



WebSphere Sensor Events Installation Guide

June 2009

This edition applies to IBM WebSphere Sensor Events version 6, release 2, 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 9BSA
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 2004, 2009.

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

Contents

Installing and configuring 1

Preparing for installation	1
Planning your single server topology	1
Planning your high availability topology	2
Packaging	3
Prerequisites	4
Installing the product	14
Installing WebSphere Sensor Events	14
Installing WebSphere Sensor Events and Location Awareness Services for WebSphere Sensor Events	22
Installing Location Awareness Services for WebSphere Sensor Events.	32
Installing a high availability system	38
Installing silently	43
Installing using Tivoli Provisioning Manager for Software	45
Installing the Sensor Data Services for WebSphere Remote Server	47
Installing and enabling IBM Tivoli License Compliance Manager	54
Installing the toolkits	54
Installing WebSphere Sensor Events Toolkit.	54
Installing IBM Data Capture and Delivery Toolkit for WebSphere Sensor Events	56
Configuring the IBM Data Capture and Delivery Toolkit for WebSphere Sensor Events	56
Verifying the installation	60
Installing a remote Data Capture and Delivery controller	61
Installing the bundle loader and a bundle list	61

Installing additional bundle lists	63
Using wildcards with the bundle loader.	64
Defining the network topology	64
Installing the WebSphere Application Server log file adapters	65
Installing the edge controller heartbeat log file adapters	66
Configuring security for WebSphere Application Server	67
Enabling security	68
Disabling security	70
Configuring Location Awareness Services for WebSphere Sensor Events.	71
Configuring the database.	71
Installing the Spatial Management Client	72
Configuring security for the Control Processing portlet	74
Using the sample subscriber and notification programs	75
Verifying your installation	76
Configuring InfoSphere Traceability Server	78
Uninstalling the product	78
Uninstalling WebSphere Sensor Events	78
Uninstalling a high availability system	79
Uninstalling the toolkits	80
Uninstalling the WebSphere Sensor Events Toolkit	80
Uninstalling the IBM Data Capture and Delivery Toolkit for WebSphere Sensor Events	80

Installing and configuring

These topics describe how to install WebSphere® Sensor Events and most of its components.

For details on installing Asset Inventory Management Services for WebSphere Sensor Events, see Installing Asset Inventory Management Services for WebSphere Sensor Events.

Preparing for installation

Use these topics to plan and prepare for your WebSphere Sensor Events installation.

Planning your single server topology

Use the scenarios described in this section to plan for your installation of WebSphere Sensor Events.

Possible topologies

WebSphere Sensor Events supports the following topology options:

- A locally installed or remote database server, which can be either DB2® or Oracle
- A locally installed or remote Bundle Repository Server
- Optional IBM® Location Awareness Services for WebSphere Sensor Events component on a Windows® operating system using a DB2 database
- Optional IBM Asset Inventory Management Services for WebSphere Sensor Events component on a Windows operating system using a DB2 database and an additional DB2e database.

Installation scenarios

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

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

Restriction: If you install DB2 remotely on a Windows operating system, be sure that your WebSphere Sensor Events server and the remote server have the same drive letter for the DB2 installation. For example, if you want to use drive F on your remote server for the DB2 installation, then your WebSphere Sensor Events server should also have a drive F.

The second task is to install WebSphere Sensor Events, and optionally Location Awareness Services for WebSphere Sensor Events.

Restriction: Location Awareness Services for WebSphere Sensor Events must be installed on a Windows operating system on the same server as

WebSphere Sensor Events.
Location Awareness Services for WebSphere Sensor Events supports a DB2 database.

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

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

Restriction: Your database server and WebSphere Sensor Events must be installed on servers with the same operating system.

After you have installed WebSphere Sensor Events, you can install IBM Asset Inventory Management Services for WebSphere Sensor Events. For details on how to install this component, see *Installing Asset Inventory Management Services for WebSphere Sensor Events*.

Planning your high availability topology

This topic helps you plan the topology of high availability for your WebSphere Sensor Events.

Requirements

- Setting up a high availability system requires a WebSphere Sensor Events Enterprise Edition license.
- All servers in the high availability system must run the same operating system.
- All cluster members must have the prerequisite software installed in the same path as the central server.

See “Prerequisite steps for a high availability system” on page 7 for more information on prerequisites.

Topology

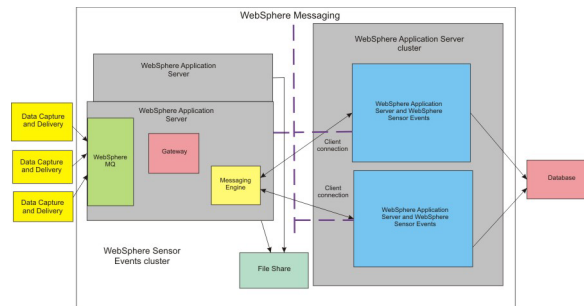
A WebSphere Sensor Events high availability topology consists of the following:

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

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

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

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



Packaging

The packaging for WebSphere Sensor Events includes the following disks and software products.

WebSphere Sensor Events

- Quick Start, including product Quick Start Guide
- WebSphere Sensor Events for Windows (Disk 1 of 2)
Contains:
 - WebSphere Sensor Events installer
 - Prerequisite middleware packages
- WebSphere Sensor Events for Windows (Disk 2 of 2)
Contains:
 - SPDs for installing with Tivoli® Provisioning Manager for Software on Windows
 - WebSphere Sensor Events bundles
 - WebSphere Sensor Events database scripts
- WebSphere Sensor Events for Linux® (Disk 1 of 2)
Contains:
 - WebSphere Sensor Events installer
 - Prerequisite middleware packages
- WebSphere Sensor Events for Linux (Disk 2 of 2)
Contains:
 - WebSphere Sensor Events bundles
 - WebSphere Sensor Events database scripts
- WebSphere Sensor Events Toolkit
- IBM Data Capture and Delivery Toolkit for WebSphere Sensor Events, including Eclipse and Equinox

WebSphere Sensor Events Enterprise Edition contains all of the disks in the aforementioned basic WebSphere Sensor Events package, as well as the following additional disks:

- High Availability for WebSphere Sensor Events Enterprise Edition for Windows
- High Availability for WebSphere Sensor Events Enterprise Edition for Linux

Additional software

These additional software and components are available for purchase:

- IBM Location Awareness Services for WebSphere Sensor Events for Windows

Location Awareness Services for WebSphere Sensor Events is an optional component that allows you to continuously track active tags in real time in predefined areas.

