read; 6 = ISO 15693 STD; 7 = ISO 15693 C370; 8 = EPC) • FeigUHF tag reader-specific properties: <ul style="list-style-type: none"> – feig.pollingreadrate - the rate at which to poll the Feig tag reader: default=666 ms – feig.pollinggpiorate - the rate at which to poll the Feig tag readers' Digital I/O: default=250 ms The special value for all tag reader pollinggpiorate properties is -1. Setting the value to -1 disables the I/O on the tag reader -- any hardware IO updates on the tag reader are subsequently ignored. • Symbol tag reader-specific properties: <ul style="list-style-type: none"> – symbol.pollingreadrate - the rate at which to poll the Symbol tag reader: default=666 ms – symbol.pollinggpiorate - the rate at which to poll the Symbol tag readers' digital I/O. The special value for all tag reader pollinggpiorate properties is -1. Setting the value to -1 disables the I/O on the tag reader -- any hardware IO updates on the tag reader are subsequently ignored.
Light Tree agent - dictates the behavior of the light trees.	<ul style="list-style-type: none"> • duration.ms.beep - the amount of time to signal when a beep request is received: ms • ignore.green.while.red - whether any green light indicators should be discarded if the light tree is currently red: default=false • duration.ms.green -default=500 the amount of time to signal when a green light request is received: default=2000 ms • duration.ms.red - the amount of time to signal when a red light request is received: default=2000 ms • io.id - ID used between agents to identify handler of IO events • portal.id - the location with which the light tree is associated • portal.name -- the unique, textual description of the portal location • selftestmode - a flag that indicates if the light tree is in self-test mode • location.association - NONE ALL READER PRINTER as describe at the top of this table • operational.invert - indicates portal health. The possible values are true or false. If the value is false and the portal is operational, then the light is on. If set to true and the portal is operational, then the light is off. The default value is false. • operational.refresh - indicates whether the configured topic should refresh the operational light. The default value is false. You should set it to true if the reader agent light tree and the light tree agent are out of synch. Then when the configured topic sends out a signal, the operational light refreshes. • operational.refresh.topic - points to the topic used to perform the operational light refresh. The default is edge/<edge_id>/signal/heartbeat, but it can point it to other topics.

Table 11. Agents and property values (continued)

Agent	Agent Property/Property Value
Duty Cycle agent - monitors the duty cycle times, which indicate how long the tag readers have been active.	<ul style="list-style-type: none"> check.interval.ms - the amount of time between checks of the duty cycle times: default = 1000 ms check.periodically - whether the agent should check the duty cycle periodically or only when requested. default = false (only when requested) sampling.period.ms - the time interval at which you want the agent to analyze if the duty cycle time has been exceeded, if <i>check.periodically</i> is set to true: default = 6000 ms limit.percent - the percentage of time which should cause the monitor to trigger: default = 10 ms portal.id - the location with which this agent is associated portal.name -- the unique, textual description of the portal location selftestmode - a flag that indicates if this agent is in self-test mode location.association - NONE ALL READER PRINTER as describe at the top of this table
Motion Sensor agent - dictates the behavior of the motion sensor.	<ul style="list-style-type: none"> delayafterquiet - the amount of time to elapse between the moment that motion is no longer detected to the moment the motion sensor is turned off: default = 2000 ms io.id - ID used between agents to identify handler of I/O events portal.id - the location with which the motion sensor is associated portal.name -- the unique, textual description of the portal location selftestmode - a flag that indicates if the motion sensor is in self-test mode location.association - NONE ALL READER PRINTER as describe at the top of this table
Switch agent - dictates the behavior of the switch.	<ul style="list-style-type: none"> io.id - ID used between agents to identify handler of I/O events portal.id - the location with which the switch is associated portal.name -- the unique, textual description of the portal location selftestmode - a flag that indicates if the switch is in self-test mode location.association - NONE ALL READER PRINTER as describe at the top of this table
<p>UniversalSensorAgent - supports light barrier sensor devices by detecting blocking situations in the enhanced Dock Door Receiving usage scenario.</p> <p>Depending on how you configure the UniversalSensorAgent, it can combine the functions of the Motion Sensor agent and the Switch agent.</p>	<ul style="list-style-type: none"> sensor.aliasname - the sensor alias name used in log messages portal.id - the location with which the sensor agent is associated portal.name - the unique, textual description of the portal location listen.topic - a device IO topic for which the sensor listens location.association - NONE ALL READER PRINTER as describe at the top of this table selftestmode - a flag that indicates if the sensor is in self-test mode statelogging - a flag that indicates whether state changes should be logged at the ERROR, INFO, or WARNING level. activelevel - the values are HIGH or LOW. If set to HIGH when the device IO topic is ON, then the sensor is active. If set to HIGH when the device IO topic is OFF, then the sensor is inactive. If set to LOW when the device IO topic is ON, then the sensor is inactive. If set to LOW when the device IO topic is OFF, then the sensor is active. publish.topic - a MicroBroker topic that the sensor publishes for this agent. Each sensor has the following output signals that indicate the sensor's status changes: <ul style="list-style-type: none"> On - sensor is active, which means that the motion sensor senses movement and the light barrier is interrupted. Off - the sensor is inactive, which means the motion sensor senses no movement and the light barrier is free. Error - the sensor is blocked or not operable, which means that the motion sensor is physically disconnected and the light barrier is permanently interrupted. <p>The sensors are controlled by a generic sensor agent that can handle three different sensors; for example, it handles the light barrier and the motion detector.</p> inactivitydelay - an amount of time in minutes and seconds that indicates the delay in the transition from active to inactive in the sensor output blockedtimeout - if a sensor signals that it is in active state for this amount of time (indicated in minutes and seconds), then the MicroBroker issues an error message <p>Important: Because the PortalControllerAgent and the UniversalSensorAgent are configurable for sensors and related MicroBroker topics, it might be confusing to understand both agent configurations. The sensor definitions for one agent are completely independent of the other.</p>

Table 11. Agents and property values (continued)

Agent	Agent Property/Property Value
<p>Filter agent - controls the tag filtering behavior for sending tag information to the WebSphere RFID Premises Server.</p> <p>Note: Items that apply to the <i>Interest</i> filter:</p> <ul style="list-style-type: none"> • Supports any number (0-N) of Interest definitions to include and exclude. • Multiple include definitions are applied such that a tag matching at least one of the Interest definitions is not filtered out. Tags matching none of the Interest definitions are filtered out. • Multiple exclude definitions are applied such that a tag matching at least one of the Interest definitions is not filtered out. Tags matching none of the Interest definitions are filtered out. • Filters defined with include and exclude definitions filter out any tags that do not pass both qualifications. The include care mask list is matched up to the include pattern mask list to specify include Interest definitions. The same matching applies for exclude lists. • The mask values should be space-delimited hex values. • Multiple masks can be defined by delimiting them with a comma. • If multiple masks are defined, the number of comma-delimited masks in the care list has to match the number of masks in the pattern list. 	<ul style="list-style-type: none"> • filters - the comma-delimited list of filters that are applied to all incoming tags. The list can include any of the following filter types: <i>Duplicates</i>, <i>DecayingDuplicates</i>, <i>CaseTags</i>, <i>EpcFilter</i>, or <i>Interest</i>. • duplicates.decay.limit.sec - the length of time since a tag was last seen that it should remain in the duplicates list: default = 5 seconds • duplicates.decay.cleanup.sec - the length of time between purges of old entries on the duplicates list: default = 2 seconds • epc.filter.value - an integer filter value that is matched against the EPC filter value for a tag. • epc.filter.strategy - strategy for filtering tags. The value can be set to either "KeepOnly" or "RemoveAll." If the value is set to "KeepOnly," the filter keeps only the tags that match the specified EPC filter value. If the value is set to "RemoveAll," the filter removes all the tags that match the EPC filter value. • 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 excludes 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. • portal.id - the location with which the filter is associated • portal.name -- the unique, textual description of the portal location • selftestmode - a flag that indicates if the filter is in self-test mode • location.association - NONE ALL READER PRINTER as describe at the top of this table • trigger.reset.topic - topic to reset the filters and clear filter cache • trigger.reset.value - value of the message to reset the filters and clear the filter cache
<p>ArcomIoDk agent - controls the general purpose I/O card on Arcom Viper devices.</p> <p>Note: This agent is used only when Arcom is being used as the edge controller.</p>	<ul style="list-style-type: none"> • green - the output pin on the Digital I/O board to which the green light is attached: default = 2 • red - the output pin on the Digital I/O board to which the red light is attached: default = 0 • amber - the output pin on the Digital I/O board to which the amber light is attached: default = 1 • heartbeat.period.ms - the amount of time between heartbeats from the edge controller to the reader: default = 10,000 ms • motion - the input pin on the Digital I/O board to which the motion sensor is attached: default = 0 • transport.connection - Device Kit transport type for connection to the reader: default = com.ibm.esc.tcpip.connection.TcpipConnection • inputpins - indicates the types of input connected to the Digital I/O board: default = switch,motion • switch - input pin on the Digital I/O board to which the switch is wired: default = 1 • beep - output pin on the Digital I/O board to which the noise signal is attached: default = 3 • device.filename - filename for the Digital I/O board: default = 0 • device.path - path to the device filename for the Digital I/O board: default = /dev/arcom/aim104/relay8 • transport.monitor.period.ms - polling rate for monitoring the Digital I/O devices: default = 250 • io.id - ID used between agents to identify the handler of I/O events • portal.id - the location with which the Arcom device is associated • portal.name -- the unique, textual description of the portal location • selftestmode - a flag that indicates if the Arcom device is in self-test mode • location.association - NONE ALL READER PRINTER as describe at the top of this table

Table 11. Agents and property values (continued)

Agent	Agent Property/Property Value
Self-test agent - controls the location when placed into self-test mode.	<ul style="list-style-type: none"> input-test-length - length of time for the input test when input is triggered: default = 30000 ms output-delay - length of time between cycles during the output test: default = 1000 ms portal.id - the location with which this agent is associated portal.name -- the unique, textual description of the portal location selftestmode - a flag that indicates if this agent is in self-test mode location.association - NONE ALL READER PRINTER as describe at the top of this table
PortalControllerAgent - a configurable agent that receives sensor signals from the Universal Sensor agent.	<ul style="list-style-type: none"> portal.id - the location with which the controller is associated portal.name - the unique, textual description of the portal location selftestmode - a flag to indicated whether the controller is in self-test mode timer.delay - indicates the delay value for each timer set to handle timeouts sensor.topic - a subscribed sensor topic sensor.initial - defines the initial state of the sensor topic. The possible values are ON or OFF. The default value is OFF location.association - NONE ALL READER PRINTER as describe at the top of this table matrix.properties - the load location the configuration property file. The possible values are: bundle: http: file: strongchecking - the possible values are ON or OFF. If the value is ON, then the controller agent issues a warning if there are problems with a transition state. This value should be ON only when you are in the process of developing the matrix.properties file and the rules for transition states. For a production environment, the value should be OFF. operationalmode - indicates the meaning of the yellow light. The possible values are READER or PORTAL. portal.initial - ON OFF - defines the initial state of the portal. If the value is set to ON, the portal starts in an active state. The default value is OFF. <p>Important: Because the PortalControllerAgent and the UniversalSensorAgent are configurable for sensors and related MicroBroker topics, it might be confusing to understand both agent configurations. The sensor definitions for one agent are completely independent of the other.</p>
Controller agent	<ul style="list-style-type: none"> portal.id - the location with which the controller is associated portal.name -- the unique, textual description of the portal location reader.id - the ID for the tag reader associated with the controller's location selftestmode - a flag to indicated whether the controller is in self-test mode location.association - NONE ALL READER PRINTER as describe at the top of this table portal.initial.state - ON OFF - defines the initial state of the portal. If the value is set to ON, the portal starts in an active state. The default value is OFF.
Application Ping agent	<ul style="list-style-type: none"> edge.id - the controller with which this agent is associated edge.name - the unique, textual description of the edge controller controller.association - NONE ALL READER PRINTER as describe at the top of this table. The default is ALL. <p>Note: These properties are set to defaults that are optimal for checking the backend system during a testing scenario. In production these property values should be set to longer time intervals.</p> <ul style="list-style-type: none"> timeinterval.error - the amount of time allowed for the backend to return with an error message. Set the value in milliseconds. The default is 30,000 ms. response.timeout - the amount of time allowed before a timeout response is issued. Set the value in milliseconds. The default is 5,000 ms. timeinterval.regular - the amount of time allowed for the backend to return with a response. Set the value in milliseconds. The default is 60,000 ms.
Health Check agent	<ul style="list-style-type: none"> portal.id - the location with which the health check is associated portal.name - the unique, textual description of the portal location selftestmode - a flag that indicates if the agent is in self-test mode. The default is OFF. location.association - NONE ALL READER PRINTER as describe at the top of this table. The default is READER. portal.initial - the initial portal state, which must match the state that is configured in the Portal Controller agent. The default is ON.

Table 11. Agents and property values (continued)

Agent	Agent Property/Property Value
Tag aggregation agent	<ul style="list-style-type: none"> • trigger.start.topic - Topic used for starting aggregation of tags • trigger.stop.topic - Topic used for stopping aggregation of tags • aggregator.publish.topic - Topic on which aggregated tags are published • portal.id - the location with which this agent is associated • portal.name -- the unique, textual description of the portal location • selftestmode - a flag to indicated whether this agent is in self-test mode • location.association - NONE ALL READER PRINTER as describe at the top of this table • trigger.start.value - message value used for starting aggregation of tags • trigger.stop.value - message value used for stopping aggregation of tags • trigger.dump.topic - topic used to publish the collection of tags and clear the cache. Can be the same value as the stop topic. • trigger.dump.value - message value used for dumping aggregation of tags • aggregator.incoming.tag.topic - topic from which the tags to be aggregated are read <p>Note: To disable Tag Aggregation, set the location.association property to NONE.</p>
Zebra printer agent	<ul style="list-style-type: none"> • transport.connection - Device Kit transport type for connection to the tag reader: default = com.ibm.esc.tcpip.connection.TcpipConnection • transport.host - IP address of the tag printer. (Determined on the tag printer settings page) • transport.remoteport - IP port for connecting to the tag printer (Determined on the tag printer settings page) • transport.comport - Serial port for connecting to the tag printer (Determined on the tag printer settings page) • printer.id - the ID for the tag printer • printer.name -- the unique, textual description of the printer • heartbeat.period.ms - the amount of time between heartbeats from the edge controller to the tag printer: default = 10,000 ms • location.association - NONE ALL READER PRINTER as describe at the top of this table
Printronix printer agent	<ul style="list-style-type: none"> • transport.connection - Device Kit transport type for connection to the tag reader: default = com.ibm.esc.tcpip.connection.TcpipConnection • transport.host - IP address of the tag printer. (Determined on the tag printer settings page) • pxml.transport.remoteport - IP port for connecting to the tag printer for pxml status information • transport.comport - Serial port for connecting to the tag printer (Determined on the tag printer settings page) • printer.id - the ID for the tag printer • printer.name -- the unique, textual description of the printer • heartbeat.period.ms - the amount of time between heartbeats from the edge controller to the tag printer: default = 10,000 ms • location.association - NONE ALL READER PRINTER as describe at the top of this table
IBM 6700 printer agent	<ul style="list-style-type: none"> • transport.connection - Device Kit transport type for connection to the reader: default = com.ibm.esc.tcpip.connection.TcpipConnection • transport.host - IP address of the tag printer. (Determined on the tag printer settings page) • pxml.transport.remoteport - IP port for connecting to the tag printer for pxml status information • transport.comport - Serial port for connecting to the tag printer (Determined on the tag printer settings page) • printer.id - the ID for the tag printer • printer.name -- the unique, textual description of the printer • heartbeat.period.ms - the amount of time between heartbeats from the edge controller to the tag printer: default = 10,000 ms • location.association - NONE ALL READER PRINTER as describe at the top of this table
Printer Controller agent	<ul style="list-style-type: none"> • printer.id - the ID for the tag printer • printer.name -- the unique, textual description of the printer • location.association - NONE ALL READER PRINTER as describe at the top of this table

Table 11. Agents and property values (continued)

Agent	Agent Property/Property Value
MicroBroker Configuration agent	<ul style="list-style-type: none"> server.port -- the server port for MicroBroker on the WebSphere RFID Premises Server server.ip -- the IP address for the instance of MicroBroker on the WebSphere RFID Premises Server bridge.topics.up -- the topics that are bridged up to the WebSphere RFID Premises Server. These topics, when published on the local broker, are forwarded to the premises server broker instance. bridge.topics.down -- the topics that are bridged down from the WebSphere RFID Premises Server. These topics, when published on the WebSphere RFID Premises Server broker, are forwarded to the edge broker instance. portal.ids -- A list of the locations with tag readers managed by the edge. Note: This property is deprecated. It is included here for compatibility with 1.0.2 edge Clients. portal.name -- the unique, textual description of the portal location edge.id -- the controller with which this agent is associated edge.name -- the unique, textual description of the edge controller controller.association -- NONE ALL READER PRINTER as describe at the top of this table
Heartbeat agent	<ul style="list-style-type: none"> heartbeat.period.ms -- the amount of time between heartbeats from the edge controller to the WebSphere RFID Premises Server: default = 60,000 ms edge.id -- the controller with which this agent is associated controller.association -- NONE ALL READER PRINTER as describe at the top of this table
Alert agent	<ul style="list-style-type: none"> threshold -- the threshold for sending alerts up to the WebSphere RFID Premises Server -- ERROR WARNING INFO DEBUG edge.id -- the controller with which this agent is associated edge.name -- the unique, textual description of the edge controller controller.association -- NONE ALL READER PRINTER as describe at the top of this table
Restart agent	<ul style="list-style-type: none"> edge.id -- the controller with which this agent is associated edge.name -- the unique, textual description of the edge controller controller.association -- NONE ALL READER PRINTER as describe at the top of this table
Edge Configuration agent	<ul style="list-style-type: none"> reload.topic -- the topic to which the configuration agent listens to receive configuration reload events. edge.id -- the controller with which this agent is associated edge.name -- the unique, textual description of the edge controller location.association -- NONE ALL READER PRINTER as describe at the top of this table
Printer Resource Manager agent	<ul style="list-style-type: none"> default.resource.urls -- URLs for the templates that are used by the tag printers associated with this edge. edge.id -- the controller with which this agent is associated edge.name -- the unique, textual description of the edge controller controller.association -- NONE ALL READER PRINTER as describe at the top of this table

Using variables for property values

For the properties listed above, 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 looks like this: `edge.name = "%CONTROLLER_ID%"`, the value in the edge XML will look like this: `edge.name = "E1"` (for Edge E1). Iterative substitutions enable values to be enumerated with each value for that substitution. For example, if the value in the database looks like this: `topics = "[LOCATIONS]%LOCATIONS%[/LOCATIONS]"`, the value in the edge XML will look like this: `topics = "P1, P2, P3,"`.

