



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

Installing and configuring 1

Installing the product	1
Planning your server topology	1
Packaging	2
Identifying hardware and software requirements	3
Prerequisites	4
Installing WebSphere RFID Premises Server	7
Installing Device Manager server for WebSphere RFID Premises Server	12
Installing silently	21
Installing using Tivoli Configuration Manager	21
Installing and enabling IBM Tivoli License Compliance Manager	24
Installing the toolkits	25
Toolkit prerequisites	25
Installing WebSphere RFID Premises Server Toolkit	26
Installing IBM RFID Data Transformation Toolkit for WebSphere RFID Premises Server	26
Installing IBM Data Capture and Delivery Toolkit for WebSphere RFID Premises Server	27
Configuring the IBM Data Capture and Delivery Toolkit for WebSphere RFID Premises Server	28
Installing the fix pack for WebSphere RFID Premises Server	31

Verifying the installation	32
Creating a cluster for WebSphere RFID Premises Server	33
Planning your cluster topology	33
Installing a cluster	34
Installing the WebSphere Application Server log file adapters	40
Installing the edge controller heartbeat log file adapters	41
Uninstalling the product	42
Uninstalling the fix pack for WebSphere RFID Premises Server	43
Uninstalling the toolkits	43
Uninstalling the WebSphere RFID Premises Server Toolkit.	43
Uninstalling the IBM RFID Data Transformation Toolkit for WebSphere RFID Premises Server	44
Uninstalling the IBM Data Capture and Delivery Toolkit for WebSphere RFID Premises Server	44
Migrating to WebSphere RFID Premises Server 6.0.x from a previous version	45
Enabling security with WebSphere Application Server	46

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 3 and the WebSphere RFID Premises Server system requirements page
- Installation prerequisites
- “Installing WebSphere RFID Premises Server” on page 7
- “Installing Device Manager server for WebSphere RFID Premises Server” on page 12
- “Installing silently” on page 21

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 42.

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 2 for more details on exactly what products and versions are included with WebSphere RFID Premises Server, and then see “Prerequisites” on page 4 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 21.

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 21 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 12.

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 47 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 53.
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 47 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 42.

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 21 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\DMScfg.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 42.

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 17, 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/ibmrfdadmin/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 22. 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 7.

If you need to uninstall the WebSphere RFID Premises Server software, refer to “Uninstalling the product” on page 42.


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 43.

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 25 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 44.

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 44.

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 7 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 53.

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 10.
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.

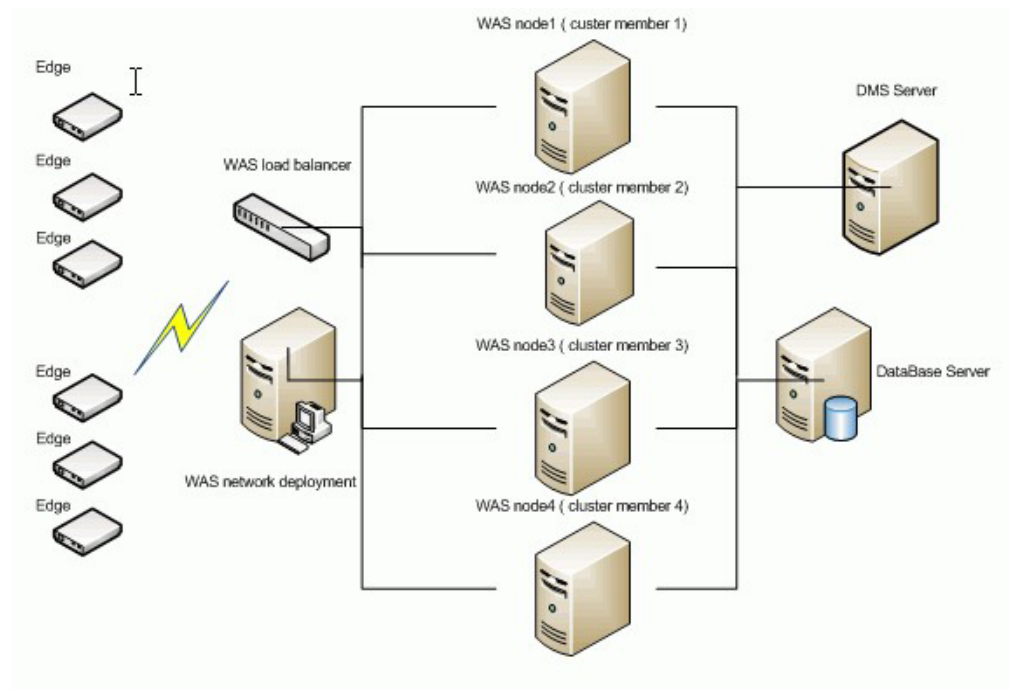
A WebSphere RFID Premises Server cluster consists of the following cluster members:

- 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.



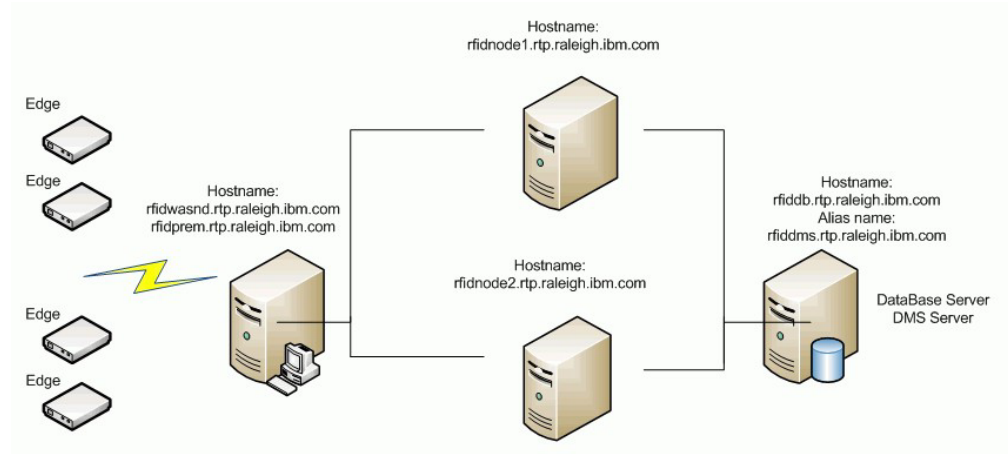
Installing a cluster

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 12.
3. Install WebSphere RFID Premises Server on the cluster nodes (rfidnode1 and rfidnode2). Follow the instructions in “Installing WebSphere RFID Premises Server” on page 7, with the following exceptions:
 - In step 9 on page 8, make sure to select the **Custom** radio button and then select to install WebSphere RFID Premises Server only.
 - In step 11 on page 8, 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.
-  **Linux** 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:
 -  **Windows** Click **Start** → **Programs** → **IBM WebSphere** → **Edge Components** → **IBM Load Balancer** → **Load Balancer**.
 -  **Linux** 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	IBM_RFID_HOME\premises\install\security\
Linux	IBM_RFID_HOME/premises/install/security/

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:**
 -  **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 47 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:**

-  `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 = 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.

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 54. 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.

Readers' Comments — We'd Like to Hear from You

RFID Premises Server
WebSphere RFID Premises Server Installation Guide
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

Please do not staple

Fold and Tape



NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
Information Development
Department 6R4A
P.O. Box 12195
Research Triangle Park, NC 27709-9990



Fold and Tape

Please do not staple

Fold and Tape

Cut or Fold
Along Line