The package for this software component includes a Quick Start CD and the component disk.

This component is also available in an enterprise edition.

- IBM Asset Inventory Management Services for WebSphere Sensor Events for Windows

Asset Inventory Management Services for WebSphere Sensor Events is an optional component that provides a data center inventory management solution that uses passive RFID technology.

The package for this software component includes a Quick Start CD, a DB2 Everyplace® Enterprise Edition disk, and the component disk.

This component is also available in an enterprise edition.

- Sensor Data Services for WebSphere Remote Server for Windows or Linux

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

The package for this software component includes a Quick Start CD and the required software product disks.

This component is also available in a central site edition.

Prerequisites

Use these topics to prepare for your WebSphere Sensor Events installation.

Hardware and software requirements

Hardware requirements

See the WebSphere Sensor Events system requirements page for information about the supported hardware for WebSphere Sensor Events and for information about the additional hardware requirements for IBM Location Awareness Services for WebSphere Sensor Events and IBM Asset Inventory Management Services for WebSphere Sensor Events.

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

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

Software requirements

Operating systems

All of the operating systems in this table are 32-bit.

Table 1. Supported operating systems

Operating system	WebSphere Sensor Events server	Location Awareness Services for WebSphere Sensor Events	Asset Inventory Management Services for WebSphere Sensor Events
Windows <ul style="list-style-type: none"> Windows Server 2003 Standard or Enterprise editions with Service Pack 2 Windows Server 2003 R2 Standard or Enterprise editions with Service Pack 2 	Yes	Yes	Yes
> Linux <ul style="list-style-type: none"> SUSE Linux Enterprise Server V10.1 SUSE Linux Enterprise Server V10.2 	Yes	No	No
> Linux <ul style="list-style-type: none"> Red Hat Enterprise Linux 5.2 Red Hat Enterprise Linux 5.3 	Yes	No	No

Notes:

- See the WebSphere Sensor Events system requirements page for the latest information about supported operating platforms.
- A high availability WebSphere Sensor Events topology is not supported with Location Awareness Services for WebSphere Sensor Events.

Browsers and other GUI software

In order to use the WebSphere Sensor Events Administrative Console, you must have Mozilla Firefox or Internet Explorer 6.0 or 7.0 installed on your operating system and JavaScript™ enabled.

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

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

Asset Inventory Management Services for WebSphere Sensor Events supports Internet Explorer 7.x versions and Mozilla Firefox 3.x versions.

Middleware

The following software is required for WebSphere Sensor Events. These software packages are installed with WebSphere Sensor Events, with the exception of Oracle. See “Packaging” on page 3 for more details on how the software is delivered. WebSphere Sensor Events can also be installed on WebSphere Process Server 6.1.2, which has the required middleware.

- WebSphere Application Server 6.1.0.23
- IBM HTTP Server 6.1.0.23
- WebSphere MQ 6.0.2.5
- DB2 Workgroup Server Edition 9.5 Fix Pack 3a, or Oracle 10.2.0.2 (11g driver) or Oracle 11.1.0.6 (11g driver) with the patched ojdbc5.jar file. See http://www.oracle.com/technology/software/tech/java/sqlj_jdbc/htdocs/jdbc_111060.html to download the patched file.

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

- WebSphere Business Events 6.2 Fix Pack 1

Notes:

- Location Awareness Services for WebSphere Sensor Events only supports the DB2 database versions listed. It does not support Oracle.
- Asset Inventory Management Services for WebSphere Sensor Events only supports the DB2 database version listed. It does not support Oracle. It also requires DB2 Everyplace Enterprise Edition 9.1.3.

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

- Tivoli Omegamon XE for Messaging for Distributed Platforms 7.0 (optional)
- Tivoli Composite Application Manager for Web Resources 6.2 (optional)
- Tivoli Enterprise Console® 3.9 Fix Pack 6 (optional)
- Tivoli Provisioning Manager for Software 5.1.1.2 (optional)
- IBM Tivoli Monitoring 6.2.1 (optional)
- IBM Tivoli Monitoring for Databases 6.2.1 (optional)

Tivoli Provisioning Manager for Software Software Package Definition (SPD)

files: WebSphere Sensor Events provides Tivoli Provisioning Manager for Software SPD files for WebSphere Application Server, DB2 Workgroup Server Edition platforms and WebSphere MQ running on Windows platforms only. You can use Tivoli Provisioning Manager for Software to install and configure these prerequisites on WebSphere Sensor Events. For instructions on how to do this, refer to “Installing using Tivoli Provisioning Manager for Software” on page 45.

Prerequisite configuration

This topic contains prerequisite information for installing WebSphere Sensor Events.

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

- “Configuring Linux for the prerequisite software” on page 7
- “Configuring Internet Explorer” on page 7
- “Configuring Mozilla Firefox” on page 7
- “Preparing your target servers for remote deployment” on page 7

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

Configuring Linux for the prerequisite software:

About this task

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

1. Prepare the Linux operating system for WebSphere Application Server.
2. Prepare the SUSE Linux Enterprise Server operating system for WebSphere Application Server.
 - SUSE Linux Enterprise Server 10
 - Red Hat Enterprise Linux 5
3. Prepare the Linux operating system for WebSphere MQ
4. Check for any entries in the `/etc/hosts` file that include the IP address, 127.0.0.2, and comment them out before installing WebSphere Sensor Events.