Substitutions for Location-based agents

%LOCATION_ID%

The location ID for the agent on the edge

%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

%PRINTER_ID%

The printer ID of the tag printer at the location

%PRINTER_COM_PORT%

The com.port for the tag printer at the location

%PRINTER_IP%

The IP address of the tag printer at the location

%PRINTER_REMOTE_PORT%

The port number of the tag printer at the location

Substitutions for controller-based agents

%PREMISES_IP%

The IP address of the WebSphere RFID Premises Server

%CONTROLLER_ID%

The edge ID of the controller

%LOGGING_THRESHOLD%

The logging threshold of the edge

%TEMPLATE_URLS%

The URLs for all templates for the manufacturers of the tag printers that are configured on the given controller

%LOCATIONS_STR%

The locations associated with the controller, in a format compatible with V1.0.2 edge clients

[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

[PRINTERS]%PRINTER_ID%[/PRINTERS]

Iterative substitution with all of the values of the printers configured on the controller

Working with readers

This section describes managing tag readers using the WebSphere RFID Premises Server Administrative Console. Tag readers are logical representations of the physical devices installed in your WebSphere RFID Premises Server network.

After you add a tag reader, you can associate it with a location. See Working with locations for more information.

This section contains the following topics:

Adding readers

Use the WebSphere RFID Premises Server Administrative Console to add new tag readers to your network topology definition.

Tag readers in the WebSphere RFID Premises Server Administrative Console are logical representations of the physical devices installed in your RFID network. After you create a tag reader, you must associate it with a location and controllers as part of the network topology definition. You can set up a tag reader to use both TCPIP and a serial port, and then indicate which to use.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **WRDI Configuration** → **Readers** from the left navigation pane. The Readers panel displays.
3. Click **New** under Readers. The Create a New Reader panel displays.
4. Enter a unique logical identifier for this tag reader. The identifier must be 10 digits (0-9) or fewer.
5. In the **Reader Name** field, enter a name for this tag reader.
6. From the **Reader Type** field, select the kind of tag reader you are adding.
7. In the **Reader IP Address** field, enter the tag reader's IP address. This field is optional if using a serial port.
8. In the **Reader IP Port Number** field, enter the port number. This field is optional if using a serial port.
9. Choose the serial port number in the **Reader Serial Port Number** field. This task is optional if using TCPIP.
10. In the **Reader Communication Protocol** field, select **TCPIP** to use the IP address and port or **SERIAL** to use a serial port.
11. Click **Create**. The new tag reader displays in the Readers panel.

Adding reader types:

1. In the WebSphere RFID Premises Server Administrative Console, click **WRDI Configuration** → **Readers** from the left navigation pane. The Readers panel displays.
2. Under Reader Types, click **New Reader Type**. The Create a New Reader Type panel displays.
3. Enter the name of the new tag reader type. After you create the reader type, you cannot modify this field.
4. Enter the tag reader model.
5. Enter the name of the tag reader manufacturer.
6. Enter a brief description of the tag reader.
7. Click **Create**. The new tag reader type displays on the Readers panel.

Modifying readers

Use the WebSphere RFID Premises Server Administrative Console to modify existing tag readers in your network topology definition.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **WRDI Configuration** → **Readers** from the left navigation pane. The Readers panel displays.

3. Click on the tag reader that you want to modify. The Edit Reader Details panel displays.
4. Make the necessary changes and click **Update**. The changes are saved.

Modifying reader types:

1. On the WebSphere RFID Premises Server Administrative Console, click **WRDI Configuration** → **Readers** from the left navigation pane. The Readers panel displays.
2. Click on the tag reader type that you want to modify. The Edit Reader Type Details panel displays.
3. Make the necessary changes and click **Update**. The changes are saved.

Deleting readers

Use the WebSphere RFID Premises Server Administrative Console to delete an existing tag reader from your network topology definition. Note that deleting a tag reader makes that resource unavailable for any associated locations and controllers.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **WRDI Configuration** → **Readers** from the left navigation pane. The Readers panel displays.
3. Click on the tag reader that you want to delete. The Edit Reader Details panel displays.
4. Click **Delete**. A confirmation message displays.
5. Click **OK** to delete the reader.

Deleting reader types:

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **WRDI Configuration** → **Readers** from the left navigation pane. The Readers panel displays.
3. Under Reader Types, click on the reader type that you want to delete. The Edit Reader Type Details panel displays.
4. Click **Delete**. A confirmation message displays.
5. Click **OK** to delete the reader.

Reader details

The following table defines the fields on the Create New Tag Reader and Edit Tag Reader Detail panels.

Field	Description
Reader ID	Enter a unique identifier 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.
Reader Name	Enter a unique, textual description of the reader.
Reader Type	Select the type of tag reader you are adding from the list of supported tag reader types.
Reader IP Address	Enter the IP address for this tag reader.
Reader IP Port Number	Enter the IP port number for communication with this tag reader. Some default port numbers are listed below, by tag reader type. You can find the default port number for your tag reader in the documentation provided by the manufacturer of the tag reader.

Field	Description
Reader Serial Port Number	Enter the serial port number for communication with this tag reader.
Reader Communication Protocol	Indicate how you want to communicate with the tag reader. Select TCPIP or SERIAL.

Reader type details

The following table defines the fields on the Create New Tag Reader Type and Edit Reader Type Details panels.

Fields

Field	Description
Name*	Enter the name of the new tag reader type. After you create the reader type, you cannot modify this field.
Manufacturer	Enter the name of the tag reader manufacturer.
Model	Enter the tag reader model.
Description	Enter a brief description of the tag reader.

* Required field.

Working with printers

This topic contains information on managing printers using the WebSphere RFID Premises Server Administrative Console.

A physical tag printer is connected to the Print, Verify, and Ship Reference User Interface through IBM's edge controller. A logical tag printer is connected to the Print, Verify, and Ship Reference User Interface through a third-party software system, such as Software Labeling System by Software, Inc. or BarTender by Seagull Scientific, Inc.

Print, Verify, and Ship supports several types of tag printer specifications. For information on the IBM RFID device validation program, supported devices, readers, and RFID device manufacturers, refer to: <http://www.ibm.com/solutions/sensors>. If your system uses a tag printer other than those that conform to the supported specifications, you can use Software or BarTender to print tags on other printer models, which might require a software license from Software, Inc. or Seagull Scientific, Inc.

Important: You can associate only one tag printer with each location.

Below is a description of the process for configuring and using physical and logical tag printers:

- If you configure a physical tag printer with a supported specification, the print request is sent to the edge controller, which retrieves the appropriate print template at startup from the premises server. The edge controller then sends the request to the physical tag printer and the job prints. See "Configuring physical printers" on page 183 and "Creating print templates" on page 184 for more information.
- If you configured a logical tag printer, such as Software or BarTender, the print request is sent to the appropriate print server, which retrieves the appropriate

print template from the premises server. The print server then sends the request to the physical tag printer and the job prints. See “Adding and configuring a logical printer” on page 181 and “Creating print templates” on page 184 for more information.

See the Chapter 7, “Print, Verify, and Ship,” on page 179 for a diagram showing the RFID network tag printer options.

Adding logical printers

Use the WebSphere RFID Premises Server Administrative Console to add new logical tag printers to your network topology.

Before beginning, ensure that you have done the following:

- You have successfully installed WebSphere RFID Premises Server. See Chapter 3, “Installing and configuring,” on page 19 for more information.
- You have successfully installed the Software or BarTender print server application on WebSphere RFID Premises Server or mapped a drive (Windows only) to a particular location on the WebSphere RFID Premises Server to get the print files.
 - **Windows** The Software print server is installed in the default directory, C:\Program Files\Software Labeling. The label.dtd file is installed in the default directory, C:\Program Files\Software Labeling\Batch
The BarTender print server is installed in the directory, C:\Program Files\SCAN_FOLDER. There is no .dtd file for BarTender.
 - **Linux** Because the Software and BarTender print servers run only on Windows, to run WebSphere RFID Premises Server on Linux, map a drive to where the Samba shared directory is located (**Tools** → **Map network drive**).



Note: If you install the Software print server application in a directory other than the default, you must add the `SOFTWARE_LABEL_DTD` property using the WebSphere RFID Premises Server Administrative Console, as described in the procedure below.

- Properties files are provided for the included templates. For more information, refer to “Creating properties files for print templates” on page 186. These properties files are located in the following directory:
 - **Windows** `WAS_PROFILE_HOME\installedApps\node_name\IBM_Premises_PVS_Console.ear\ibmrfid_premises_pvsapp.war\config\labels`
 - **Linux** `WAS_PROFILE_HOME/installedApps/node_name/IBM_Premises_PVS_Console.ear/ibmrfid_premises_pvsapp.war/config/labels`
 - `SampleCaseTag.properties`
 - `SamplePalletTag.properties`
 - `SampleDynamicCaseTag.properties`
 - `SampleDynamicPalletTag.properties`

Note: These files are stored in the above location by default. However, you can change their location by modifying the `labels.location` attribute in the `pvsapp.properties` file. The `pvsapp.properties` 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`

After modifying pvsapp.properties file, restart WebSphere Application Server.

- The following logical print template files exist in this directory:
 -  `IBM_RFID_HOME\premises\pvs\templates`
 -  `IBM_RFID_HOME/premises/pvs/templates`
 - SampleCaseTag.lwl (Loftware)
 - SamplePalletTag.lwl (Loftware)
 - SampleDynamicCaseTag.lwl (Loftware) and SampleDynamicCaseTag.btw (BarTender)
 - SampleDynamicPalletTag.lwl (Loftware) and SampleDynamicPalletTag.btw (BarTender)

Important: To use the BarTender print templates SampleDynamicCaseTag.btw and SampleDynamicPalletTag.btw that come with WebSphere RFID Premises Server, you must first set the delimitation character to an exclamation point (!) in the printer properties for the logical printer defined in the WebSphere RFID Premises Server Administrative Console.

When you submit a print job to a logical tag printer, the logical printer reads the print template that you created in the WebSphere RFID Premises Server Administrative Console. The print template files contain information necessary to communicate with the tag printers in your network. For additional information, see Creating print templates.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays. .
2. Navigate to **WRDI Configuration** → **Printers** from the left navigation panel. The Printers panel displays.
3. Click **New Logical Printer**. The Create a new Logical Printer panel displays.
4. In the **Printer ID** field, enter a unique logical identifier for this printer. The identifier must be 10 digits (0-9) or fewer.
5. In the **Printer Name** field, enter a unique description of the printer.
6. From the menu in the **Logical Printer Name** field, select **Loftware** or **BarTender**.
7. Click **Create Logical**. The new logical printer is saved and the Printers panel displays.
8. If you are defining a Loftware logical printer in a directory other than the default, add the LOFTWARE_LABEL_DTD property with the correct directory. Otherwise, continue to the next step.
9. On the Printers panel, click on the newly created printer. The Edit Logical Printer Details panel displays.
10. Ensure that the properties are correct for the logical printer or modify them. 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.

11. Click **Update**.

12. Create a print template for the logical tag printer by following the instructions in “Creating print templates” on page 184.

Create a new logical printer panel:

The following table defines the fields on the Create a new Logical Printer panel.

Logical printer details

Field	Description
Printer ID	Enter the ID of the tag printer. Note: The identifier must be 10 digits (0-9) or fewer.
Printer Name	Enter a unique, textual description of the printer.
Logical Printer Name	Choose either Software or Bartender.
Printer Properties	Modify the property name and value as necessary for this logical printer.

Adding physical printers

Use the WebSphere RFID Premises Server Administrative Console to add new physical tag printers to your network topology. After adding a printer, you can associate it with a location. WebSphere RFID Premises Server allows only one printer to be associated with a location.

For information on the IBM RFID device validation program, supported devices, readers, and RFID device manufacturers, refer to: <http://www.ibm.com/solutions/sensors>.

Follow the instructions below to configure your installed tag printer for Print, Verify, and Ship using the WebSphere RFID Premises Server Administrative Console.

If your system uses a tag printer other than those that conform to the supported specifications, you can configure a logical tag printer, such as Software and Bartender, that enables the Print, Verify, and Ship application to work with your tag printer. See “Adding and configuring a logical printer” on page 181 for more information.

Before beginning, ensure that you have successfully installed the WebSphere RFID Premises Server. See Chapter 3, “Installing and configuring,” on page 19 for more information.

Also, before creating a new printer, you must have added a printer type. You can add the printer type by creating the appropriate printer agents and agent properties. For more information about configuration, see “Modifying the property values of agents” on page 116.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **WRDI Configuration** → **Printers** in the left navigation panel. The Printers panel displays.
3. Click **New Printer**. The Create a new Printer panel displays.
4. Enter a unique, logical identifier for this printer. The identifier must be 10 digits (0-9) or fewer.
5. Enter a unique, textual description of the printer.

6. Select a printer in the **Printer Type** field.
7. Enter the printer's IP address in the **Printer IP Address** field. This field is optional if using a serial port.
8. Enter the port number in the **Printer IP Port Number** field. This field is optional if using a serial port.
9. Choose the serial port number in the **Printer Serial Port Number** field. This task is optional if using TCPIP.
10. In the **Printer Communication Protocol** field, select **TCPIP** to use the IP address and port or select **SERIAL** to use a serial port.
11. Click **Create**. The new printer displays in the Printers panel.
12. Create a print template for the printer by following the instructions in "Creating print templates" on page 184.

Modifying printers

Use the WebSphere RFID Premises Server Administrative Console to modify existing physical and logical tag printers.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **WRDI Configuration** → **Printers** from the left panel. The Printers panel displays.
3. Click the printer ID of the tag printer that you want to modify. The Edit Printer Details panel displays.
4. Modify the printer:
 - If you are modifying a logical tag printer and want to add a new **Property Name** and **Value**, enter the information and click **Add Property**. To make changes to an existing property, make the necessary changes to the property or value and click **Modify Property**.
 - If you are modifying a physical printer, make the necessary changes.
5. When you are finished, click **Update**.

Deleting printers

Use the WebSphere RFID Premises Server Administrative Console to delete existing logical and physical tag printers.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **WRDI Configuration** → **Printers** from the left panel. The Printers panel displays.
3. Click the printer ID of the tag printer that you want to delete. The Edit Printer Details panel displays.
4. Click **Delete**. A confirmation message displays.
5. Click **OK** to delete the tag printer.

Printer details

The following table defines the fields on the Edit Printer Properties panel.

Fields

Field	Description
Printer ID	Enter a unique identifier for this tag printer. After you create the printer, you cannot modify this field. Note: The identifier must be 10 digits (0-9) or fewer.

Field	Description
Printer Name	Enter a unique, textual description of the printer.
Controller	The controller associated with this printer. See Adding Controllers for more information.
Printer Type	Select the type of tag printer you are adding from the list of supported tag printer types.
Printer IP Address	Enter the IP address for this tag printer.
Printer IP Port Number	Enter the IP port number for communication with this tag printer. You can find the default port number for your tag printer in the documentation provided by the tag printer manufacturer. Note: WebSphere RFID Premises Server supports several tag printer specifications. For information on the IBM RFID device validation program, supported devices, readers, and RFID device manufacturers, refer to: http://www.ibm.com/solutions/sensors .
Printer Serial Port Number	Enter the serial port number for communication with this printer.
Printer Communication Protocol	Indicate how you want to communicate with the tag printer. Select TCP/IP or SERIAL.

Checking the value on a tag in a Printronix printer

This topic explains how you can easily view the value of a tag on a Printronix printer. It describes how to simulate a write to the tag by aligning the antennae in the tag with the reader in the printer.

Sometimes the Test function, from the RFID Control menu, cannot read the tag value if the tags have been calibrated as Tear-Off Strip. This procedure helps you determine if blank tags have a pre-programmed quality code. Alien tags might have a hexadecimal value of **A5A5** in the upper-most tag data bits prior to programming. The Precheck Tags menu item on the RFID Control menu enables the tag pre-check to see if this value is present; tags not containing the value automatically fail. You can also use this procedure to check the value of a tag that has already printed. Remember to roll the tags back into the printer before testing.

- From the Quick Setup menu:
 - Change the Media Handling property to Continuous.
 - Run **Auto Calibration**.
- From the WebSphere RFID Premises Server Control menu, navigate to the RFID Test property and click **Enter**. The value on the tag appears on the printer LCD.
- To align the tags correctly, go to the Quick Setup menu:
 - Change the Media Handling property back to Tear-Off Strip.
 - Run **Auto Calibration**.

Working with print templates

This section contains information on managing print templates using the WebSphere RFID Premises Server Administrative Console.

A print template in the WebSphere RFID 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:

	<code>IBM_RFID_HOME\premises\pvs\templates</code>
	<code>IBM_RFID_HOME/premises/pvs/templates</code>

They can be customized to meet your specific label requirements.

When you create a print template in the WebSphere RFID Premises Server Administrative Console, that information is stored in the WebSphere RFID Premises Server database. When the edge controller is started, it receives the location information for all of the currently defined templates. When you submit a print job from the Print, Verify, and Ship Reference User Interface, the edge controller reads the name of the template from the print request and retrieves the required template from the previously defined location. The edge controller then completes the fields of the template with the appropriate data from the print request.

You can create print templates for two types of printers: logical and physical. A print template for a logical tag 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 and the Bartender print template must be on the Bartender server to access it. A print template for a physical tag printer must be stored on an IBM HTTP Server so that the edge controller can download it during RFID Data Transformation startup. The IBM HTTP Server can reside on either the same server as WebSphere RFID 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 RFID Premises Server Administrative Console to add new print templates to your network topology.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays. .
2. Navigate to **WRDI Configuration** → **Print Templates** from the left panel. The Print Templates panel displays.
3. Click **New**. The Create a New Print Template panel displays.
4. Enter the name of the template in the **Print Template Name** field.