Configuring Internet Explorer:

About this task

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

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

Configuring Mozilla Firefox:

About this task

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

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

Preparing your target servers for remote deployment: If you plan on installing the database server, WebSphere Sensor Events, and the Bundle Repository Server on different servers, add the host name or IP address of those target servers into the hosts file of each target server. This can prevent possible installation failures during remote deployment.

Prerequisite steps for a high availability system

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

Before you begin

Remember: Setting up a high availability system requires a WebSphere Sensor Events Enterprise Edition license.

1. Install WebSphere Sensor Events on a central server.

For a high availability system installation, do not choose to install WebSphere Business Events on the same WebSphere Application Server profile or server as the WebSphere Sensor Events server. If you do, you will need to uninstall WebSphere Business Events before continuing with the high availability installation steps. For information on how to install WebSphere Business Events in a cluster, refer to the WebSphere Business Events Information Center.

Be sure to verify that your installation is successful, and that your environment is set up for remote Data Capture and Delivery controllers. See “Planning your high availability topology” on page 2 and “Installing a remote Data Capture and Delivery controller” on page 61 for more information.

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

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

Note: Do not federate your WebSphere Sensor Events into the network deployment environment.

3. On a cluster node server, install the following prerequisite software:

- WebSphere Application Server 6.1.0.23
- a database client, either DB2 Workgroup Server Edition or Oracle. See the WebSphere Sensor Events software requirements for more information.
- a WebSphere MQ 6.0.2.5 client. To install this, copy the contents of the *MQ_INSTALL_ROOT\java\lib* directory from your central server to same path on your node server. *MQ_INSTALL_ROOT* is the installation path for WebSphere MQ.

Important:

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

For more detailed information on clustering, see Creating clusters.

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

```
addNode WASND_host WASND_SOAP_port
```

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

5. Optional: Delete servers from WebSphere Application Server Network Deployment.
 - a. Open the WebSphere Application Server Network Deployment administrative console.
 - b. Navigate to **Servers** → **Application servers**. You will see all servers from each cluster node.
 - c. Select all servers and delete them.
 - d. Save the master configuration.
6. If you have WebSphere Application Server security enabled, disable it. The installer cannot run properly with security enabled.
7. Restart the deployment manager, all node agents, and all servers.

What to do next

Follow the instructions for “Installing a high availability system” on page 38.

Toolkit prerequisites

This topic contains prerequisite information for installing the toolkits available with WebSphere Sensor Events.


Prerequisites for WebSphere Sensor Events Toolkit

WebSphere Sensor Events Toolkit requires the following hardware and software.

Hardware

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

Software

-  Windows XP, or Windows Server 2003 Standard or Enterprise editions with Service Pack 2, or Windows Server 2003 R2 Standard or Enterprise editions with Service Pack 2

Note: WebSphere Sensor Events Toolkit is not supported on Linux.

- Rational® Application Developer for WebSphere Software 7.5.1 or 7.5.3
- DB2 Workgroup Server Edition 9.5 Fix Pack 3a, or Oracle 10.2.0.2 (11g driver) or Oracle 11.1.0.6 (11g driver) with the patched ojdbc5.jar file. See http://www.oracle.com/technology/software/tech/java/sqlj_jdbc/htdocs/jdbc_111060.html to download the patched file.

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

- IBM HTTP Server 6.1.0.21
- WebSphere MQ 6.0.2.5
- WebSphere Application Server 6.1.0 Fix Pack 21 installed on the WebSphere Application Server runtime that is installed with Rational Application Developer for WebSphere Software

Prerequisites for IBM Data Capture and Delivery Toolkit for WebSphere Sensor Events

This toolkit requires the following software:

-  Windows XP

In addition, Eclipse 3.4.2 is required for the toolkit. Eclipse can be installed by extracting the eclipse-SDK-3.4.2-win32.zip file into a local directory. The .zip file is available on the disk containing the IBM Data Capture and Delivery Toolkit for WebSphere Sensor Events.

If you are installing the IBM Data Capture and Delivery Toolkit for WebSphere Sensor Events on a server that does not have a network connection, then Equinox must be installed manually. To install Equinox, extract the eclipse-equinox-3.4.2.zip file into the Eclipse 3.4.2 directory, making sure that the features and plugins directories overwrite the same directories in the Eclipse directory.

If you intend to extend the IBM Data Capture and Delivery Toolkit for WebSphere Sensor Events, it is recommended that you compile all code changes against the Minimum Platform Environment/JCL: CDC/Foundation v1.1. Data Capture and Delivery requires a Java™ environment (JCL) equivalent to or larger than CDC/Foundation version 1.1, thus a full J2SE is more than sufficient.

Note: If you are using a high availability configuration, J2SE is required for the Data Capture and Delivery platform.

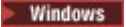

Configuring the installation program paths

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

Changing the deployment package path:

About this task

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

	C:\Program Files\SolutionFiles\wizard\1
	/opt/SolutionFiles/wizard/1

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

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



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

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

1. Click **Edit** → **Preferences** in menu on the Welcome panel.
2. The Deployment Preferences panel appears and you can modify the deployment package path to your desired location.



3. Click **OK** when you are finished with your changes to return to the Welcome panel.

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

	C:\Program Files\SolutionFiles
	/opt/SolutionFiles

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

- Create a new response file on your local server and include the desired installation path for the `installLocation.value` variable. Then, from a command line, issue the following command using the **-options** parameter to specify the new response file. Replace *path to new response file* with the name and location of the new response file:

	WindowsSetup.exe -options " <i>path to new response file</i> "
	LinuxSetup.exe -options " <i>path to new response file</i> "

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

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

Prerequisite software files

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

File locations

Windows

These files are located on the first disk for WebSphere Sensor Events for Windows operating systems.

- `disk_root\bin\com\ibm\jsdt\webserver\tree\db2win.xx.jar`
- `disk_root\bin\com\ibm\jsdt\webserver\tree\ihswin.xx.jar`
- `disk_root\bin\com\ibm\jsdt\webserver\tree\ihspfwin.xx.jar`
- `disk_root\bin\com\ibm\jsdt\webserver\tree\mqwin.xx.jar`
- `disk_root\bin\com\ibm\jsdt\webserver\tree\mq6rp2fp5win.xx.jar`
- `disk_root\bin\com\ibm\jsdt\webserver\tree\waswin.xx.jar`
- `disk_root\bin\com\ibm\jsdt\webserver\tree\waswswin.xx.jar`
- `disk_root\bin\com\ibm\jsdt\webserver\tree\wasupdateinstallerwin.xx.jar`
- `disk_root\bin\com\ibm\jsdt\webserver\tree\wbewin.xx.jar.1.2`

These files are located on the second disk for WebSphere Sensor Events for Windows operating systems.

- `disk_root\disk2\bin\com\ibm\jsdt\webserver\tree\wbewin.xx.jar.2.2`

- *disk_root\disk2\bin\com\ibm\jsdt\webserver\tree\premiseswin.xx.jar*
- *disk_root\disk2\bin\com\ibm\jsdt\webserver\tree\wseitlm.xx.jar*
- *disk_root\disk2\bin\com\ibm\jsdt\webserver\tree\lasitlm.xx.jar*

Linux

These files are located on the first disk for WebSphere Sensor Events for Linux operating systems.

- *disk_root/bin/com/ibm/jsdt/webserver/tree/db2linux.xx.jar*
- *disk_root/bin/com/ibm/jsdt/webserver/tree/ihslinux.xx.jar*
- *disk_root/bin/com/ibm/jsdt/webserver/tree/ihsfplinux.xx.jar*
- *disk_root/bin/com/ibm/jsdt/webserver/tree/mqlinux.xx.jar*
- *disk_root/sat_installer/bin/com/ibm/jsdt/webserver/tree/mq6rp2fp5linux.xx.jar*
- *disk_root/bin/com/ibm/jsdt/webserver/tree/waslinux.xx.jar*
- *disk_root/bin/com/ibm/jsdt/webserver/tree/waswslinux.xx.jar*
- *disk_root/bin/com/ibm/jsdt/webserver/tree/wasupdateinstallerlinux.xx.jar*
- *disk_root/bin/com/ibm/jsdt/webserver/tree/wbelinux.xx.jar.1.2*

These files are located on the second disk for WebSphere Sensor Events for Linux operating systems.

- *disk_root/disk2/bin/com/ibm/jsdt/webserver/tree/wbelinux.xx.jar.2.2*
- *disk_root/disk2/bin/com/ibm/jsdt/webserver/tree/premiseslinux.xx.jar*
- *disk_root/disk2/bin/com/ibm/jsdt/webserver/tree/wseitlm.xx.jar*

WebSphere Business Events file locations

If you need to set up WebSphere Business Events on a remote server, the *wbewin.xx.jar* and *wbelinux.xx.jar* files are also located in the WBE path on the second disks for WebSphere Sensor Events for both Windows and Linux operating systems.

Creating the database, tablespace, tables, and data

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

If you choose to install WebSphere Business Events remotely, then you will need to manually create the DB2 or Oracle database. See the WebSphere Business Events Information Center for more information.

Creating the database manually:

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

About this task

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

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

1. Create the WebSphere Sensor Events database for DB2 or Oracle.

For a local or remote DB2 database:

- a. Open the DB2 Control Center.
- b. Right-click **All Databases** and select **Create Database** → **Standard**.
 - 1) Enter IBMRFID as the database name.

Note: Linux commands are case-sensitive.

- 2) Select the option to **Enable database for XML (Code set will be set to UTF-8)**. For more information on this option, refer to the DB2 information center.
- c. Click **Finish**. Do not fine tune the database when it is created.
- d. Exit the DB2 Control Center.
- e. (Optional) Catalog the remote database, IBMRFID, to the local machine.

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

2. When installing WebSphere Sensor Events, select the option to create tables and populate the data for the database.

Creating the databases using scripts:

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

Before you begin

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

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

Example

For DB2:

 Windows

```
createIBMRfid_db2.bat dbName longTablespaceFile longTempTablespaceFile
```

 Linux

```
createIBMRfid_db2.sh dbName longTablespaceFile longTempTablespaceFile
```

For Oracle:

 Windows

```
createIBMRfid_oracle.bat dbUser dbPassword dbSpec longTablespaceFile
```

 Linux

```
createIBMRfid_oracle.sh dbUser dbPassword dbSpec longTablespaceFile
```

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

Installing the product

Use these topics to install WebSphere Sensor Events and its components.

Installing WebSphere Sensor Events

Follow the steps in this topic to install WebSphere Sensor Events and its prerequisite middleware.

Before you begin

Stop all WebSphere Application Server profiles before you run the installer.

Important installation tips:

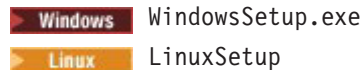
- When specifying installation paths, make sure the directories contains only US English ASCII characters. Also enter only US English ASCII characters in directory paths in properties files.
 - Enter a password that meets the password rules of the target machine. A password that is not valid will cause installation to fail.
1. Check your hardware and operating system and make sure that they meet the necessary requirements.
 2. Make sure that you have completed all the prerequisite steps necessary for your environment. If you would like to modify the path used by the deployment wizard, follow the steps in “Changing the deployment wizard path” on page 11 before launching the installation program.
 3. Make sure your database is encoded for UTF-8.
 - If you plan to use DB2 as your database server, and you would like to use an existing database, make sure that database was created with the option to **Enable database for XML (Code set will be set to UTF-8)**. If your DB2 database was not created with that option, you will need to delete and recreate that database if you want to use it.
 - If you are using Oracle, make sure that the database was created with the Unicode AL32UTF8 character set.

The installer will create a database for you, but you have the option to install one manually as well.

4. If you have a Windows operating system and you are running Terminal Server and Terminal Server Licensing, run the change user /install Windows command before starting the WebSphere Sensor Events installation program.

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

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



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

You can also run the installation program in silent mode. Refer to “Installing silently” on page 43 for further instructions.