Note: For physical tag printers, the templates use the following naming convention: *manufacturer-template_name-template.zip*. The print template name must be identical to the template name used in the manufacturer's .zip file. For example, if the template file name is zebra-LWCASE-template.zip, you must enter LWCASE in the **Print Template Name** field.

5. Select the printer manufacturer from the **Printer Type** field. If you are creating a print template for a logical tag printer, select **LOGICAL**.
6. Enter the location of the template file in the **Properties Location URL** field.

- If you are creating a print template for a physical tag printer, use the following convention: `http://server_name/path/zip_filename`. For example: `http://myserver.com/templates/zebra-LWCASE-template.zip`.
 - If you are creating a print template for a Loftware logical tag printer, use the following convention: `file://Loftware_label_name`. For example: `file://Logical1-template.lwl`.
 - If you are creating a print template for a Bartender logical tag printer, use this convention: `file://Bartender_label_name`. For example: `file://Logical1-template.btw`.
7. Click **Create**. The print template is saved.
 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 186 for more information.

Modifying print templates

Use the WebSphere RFID Premises Server Administrative Console to modify existing print templates.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **WRDI Configuration** → **Print Templates** from the left panel. The Print Templates panel displays.
3. Click on 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 RFID Premises Server Administrative Console to delete existing print templates from your network topology.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **WRDI Configuration** → **Print Templates** from the left 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.
Printer Type	Select the type of tag printer for which you are creating the print template. The tag printer types display in the Print Templates panel. See “Working with printers” on page 128 for more information.
Properties Location URL	Enter the location of the properties file for the tag printer; for example, enter: <code>file://SampleCaseTag.lwl</code> . See “Creating print templates” on page 184 for more information.

Working with locations

This section contains information on working with locations using the WebSphere RFID Premises Server Administrative Console.

Locations correspond to the physical locations at which your physical devices, such as tag readers, are installed. There are two kinds of locations: **container** locations and **contained** locations. Contained locations display beneath their respective container locations on the Locations panel.

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.

This section contains the following topics:

Adding locations

Use the WebSphere RFID Premises Server Administrative Console to add new locations to your network topology definition.

Locations in the WebSphere RFID 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 RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **WRDI Configuration** → **Locations** from the left navigation pane. The Locations panel displays.
3. Click the container location to which you are adding a contained location. The Edit Location Details panel displays.
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 RFID 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 RFID 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.

Modifying locations

Use the WebSphere RFID Premises Server Administrative Console to modify locations in your network topology.

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 RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **WRDI Configuration** → **Locations** from 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.

Deleting locations

Use the WebSphere RFID Premises Server Administrative Console to delete locations from your network topology.

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 RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **WRDI 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.

Location details for WebSphere RFID Device Infrastructure

The following table defines the fields on the Create New Location and Edit Location Detail panels. This information refers to WebSphere RFID Device Infrastructure locations.

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 location contacts” on page 139 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 location contacts” on page 139 for more information.
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 locations” on page 136 for more information.
Controller**	Displays the controller associated with this location. See “Adding controllers” on page 140 for more information.
Address	Enter the street, city, state, and zip code for the location.

Field	Description
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.

Working with location contacts

This section describes how to manage location contact information using the WebSphere RFID 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 location contacts

Use the WebSphere RFID Premises Server Administrative Console to add new location contacts to your network topology definition.

Location contacts specify important information about the primary RFID contact person at a location. You can associate a contact with multiple locations. See Adding Locations for more information.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **WRDI 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 location contacts

Use the WebSphere RFID Premises Server Administrative Console to modify existing location contacts in your network topology definition.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **WRDI 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 location contacts

Use the WebSphere RFID Premises Server Administrative Console to delete existing location contacts from your network topology definition.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.

2. Click **WRDI 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 Locations for more information.

* Required field

** This field only displays on the Contact Details panel.

Working with controllers

This section explains edge controllers and working with them using the WebSphere RFID Premises Server Administrative Console.

The edge controller is the component that interacts with and controls tag readers. It processes, filters, and communicates with the WebSphere RFID Premises Server.

The following topics provide instructions for working with controllers:

Adding controllers

Use the WebSphere RFID Premises Server Administrative Console to add new edge controllers to your network topology definition.

Controllers in the WebSphere RFID Premises Server Administrative Console are logical representations of the physical edge devices in your WebSphere RFID 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 RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **WRDI Configuration** → **Controllers** from 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 **MAC Address** field, enter the edge controller's MAC address.
7. Select an alert threshold to determine the level of information to be included in the edge controller log file.
8. 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.
9. Click **Create**. The new edge controller displays in the Controllers panel.

Modifying controllers

Use the WebSphere RFID Premises Server Administrative Console to modify existing controllers in your network topology definition.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **WRDI 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.

Deleting controllers

Use the WebSphere RFID Premises Server Administrative Console to delete existing controllers from your network topology definition.

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 RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **WRDI Configuration** → **Controllers** from 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.

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.
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.
Alert Threshold	<p>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 RFID Premises Server; the lower the alert level, the higher the number of events that are sent to the log file.</p> <p>Choose from the following alert thresholds, from highest to lowest -- for example, selecting debug generates the greatest number of alerts.</p> <ul style="list-style-type: none">• error (default)• warning• info• debug <p>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.</p>
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.

Restarting controllers from the console

Use the Reload Configuration function on the Controllers panel to remotely restart an edge controller from the WebSphere RFID Premises Server Administrative Console.

Each time you change a configuration, you must restart the affected edge 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 an edge controller, the changes are not implemented until you restart the edge controller.

By default, the **Reload Configuration** button is set to reload instead of restart. If you are using Data Capture and Delivery, this setting only works with local Data Capture and Delivery. If you are using remote Data Capture and Delivery, you need to edit this line in flow number 4 of the bridge.properties file:

```
flow.4.transformation.0.input.topic.reload.config=reload/+
```

For remote Data Capture and Delivery, the line should change to:
`flow.4.transformation.0.input.topic.reload.config=restart/+`

For an explanation of local and remote Data Capture and Delivery controllers, refer to “Data Capture and Delivery controller” on page 6.

Follow these steps to restart an edge controller from the WebSphere RFID Premises Server Administrative Console.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. Depending on your configuration, navigate to either **WRDI Configuration** → **Controllers** or to **Data Capture Configuration** → **Controllers** from the left navigation pane. The Controllers panel displays.
3. Click on the controller that you want to restart. The Edit Controller Details panel displays.
4. Click **Reload Configuration**. The edge controller restarts.

Note: All locations associated with this edge controller are disabled while the device is restarting.

Managing event processing

This section describes how to work with event templates and tasks using the WebSphere RFID Premises Server Administrative Console.

Working with event templates

This topic contains information on managing event templates using the WebSphere RFID Premises Server Administrative Console.

An **event** is a type of action that takes place in the WebSphere RFID 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 edge controller, WebSphere RFID Premises Server, and enterprise system.

This section contains the following topics:

Adding event templates

Use the WebSphere RFID Premises Server Administrative Console to add new event templates to your network topology definition.

An *event* is a type of action that takes place in the WebSphere RFID Premises Server network, such as a new tag read. You define event templates in the network topology so that the event information can be transmitted across the appropriate communication channels and coordinated between the edge controller, premises server, and enterprise system. After events are created, you can associate them with a custom task, if one exists, or direct them to an output channel to be forwarded to another destination, such as a Java Message Service queue. You can also associate the event with both a custom task and an output channel.

See Adding Output Channels and Adding Tasks for more information.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.

2. Click **Event Processing Configuration** → **Event Templates** from the left navigation pane. The Event Templates panel displays.
3. Click **New**. The Create New 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. Click **Create Event Template**. The event template is saved.

Modifying event templates

Use the WebSphere RFID Premises Server Administrative Console to modify existing event templates in your network topology definition.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **Event Processing Configuration** → **Event Templates** from the left navigation pane. The Event Templates panel displays.
3. Under the Actions column, click the **View Template Properties** link for the event template that you want to modify. The Edit Event Template Details panel displays.
4. Make the necessary changes and click **Update Event Template**. The changes are saved.

Deleting event templates

Use the WebSphere RFID Premises Server Administrative Console to delete existing event templates from your network topology definition.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **Event Processing Configuration** → **Event Templates** from the left navigation pane. The Event Templates panel displays.
3. Under the Actions column, click the **View Template Properties** link for the event template that you want to delete. The Edit Event Template Details panel displays.
4. Click **Delete Event Template**. A confirmation message displays.
5. Click **OK** to delete the event template.

Note: If you delete an event template that is associated with a task, the task remains but is no longer associated with an event template. You can either delete the task or associate it with another template.

Event details

The following table defines the fields in the Create New Event Template and Edit Event Template Details 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.

Field	Description
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 RFID Premises Server to the edge controller or enterprise using the WebSphere RFID Premises Server Administrative Console.

This section contains the following topics:

Creating output channels

Use the WebSphere RFID Premises Server Administrative Console to define the output channels for the WebSphere RFID Premises Server.

These channels are output paths for messages sent from the premises server to either the edge 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 RFID Premises Server and edge 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 RFID Premises Server Administrative Console. Refer to the WebSphere Application Server Information Center at <http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/topic/> for more information. For other types of output channels, proceed to the next step.
2. Open the WebSphere RFID Premises Server Administration Console. The Welcome page displays.
3. Click **Event Processing Configuration** → **Output Channels** from 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 Output 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 RFID Premises Server Administrative Console to add defined output channels to event templates.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **Event Processing Configuration** → **Event Templates** from the left navigation pane. The Event Templates panel displays.
3. Select an event template to modify and click **edit**.
4. Move the desired channels from the **All Channels** column to the **Selected Channels** column using the arrow button.

Note: If a desired output channel does not appear in the **All Channels** column, it must be created. Refer to the instructions for creating an output channel.

Modifying output channels

Use the WebSphere RFID Premises Server Administrative Console to modify the output channels for the WebSphere RFID Premises Server.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **Event Processing Configuration** → **Output Channels** from the left navigation pane. The Output Channels panel displays.
3. Click the output channel that you want to modify. The “Output Channel details” panel displays.
4. Make the necessary changes and click **Update**. The changes are saved.

Deleting output channels

Use the WebSphere RFID Premises Server Administrative Console to delete output channels for the WebSphere RFID Premises Server.

Note: Do not delete *edge.out.channel* because that is the channel used to communicate with Data Capture and Delivery runtime.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **Event Processing Configuration** → **Output Channels** from the left navigation pane. The Output Channels panel displays.
3. Click the output channel that you want to delete. The “Output Channel details” panel displays.
4. Click **Delete**. The output channel is deleted.

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 re-add it to the event templates.

Output Channel details

The following table defines the fields in the Create New Output 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.

Field	Description
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.
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

Working with tasks

This section provides information on how to manage tasks using the WebSphere RFID Premises Server Administrative Console. A task, which is an event handler, coordinates the communication of an event among an edge controller, WebSphere RFID Premises Server, and enterprise system.

This section contains the following topics:

Adding tasks

Use the WebSphere RFID Premises Server Administrative Console to add new tasks to your network topology definition.

A task is a custom piece of software, or event handler, that coordinates the communication of an event among an edge controller, WebSphere RFID Premises Server, and enterprise system. For example, the *dock door receiving* event task organizes the delivery of tag information received from the edge controller to the WebSphere RFID Premises Server and out to the enterprise.

The dock door receiving event task is created by default when you install the WebSphere RFID Premises Server. However, you can use the Tasks panel to create custom tasks to satisfy usage scenarios unique to your enterprise.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **Event Processing Configuration** → **Tasks** from the left navigation pane. The Tasks panel displays.
3. Click **New**. The Create New Task panel displays.
4. In the **Task ID** field, enter a unique identifier for this task.
5. Enter a brief description of the task.
6. From the **Available Events** column, select the events that you want to associate with the task and click the **right arrow**. The events display in the **Selected Events** column.
7. Click **Create**. The task is saved.

Modifying tasks

Use the WebSphere RFID Premises Server Administrative Console to modify existing tasks in your network topology definition.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **Event Processing Configuration** → **Tasks** from the left navigation pane. The Tasks panel displays.
3. Click on the task that you want to modify. The Edit Task Details panel displays.
4. Make the necessary changes and click **Update**. The changes are saved.

Deleting tasks

Use the WebSphere RFID Premises Server Administrative Console to delete existing tasks from your network topology definition.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **Event Processing Configuration** → **Tasks** from the left navigation pane. The Tasks panel displays.
3. Click on the task that you want to delete. The Edit Task Details panel displays.
4. Click **Delete**. A confirmation message displays.
5. Click **OK** to delete the task.

Task details

The following table defines the fields on the Create New Task and Edit Task Details panels.

Fields

Field	Description
Task ID*	Enter a unique identifier for the task you are defining. After you create the task, you cannot modify this field.
Description	Enter a description of this task.
Available Events	The list of available events to associate with the task you are defining. Select an event and click the right arrow to associate the event with this task.
Selected Events*	The list of events currently associated with the task. Click the left arrow to disassociate this event with the task.

* Required field.

Managing the EPC configuration

Use the EPC Configuration function in the WebSphere RFID 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 155.
- Serial number configuration - see “Working with serial numbers” on page 157.
- EPCglobal company prefix index - see “Working with the EPCglobal company prefix index” on page 160.

Working with pack types

This section contains information on managing pack types using the Profile Configuration feature in the WebSphere RFID Premises Server Administrative Console.

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). An example of an invalid containment hierarchy cycle is 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 12. Input Types and Matching Encoding Types

Input Type	Encoding Type
DOD	<ul style="list-style-type: none"> • usdod-64 • usdod-96
GIAI	<ul style="list-style-type: none"> • giai-64 • giai-96
GID	<ul style="list-style-type: none"> • gid-96
GLN	<ul style="list-style-type: none"> • sgln-96 • sgln-64
GRAI	<ul style="list-style-type: none"> • grai-96 • grai-64
GTIN14	<ul style="list-style-type: none"> • sgtin-64 • sgtin-96
SSCC18	<ul style="list-style-type: none"> • ssc-96 • ssc-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 156 for more information.

This section contains the following topics:

- “Adding pack types” on page 151
- “Modifying pack types” on page 151
- “Deleting pack types” on page 152

Adding pack types

Use the Profile Configuration feature in the WebSphere RFID 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 RFID 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 RFID 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 156, to create a customer profile containing these pack types.

Modifying pack types

Use the WebSphere RFID Premises Server Administrative Console to modify your existing pack types.

1. Open the WebSphere RFID 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 RFID Premises Server Administrative Console to delete pack types from your network topology.

1. Open the WebSphere RFID 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 RFID 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.

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). An example of an invalid containment hierarchy cycle is 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 13. Input Types and Matching Encoding Types

Input Type	Encoding Type
DOD	<ul style="list-style-type: none"> • usdod-64 • usdod-96
GIAI	<ul style="list-style-type: none"> • giai-64 • giai-96
GID	<ul style="list-style-type: none"> • gid-96
GLN	<ul style="list-style-type: none"> • sglN-96 • sglN-64
GRAI	<ul style="list-style-type: none"> • grai-96 • grai-64
GTIN14	<ul style="list-style-type: none"> • sgtin-64 • sgtin-96
SSCC18	<ul style="list-style-type: none"> • 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 156 for more information.

1. Open the WebSphere RFID 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 RFID 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 156, 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.
Input Type	The UCC EAN format of the customer product code. See “Configuring pack types” on page 152 for a list of available input types.

Field	Description
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 152 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 RFID Premises Server Administrative Console. See “Creating print templates” on page 184 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 RFID Premises Server Administrative Console.

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

This section contains the following topics:

Adding profiles

Use the WebSphere RFID Premises Server Administrative Console to add new profiles to your network topology.

1. Open the WebSphere RFID 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 RFID Premises Server Administrative Console to modify existing profiles in your network topology.

1. Open the WebSphere RFID 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 RFID Premises Server Administrative Console to delete electronic product code (EPC) profiles from the network topology.

1. Open the WebSphere RFID 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 RFID Premises Server Administrative Console to create a customer profile to use in the Print, Verify, and Ship Reference User Interface.

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 RFID 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 RFID Premises Server Administrative Console.

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**.

This section contains the following topics:

Adding serial numbers

Use the WebSphere RFID Premises Server Administrative Console to add new serial numbers to your network topology.

1. Open the WebSphere RFID 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 RFID Premises Server Administrative Console to modify existing electronic product code (EPC) serial numbers.

1. Open the WebSphere RFID 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 RFID Premises Server Administrative Console to delete electronic product code (EPC) serial numbers from your network topology.

1. Open the WebSphere RFID 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 RFID Premises Server Administrative Console to determine the EPC serial numbers associated with each customer's products.

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 RFID 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 <i>sgtin</i> , <i>sscc</i> , <i>grai</i> , and <i>giai</i> .) The company prefix that is part of the URI. It is associated with a specific pack type.
Extension digit	(For ID URI type <i>sscc</i> .) While similar in function to an indicator digit, see below, EAN.UCC gives them different names.
Indicator digit	(For ID URI type <i>sgtin</i> .) A numeric value in the URI that differentiates between containers.
Asset type	(For ID URI type <i>grai</i> .) A numeric value used to define a returnable asset such as a pallet, keg, or other carrier.
Item reference	(For ID URI type <i>sgtin</i> .) 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 <i>usdod</i> .) 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 <i>gid</i> .) 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 <i>gid</i> .) 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 RFID 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 RFID Premises Server Administrative Console to add new company prefixes to your local database of the EPCglobal Company Prefix Index.

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 RFID 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 RFID Premises Server Administrative Console to modify existing company prefixes.

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 RFID 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 RFID Premises Server Administrative Console to delete a company prefix.

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 RFID 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.

Reporting

This section contains the following topics that you can use to gather information about your WebSphere RFID Premises Server system configuration.

Viewing tags

Use the WebSphere RFID Premises Server Administrative Console to view tag information that has registered in your WebSphere RFID Premises Server network.

You can register all tag reads that are received in your RFID network by setting the `com.ibm.rfid.premises.tag.persistence` parameter to **true** in your `premises.properties` file. If this value is set to **true**, all tags read in the network display in the Tags panel on the WebSphere RFID Premises Server Administrative Console. If the value is set to **false**, no tag information is registered.