6. Select the radio button beside the **I accept both the IBM and the non-IBM terms** statement if you agree to the license agreement and click **Next** to continue.
7. When the Welcome panel appears you can either:
 - Click **Next** to continue installing the product.
 - Or, if you would like to change the default path used for the deployment package, follow the instructions in “Changing the deployment package path” on page 10 before continuing with the next steps.
8. On the Select Tasks panel, click **Next** to install the product and to choose the database type.
9. Choose to use either DB2 or Oracle as your local or remote database.
 - If you choose DB2 and do not have it installed on your server, then the installer will install it for you if you want it installed locally. If you already have DB2 installed on your local server, then the installer will recognize that it is already there and check to make sure it meets the requirements.
 - Choose Oracle if you have an existing installation of that database that you would like to use.
10. Choose to install WebSphere Sensor Events only and click **Next**. If you would like to install both WebSphere Sensor Events and IBM Location Awareness Services for WebSphere Sensor Events, refer to “Installing WebSphere Sensor Events and Location Awareness Services for WebSphere Sensor Events” on page 22. If you would like to install Location Awareness Services for WebSphere Sensor Events on top of an existing WebSphere Sensor Events installation, refer to “Installing Location Awareness Services for WebSphere Sensor Events” on page 32.
11. Click **Next** to install the required Bundle Repository Server.

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

12. On the Specify Target Computers panel for your database server, specify the target computer for DB2 or your existing Oracle database and click **Next**.
 - For a local server installation for DB2 or an existing installation of Oracle, the default value is localhost. You can either keep this value or change it.
 - If you are installing the product and DB2 on separate servers, specify the fully qualified host name, operating system, user ID, and password of the server where DB2 should be installed.

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

Remember: You must install the required middleware on the remote server before installing Bundle Repository Server.



- Optionally, use the **Test connections** button to test access to the remote target computer. Firewalls can have an adverse effect on the installation even though the connection test result is successful.
15. Enter your database configuration information.
- If you already have a database server installed, enter the correct user ID and password for that database server. If you are installing DB2, enter a user ID and password to be created.

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

- If you are using Oracle, enter your correct JDBC JAR path.
- If you would like the installation program to run database scripts to create tables and populate data on the database you have provided, check **Create and populate 6.2 tables** and click **Next**. This option is especially useful for remote databases, reinstallation on the same server, and clustered environments.
- If you have already created your database manually with the scripts provided, select **Do not change the database**. The database creation is required for the successful installation of WebSphere Sensor Events.

Restriction: If you install DB2 remotely on a Windows operating system, be sure that your WebSphere Sensor Events server and the remote server have the same drive letter for the DB2 installation. For

example, if you want to use drive F on your remote server for the DB2 installation, then your WebSphere Sensor Events server should also have a drive F.

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

Important:

- If you have an existing version of WebSphere Application Server that is 6.1.0.0 or later (but not the required version 6.1.0.23), and you want the installer to update your WebSphere Application Server version, then you must have WebSphere Application Server stopped before deploying the WebSphere Sensor Events installation.
 - WebSphere Application Server security is not enabled by the installer. You must set up and configure security separately.
 - If you are going to use any WebSphere Sensor Events APIs or the Print, Verify, and Ship application, make sure that the profile you choose to use has the **HTTP transport port** set to 9080.
 - If you do not plan to install WebSphere Application Server and the WebSphere Application Server profile path on the default drive (such as the C drive on Windows operating systems), you can change the installation directory on the **Installation** tab and the profile path on the **Advanced** tab. Make sure your WebSphere Application Server profile path reflects the correct drive location for your installation.
18. Enter your IBM HTTP Server configuration information and click **Next**.
 19. Enter the installation directory for the WebSphere Application Server Web server plug-ins.

The default value in this panel creates a new **Plugins** directory in the WebSphere directory. If you choose to use an existing directory for your plug-ins, make sure that the existing directory does not already contain any files. If it does, then the installation could fail.
 20. Enter the configuration information for WebSphere Business Events.
 21. Enter the installation directory for WebSphere Sensor Events.



Reminder: If you changed the default installation path for WebSphere Application Server, make sure that you modify the installation path for WebSphere Sensor Events to match the WebSphere Application Server path.

22. Enter the configuration information for Bundle Repository Server.
23. On the Summary Panel, confirm your choices. The summary provides a list of tasks that you selected and an estimated time for their completion.
 - To start all installation and configuration tasks, click **Deploy all**.
 - If you only want to start a specific task, click **Deploy task**, but make sure that the tasks you choose are in the correct sequence on the panel. For

example, you cannot deploy WebSphere Sensor Events before deploying DB2 if you do not already have a database installed.

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

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



	C:\Program Files\SolutionFiles\logs
	opt/SolutionFiles/logs

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

Results

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

- WebSphere Sensor Events in this default location:

	C:\Program Files\IBM\RFID
	/opt/IBM/RFID

- WebSphere Application Server
- WebSphere MQ
- IBM HTTP Server
- WebSphere Business Events
- DB2 Workgroup Server Edition (if you selected to install it)
- a Bundle Repository Server (installed either locally or remotely)

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

What to do next

Complete the “Post-installation steps.”



Post-installation steps Before you begin

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

1. Make sure that the `cache.refresh.interval` property for the System Agent has been met before trying to access the WebSphere Sensor Events server.

Note: This property is configurable for time delays at startup and after updates. The default value is 60 seconds. Be aware of this delay because if an application tries to query the agent property information within that first minute, it cannot be successfully retrieved.



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

	<code>C:\Program Files\IBM\WebSphere\AppServer</code>
	<code>/opt/IBM/WebSphere/AppServer</code>

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

3. Make sure that the correct file paths are specified for the edge alerts and heartbeat log files in the SystemAgent.
See Log file locations and settings for the default installation locations of the edge alerts and heartbeat log files.
4. Make sure that the delete filter for Data Capture and Delivery is set correctly in the SystemAgent. See Setting the delete filter for Data Capture and Delivery.

5. Make sure that the DC Queue Manager is running.

-  Open the WebSphere MQ explorer and look for `IBM.DC.QM` in the Queue Managers folder. If there is a green arrow next to the queue manager, then it is running.
-  Run the command `dspmqr` in `/opt/mqm/bin`. This command tells you the current status of a queue manager.

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

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:

- `AMITJ2EE`
- `IBM_WSE_ALE_Application`
- `IBM_WSE_Admin_Console`
- `IBM_WSE_Bundles_Management`

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

- `IBM_WSE_Container_Tracking`
- `IBM_WSE_Diagnostics`
- `IBM_WSE_DockDoor_Receiving`
- `IBM_WSE_EPCIS_Connector`
- `IBM_WSE_Engine`

- IBM_WSE_Event_Monitor
 - IBM_WSE_Gateway
 - IBM_WSE_PVS_Console
 - IBM_WSE_RUC
 - IBM_WSE_RUC_BackendImpl
 - IBM_WSE_Server
 - IBM_WSE_Server_BIRT
 - IBM_WSE_Track_Trace
 - wberuntimeear
7. Open the WebSphere Sensor Events Administrative Console to verify that it is accessible.
 8. Check for errors in the WebSphere Application Server and WebSphere Sensor Events log files. Refer to Log file locations and settings for information about where to find the log files.
 9. Open the config.ini file in the *IBM_RFID_HOME*\dts\configuration directory and update the server IP address, port number, bundle list file, and Data Capture and Delivery controller, as necessary.

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

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

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

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

com.ibm.rfid.edge.config.url=http://IP_address:port_number/ibmrfidadmin/premises.s1?action=getconfig&edge=E2&version=6.1


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

Note: This step and the next one help you associate WebSphere Sensor Events to a local Data Capture and Delivery device that you can use to verify your installation. In a production environment you should use remote Data Capture and Delivery controllers. See “Installing a remote Data Capture and Delivery controller” on page 61 for details on how to install them.

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

The default is the localhost address, 127.0.0.1.

PREFIX http://IP_address/bundles/

11. If Data Transformation service is started as a service, stop it and complete the following steps as they apply to your topology and desired configuration.
 - a. Stop the Data Transformation service.
 -  **Windows** For Windows operating systems, stop the service by going to **Start → Control Panel → Administrative tools → Services**. Select **IBM WebSphere Sensor Events DT Service** and click **Stop**.

- **Linux** For Linux operating systems, run the `ibm_dts_service stop` command in the `IBM_RFID_HOME/dts` directory.
- b. Modify the startup sequence for WebSphere Application Server, IBM HTTP Server, WebSphere MQ, and Data Transformation service.

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

- 1) Run this command.

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

```
sc config IBMWebSphereSensorEventsDTService depend=
"MQSeriesServices/IBMHTTPServer6.1/IBMwas61Service - PremisesNode"
```

- 2) Go to **Start → Control Panel → Administrative tools → Services**.
- 3) Select **IBM WebSphere Sensor Events DT Service**, right-click and select **Properties → Dependencies**.

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

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

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

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

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

12. Restart the Data Transformation service manually.

- **Windows** For Windows operating systems, run the `dts.bat` file in the `IBM_RFID_HOME/dts` directory.
- **Linux** For Linux, run the `dts.sh` file in the `IBM_RFID_HOME/dts` directory.

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

13. Check the log files for any failures in loading the bundles.
14. Tune your database to improve performance.
15. If you are using the Print, Verify, and Ship example usage scenario, edit the contents of the `pvsapp.properties` file to point to the correct directory and host name for your IBM HTTP Server. Specifically, modify the following properties: `premises.hostname`, `report.location.csv`, and `report.location.csv.url`. The `pvsapp.properties` file is located in the

```
\installedApps\profile_cell_name\IBM_WSE_PVSConsole.ear\  
ibmrfd_premises_pvsapp.war\config\ directory.
```

16. If you are using the Print, Verify, and Ship example usage scenario, enable ALE.
 - a. Open the WebSphere Application Server administrative console.
 - b. Navigate to **Resources** → **JMS** → **Activation specifications** → **ALEWrapperAS**.
 - c. Change the text in the **Message selector** field to `ibmse='RfidInventory/TagReport'` OR `ibmse='RfidInventory/TagAggregationReport'` OR `ibmse LIKE '%/report/TagReport'` OR `ibmse LIKE '%/report/TagAggregationReport'`.
17. If you are planning to use the Container Tracking use case, modify the message selector.
 - a. Open the WebSphere Application Server administrative console.
 - b. Navigate to **Resources** → **JMS** → **Activation specifications** → **IBMCTTagReadAS**.
 - c. Change the text in the **Message selector** field to `ibmse='RfidInventory/TagReport'` OR `ibmse='RfidInventory/TagAggregationReport'` OR `ibmse LIKE '%/report/TagReport'` OR `ibmse LIKE '%/report/TagAggregationReport'`.
18. Restart WebSphere Application Server.
19. Verify the WebSphere Sensor Events installation. Choose **R2** as your simulated test reader.
20. If you plan to use WebSphere Business Events and you changed the default installation location for WebSphere Business Events, or you changed the default installation location for WebSphere Application Server, then you must set the following environment variables before running the WebSphere Business Events cmdline connector (cmdline script) or starting the WebSphere Business Events connectors (connectors script):
 - **WBE_HOME** - set this to the installation directory.
For example, for Windows operating systems:
`set WBE_HOME=C:\Program Files\IBM\WBE62`
For Linux operating systems:
`export WBE_HOME=/opt/IBM/WBE62`
 - **WBE_WAS_HOME** - set this to the WebSphere Application Server Network Deployment installation location. This is only needed if the default WebSphere Application Server installation location was not used.See the WebSphere Business Events Information Center for more information.

What to do next

Check the WebSphere Sensor Events Support site for any product-related fixes.

If you need to uninstall the WebSphere Sensor Events software, refer to “Uninstalling WebSphere Sensor Events” on page 78.