To determine the status of the persistence parameter, click **Reporting** → **Configuration Variables** in the left navigation pane. See “Viewing configuration variables” on page 72 for more information.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **Reporting** → **Tags** from the left navigation pane. The Tags panel displays filter fields for you to search your tags.
3. Enter filter criteria and click **Search** to display a list of tags. For information on entering search criteria, refer to “Searching for products” on page 196.

Tag details

The following tables define the fields on the Tags panel.

Available fields before searching

No tags are displayed before you search. You can filter the tags before searching, and you can define how many tag results appear on each page. 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 following property in the `premises.properties` file:

`com.ibm.rfid.premises.taghistory.search.filter.date.format`

Table 14. Available fields before searching

Field		Description
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 . You can also use the percent sign (%) wildcard at the beginning, middle, or end of your search criteria to match zero or more characters.
Page Size		A number that indicates how many tags are displayed on each page. The default page size is 50.
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.
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.

Available fields after searching

After you click **Search**, the following fields are available in the results.

Table 15. Available fields after searching

Field	Description
Tag ID	The unique identifier assigned to each tag read through the system. Click a tag ID to view more detailed information about that tag, such as tag extensions.
Tag History	Click a Tag History link to view more detailed information about the tag history, such as the location and the tag reader through which the tag was read.
Date/Time Stamp	The date and time that the tag was read through the system.
Location	The location where the tag was read.

You can navigate your search results using the arrows indicating first page, previous page, next page, and last page.

Viewing configuration variables

Use the WebSphere RFID Premises Server Administrative Console to view the configuration variables for the WebSphere RFID Premises Server.

The Configuration Variables panel is a read-only panel that displays the parameters from your `premises.properties` file. This file is located on the WebSphere RFID Premises Server in these directories:

	C:\Program Files\IBM\RFID\premises\properties
	/opt/ibm/rfid/premises/properties

You can examine the current settings on the WebSphere RFID Premises Server from the WebSphere RFID Premises Server Administrative Console without actually locating the properties file on the WebSphere RFID Premises Server. Although modifying the behavior of the server requires making changes to the properties file on the server and then stopping and restarting the server, the Configuration Variables panel allows you to view the current settings without accessing the actual file.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **Reporting** → **Configuration Variables** from the left navigation pane. The Configuration Variables panel displays.

Disabling tag aggregation

The Tag Aggregation function enables edge controllers in dock door receiving scenarios to capture and group tag information from one event to another, to process those tags as a unit, and to use that grouped information in other usage scenarios.

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 the property values of agents” on page 116 for WebSphere RFID Device Infrastructure agents and “Modifying a Data Capture and Delivery agent by downloading agent properties” on page 79 and “Modifying Data Capture and Delivery agent properties for a PID” on page 79 for Data Capture and Delivery agents.

Disabling tag persistence

This topic describes how to disable tag persistence.

If you do not want your tag read data to persist on WebSphere RFID Premises Server, set the following flag to `false` in the following file:

- **File:**

	IBM_RFID_HOME\premises\properties\premises.properties
	IBM_RFID_HOME/premises/properties/premises.properties

- **Parameter:** `com.ibm.rfid.premises.tag.persistence=[false | true]`

This properties file contains comments that explain each setting. You can modify the other settings to change other aspects of the WebSphere RFID Premises Server behavior. For example, the “tag read persistence” setting has the following description:

```
#####  
# com.ibm.rfid.premises.tag.persistence  
#  
# Indicates if the Premises Server should persist tag and tag
```

```
# history information in the database. Values:
# true = persist tag and tag history
# false = no persistence
#
# Default = true
#####
com.ibm.rfid.premises.tag.persistence=false
```

Note: After modifying the `premises.properties` file, you must restart the WebSphere RFID Premises Server.

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 RFID 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 RFID 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 `premises.properties` file. 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 RFID Premises Server and answered by the back-end RFID system. A value of `true` means that the Application Ping Request is answered by WebSphere RFID Premises Server.

The default value is `false`.

To view the Application Ping configuration settings in the WebSphere RFID Premises Server Administrative Console, use the instructions in “Viewing configuration variables” on page 72. 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 Data Capture and Delivery 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.

Delete filter configuration settings

The setting for the delete filter is configurable in the `premises.properties` file.

- 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 as follows:

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.

```
com.ibm.rfid.premises.edgeconfig.delete.filter=!((service.pid=com.ibm.rfid.bundle.loader)
(service.pid=com.ibm.rfid.edge.config))
```

- 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 as follows:

```
com.ibm.rfid.premises.edgeconfig.delete.filter=(&(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 as follows:

```
com.ibm.rfid.premises.edgeconfig.delete.filter=((!((!((!((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))))))
```

To view the delete filter configuration settings in the WebSphere RFID Premises Server Administrative Console, use the instructions in “Viewing configuration variables” on page 72. Look for

`com.ibm.rfid.premises.edgeconfig.delete.filter` in the Name column. The current set value for each configuration variable is in the **Value** column.

Verifying the WebSphere RFID Premises Server installation and setup

This section describes how to start and stop the simulated reader that enables you to verify the installation and setup of your WebSphere RFID Premises Server.

A simulated reader helps you to verify that the WebSphere RFID Premises Server and related software, such as MQ and DB2, are correctly installed and configured. You indicate how long you want the simulated reader to run by setting the `com.ibm.rfid.simulatedd.reader.timeout` property in the `premises.properties` file. You must also modify the value of the `com.ibm.rfid.applping.shortcut` to `true`. For more information and instructions, refer to “Verifying the installation” on page 50.

This section contains the following topics:

Starting a simulated reader

This topic describes how to start a simulated reader using the WebSphere RFID Premises Server Administrative Console.

Be sure that the property, `com.ibm.rfid.applping.shortcut`, in the `premises.properties` file is set to *True*. If you have to change the value to *True*, restart WebSphere Application Server before continuing.

Use the start function to begin the tag-reading process that verifies that all software is installed and configured correctly.

1. Open the WebSphere RFID 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 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 RFID Premises Server Administrative Console.

Use the stop function to end the tag-reading process of the simulated reader.

1. Open the WebSphere RFID 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 RFID Premises Server Administrative Console.

Use the **Reset Reader** button to reset the WebSphere RFID Premises Server Administrative Console when the reader does not respond to a start or stop request.

1. Open the WebSphere RFID 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 RFID Premises Server

This topic describes how to run the simulated reader and simulated WebSphere RFID Premises Server together on the same machine.

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. Launch the DataCapture-FullSim configuration script.

Running only the simulated reader

Complete the following steps if you only want to run the simulated reader:

1. Add the following line to the hosts.etc file so that Data Capture and Delivery can connect to WebSphere RFID Premises Server: <premises ip>
rfid_host_name
2. Launch the DataCapture-RdrSim configuration script.

Chapter 5. Developing an IBM RFID solution

WebSphere RFID Premises Server ships with three toolkits that help you develop a WebSphere RFID solution for your environment.

The three toolkits are:

WebSphere RFID Premises Server Toolkit

Enables developers to create and test custom WebSphere RFID Premises Server applications in the Rational Application Developer for WebSphere Software WebSphere Test Environment (WTE).

IBM RFID Data Transformation Toolkit for WebSphere RFID Premises Server

Enables developers to create OSGi bundles like those shipped with WebSphere RFID Premises Server.

IBM Data Capture and Delivery Toolkit for WebSphere RFID Premises Server

Enables developers to create OSGi bundles and test them on a workstation. It also explains how developers deploy bundles to edge devices and WebSphere RFID Premises Server, and how to manage them.

For information on how to install these toolkits, see “Installing the toolkits” on page 43

WebSphere RFID Premises Server API

The WebSphere RFID Premises Server application programming interface (API) enables customers to create custom applications that interface with a WebSphere RFID Premises Server. Use the WebSphere RFID Premises Server Toolkit to create applications using the WebSphere RFID Premises Server API.

The APIs provide access to a wide range of WebSphere RFID Premises Server information, and can be applied to a wide variety of usage scenarios. WebSphere RFID 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 RFID Premises Server API.

You can use the WebSphere RFID Premises Server API to communicate with the WebSphere RFID Premises Server Application Level Events (ALE) engine and the “Common Services” J2EE application that is installed with WebSphere RFID Premises Server. The Common Services are a set of services-oriented Web services that sits on top of session EJBs, which are capable of interacting with other key WebSphere RFID Premises Server EJBs. Both types of communication use Simple Object Access Protocol (SOAP) calls. You can also use the WebSphere RFID Premises Server API to communicate with any Electronic Product Code Information System (EPCIS) by creating and sending Object and Aggregate Events.

The WebSphere RFID 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 RFID 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 RFID Premises Server).

For more information about the WebSphere RFID Premises Server Java API, refer to the WebSphere RFID Premises Server API Javadoc.

Note: The WebSphere RFID Premises Server API requires Java version 1.4. You must use Java version 1.4 to program applications using the WebSphere RFID Premises Server API. You can use the WebSphere RFID Premises Server API to program many types of applications including J2EE applications, portlets, and standalone Java applications.

Chapter 6. Tuning

Use these topics to adjust the configuration and improve the performance of the WebSphere RFID Premises Server infrastructure and components.

Changing MQ settings to improve performance

This topic describes how you might see performance improvements by changing certain MQ settings.

You might find that performance improves when the following changes are made to the WebSphere RFID Premises Server installation.

1. Change the number of persistence and task queues to 1. In the `RFID_HOME\premises\premises.properties` file, change the following properties:
 - `com.ibm.rfid.premises.multipersistence.queue.count=1` (previous value was 4)
 - `com.ibm.rfid.premises.multitask.queue.count=1` (previous value was 2)
2. Change the following queue listener properties:
 - a. On the WebSphere Application Server Administrative Console, click **Application servers** → **server1** → **Message Listener Service** → **Listener Ports**.
 - b. Click on **edgelistener** and change the maximum sessions to 1, maximum retries to 2, and maximum messages to 10.
 - c. Click on **tasklistener** and change the maximum sessions to 2, maximum retries to 2, and maximum messages to 10.
 - d. Click on **persistencelistener** and change the maximum sessions to 6, maximum retries to 2, and maximum messages to 1.
3. Change the number of logprimary files, of the IBM.RFID.QM, to 4, the number of logsecondary files to 2, the value of logfilepages to 16384, and the value of logbuffer pages to 4096.
 - From the MQ Explorer, stop IBM.RFID.QM
 - a. Delete IBM.RFID.QM.
 - b. Open the `premises_svr_mqm_cfg.bat` file in the `RFID_HOME\premises\install\servers\mq` directory.
 - c. Change the following line to this:

```
echo ----- Creating MQ Queue Manager %CUSTRFIDQM% ----- >> %INSTALL_LOG%
"%MQ_JAVA_DATA_PATH%\bin\crtmqm" -lp 4 -ls 2 -lf 16384 %CUSTRFIDQM% 1>> %INSTALL_LOG% 2>&1
```

The `-lp` argument changes the number of primary log files.
The `-ls` argument changes the number of secondary log files.
The `-lf` argument changes the number of log file pages.
4. Run the following MQ files in the order listed from a command prompt.

Table 16. MQ files

Filename	Directory
<code>premises_svr_mqm_cfg.bat</code>	<code>RFID_HOME\premises\install\servers\mq\</code>
<code>event_svr_mq_cfg.bat</code>	<code>RFID_HOME\premises\install\servers\mq\</code>
<code>kimono_mq_cfg.bat</code>	<code>RFID_HOME\premises\install\kimono\mq\</code>
<code>pvs_mq_cfg.bat</code>	<code>RFID_HOME \premises\install\pvs\mq\</code>

- Stop MQ from Services.
 - a. Start MQ from Services
 - b. Start IBM.RFID.QM.
 - c. Open the MQ Explorer.
 - 1) Right-click IBM.RFID.QM and select **Properties**.
 - 2) Click **Log**, and then change the value of Log buffer pages to **4096**.
 - 3) Click **OK**.
 - d. Restart the WebSphere RFID Premises Server.

Disabling ALE messages

This topic explains how to disable ALE messages if you do not use them.

Do the following to disable ALE messages:

- Edit the bridge.properties file located in the C:\Program Files\IBM\RFID\dts directory. Comment out the ALE Tag Read Event Flow route (Route 8) as shown below.

```
#####
# ALE Tag Read Event Flow #
#####
#flow.8.type=outbound
#flow.8.qos=1
#flow.8.source.0.name=receiving/portal/+/signal/tags
#flow.8.target.jmsType=jmsText
#flow.8.target.name=ALE.TAG.INPUT.Q
#flow.8.transformation.0.className=com.ibm.micro.bridge.plugin.transform.ALETagReadTransformation
#flow.8.transformation.0.input.location.index=2
#flow.8.transformation.0.input.message.entry=<ReadEvent antenna="" count="" reader="" tagdata=""
#tagid="" timestamp=""/>
#flow.8.transformation.0.input.message.prefix=<?xml version='1.0' encoding='UTF-8'?> <TagList
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="tagList.xsd">
#flow.8.transformation.0.input.message.regex=~
#flow.8.transformation.0.input.message.suffix=</TagList>

#flow.8.transformation.0.input.premises.port=9080
```

Increasing memory used by RFID Data Transformation

This topic explains how to increase the amount of memory that is used by RFID Data Transformation.

Do the following to increase memory:

1. Open the dts.bat file found in the C:\Program Files\IBM\RFID\dts directory.
2. Change the minimum and maximum memory of RFID Data Transformation from 64 to **256**.

```
"%JCLPATH%\java" -Xmx256M -Xms256M -Xgcpolicy:optavgpause -Xlp %VMOPTIONS%
-jar org.eclipse.osgi_3.2.2.R32x_v20070118.jar -console @goto javahome
```

The example below is the *original* file:

```
"%JCLPATH%\java" -Xmx64M -Xms64M -Xgcpolicy:optavgpause -Xlp %VMOPTIONS%
-jar org.eclipse.osgi_3.2.2.R32x_v20070118.jar -console -verbosegc @goto javahome
```

Tuning the databases to improve performance



Use the steps in this topic to improve your database performance.

Tuning DB2 Universal Database



To tune your 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 CDs and when you install the product. The scripts are located in these paths:

Before installation:

-  On CD 20 in db_script\performance_tuning_db2.bat
-  On CD 21 in db_script/performance_tuning_db2.sh

After installation:

-  *IBM_RFID_HOME\premises\install\db\performance_tuning_db2.bat*
-  *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
```

Tuning Oracle

Important: In order to use these performance tuning steps, you must have the Oracle 10g 10.1.0.2 JDBC driver.

- Apply all Oracle configuration changes to a default Oracle installation.
- Do not run any configuration scripts after Oracle installation.
- Only apply the configuration changes listed in the following steps.
- Enter all commands using the Oracle sqlplus utility.
- For all commands, be sure to use the directory paths and database instance name that are correct for the server.

1. Create a new table space for indices using this command:

```
CREATE TABLESPACE "USERS_IDX"
noLOGGING
DATAFILE 'c:\oracle\ORADATA\ibmrfid\USERS_IDX_1.dbf'
SIZE 500M REUSE AUTOEXTEND
ON NEXT 200K MAXSIZE 3000M EXTENT MANAGEMENT
LOCAL SEGMENT SPACE MANAGEMENT MANUAL;
```

2. Allow the user SAGE access to the USERS_IDX table space using this command:

```
ALTER USER "SAGE" QUOTA UNLIMITED ON "USERS_IDX";
```

3. Move indices to a new table space using these commands:

```
alter index SAGE.CC1119257758767 rebuild tablespace users_idx;
alter index SAGE.CC1119257886811 rebuild tablespace users_idx;
alter index SAGE.PK_ADDRESS rebuild tablespace users_idx;
alter index SAGE.PK_AGGREGATETAGEXTENSION rebuild tablespace users_idx;
alter index SAGE.PK_BASECHANNELCONFIG rebuild tablespace users_idx;
alter index SAGE.PK_CHANNELPARAMETER rebuild tablespace users_idx;
alter index SAGE.PK_CHANNELTEMPLATE rebuild tablespace users_idx;
alter index SAGE.PK_CNT_AGENTS rebuild tablespace users_idx;
```

```

alter index SAGE.PK_CNT_AGTS_ENT rebuild tablespace users_idx;
alter index SAGE.PK_CNT_AGTS_PROPS rebuild tablespace users_idx;
alter index SAGE.PK_CONTACT rebuild tablespace users_idx;
alter index SAGE.PK_CONTROLLER rebuild tablespace users_idx;
alter index SAGE.PK_CONTROLLER_TASK rebuild tablespace users_idx;
alter index SAGE.PK_DCAGENT rebuild tablespace users_idx;
alter index SAGE.PK_DCAGENTPROP rebuild tablespace users_idx;
alter index SAGE.PK_DCCONTROLLERAGENT rebuild tablespace users_idx;
alter index SAGE.PK_DCCTRLAGENTS rebuild tablespace users_idx;
alter index SAGE.PK_DCCTRLAGENT rebuild tablespace users_idx;
alter index SAGE.PK_DCCTRLAGTPROPS rebuild tablespace users_idx;
alter index SAGE.PK_DEVICE rebuild tablespace users_idx;
alter index SAGE.PK_DEVICETYPE rebuild tablespace users_idx;
alter index SAGE.PK_EMAILCHANNELCONFIG rebuild tablespace users_idx;
alter index SAGE.PK_ENTCATMETA rebuild tablespace users_idx;
alter index SAGE.PK_ENTITYCATEGORY rebuild tablespace users_idx;
alter index SAGE.PK_ENTITYTYPE rebuild tablespace users_idx;
alter index SAGE.PK_ENTITYTYPEINSTANCE rebuild tablespace users_idx;
alter index SAGE.PK_ENTTYPINSMETA rebuild tablespace users_idx;
alter index SAGE.PK_ENTTYPMETA rebuild tablespace users_idx;
alter index SAGE.PK_EPCCOMPANYPREFIXINDEX rebuild tablespace users_idx;
alter index SAGE.PK_EPCCENCODINGTYPE rebuild tablespace users_idx;
alter index SAGE.PK_EPCINPUTTYPE rebuild tablespace users_idx;
alter index SAGE.PK_EPCSERIALNUMBER rebuild tablespace users_idx;
alter index SAGE.PK_EVENTPARAMETER rebuild tablespace users_idx;
alter index SAGE.PK_EVENTPARAMETER_EVENTTEMPLA3 rebuild tablespace users_idx;
alter index SAGE.PK_EVENTTEMPLATE rebuild tablespace users_idx;
alter index SAGE.PK_EVENTTEMPLATE_TASK rebuild tablespace users_idx;
alter index SAGE.PK_HTTPCHANNELCONFIG rebuild tablespace users_idx;
alter index SAGE.PK_JMSCHANNELCONFIG rebuild tablespace users_idx;
alter index SAGE.PK_JMSTOPICCONFIG rebuild tablespace users_idx;
alter index SAGE.PK_LOCATION rebuild tablespace users_idx;
alter index SAGE.PK_LOGICALPRINTERPROPERTY rebuild tablespace users_idx;
alter index SAGE.PK_MQCHANNELCONFIG rebuild tablespace users_idx;
alter index SAGE.PK_OBJECTLINK rebuild tablespace users_idx;
alter index SAGE.PK_PRINTDATA rebuild tablespace users_idx;
alter index SAGE.PK_PRINTER rebuild tablespace users_idx;
alter index SAGE.PK_PRINTERTYPE rebuild tablespace users_idx;
alter index SAGE.PK_PRINTJOBS rebuild tablespace users_idx;
alter index SAGE.PK_PRINTSTATISTICS rebuild tablespace users_idx;
alter index SAGE.PK_PRINTTEMPLATE rebuild tablespace users_idx;
alter index SAGE.PK_RDR_AGENTS rebuild tablespace users_idx;
alter index SAGE.PK_RDR_AGTS_LOCS rebuild tablespace users_idx;
alter index SAGE.PK_RDR_AGTS_PROPS rebuild tablespace users_idx;
alter index SAGE.PK_READER rebuild tablespace users_idx;
alter index SAGE.PK_READERTYPE rebuild tablespace users_idx;
alter index SAGE.PK_RFIDANTENNA rebuild tablespace users_idx;
alter index SAGE.PK_SC_PACKTYPE rebuild tablespace users_idx;
alter index SAGE.PK_SC_PROFILE rebuild tablespace users_idx;
alter index SAGE.PK_SC_PROFILE_PROPERTIES rebuild tablespace users_idx;
alter index SAGE.PK_STATUS rebuild tablespace users_idx;
alter index SAGE.PK_TAG rebuild tablespace users_idx;
alter index SAGE.PK_TAGEXTENSION rebuild tablespace users_idx;
alter index SAGE.PK_TAGHISTORY rebuild tablespace users_idx;
alter index SAGE.PK_TASK rebuild tablespace users_idx;
alter index SAGE.PK_TASK_LOCATION rebuild tablespace users_idx;
alter index SAGE.PK_USERACCTEJB rebuild tablespace users_idx;
alter index SAGE.PK_CNT_AGENTS rebuild tablespace users_idx;
alter index SAGE.PK_CNT_AGTS_ENT rebuild tablespace users_idx;
alter index SAGE.PK_CNT_AGTS_PROPS rebuild tablespace users_idx;
alter index SAGE.PK_RDR_AGENTS rebuild tablespace users_idx;
alter index SAGE.PK_RDR_AGTS_LOCS rebuild tablespace users_idx;
alter index SAGE.PK_RDR_AGTS_PROPS rebuild tablespace users_idx;
alter index SAGE.PK_SUBLOCATION rebuild tablespace users_idx;
alter index SAGE.PK_OBJINSMETA rebuild tablespace users_idx;
alter index SAGE.PK_UPDATESITE rebuild tablespace users_idx;

```

4. Disable logging for the USERS table space using the Oracle Enterprise Manager Console (OEM).
 - a. In the OEM, select **Network** → **Databases** → **IBMRFID** → **Storage** → **Tablespaces** → **Users**.
 - b. On the Storage tab in the Enable Logging section, select **No**.
5. Using the OEM, increase the size of the redo logs to 100 MB and use only one log in each group (this step should already be done by the default Oracle installation). In the OEM, select **Network** → **Databases** → **IBMRFID** → **Storage** → **Redo Log Groups** to verify the settings.
6. Using the OEM, select **Network** → **Databases** → **IBMRFID** → **Storage** → **Tablespaces** → **Users** → **Datafiles**.
 There should only be one data file listed in the tree on the left. Select the data file and change the following properties:
 - On the General tab set the size to 500 MB
 - On the Storage tab set the following:
 - automatically extend datafile when full
 - increment = 100 MB
 - maximum value = 32767 MB
7. Exit the OEM.
8. For Oracle, use a new init.ora file based upon the following settings.
 - a. Be sure to check that all paths, *db_name*, *instance_name*, *service_names*, and *undo_tablespace* are the correct values for the current Oracle system.
 - b. Put this init.ora file in the *ORACLE_HOME*\database directory.
 - c. Name the file *initDB_NAME.ora* where *DB_NAME* is the name of the database. For example, *initIBMRFID.ora* for the IBMRFID database.

```
background_dump_dest = C:\oracle\admin\ibmrfid\bdump
backup_tape_io_slaves = TRUE
compatible = 9.2.0
control_files = ('C:\oracle\oradata\ibmrfid\control01.ctl',
'C:\oracle\oradata\ibmrfid\control02.ctl', 'C:\oracle\oradata\ibmrfid\control03.ctl')
cursor_space_for_time = TRUE
db_block_buffers = 76800
db_block_size = 8192
db_file_multiblock_read_count = 8
db_files = 1024
db_name = IBMRFID
event = '10126 trace name context forever, level 1'
global_names = FALSE
instance_name = IBMRFID
java_pool_size = 25165824
job_queue_processes = 4
large_pool_size = 8388608
log_archive_dest_1 = 'LOCATION=C:\ORACLE\ORA92\RDBMS'
log_buffer = 32768
log_checkpoint_interval = 10000
log_checkpoint_timeout = 1800
max_dump_file_size = 10240
max_enabled_roles = 30
open_cursors = 300
open_links = 4
oracle_trace_collection_name = ''
os_authent_prefix = ''
parallel_max_servers = 5
processes = 150
remote_login_passwordfile = EXCLUSIVE
service_names = IBMRFID
shared_pool_size = 201326592
sort_area_retained_size = 65536
sort_area_size = 500536
undo_management = AUTO
undo_retention = 1800
undo_suppress_errors = TRUE
undo_tablespace = UNDOTBS1
user_dump_dest = C:\oracle\admin\ibmrfid\udump
```

9. Use sqlplus and run the following Oracle scripts while logged in as sysdba. These scripts are found in the *ORACLE_HOME*\rdbms\admin directory.
 - a. To log in to sqlplus as sysdba, enter sqlplus without any parameters.

- b. When prompted for the user name, enter *ID/PASSWORD@DB_NAME* as sysdba.
 - initxa.sql
 - initjvm2.sql
 - initjvm4.sql
 - initjvm5.sql
10. While still logged into sqlplus as sysdba, enter the following commands:


```
shutdown immediate
create spfile from pfile;
startup
```

Note: To make future changes, modify the *initDB_NAME.ora* file then run these commands to update the spfile.
11. While still logged into sqlplus as sysdba, reanalyze the table statistics by entering the command:


```
exec dbms_stats.gather_schema_stats('SAGE');
```
12. Exit sqlplus.

Configuring WebSphere Application Server for Oracle

Update WebSphere Application Server to use the Oracle 10g 10.1.0.2 JDBC driver.

1. Download the Oracle 10g 10.1.0.2 JDBC driver from metalink.oracle.com or from another Oracle download site.
2. Place the 10g JDBC driver JAR file in the *ORACLE_HOME\jdbc\lib* directory.
3. Start WebSphere Application Server if it is not already running.
4. Open a Web browser and go to the WebSphere Application Server Administrative Console.
5. Navigate to **Resources** → **JDBC Providers**.
6. Select the Node scope and click **Apply**.
7. In the JDBC Providers list, click **OracleJDBCThinDriver** to see the configuration properties.
8. Modify the classpath to point to the 10g JDBC driver JAR file and click **OK**.
9. Follow the same process to change the classpath for the OracleJDBCThinDriverXA JDBC provider.
10. Click **OracleJDBCThinDriver**:
 - a. Then, click **Data Sources** → **IBMSESSION**.
 - b. For the Data Store helper class name, select **Oracle10g data store helper** and click **OK**.
11. Click **OracleJDBCThinDriverXA**:
 - a. Then, click **Data Sources** → **IBMRFID**.

Note: IBMRFID should be the database name.
 - b. For the Data Store helper class name, select **Oracle10g data store helper** and click **OK**.
12. Click **Save** on the WebSphere Application Server Administrative Console tool bar.
13. Click **Save** to save the master configuration.
14. Restart WebSphere Application Server.

Tuning the timeout value for a tag printer

This topic describes how to tune the timeout value for tag printers.

If you are printing an extremely large numbers of tags, the tag printer might time out. If it times out, you must increase the session timeout property value.

The session timeout value is a WebSphere-wide property. To modify it, you must modify the WebSphere-wide session timeout value. Follow the directions below.

1. Log on to the WebSphere Application Server Administrative Console.
2. Expand **Servers** → **Application Servers** → **server1**.
3. Expand **Container Settings** → **Container Service**.
4. Click **Transaction Service**.
5. Set the **Total transaction lifetime timeout** field to the desired value.
6. Click **OK**.
7. Click **Save** to save the configuration.

Chapter 7. Print, Verify, and Ship

Note: Print, Verify, and Ship is not shipped with WebSphere RFID Premises Server 6.0 or later. However, if you are using WebSphere RFID Device Infrastructure 1.1.1, it is still supported.

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.

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.

When you installed WebSphere RFID 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 RFID Premises Server is installed on your local server (Windows platforms only), you can access the interface by selecting **Start** → **Programs** → **IBM WebSphere RFID** → **Premises Server version** → **PVS Reference User Interface**.
- The WebSphere RFID Premises Server Administrative Console, which contains functions required for configuring the Print, Verify, and Ship Reference User Interface. You can access the WebSphere RFID Premises Server Administrative Console by typing `http://premises_server_hostname:9080/ibmrfidadmin` in the **Address** field of your Web browser and entering the default user name and password, `ibmrfidadmin`. If WebSphere RFID Premises Server is installed on your local server, you can access the administrative console by selecting **Start** → **Programs** → **IBM WebSphere RFID** → **Premises Server version** → **Administrative Console**.

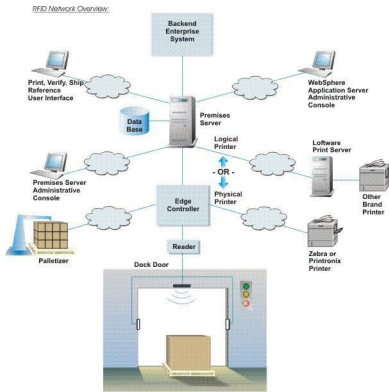
WebSphere RFID Premises Server supports several types of tag printer and tag reader specifications. For information on the IBM RFID device validation program, supported devices, readers, and RFID device manufacturers, refer to:
<http://www.ibm.com/solutions/sensors> .

This section contains instructions for the following tasks to be completed in order:

1. “Configuring printers” on page 180 - refer to this section to use the WebSphere RFID Premises Server Administrative Console to configure the necessary physical tag printers, logical tag printers, and print templates used for printing tag labels. The Print, Verify, and Ship Reference User Interface currently supports several printer specifications, and you can also install the Loftware or Bartender logical printer software to enable communication with printers beyond the scope of the supported specifications. See “Configuring physical printers” on page 183, “Adding and configuring a logical printer” on page 181, and “Creating print templates” on page 184 for more information.

2. “Configuring EPC commissioning details” on page 188 - refer to this section to use the WebSphere RFID Premises Server Administrative Console to configure the information required for converting suppliers’ product codes to Electronic Product Code (EPC) format.

The following diagram illustrates the RFID network configured with the Print, Verify, and Ship Reference User Interface.



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 192 for more information.

Configuring printers

The Print, Verify, and Ship scenario supports two types of tag printers: physical printers and logical printers.

A physical tag printer is connected to the Print, Verify, and Ship Reference User Interface through IBM’s edge controller. A logical tag printer is connected to the Print, Verify, and Ship Reference User Interface through a third-party software system, such as Software Labeling System by Software, Inc. or BarTender by Seagull Scientific, Inc.

Print, Verify, and Ship supports several types of tag printer specifications. For information on the IBM RFID device validation program, supported devices, readers, and RFID device manufacturers, refer to: <http://www.ibm.com/solutions/sensors> . If your system uses a tag printer other than those that conform to the supported specifications, you can use Software or BarTender to print tags on other printer models, which might require a software license from Software, Inc. or Seagull Scientific, Inc.

Important: You can associate only one tag printer with each location.

Below is a description of the process for configuring and using physical and logical tag printers:

- If you configure a physical tag printer with a supported specification, the print request is sent to the edge controller, which retrieves the appropriate print template at startup from the premises server. The edge controller then sends the

request to the physical tag printer and the job prints. See “Configuring physical printers” on page 183 and “Creating print templates” on page 184 for more information.

- If you configured a logical tag printer, such as Software or BarTender, the print request is sent to the appropriate print server, which retrieves the appropriate print template from the premises server. The print server then sends the request to the physical tag printer and the job prints. See “Adding and configuring a logical printer” and “Creating print templates” on page 184 for more information.

See the Chapter 7, “Print, Verify, and Ship,” on page 179 for a diagram showing the RFID network tag printer options.

Adding and configuring a logical printer

Logical printers enable you to print tag labels to printers supported by the commercial printing software Software by Software, Inc. and BarTender by Seagull Scientific.



Before beginning, ensure that you have done the following:

- You have successfully installed WebSphere RFID Premises Server. See Chapter 3, “Installing and configuring,” on page 19 for more information.
- You have successfully installed the Software or BarTender print server application on WebSphere RFID Premises Server or mapped a drive (Windows only) to a particular location on the WebSphere RFID Premises Server to get the print files.
 - **Windows** The Software print server is installed in the default directory, C:\Program Files\Software Labeling. The label.dtd file is installed in the default directory, C:\Program Files\Software Labeling\Batch
The BarTender print server is installed in the directory, C:\Program Files\SCAN_FOLDER. There is no .dtd file for BarTender.
 - **Linux** Because the Software and BarTender print servers run only on Windows, to run WebSphere RFID Premises Server on Linux, map a drive to where the Samba shared directory is located (**Tools** → **Map network drive**).

Note: If you install the Software print server application in a directory other than the default, you must add the SOFTWARE_LABEL_DTD property using the WebSphere RFID Premises Server Administrative Console, as described in the procedure below.



- Properties files are provided for the included templates. For more information, refer to “Creating properties files for print templates” on page 186. These properties files are located in the following directory:
 - **Windows** WAS_PROFILE_HOME\installedApps\node_name\IBM_Premises_PVS_Console.ear\ibmrfid_premises_pvsapp.war\config\labels
 - **Linux** WAS_PROFILE_HOME/installedApps/node_name/IBM_Premises_PVS_Console.ear/ibmrfid_premises_pvsapp.war/config/labels
 - SampleCaseTag.properties
 - SamplePalletTag.properties
 - SampleDynamicCaseTag.properties
 - SampleDynamicPalletTag.properties

Note: These files are stored in the above location by default. However, you can change their location by modifying the `labels.location` attribute in the `pvsapp.properties` file. The `pvsapp.properties` file is located in this directory:

-  `WAS_PROFILE_HOME\installedApps\node_name\IBM_Premises_PVS_Console.ear\ibmrfid_premises_pvsapp.war\config`
-  `WAS_PROFILE_HOME/installedApps/node_name/IBM_Premises_PVS_Console.ear/ibmrfid_premises_pvsapp.war/config`

After modifying `pvsapp.properties` file, restart WebSphere Application Server.

- The following logical print template files exist in this directory:

-  `IBM_RFID_HOME\premises\pvs\templates`
-  `IBM_RFID_HOME/premises/pvs/templates`
- `SampleCaseTag.lwl` (Loftware)
- `SamplePalletTag.lwl` (Loftware)
- `SampleDynamicCaseTag.lwl` (Loftware) and `SampleDynamicCaseTag.btw` (BarTender)
- `SampleDynamicPalletTag.lwl` (Loftware) and `SampleDynamicPalletTag.btw` (BarTender)

Important: To use the BarTender print templates `SampleDynamicCaseTag.btw` and `SampleDynamicPalletTag.btw` that come with WebSphere RFID Premises Server, you must first set the delimitation character to an exclamation point (!) in the printer properties for the logical printer defined in the WebSphere RFID Premises Server Administrative Console.

When you submit a print job to a logical tag printer, the logical printer reads the print template that you created in the WebSphere RFID Premises Server Administrative Console. The print template files contain information necessary to communicate with the tag printers in your network. For additional information, see *Creating print templates*.

Use these steps to add and configure the Loftware or BarTender logical tag printer. For information on configuring physical printers, refer to “Configuring physical printers” on page 183.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays. .
2. Navigate to **WRDI Configuration** → **Printers** from the left navigation panel. The Printers panel displays.
3. Click **New Logical Printer**. The Create a new Logical Printer panel displays.
4. In the **Printer ID** field, enter a unique logical identifier for this printer. The identifier must be 10 digits (0-9) or fewer.
5. In the **Printer Name** field, enter a unique description of the printer.
6. From the menu in the **Logical Printer Name** field, select **Loftware** or **BarTender**.
7. Click **Create Logical**. The new logical printer is saved and the Printers panel displays.
8. If you are defining a Loftware logical printer in a directory other than the default, add the `LOFTWARE_LABEL_DTD` property with the correct directory. Otherwise, continue to the next step.

9. On the Printers panel, click on the newly created printer. The Edit Logical Printer Details panel displays.
10. Ensure that the properties are correct for the logical printer or modify them. 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.

11. Click **Update**.
12. Create a print template for the logical tag printer by following the instructions in “Creating print templates” on page 184.

Configuring physical printers

The Print, Verify, and Ship Reference User Interface supports several types of tag printer specifications.

For information on the IBM RFID device validation program, supported devices, readers, and RFID device manufacturers, refer to: <http://www.ibm.com/solutions/sensors>.

Follow the instructions below to configure your installed tag printer for Print, Verify, and Ship using the WebSphere RFID Premises Server Administrative Console.