Installing WebSphere Sensor Events and Location Awareness Services for WebSphere Sensor Events

Follow the steps in this topic to install WebSphere Sensor Events, IBM Location Awareness Services for WebSphere Sensor Events, and their prerequisite middleware.

Before you begin

Stop all WebSphere Application Server profiles before you run the installer.

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

Important installation tips:

- When specifying installation paths, make sure the directories contains only US English ASCII characters. Also enter only US English ASCII characters in directory paths in properties files.
 - Enter a password that meets the password rules of the target machine. A password that is not valid will cause installation to fail.
1. Check your hardware and operating system and make sure that they meet the necessary requirements.
 2. Make sure that you have completed all the prerequisite steps necessary for your environment. If you would like to modify the path used by the deployment wizard, follow the steps in “Changing the deployment wizard path” on page 11 before launching the installation program.
 3. If you would like to use an existing DB2 database, make sure that database was created with the option to **Enable database for XML (Code set will be set to UTF-8)**. If your DB2 database was not created with that option, you will need to delete and recreate that database if you want to use it.
The installer will create three databases for you, but you have the option to install databases manually as well.
 4. If you are running Terminal Server and Terminal Server Licensing, run the change user /install Windows command before starting the installation program.

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

5. Run the installation program located in the root directory of the first WebSphere Sensor Events disk for Windows.

Location Awareness Services for WebSphere Sensor Events is only supported on Windows.

WindowsSetup.exe

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

You can also run the installation program in silent mode. Refer to “Installing silently” on page 43 for further instructions.

6. Select the radio button beside the **I accept both the IBM and the non-IBM terms** statement if you agree to the license agreement and click **Next** to continue.
7. When the Welcome panel appears you can either:
 - Click **Next** to continue installing the product.
 - Or, if you would like to change the default path used for the deployment package, follow the instructions in “Changing the deployment package path” on page 10 before continuing with the next steps.
8. On the Select Tasks panel, click **Next** to install the product and to choose the database type.
9. Choose to use DB2 as either your local or remote database. If you do not have DB2 installed on your server, then the installer will install it for you if you want it installed locally. If you already have DB2 installed on your local server, then the installer will recognize that it is already there and check to make sure it meets the requirements.
10. Choose to install WebSphere Sensor Events and IBM Location Awareness Services for WebSphere Sensor Events and click **Next**. If you would like to install only WebSphere Sensor Events, refer to “Installing WebSphere Sensor Events” on page 14. If you would like to install Location Awareness Services for WebSphere Sensor Events on top of an existing WebSphere Sensor Events installation, refer to “Installing Location Awareness Services for WebSphere Sensor Events” on page 32.
11. Click **Next** to install the required Bundle Repository Server.

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

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

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

Remember: You must install the required middleware on the remote server before installing Bundle Repository Server.

- Optionally, use the **Test connections** button to test access to the remote target computer. Firewalls can have an adverse effect on the installation even though the connection test result is successful.
15. Enter your database configuration information.
- If you already have a database server installed, enter the correct user ID and password for that database server. If you are installing DB2, enter a user ID and password to be created.

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

- If you would like the installation program to run database scripts to create tables and populate data on the database you have provided, check **Create and populate 6.2 tables** and click **Next**. This option is especially useful for remote databases, reinstallation on the same server, and clustered environments.
- If you have already created your database manually with the scripts provided, select **Do not change the database**. The database creation is required for the successful installation of WebSphere Sensor Events.

Restriction: If you install DB2 remotely on a Windows operating system, be sure that your WebSphere Sensor Events server and the remote server have the same drive letter for the DB2 installation. For example, if you want to use drive F on your remote server for the DB2 installation, then your WebSphere Sensor Events server should also have a drive F.

16. Enter the installation directory for WebSphere MQ or accept the default installation directory and click **Next**.
17. Enter your WebSphere Application Server configuration information and click **Next**.

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

Important:

- WebSphere Application Server security is not enabled by the installer. You must set up and configure security separately.
 - If you are going to use any WebSphere Sensor Events APIs or the Print, Verify, and Ship application, make sure that the profile you choose to use has the **HTTP transport port** set to 9080.
18. Enter your IBM HTTP Server configuration information and click **Next**.
 19. Enter the installation directory for the WebSphere Application Server Web server plug-ins.
The default value in this panel creates a new Plugins directory in the WebSphere directory. If you choose to use an existing directory for your plug-ins, make sure that the existing directory does not already contain any files. If it does, then the installation could fail.
 20. Enter the required information for DB2 Workgroup Server Edition Client.
 21. Enter the configuration information for WebSphere Business Events.
 22. Enter the installation directory for WebSphere Sensor Events.
 23. Enter the configuration information for Location Awareness Services for WebSphere Sensor Events.

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

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

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

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

C:\Program Files\SolutionFiles\logs

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

Results

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

- WebSphere Sensor Events in this default location:
C:\Program Files\IBM\RFID
- IBM Location Awareness Services for WebSphere Sensor Events in this default location:
C:\LAS
- WebSphere Application Server
- WebSphere MQ
- IBM HTTP Server
- WebSphere Business Events
- DB2 Workgroup Server Edition (if you selected to install it)
- a Bundle Repository Server (installed either locally or remotely)

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

What to do next

Complete the “Post-installation steps.”

Post-installation steps Before you begin

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

1. Make sure that the cache.refresh.interval property for the System Agent has been met before trying to access the WebSphere Sensor Events server.

Note: This property is configurable for time delays at startup and after updates. The default value is 60 seconds. Be aware of this delay because if an application tries to query the agent property information within that first minute, it cannot be successfully retrieved.

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

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

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

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

4. Make sure that the delete filter for Data Capture and Delivery is set correctly in the SystemAgent. See Setting the delete filter for Data Capture and Delivery.
5. Make sure that the DC Queue Manager is running.
 - a. Open the WebSphere MQ explorer.
 - b. Look for IBM.DC.QM in the Queue Managers folder. If there is a green arrow next to the queue manager, then it is running.