If your system uses a tag printer other than those that conform to the supported specifications, you can configure a logical tag printer, such as Loftware and Bartender, that enables the Print, Verify, and Ship application to work with your tag printer. See “Adding and configuring a logical printer” on page 181 for more information.

Before beginning, ensure that you have successfully installed the WebSphere RFID Premises Server. See Chapter 3, “Installing and configuring,” on page 19 for more information.

Also, before creating a new printer, you must have added a printer type. You can add the printer type by creating the appropriate printer agents and agent properties. For more information about configuration, see “Modifying the property values of agents” on page 116.

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **WRDI Configuration** → **Printers** in the left navigation panel. The Printers panel displays.
3. Click **New Printer**. The Create a new Printer panel displays.
4. Enter a unique, logical identifier for this printer. The identifier must be 10 digits (0-9) or fewer.
5. Enter a unique, textual description of the printer.
6. Select a printer in the **Printer Type** field.

7. Enter the printer's IP address in the **Printer IP Address** field. This field is optional if using a serial port.
8. Enter the port number in the **Printer IP Port Number** field. This field is optional if using a serial port.
9. Choose the serial port number in the **Printer Serial Port Number** field. This task is optional if using TCPIP.
10. In the **Printer Communication Protocol** field, select **TCPIP** to use the IP address and port or select **SERIAL** to use a serial port.
11. Click **Create**. The new printer displays in the Printers panel.
12. Create a print template for the printer by following the instructions in "Creating print templates."

Creating print templates

Use the Print Templates feature in the WebSphere RFID Premises Server Administrative Console to create a template to use for printing tag labels in the Print, Verify, and Ship Reference User Interface.

A print template in the WebSphere RFID 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	<code>IBM_RFID_HOME\premises\pvs\templates</code>
 Linux	<code>IBM_RFID_HOME/premises/pvs/templates</code>

They can be customized to meet your specific label requirements.

When you create a print template in the WebSphere RFID Premises Server Administrative Console, that information is stored in the WebSphere RFID Premises Server database. When the edge controller is started, it receives the location information for all of the currently defined templates. When you submit a print job from the Print, Verify, and Ship Reference User Interface, the edge controller reads the name of the template from the print request and retrieves the required template from the previously defined location. The edge controller then completes the fields of the template with the appropriate data from the print request.

You can create print templates for two types of printers: logical and physical. A print template for a logical tag printer must be stored on the file system of the logical printer software. For example, the .lwl Software print template must be on the Software server to access it and the Bartender print template must be on the Bartender server to access it. A print template for a physical tag printer must be stored on an IBM HTTP Server so that the edge controller can download it during RFID Data Transformation startup. The IBM HTTP Server can reside on either the same server as WebSphere RFID 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

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays. .
2. Navigate to **WRDI Configuration** → **Print Templates** from the left panel. The Print Templates panel displays.
3. Click **New**. The Create a New Print Template panel displays.
4. Enter the name of the template in the **Print Template Name** field.

Note: For physical tag printers, the templates use the following naming convention: *manufacturer-template_name-template.zip*. The print template name must be identical to the template name used in the manufacturer's .zip file. For example, if the template file name is zebra-LWCASE-template.zip, you must enter LWCASE in the **Print Template Name** field.

5. Select the printer manufacturer from the **Printer Type** field. If you are creating a print template for a logical tag printer, select **LOGICAL**.
6. Enter the location of the template file in the **Properties Location URL** field.
 - If you are creating a print template for a physical tag printer, use the following convention: *http://server_name/path/zip_filename*. For example: *http://myserver.com/templates/zebra-LWCASE-template.zip*.
 - If you are creating a print template for a Loftware logical tag printer, use the following convention: *file://Loftware_label_name*. For example: *file://Logical1-template.lwl*
 - If you are creating a print template for a Bartender logical tag printer, use this convention: *file://Bartender_label_name*. For example: *file://Logical1-template.btw*
7. Click **Create**. The print template is saved.
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 186 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 RFID Premises Server Administrative Console

Sample print templates are provided in the following directories:

	<i>IBM_RFID_HOME\premises\pvs\templates</i>
	<i>IBM_RFID_HOME/premises/pvs/templates</i>

You can use a sample print template and customize it to meet your specific label requirements.

When you create a custom print template, the information is stored in the WebSphere RFID Premises Server database. When the edge controller is started, it receives the location information for all of the currently defined templates. When

you submit a print job from the Print, Verify, and Ship Reference User Interface, the edge controller reads the name of the custom template from the print request and retrieves the required template from the previously defined location. The edge controller then completes the fields of the custom template with the appropriate data from the print request.

You can create custom print templates for both logical and physical tag printers. 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. A custom print template for a physical printer must be stored on an IBM HTTP Server so that the edge controller can download it during RFID Data Transformation startup. The IBM HTTP Server can reside on either the same server as WebSphere RFID Premises Server or on another server in the network.

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 RFID Premises Server after you create a new print template.

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 191.

The easiest way to create a new properties file is to modify one of the existing files located in the directory.

```
Windows WAS_PROFILE_HOME\installedApps\server_name\  
IBM_Premises_PVS_Console.ear\ibmrfid_premises_pvsapp.war\config  
Linux WAS_PROFILE_HOME/installedApps/server_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 located in the directory.

```
Linux WAS_PROFILE_HOME\installedApps\nodename\  
IBM_Premises_PVS_Console.ear\ibmrfid_premises_pvsapp.war\config  
Windows WAS_PROFILE_HOME/installedApps/nodename/  
IBM_Premises_PVS_Console.ear/ibmrfid_premises_pvsapp.war/config
```

If you modify the pvsapp.properties file, you must stop and then restart either WebSphere Application Server server 1 or the Premises_PVSConsole enterprise

application from the WebSphere Application Server Administrative Console. Use the following steps to stop and restart the Premises_PVSConsole enterprise application:

1. Log on to the WebSphere Application Server Administrative Console.
2. Click **Applications** → **Enterprise Applications**.
3. Stop and restart Premises_PVSConsole.

Use the following steps to create properties files for print templates:

1. Open one of the existing template properties files from the \labels directory.
2. Modify the static properties in the file to match the information needed for your print template:
 - If you are using a Software print template, use the Software 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:

Table 17. Sample .csv file

0	TEMPLATE	\$TEMPLATE_NAME
1	RFID	\$TAG
3	STRING	productname
4	STRING	productdescription
5	STRING	productquantity
6	STRING	manufacturerid
9	STRING	manufacturername

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 \labels 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 RFID Data Transformation service on both the WebSphere RFID Premises Server and the edge controller.

Note: You must restart WebSphere RFID Premises Server each time you make changes to these properties files.

To stop and restart the WebSphere RFID Premises Server:

- Run `WAS_HOME \bin\stopServer server1` to stop.
- Run `WAS_HOME \bin\startServer server1` to start.

 Windows	<i>stopServer.bat</i> and <i>startServer.bat</i>
 Linux	<i>stopServer.sh</i> and <i>startServer.sh</i>

Important: When using a properties file in the Print, Verify, and Ship Reference User Interface that contains non-English characters, be sure to run the J2SE utility, *native2ascii*, against the properties file to convert the non-English characters to their Unicode ASCII equivalent. The properties files are required when adding print templates to the WebSphere RFID Premises Server Administrative Console.

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 module in the WebSphere RFID 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 RFID 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 152 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 156 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 158 for more information.
4. Configure EPC conversions -- Configure WebSphere RFID Premises Server to convert EPC codes to SSCC and GTIN. Refer to "Configuring EPC conversions" for more information.

Configuring EPC conversions

Use the following procedures to configure the premises server to convert raw tag data into EPCGlobal Tag Data Standard 1.27 formats.

You can configure the WebSphere RFID Premises Server to convert all tags (including 64-bit tags) or only 96-bit tags by modifying the appropriate settings in the *premises.properties* and *bridge.properties* files.

In the *premises.properties* file, the three configuration properties for tag conversion are:

- `com.ibm.rfid.premises.event.tagread.bridgeEPCConversion`

This property determines if tag conversion should occur on the bridge or on WebSphere RFID Premises Server. Setting the property to false means that the tags will be converted on WebSphere RFID Premises Server.

Setting this property to true means that the tags will be converted on the bridge.

Important: If you are converting 64-bit tags, then you must set this property to false so that conversion will occur on the Premises server. If conversion occurs on the bridge, a 64-bit tag will be sent as a raw_uri value, regardless of the settings.

- `com.ibm.rfid.premises.event.tagread.primary.epcformat`

This property is the primary tag format. This is the format for the tagid attribute. The default for this property is raw. The raw property value means that the tagid appears in raw hex form.

- `com.ibm.rfid.premises.event.tagread.secondary.epcformat`

This property is the secondary tag format. This property notifies WebSphere RFID Premises Server to convert the original tagid raw hex value to this secondary EPC format. The secondary format is sent to the back-end server as tag read metadata. The secondary tag format has no default value. If it is commented out or does not appear in the properties file, there are no changes to the message.

In the `bridge.properties` file, the two configuration properties for tag conversion are:

- `route.3.transformation.0.message.epcprimaryfmt`

This property defines the primary tag conversion format. The default for this property is raw. The raw property value means that the tagid appears in raw hex form.

- `route.3.transformation.0.message.epcsecondaryfmt`

This property defines the secondary tag conversion format. The default for this property is none.

The valid values for both EPC format properties are as follows. One of the following may be specified per property.

- The value, `raw`, designates the current raw hex format, for example, `3114f4e4e45ca3c003000000`.
- The value, `raw_uri`, designates the EPCGlobal raw hex URI format, for example, `urn:epc:raw:96.x3114F4E4E45CA3C000000000`.
- The value, `tag_uri`, designates the EPCGlobal tag URI format, for example, `urn:epc:tag:sscc-96:0.4012345.1554235392`.
- The value, `id_uri`, designates the EPCGlobal id URI format, for example, `urn:epc:id:sscc:4012345.1554235392`.

For additional details about standard EPC formats, refer to the EPCGlobal specification, *EPC_Tag Data Specification 1.1Rev 1.27*.

Converting all tags

Use this procedure to configure the Premises server to convert all tags, including 64-bit tags.

1. Open the `premises.properties` file. This file is located on WebSphere RFID Premises Server, in the directory:

 `IBM_RFID_HOME\premises\properties`

 *IBM_RFID_HOME/premises/properties*

2. Find the section labelled Properties EPC conversion.
3. Edit the two properties,
`com.ibm.rfid.premises.event.tagread.primary.epcformat` and
`com.ibm.rfid.premises.event.tagread.secondary.epcformat`, using the
conversion values described above. Set the
`com.ibm.rfid.premises.event.tagread.bridgeEPCCConversion` property to `false`.
4. Save the file with your changes.
5. Open the `bridge.properties` file located in *IBM_RFID_HOME\dts*, and find the
section labelled Route 3.
6. Set the `route.3.transformation.0.message.epcprimaryfmt` property to `raw` and
the `route.3.transformation.0.message.epcsecondaryfmt` property to `none`.
7. Save the file with your changes.
8. Stop and restart WebSphere Application Server1 and RFID Data
Transformation.

To stop and restart the WebSphere RFID Premises Server:

- Run *WAS_HOME \bin\stopServer server1* to stop.
- Run *WAS_HOME \bin\startServer server1* to start.

 *stopServer.bat* and *startServer.bat*

 *stopServer.sh* and *startServer.sh*

This is an example of the `premises.properties` settings:

```
com.ibm.rfid.premises.event.tagread.bridgeEPCCConversion=false
com.ibm.rfid.premises.event.tagread.primary.epcformat=tag_uri
com.ibm.rfid.premises.event.tagread.secondary.epcformat=id_uri
```

This is an example of the `bridge.properties` settings:

```
route.3.transformation.0.message.epcprimaryfmt=raw
route.3.transformation.0.message.epcsecondaryfmt=none
```

Converting 96-bit tags

Use this procedure to configure WebSphere RFID Premises Server to convert 96-bit tags.

Note: If you change the configuration settings in the `premises.properties` file so that conversion occurs on the bridge, all conversion settings on WebSphere RFID Premises Server will be ignored.

1. Open the `premises.properties` file. This file is located on WebSphere RFID Premises Server, in the directory:

 *IBM_RFID_HOME\premises\properties*

 *IBM_RFID_HOME/premises/properties*

2. Find the section labelled Properties EPC conversion.
3. Edit the two properties,
`com.ibm.rfid.premises.event.tagread.primary.epcformat` and
`com.ibm.rfid.premises.event.tagread.secondary.epcformat`, using the
conversion values described above. Set the
`com.ibm.rfid.premises.event.tagread.bridgeEPCCConversion` property to `true`.
4. Save the file with your changes.
5. Open the `bridge.properties` file located in *IBM_RFID_HOME\dts*, and find the
section labelled Route 3.

6. Edit the `route.3.transformation.0.message.epcprimaryfmt` and `route.3.transformation.0.message.epcsecondaryfmt` properties, using the conversion values described above.
7. Save the file with your changes.
8. Stop and restart WebSphere Application Server1 and RFID Data Transformation:

This is an example of the `premises.properties` settings:

```
com.ibm.rfid.premises.event.tagread.bridgeEPCConversion=true
com.ibm.rfid.premises.event.tagread.primary.epcformat=raw
com.ibm.rfid.premises.event.tagread.secondary.epcformat=raw
```

This is an example of the `bridge.properties` settings:

```
route.3.transformation.0.message.epcprimaryfmt=tag_uri
route.3.transformation.0.message.epcsecondaryfmt=id_uri
```

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.

<code>\$BUSINESSREFERENCEID</code>	Synonym for <code>\$PURCHASEORDERID</code>
<code>\$CASESPERPALLET</code>	Value in <code>PVS.PRODUCTDATA.CASESPERPALLET</code>
<code>\$DESCRIPTION</code>	Value in <code>PVS.PRODUCTDATA.DESCRPTION</code>
<code>\$GID</code>	Value in <code>PVS.PRODUCTDATA.GID</code>
<code>\$ITEMSPERCASE</code>	Value in <code>PVS.PRODUCTDATA.ITEMSPERCASE</code>
<code>\$MANUFACTURERID</code>	Value in <code>PVS.PRODUCTDATA.MANUFACTURE</code>
<code>\$MANUFACTURERNAME</code>	Value in <code>PVS.MANUFACTURER.MANUFACTURERNAME</code>
<code>\$PARTNUMBER</code>	Value in <code>PVS.PRODUCTDATA.PARTNUMB</code>
<code>\$PRODUCTNAME</code>	Value in <code>PVS.PRODUCTDATA.PRODUCTNAME</code>
<code>\$PRODUCTQUANTITY</code>	For cases: Value in <code>PVS.PRODUCTDATA.ITEMSPERCASE</code> . For pallets: Value in <code>PVS.PRODUCTDATA.ITEMSPERCASE</code> multiplied by the value in <code>PVS.PRODUCTDATA.CASESPERPALLET</code> . For other pack types: defaults to "1."
<code>\$PURCHASEORDERID</code>	Current purchase order number
<code>\$SHIPFROMCITY</code>	Value in <code>PVS.PODATA.SHIPFROMCITY</code>
<code>\$SHIPFROMCOMPANY</code>	Value in <code>PVS.PODATA.SHIPFROMCOMPANY</code>
<code>\$SHIPFROMCOUNTRY</code>	Value in <code>PVS.PODATA.SHIPFROMCOUNTRY</code>
<code>\$SHIPFROMNAME</code>	Value in <code>PVS.PODATA.SHIPFROMNAME</code>
<code>\$SHIPFROMSTATE</code>	Value in <code>PVS.PODATA.SHIPFROMSTATE</code>
<code>\$SHIPFROMSTREET</code>	Value in <code>PVS.PODATA.SHIPFROMSTREET</code>
<code>\$SHIPFROMZIP</code>	Value in <code>PVS.PODATA.SHIPFROMZIP</code>
<code>\$SHIPTOCITY</code>	Value in <code>PVS.PODATA.SHIPTOCITY</code>
<code>\$SHIPTOCOMPANY</code>	Value in <code>PVS.PODATA.SHIPTOCOMPANY</code>

\$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 RFID 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 191.

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 RFID 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 193 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 199 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 202 for more information.

- **Report** - use the Report panel to run reports on items that have been printed and verified. See “Generating reports” on page 203 for more information.

WebSphere RFID Premises Server supports several types of printer specifications and reader specifications. For information on the IBM RFID device validation program, supported devices, readers, and RFID device manufacturers, refer to: <http://www.ibm.com/solutions/sensors> .

See “Printing RFID tag labels” to get started.

Opening the user interface

This topic describes how to open the Print, Verify, and Ship Reference User Interface.

1. Open a new Web browser.

Note: Use Internet Explorer 6.0 to open the Print, Verify, and Ship Reference User Interface. Ensure that JavaScript is enabled.

2. Type `http://premises_server_hostname:9080/RFIDPrintWeb/` in the **Address** field of your Web browser.

Note: If WebSphere RFID Premises Server is installed on your local server, you can access the Print, Verify, and Ship Reference User Interface by selecting **Start** → **Programs** → **IBM WebSphere RFID Premises Server version** → **PVS Reference User Interface**.

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 194 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 195, “Searching for products” on page 196, or “Scanning or entering GID codes” on page 197 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 197 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 197 for more information.
 - If you configured a physical tag printer, the edge controller received the print request from WebSphere RFID Premises Server. The edge controller

now sends the request to the physical printer and the job prints. See “Configuring physical printers” on page 183 and “Creating print templates” on page 184 for more information.

- If you configured a logical tag printer, Loftware or Bartender, the print request is sent to the appropriate print server, which retrieves the appropriate print template from WebSphere RFID Premises Server. The print server then sends the request to the physical tag printer and the job prints. See “Adding and configuring a logical printer” on page 181 and “Creating print templates” on page 184 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” 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 195 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 197 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 197 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\hostname_or_nodename\
IBM_Premises_PVS_Console.ear\ibmrfd_premises_pvsapp.war\config
Linux WAS_PROFILE_HOME/installedApps/hostname_or_nodename/
IBM_Premises_PVS_Console.ear/ibmrfd_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.

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 RFID 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 RFID Premises Server is installed on your local machine and it is running on Windows, you can access the interface by selecting **Start** → **Programs** → **IBM WebSphere RFID** → **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 RFID 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.

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:

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 194.
- 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” and “Scanning or entering GID codes” on page 197 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 RFID Premises Server Administrative Console display in this field. See “Creating print templates” on page 184 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.

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” on page 197. To select products from an existing purchase order or catalog, see “Selecting products from a purchase order or catalog” on page 195.

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.

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.

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 194 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 194 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 RFID 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.

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.

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 `sgt in96` 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 197 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 200 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.

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 RFID 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 RFID 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 turned on, but not yet ready.



- - the reader status is unavailable.



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

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 RFID 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 RFID Premises Server Administrative Console. In release 6.0 and later, 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 RFID Premises Server Administrative Console.
 - b. Depending on the version of the edge that you are running, click either **Data Capture Configuration** or **WRDI 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 the Data 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 RFID 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 RFID 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 Console before continuing.

The following icons represent the status of the reader:



- - The reader is turned on, but not yet ready.



- - The reader status is unavailable.



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

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.

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\
IBM_Premises_PVS_Console.ear\ibmrfd_premises_pvsapp.war\config
 **Linux** WAS_PROFILE_HOME/installedApps/
IBM_Premises_PVS_Console.ear/ibmrfd_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.

Chapter 8. Troubleshooting

This section contains information about troubleshooting including what information you should gather before you begin troubleshooting, information about error messages and logging, and scenario-based troubleshooting tips and techniques.

Debugging and troubleshooting Data Capture and Delivery

This section contains some tips for debugging and troubleshooting your Data Capture and Delivery configuration.

This section contains the following topics:

Verifying that the WebSphere RFID Premises Server is generating correct XML

Verify that the WebSphere RFID Premises Server is generating the correct XML for Data Capture and Delivery by going to the following URL: `http://premises_server_hostname:9080/ibmrfidadmin/premises.sl?action=getconfig&edge=edge_ID`

The Portal Controller Agent gets the `matrix.properties` file from the location specified in the `edge.xml` file:

```
<configuration
    factoryPid="com.ibm.rfid.agent.portalcontroller.bundle.PortalController
    AgentManagedServiceFactoryActivator">
<properties>
    <property key="matrix.properties"
        value="http://premises_server_hostname/matrix_simple.properties"/>
```

Enabling tracing for your Equinox or Eclipse launch configuration

To enable tracing, you can set the following system properties in either the `config.ini` file for Equinox or your Eclipse launch configuration:

Table 18.

Property	Description
<code>edge.log.threshold=DEBUG</code>	Indicates which level of logging to enable for Data Capture and Delivery.
<code>org.eclipse.soda.sat.core.util.logLevel=DEBUG</code>	Indicates which level of logging to enable for the Service Activation Toolkit. This level should be the same level as specified for the <code>edge.log.threshold</code> property.
<code>com.ibm.rfid.mbafe.tracing=true</code>	Enables additional tracing in MicroBroker Application Framework. Set this value if you suspect a problem with the bridge.

After setting the `edge.log.threshold` property, 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 WebSphere RFID Premises Server Administrative 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.

The alert agent (`com.ibm.rfid.agent.alert`) is responsible for forwarding log messages to the WebSphere RFID Premises Server. To change the level of messages that are forwarded, change the threshold property in the `edge.xml` section for the alert agent. Although it is possible to set the alert threshold to **Debug**, it causes additional traffic to the WebSphere RFID Premises Server, and is not recommended. The alert threshold should be set to **Info**, **Warning**, or **Error**.

To enable additional tracing on Data Capture and Delivery agents, set the tracing property to **True** in the `edge.xml` file that corresponds to the agents you want to enable. To modify the tracing property for all agents, enter the following:

```
<?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>
```

The command above disables tracing for all P1/E1 configurations.

Suspecting that MicroBroker is the problem

If you suspect that MicroBroker is the problem, you can modify the MicroBroker trace level by setting the following system property:

```
com.ibm.rfid.mbafe.microbroker.trace.level = min | 1 | 2 | 3 | 4 | 5 | max
```

When MicroBroker encounters a severe error, it dumps its trace buffer to the `MicroBroker\diagnostics` directory, along with an FFDC (First Failure Data Capture) file that contains other information.

If more tracing is needed, there is a MicroBroker Application Framework bundle that periodically forces a MicroBroker trace dump. Because the dump files are approximately 18 KB each in size, they take up a sizeable amount of disk space over time. The bundle to install is `com.ibm.rfid.mbafe.broker.trace`. You also need to set the following system property to specify how often to dump the trace buffer:

```
com.ibm.rfid.mbafe.microbroker.trace.interval = time-in-milliseconds
```

An example of a time interval is **5000**, for five second intervals.

You can also use the MicroBroker console to monitor the edge. However, because it monitors MicroBroker messages, the default is that it only sees messages that are bridged onto the MicroBroker bus.

Suspecting a problem within your WebSphere MQ environment

If you are using WebSphere MQ in your environment and suspect a problem with it, you can enable MQ-specific logging. 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

Monitoring messages using the Edge Event Monitor tool

You can monitor messages on the edge using the Edge Event Monitor tool. For information on using it, see the Edge Event Monitor tool documentation.

Using Notification Service to troubleshoot

Tools like the Edge Event Monitor can see Notification Service messages by way of an API. The MicroBroker console has limited support for this API and can be used if, for some reason, Edge Event Monitor is not available.

Publishing a topic to Notification Service

To publish a topic to Notification Service using the MicroBroker console, check the **NS** checkbox to the left of the **Publish** button. (The **MB** checkbox indicates that the topic should be published to the MicroBroker bus.)

Subscribing to Notification Service topics

To subscribe to Notification Service topics, publish this special topic to the MicroBroker bus, `mbaf/tooling/subscribe/ns/tool-id`, where *tool-id* is a unique identifier that you create. (For example, the tool ID for Edge Event Monitor is **eem**.) The tool ID allows the Notification Service bridge to maintain separate subscription lists for multiple tools that might be listening at the same time without them interfering with each other. The data for the subscribe topic is a comma-delimited list of Notification Service topics to which you can subscribe.

Unsubscribing to Notification Service topics

To unsubscribe all topics for a given tool ID, publish the following topic to the MicroBroker bus: `mbaf/tooling/unsubscribe/tool-id`.

To unsubscribe all topics for all tools, publish the following topic to the MicroBroker bus: `mbaf/tooling/reset`. This topic resets the Notification Service bridge to its default state, which is to only forward topics that are being bridged to the WebSphere RFID Premises Server.

Because the Edge Event Monitor tool does all of this automatically, it is the preferred tool for monitoring the edge.

Using IBM Support Assistant

IBM Support Assistant (ISA) is part of the WebSphere RFID 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 RFID Premises Server, WebSphere Application Server, Device Manager server, WebSphere MQ, and your DB2 Universal Database 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 RFID Premises Server supports versions 3.0 and 3.0.1 of IBM Support Assistant (ISA). You can install more than one version of ISA on the same system.

ISA can be installed locally with WebSphere RFID Premises Server and WebSphere Application Server, or you can install it on a remote system.

1. Install WebSphere RFID Premises Server.
2. Install ISA 3.0.1.
3. Locate the ISA plug-in files:

Windows:

`IBM_RFID_HOME\premises\isa\plugin\com.ibm.esupport.client.product.SSAN9K60`

Linux:

`IBM_RFID_HOME/premises/isa/plugin/com.ibm.esupport.client.product.SSAN9K60`

4. Use the ISA updater to install the WebSphere RFID Premises Server plug-in. Alternatively, you can download and install the WebSphere RFID 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 information

Use this table as a guideline to gather the appropriate values to help you troubleshoot your issue.

Parameter	Value
WebSphere RFID Premises Server installation directory	
WebSphere Application Server installation directory	
Location of the edge alerts and heartbeat log files	
Location of the premises.properties file	
WebSphere RFID Premises Server name and port number	
Tag reader or tag printer IP address	
Tag reader or tag printer model	

Error messages and logging

If you are experiencing a problem, check the error messages and log information. 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 edge controller and WebSphere RFID Premises Server.

Quality of Service for messages from the edge controller

The default configuration for the edge controller is QOS level: **QOS 1** and QOS persistence: **memory only**. This means that messages, including tag reads, are assured to flow from the edge controller to WebSphere RFID Premises Server, except when the edge controller has been turned off, the RFID Data Transformation has been stopped during network outages, or WebSphere RFID Premises Server is down.

Reasons for these default settings:

- The tags must be delivered to the WebSphere RFID 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 edge controller.
- Storing tags in a file or database might fill up the device file system and cause operating system problems.
- DB2e persistence significantly slows down the edge controller.

Tag reads eventually flow to the back end, as long as the edge controller is not rebooted or restarted, regardless of network communications between the edge controller and WebSphere RFID Premises Server. Tags cannot be read or queued at all when the network between the tag reader and the edge controller is down because there is no quality of service supported by the tag reader protocols.

QOS levels

At the edge controller, there are three QOS levels at which messages can be configured to be delivered from the edge controller to WebSphere RFID Premises Server:

QOS 0

Messages are delivered at most once. If there is a disruption in the network or on the edge controller software, the message is not 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

There are three ways to configure persistence on the edge 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 RFID Data Transformation service.

DB2e Persistence

Messages are persisted in a local database until they can be delivered at the above quality of service. This method survives an unclean shutdown, like turning off the edge controller.

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 edge controller has a heartbeat to the reader to make sure that the reader is still there. The edge controller also heartbeats back to the WebSphere RFID Premises Server. If WebSphere RFID Premises Server does not hear the heartbeat from the edge controller within the timeout period, it assumes that the edge controller is down or disconnected.



The heartbeat from the edge controller to the WebSphere RFID Premises Server contains the current status of the heartbeats from the edge controller to the tag reader. The WebSphere RFID Premises Server can tell from the edge controller heartbeat if the tag readers are down.

Log file locations and settings



This topic lists the locations and settings of the log files.

Installation log files for WebSphere RFID Premises Server and Device Manager server



install.log

 Windows	<i>IBM_RFID_HOME\logs\install.log</i>
 Linux	<i>IBM_RFID_HOME/logs/install.log</i>

dms_config_trace.log



 Windows	<i>IBM_RFID_HOME\DeviceManager\log\dms_config_trace.log</i>
 Linux	<i>IBM_RFID_HOME/DeviceManager/log/dms_config_trace.log</i>

Alert error log for the edge controller

- **File name:** There can be up to 10 alert log files. The log file name is edge-alert.x.log where x is a number from 0 to 9.
- **Default location:**
 -  **Windows** *IBM_RFID_HOME\logs*
 -  **Linux** *IBM_RFID_HOME/logs*
- **Format:**
 - Timestamp -- Time error issued from edge controller
 - Alerttype -- information, warning, error
 - Edge ID -- logical ID of the edge device
 - Message -- java exception or a message with the format of:



Reader *readerid* is ON/OFF

Heartbeat log for the edge controller

- **File name:** edge-heartbeats.log
- **Default location:**
 -  **Windows** IBM_RFID_HOME\logs
 -  **Linux** IBM_RFID_HOME/logs
- **Format:**
 - Timestamp -- Heartbeat time
 - Location ID -- location ID (for now this is the portal ID of the tag reader)
 - EdgeID -- logical ID of the edge device reporting heartbeat
 - ReaderID -- logical tag Reader ID
 - Message -- heartbeat messages of the format:
ON/OFF
edgeid=UP/DOWN
readerid=UP/DOWN

WebSphere Application Server and WebSphere RFID Premises Server log files

The WebSphere Application Server log files also contain information for WebSphere RFID Premises Server.

- **File names:** SystemOut.log, SystemErr.log, and trace.log
- **Location:**
 -  **Windows** WAS_PROFILE_HOME\logs\server1
 -  **Linux** WAS_PROFILE_HOME/logs/server1

Note: The default installation directory for WebSphere Application Server is C:\Program Files\IBM\WebSphere\AppServer on Windows and /opt/IBM/WebSphere/AppServer on Linux. 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 “Troubleshooting techniques” on page 65 for details on how to enable tracing on WebSphere Application Server for WebSphere RFID Premises Server.

DB2 Universal Database log files

- **File names:** db2diag.log and jdbcerr.log
- **Default location:**
 -  **Windows** C:\Program Files\IBM\SQLLIB\DB2
 -  **Linux** /opt/IBM/SQLLIB/DB2

RFID Data Transformation service

- **File name:** DTSruntime.log
- **Default location:**
 -  **Windows** IBM_RFID_HOME\logs
 -  **Linux** IBM_RFID_HOME/logs



Note: *IBM_RFID_HOME* is an environment variable created when you installed WebSphere RFID Premises Server. If you modified the installation directory for WebSphere RFID Premises Server, be sure to use the modified installation path.

How to modify logging levels and output

This topic describes how to turn logging on and off and how to modify logging levels, files names, and paths.

Turning logging on and off

1. Open the file:

	<code>IBM_RFID_HOME\premises\properties\premises.properties</code>
	<code>IBM_RFID_HOME/premises/properties/premises.properties</code>

2. Modify the settings in this file.
 - To turn logging off, specify the value, "false," in place of the log file name.
 - To turn logging on, specify a log file name in the format *.log.
3. Save the file and close it.
4. Restart WebSphere Application Server.

Modifying logging levels

You can modify logging levels of the edge controller, modify the logging levels of the WebSphere RFID Premises Server using WebSphere Application Server, or modify the logging levels of the WebSphere RFID Premises Server OSGi stack. Follow the directions below.

Modifying the logging levels of the edge controller

1. Open the WebSphere RFID Premises Server Administrative Console. The Welcome page displays.
2. Click **Controllers** from the left navigation pane. Choose the correct **Controllers** link depending on your environment, either Data Capture and Delivery or WebSphere RFID Device Infrastructure. The Controllers panel displays.
3. Click to select the edge controller for which you are modifying the logging levels. The Edit Controller Details panel displays.
4. Modify the **Alert Threshold** value. Valid levels are **Error**, **Warning**, **Info**, and **Debug**.

Note: The Debug level causes a large increase in the amount of traffic going to WebSphere RFID Premises Server, and is not a recommended value for continuous operations.

Refer to the Edge controller details panel description for more information.

5. Click the **Reload Configuration** button to apply the new value.
6. Restart the edge controller. All locations associated with this edge controller are disabled while the device is restarting.

Modifying the logging levels of WebSphere RFID Premises Server using WebSphere Application Server

1. Open the WebSphere Application Server Administrative Console.
2. Browse to **Troubleshooting** → **Logs and Trace** → **server1** → **Diagnostic Trace**.

3. Use the Configuration page 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 RFID Premises Server:
 - RFIDALE
 - com.ibm.kimono.*
 - com.ibm.rfid.*
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 the logging levels of the WebSphere RFID Premises Server OSGi stack

1. Open the *IBM_RFID_HOME/dts/com.ibm.rfid.dts.log.connector.properties* file.
2. Edit the property, *com.ibm.rfid.premises.logging.file.level*. The valid values are SEVERE , WARNING , INFO , and ALL. The value ALL is equivalent to **Debug**.
3. Save the file and close it.
4. Restart the RFID Data Transformation service.

Modifying log file names and paths

By default, IBM Tivoli Monitoring monitors the files, *edge-heartbeats.log* and *edge-alerts.log*. It looks for these files in the *IBM\RFID\logs* directory. To change these default values, modify the *LogSources* variable in the *tecad_win.conf* file. *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:

	<i>IBM_RFID_HOME\monitoring</i>
	<i>IBM_RFID_HOME/monitoring</i>

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.

Error messages

This topic contains lists of messages that display for the Data Capture and Delivery controller and WebSphere RFID Premises Server, and is intended for reference purposes only. Some of these messages are generated automatically, while others require tracing to be enabled.

WebSphere RFID Premises Server error messages

WebSphere RFID Premises Server tracing events

The following table contains informational messages generated by WebSphere RFID 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}
StartStopReadingHandlerBean	StartStopReadingHandlerBean	Received Start/Stop eventReceived Start/Stop command: {event} {alias} {location}

WebSphere RFID Premises Server J2EE application messages

The following list contains externalized messages that can be logged by the WebSphere RFID Premises Server J2EE applications that run in WebSphere Application Server.

- An input message could not be parsed into the XML format expected by WebSphere RFID 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)	<i>data_format_exception_message</i> default value assumed: <i>default_value</i> .
ApplicationPingAgent	doApplicationPing()	Edge ID - Application Ping after timeout - received pong sequence number (<i>receive_sequence_number</i>) was greater than the ping sent (<i>send_sequence_number</i>).
	handleTopicToEdge(String)	Edge ID - Application Ping - received pong sequence number (<i>receive_sequence_number</i>) was not equal to the ping sent (<i>send_sequence_number</i>).
	logPingPongInfo(String)	Edge ID - Application Ping/Pong sequence = <i>sequence_number</i> .

Agent Name	ID	Message
FilterAgent	filtersChanged()	Stopping to wait for filter(s): <i>unavailable_filters</i> .
	handleTopicReaderTags(Object)	Allowing tag through: <i>tag</i> .
	tryToStart()	Starting. Waiting for filter(s): <i>unavailable_filters</i> .
HealthCheckAgent	handleTopicPortalStatus(Object)	Portal <i>ID</i> - HealthCheck status <i>up_or_down</i> - while portal is enabled.
PortalControllerAgent	handleTopicControllerCommand(Object)	Current sensor matrix state: <i>state</i> .
	handleTopicPalletFeedback(Object)	Portal enabled. Tag rejected. Tag acknowledged.
	handleTopicTimeout(int, Object)	<i>Portal_ID</i> - Timeout occurred at timer <i>ID</i> .
	processMatrix()	<i>Portal_ID</i> - State transition: <i>current_state_name</i> -> <i>next_state_name</i> .
	setPortal(Boolean)	Portal enabled Portal disabled
RestartAgent	handleRestartTopic(String)	Restart request received, Edge <i>ID</i> about to restart.
RFIDMapAgent	handlePublishArrived_content(String, Object)	<i>tag_count_log</i>
	handlePublishArrived(String, Object)	Self test: received unknown format data.
TagAggregatorAgent	handleTopicDumpTags()	Sending tag aggregation to Premises. Collection count: <i>aggregated_tag_count</i> .
UniversalSensorAgent	logWithLevel(int, String)	<i>log_message</i>

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 <i>get_description</i> - ApplicationPing <i>message</i> - Application Ping/Pong sequence = <i>sequence_number:reason</i> .
HealthCheckAgent	handleTopicAppPingSignalStatus(Object)	Portal <i>ID</i> - HealthCheck status changed to UP - application ping is OK. Portal <i>ID</i> - HealthCheck status changed to DOWN - application ping timeout.
	handleTopicDeviceSignalHealth(int)	Portal <i>ID</i> - HealthCheck status changed to <i>up_or_down</i> - reader signaled health <i>up_or_down</i> .
	handleTopicDevicesSignalStatus(String, String)	Portal <i>ID</i> - HealthCheck status changed to UP - sensor <i>topic</i> is <i>on_or_off</i> . Portal <i>get_description</i> - HealthCheck status changed to DOWN - sensor has error.

Agent Name	ID	Message
PortalControllerAgent	handleTopicHealthSignal(Object)	System health down. Performing a reset...
	handleTopicReaderSignalStatus(Object)	Reader error detected. Performing a reset...
	handleTopicSensor(int, Object)	Error at sensor <i>ID</i> 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: <i>states</i> .
	setDataExtension(SensorMatrixRow)	Got reply with correct topic: <i>topic</i> , but different data: <i>data</i> .
	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)	<i>tag_count_log</i>
TagAggregatorAgent	checkCollectionSizeAndWarn()	Tag Aggregator collection list has grown to <i>size</i> elements.
UniversalSensorAgent	logWithLevel(int, String)	<i>log_message</i>

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): <i>unavailable_filters</i> .
PortalControllerAgent	handleTopicHealthSignal(Object)	Unexpected health signal value: <i>value</i> .
	handleTopicPalletFeedback(Object)	Unexpected pallet feedback value: <i>value</i> .
	handleTopicPortalCommand(Object)	Unexpected portal command value: <i>value</i> .
	handleTopicReaderSignalStatus(Object)	Unexpected reader signal value: <i>value</i> .
	handleTopicSensor(int, Object)	Unexpected sensor topic value: <i>value</i> .
	handleTopicSwitchSignal(Object)	Unexpected switch signal value: <i>value</i> .
	handleTopicTimeout(int, Object)	Unexpected timeout topic value from timer <i>ID</i> : <i>value</i> .
	loadPropertiesFromURL(String)	Cannot load properties. URL <i>URL</i> is malformed (<i>error</i>)
	processMatrix()	Processing matrix failed: <i>illegal_argument_exception</i> . Performing a reset...
	setDataExtension(SensorMatrixRow)	Timeout while waiting for <i>notification_topic</i> .
RFIDMapAgent	handlePublishArrived_content(String, Object)	Sending tag aggregation to Premises. Collection count: <i>tag_count</i> .

Agent Name	ID	Message
TagAggregatorAgent	getSubscriptions()	Tag aggregator agent has invalid topics and values for Start and Stop triggers. Configure separate topics or values for stop and start events.
UniversalActorAgent	handleControlAllTopic(Object)	Expected Boolean value with topic <i>topic</i> , but got object of class: <i>class</i> .
	handleControlTopic(Actor, String, Object)	Expected Boolean value with topic <i>topic</i> , but got object of class <i>class</i> .
UniversalSensorAgent	logWithLevel(int, String)	<i>log_message</i>
	setLogLevel(String)	Unknown value <i>log_level</i> in configuration property <i>sensor.stateloggging</i> - using DEBUG as default value.
Publication	publish	<i>message</i>

OSGi Application Framework error messages

The following list contains error messages that display for the OSGi Application Framework.

- Failed to find properties file.
- Failed to find properties resource.
- The method {0} should have been overridden.
- A bundle should be transient or uninstallable, not both.
- Consider using BaseBundleActivator's method {0} instead of {1}.
- The bundle exports multiple instances of the same service.
- Exported service was not created.
- Failed to get properties.
- The BundleContext used to start and stop the manager must be identical.
- LDAP filter contains questionable whitespace - {0}
- Service is not declared as exported by the bundle. Check bundle manifest.
- Service is not declared as imported by the bundle. Check bundle manifest.
- Transient bundles do not typically export services.
- Unknown BundleEvent {1}
- Unknown BundleContext
- Dependent is null
- Prerequisite is null
- Unknown FrameworkEvent {1}
- Failed to acquire service matching the filter {0}.
- Owner already exists
- Owner cannot be null
- Record is already released
- Unknown ServiceEvent {0}
- The log level {0} is unknown
- Record must not be registered
- Record must not have a service object
- Record must not represent an on-demand service
- Detector already released
- Owner already exists
- The property {0} is unknown

- Entry already exists for key {0}
- The bundle {0} cannot be added to the TransientBundleManager
- Bundle must be in the STARTING state to be added to the TransientBundleManager
- Failed to uninstall bundle

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

Troubleshooting tips

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

Note: 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 RFID Data Transformation logs and contact your IBM representative for further assistance.

- “Installation fails on Linux” on page 220

- “The back-end system does not receive messages”
- “The edge controller cannot connect to WebSphere RFID Premises Server” on page 221
- “Connection between the tag reader and edge controller is interrupted” on page 221
- “The edge controller is unable to obtain configuration from WebSphere RFID Premises Server” on page 221
- “The edge controller is unable to communicate with the tag reader” on page 221
- “WebSphere RFID Premises Server does not work after stopping and restarting” on page 222
- “WebSphere RFID Premises Server does not work in general” on page 222
- “Queue filled to maximum depth in the WebSphere MQ RFID Queue Manager” on page 222
- “Incorrectly labeled ALE information messages in the WebSphere Application Server logs” on page 222
- “Installer cannot run a second time if either WebSphere RFID Premises Server or Device Manager server is already installed on the server” on page 223
- “RFID Data Transformation fails to stop” on page 223
- “Unable to start the device agent on WebSphere RFID Premises Server” on page 223
- “Usage of direct JNDI lookup of resources has been deprecated” on page 224
- “A NullPointerException occurs when OSGi starts” on page 224

Installation fails on Linux

The installation of WebSphere RFID 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.

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.
- Open MQ explorer and check if the current depths of TASK.Q and EDGE.IN.Q are 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 RFID Data Transformation service is running. Check the runtime log

	C:\Program Files\IBM\RFID\logs\DTSRuntime.log
	/opt/IBM/RFID/logs/DTStruntime.log

Stop and start the RFID Data Transformation service if the log shows errors or exceptions.

The edge controller cannot connect to WebSphere RFID Premises Server

Perform 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 RFID 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 RFID Premises Server from the edge controller, check cables and hardware connections.
- Check the network connection between the edge controller and WebSphere RFID Premises Server. Try to Telnet into the edge controller and "ping" WebSphere RFID 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 RFID 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 RFID 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 RFID Data Transformation log.
- Check the tag reader. Attempt to telnet to the reader using the reader port defined at the "Reader details" on page 127 panel on the WebSphere RFID Premises Server Administrative Console. 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 RFID Data Transformation log and contact your IBM representative for additional assistance.

WebSphere RFID 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 Universal Database (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 RFID Data Transformation is running. If not, start **IBM WebSphere Premises Server DT Service** from the Services panel.

WebSphere RFID 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.

Queue filled to maximum depth in the WebSphere MQ RFID Queue Manager

Check to see if the maximum queue depth has been reached. Check the current depth of the queues in IBM.RFID.QM using MQ Explorer.

If you have reached the maximum queue depth, perform the following workaround steps:

1. Stop WebSphere Application Server.
2. Stop the RFID 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 RFID Data Transformation on the WebSphere RFID Premises Server.
6. Monitor the affected queue depths until they fall to zero.
7. Restart the RFID Data Transformation on all edge controllers.

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.

Installer cannot run a second time if either WebSphere RFID Premises Server or Device Manager server is already installed on the server

The installation wizard cannot distinguish which feature has already been installed. If you are installing both WebSphere RFID Premises Server and Device Manager server on the same server, choose to install both (**Typical**) when prompted. If you choose to install one and then later want to install the other, then you will need to uninstall and reinstall the product.

RFID Data Transformation fails to stop

If the RFID Data Transformation test bundle (`com.ibm.rfid.dts.test_version`) is running, RFID Data Transformation will not shut down properly. Stop the test bundle before stopping the RFID Data Transformation service.

To stop the test bundle, complete the following steps:

1. From the RFID Data Transformation command prompt in the window where you started RFID Data Transformation, type `ss` to list the installed bundles.

Text similar to the following displays.

```
ss
Framework is launched.
id      State      Bundle
0       ACTIVE    system.bundle_version
1       ACTIVE    org.eclipse.equinox.common_version
2       ACTIVE    org.eclipse.core.jobs_version
3       ACTIVE    org.eclipse.equinox.registry_version
4       ACTIVE    org.eclipse.equinox.preferences_version
5       ACTIVE    org.eclipse.core.contenttype_version
6       ACTIVE    org.eclipse.osgi.services_version
7       ACTIVE    org.eclipse.equinox.log_version
8       ACTIVE    org.eclipse.core.runtime_version
9       ACTIVE    org.eclipse.soda.sat.core_version
10      ACTIVE    com.ibm.rfid.dts.mq.jar_version
11      ACTIVE    com.ibm.rfid.dts.log.connector_version
12      RESOLVED  com.ibm.rfid.dts.consolelog_version
13      ACTIVE    com.ibm.micro.utils_version
14      ACTIVE    com.ibm.micro_version
15      ACTIVE    com.ibm.mqttlocalclient_version
16      ACTIVE    com.ibm.mqttclient_version
17      ACTIVE    com.ibm.micro.bridge.mq.jms_version
18      ACTIVE    com.ibm.esc.epc_version
19      ACTIVE    com.ibm.rfid.mbaaf_version
21      ACTIVE    com.ibm.rfid.dts.mbridge_version
22      ACTIVE    com.ibm.rfid.dts.mbadmin_version
23      RESOLVED  com.ibm.rfid.dts.test_version
24      RESOLVED  com.ibm.rfid.bundle.loader_version
25      ACTIVE    com.ibm.rfid.dts.Win32Service_version
```

2. Identify the ID number of the `com.ibm.rfid.dts.test_version` bundle and type `stop ID_number`.

Unable to start the device agent on WebSphere RFID Premises Server

You are unable to configure the device adapter with WebSphere RFID Premises Server. In order to configure the device adapter, the core bundle list needs to be updated and copied 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`):

- `local_dc_core.txt` is for running Data Capture and Delivery bundles inside the RFID Data Transformation service on WebSphere RFID Premises Server.

- `remote_dc_core.txt` is for running Data Capture and Delivery bundles that are remote to the RFID 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 (`local_dc_core.txt` or `remote_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 RFID 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 RFID Data Transformation service or the remote Data Capture and Delivery controller.
6. Start the bundle loader bundle (`com.ibm.rfid.bundle.loader_version.jar`).

Usage of direct JNDI lookup of resources has been deprecated

See J2CA0294W: Deprecated usage of direct JNDI lookup of resource for details.

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.

Troubleshooting techniques

Use these instructions to help you troubleshoot your problem.

Checking the depth of MQ Queues

1. Open MQ Explorer.
2. Select **Start** → **Programs** → **IBM WebSphere MQ** → **WebSphere MQ Explorer**.
3. Check the depths of the RFID queues. Queues usually process and go to zero quickly. If the depth of any queue is greater than zero, it indicates a problem.

Enabling WebSphere RFID Premises Server trace with WebSphere Application Server

1. Open a Web browser.
2. Go to `http://premises_IP_address:9060/ibm/console`.
3. Go to **Troubleshooting** → **Logs and Trace** → **server1** → **Diagnostic Trace** → **Change Log Detail Levels** → **Groups**.
4. Modify the Trace Specification to `RFIDALE=all: com.ibm.rfid.*=all: com.ibm.kimono.*=all`.
5. Click **Apply** → **OK** → **Save** and **Save** again.

MQ queues

Queues can be used for troubleshooting. Queues usually process and go to zero quickly. If you open MQ and any of the queues are not zero, it indicates a problem.

Tip: For an advanced troubleshooting technique, you can stop individual queues from processing to help isolate where the problem is occurring.

Note: MQ queues for WebSphere RFID Premises Server are named from the premises server point-of-view. "IN" queues are coming "in" to WebSphere RFID Premises Server. "OUT" queues are going "out" from WebSphere RFID Premises Server to the MicroBroker (for the edge controller) and the back-end adapters.

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 RFID 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 queues

These are internal queues.

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 as heartbeats and alerts.

PERSISTENCE.Q, PERSISTENCE.Q1, PERSISTENCE.Q2, and PERSISTENCE.Q3

These queues process tag persistence messages when tag persistence is enabled in the premises.properties file. The PERSISTENCE.Q1, PERSISTENCE.Q2, and PERSISTENCE.Q3 queues are used only when com.ibm.rfid.premises.multipersistence.queue.count is set to 4 in the

premises.properties file. To use fewer persistence queues, decrease the value of `com.ibm.rfid.premises.multipersistence.queue.count`.

TAGMONITOR.OUT.Q

This queue monitors tag reads as they occur in real-time.

TASK.Q, TASK.Q1

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. TASK.Q1 is used only when `com.ibm.rfid.premises.multitask.queue.count` is set to 1 in the premises.properties file.

Troubleshooting MicroBroker issues

The IBM Data Capture and Delivery Toolkit for WebSphere RFID Premises Server comes with a useful tool called *MicroBroker Explorer* that is designed to help troubleshoot problems related to MicroBroker.

The MicroBroker Explorer is configured as part of Eclipse, and enables you to view agents and topics in a graphical user interface.

The MicroBroker Explorer presents the MicroBroker Application Framework agents that are connected to the MicroBroker and the topics that have flowed over the MicroBroker. MicroBroker can run on either a local or remote target device. The MicroBroker Explorer is designed to help understand the behavior of an application and to make diagnosing and fixing problems easier.

For detailed information, refer to the online Help in IBM Data Capture and Delivery Toolkit for WebSphere RFID Premises Server. In the Help file, open the MicroBroker Application Framework topic and navigate to **Tools** → **Microbroker Explorer**.

Chapter 9. Reference information

These topics are provided as additional reference information to help you.

Accessibility features for WebSphere RFID 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 RFID Premises Server. These features support:

- Keyboard-only operation.
- Interfaces that are commonly used by screen readers.

Tip: The WebSphere RFID Premises Server Information Center and its related publications are accessibility-enabled for the IBM Home Page Reader. You can operate all features using the keyboard instead of the mouse.

Keyboard navigation

This product 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 RFID Premises Server provides a plugin to the IBM Support Assistant. The IBM Support Assistant is a collection of pointers to various IBM support resources online. The WebSphere RFID Premises Server plugin for IBM Support Assistant contains pointers to additional support resources that are specific to WebSphere RFID Premises Server. For more information on how to download and install the IBM Support Assistant and the corresponding WebSphere RFID Premises Server plugin, refer to “Using IBM Support Assistant” on page 207.

WebSphere Application Server

- WebSphere Application Server product support page: <http://www.ibm.com/software/webservers/appserv/was/support/>
- WebSphere Application Server training and certification: <http://www.ibm.com/software/info1/websphere/index.jsp?tab=education/index>
- WebSphere Application Server information library: <http://www.ibm.com/software/webservers/appserv/was/library/library60.html>

- WebSphere Application Server 6.0.x Information Center: <http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp>

WebSphere MQ

- WebSphere MQ product support page: <http://www.ibm.com/software/integration/wmq/support/>
- WebSphere MQ training and certification: <http://www.ibm.com/software/integration/websphere/education/>
- WebSphere MQ information library: <http://www.ibm.com/software/integration/wmq/library/>

DB2 Universal Database

- DB2 Universal Database (DB2) product support page: <http://www.ibm.com/software/data/db2/udb/support/>
- DB2 training and certification: <http://www.ibm.com/software/data/education>
- DB2 information library: <http://www.ibm.com/software/data/technical/>
- DB2 Universal Database 8.2.4 Information Center: <http://publib.boulder.ibm.com/infocenter/db2help/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 Enterprise Console

- Tivoli Enterprise Console product support page: <http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliEnterpriseConsole.html>
- Tivoli training and certification: <http://www.ibm.com/software/tivoli/education/>
- 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 Configuration Manager

- Tivoli Enterprise Console product support page: <http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliConfigurationManager.html>
- Tivoli Configuration Manager 4.2.3 Information Center: http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp?topic=/com.ibm.tivoli.itcm.doc/CM_PI.htm

Tivoli Systems Management Information Center

- Tivoli Systems Management Information Center: <http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp>

Copyright notice and trademarks

Copyright notice

© Copyright IBM Corporation 2004, 2007. All rights reserved. May only be used pursuant to an IBM software license agreement. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into

any computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual, or otherwise, without prior written permission of IBM Corporation. IBM Corporation grants you limited permission to make hardcopy or other reproductions of any machine-readable documentation for your own use, provided that each such reproduction shall carry the IBM Corporation copyright notice. No other rights under copyright are granted without prior written permission of IBM Corporation. The document is not intended for production and is furnished "as is" without warranty of any kind. **All warranties on this document are hereby disclaimed, including the warranty of non-infringement and the implied warranties of merchantability and fitness for a particular purpose.**

U.S. Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corporation.

Trademarks

IBM, WebSphere, Tivoli, MQSeries, DB2, Redbooks, and Tivoli Enterprise Console are trademarks of the IBM Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Internet Explorer, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Pentium is a registered trademark of Intel[®] Corporation or its subsidiaries in the United States and other countries

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Adobe, Acrobat, Portable Document Format (PDF), and PostScript are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

Alien is a trademark or registered trademark of Alien Technology Corporation in the U.S and other countries.

TAGSYS is a registered trademark of TAGSYS S.A.

Zebra is a registered trademark of ZIH Corporation.

Intermec is a registered trademark of Intermec Technologies Corporation.

Printronix is a registered trademark of Printronix, Inc.

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.

OBID and OBID i-scan are trademarks of FEIG ELECTRONIC GmbH.

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

RFID Premises Server
WebSphere RFID Premises Server Information Center
Version 6.0.0.1

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



Cut or Fold
Along Line

Fold and Tape

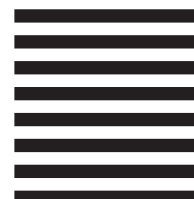


NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
Information Development
Department 6R4A
P.O. Box 12195
Research Triangle Park, NC 27709-9990



Fold and Tape

Cut or Fold
Along Line