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

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:

- AMITJ2EE
- AtlasAlertHandlerEJB
- AtlasEmailSampleServiceEAR
- AtlasEventSubscriberEAR
- AtlasImportEAR
- AtlasReportingServletEAR
- AMITJ2EE
- IBM_WSE_ALE_Application
- IBM_WSE_Admin_Console
- IBM_WSE_Bundles_Management

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

- IBM_WSE_Container_Tracking
- IBM_WSE_Diagnostics
- IBM_WSE_DockDoor_Receiving
- IBM_WSE_EPCIS_Connector
- IBM_WSE_Engine
- IBM_WSE_Event_Monitor
- IBM_WSE_Gateway
- IBM_WSE_PVS_Console
- IBM_WSE_RUC
- IBM_WSE_RUC_BackendImpl
- IBM_WSE_Server
- IBM_WSE_Server_BIRT
- IBM_WSE_Track_Trace
- wberuntimeear

7. Open the WebSphere Sensor Events Administrative Console to verify that it is accessible.
8. Check for errors in the WebSphere Application Server and WebSphere Sensor Events log files. Refer to Log file locations and settings for information about where to find the log files.

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

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

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

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

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

```
com.ibm.rfid.edge.config.url=http://IP_address:port_number/ibmrfidadmin/premises.s1?action=getconfig&edge=E2&version=6.1
```

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

Note: This step and the next one help you associate WebSphere Sensor Events to a local Data Capture and Delivery device that you can use to verify your installation. In a production environment you should use remote Data Capture and Delivery controllers. See “Installing a remote Data Capture and Delivery controller” on page 61 for details on how to install them.

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

The default is the localhost address, 127.0.0.1.

PREFIX http://IP_address/bundles/

11. If Data Transformation service is started as a service, stop it and complete the following steps as they apply to your topology and desired configuration.
 - a. Stop the Data Transformation service by going to **Start → Control Panel → Administrative tools → Services**.
 - b. Select **IBM WebSphere Sensor Events DT Service** and click **Stop**.
 - c. Modify the startup sequence for WebSphere Application Server, IBM HTTP Server, WebSphere MQ, and Data Transformation service.

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

- 1) Run this command.

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

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

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

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

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

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

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

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

13. Check the log files for any failures in loading the bundles.
14. Tune your database to improve performance.
15. If you are using the Print, Verify, and Ship example usage scenario, edit the contents of the `pvsapp.properties` file to point to the correct directory and host name for your IBM HTTP Server. Specifically, modify the following properties: `premises.hostname`, `report.location.csv`, and `report.location.csv.url`. The `pvsapp.properties` file is located in the `\installedApps\profile_cell_name\IBM_WSE_PVSConsole.ear\ibmrfd_premises_pvsapp.war\config\` directory.
16. If you are using the Print, Verify, and Ship example usage scenario, enable ALE.
 - a. Open the WebSphere Application Server administrative console.
 - b. Navigate to **Resources** → **JMS** → **Activation specifications** → **ALEWrapperAS**.
 - c. Change the text in the **Message selector** field to `ibmse='RfidInventory/TagReport'` OR `ibmse='RfidInventory/TagAggregationReport'` OR `ibmse LIKE '%/report/TagReport'` OR `ibmse LIKE '%/report/TagAggregationReport'`.
17. If you are planning to use the Container Tracking use case, modify the message selector.
 - a. Open the WebSphere Application Server administrative console.
 - b. Navigate to **Resources** → **JMS** → **Activation specifications** → **IBMCTTagReadAS**.
 - c. Change the text in the **Message selector** field to `ibmse='RfidInventory/TagReport'` OR `ibmse='RfidInventory/TagAggregationReport'` OR `ibmse LIKE '%/report/TagReport'` OR `ibmse LIKE '%/report/TagAggregationReport'`.
18. Restart WebSphere Application Server.
19. Verify the WebSphere Sensor Events installation. Choose **R2** as your simulated test reader.
20. If you plan to use WebSphere Business Events and you changed the default installation location for WebSphere Business Events, or you changed the default installation location for WebSphere Application Server, then you must set the following environment variables before running the WebSphere Business Events cmdline connector (`cmdline script`) or starting the WebSphere Business Events connectors (`connectors script`):

- WBE_HOME - set this to the installation directory.
For example, for Windows operating systems:
set WBE_HOME=C:\Program Files\IBM\WBE62
For Linux operating systems:
export WBE_HOME=/opt/IBM/WBE62
- WBE_WAS_HOME - set this to the WebSphere Application Server Network Deployment installation location. This is only needed if the default WebSphere Application Server installation location was not used.

See the WebSphere Business Events Information Center for more information.

21. Enable security for WebSphere Application Server.
22. Synchronize the DB2 server time and WebSphere Application Server time prior to running your configuration because location events use the DB2 server time for event creation, but Common Event Infrastructure (CEI) events use the WebSphere Application Server time for event creation.
23. Configure and verify the Location Awareness Services for WebSphere Sensor Events installation.
24. For reporting, the browser runs only on the server with WebSphere Application Server by default. To modify the target URL for the reports, follow these steps.

Note: Before running the commands, substitute the following symbolic parameters with your specific environment values.

- %1 is WAS_HOME, such as C:\Progra~1\IBM\WebSphere\AppServer

Tip: DOS short names are required for directories containing blanks.

- %2 is name of the profile, such as AppSrv01
- %3 is name of the server, such as server1

- a. Stop WebSphere Application Server.
- b. Uninstall the portlet with the following command:

```
%1\profiles\%2\bin\wsadmin -conntype NONE
-c "$AdminApp update isclite modulefile {-operation
delete -contenturi AtlasPortletsAdministrationReports.war -server
%3}"
```

If you receive an error at this point, call IBM Support to help resolve the issue.

- c. If no error occurs, save the changes using the following command:

```
%1\profiles\%2\bin\wsadmin -conntype
NONE -c "$AdminConfig save"
```

If you receive an error at this point, call IBM Support to help resolve the issue.

- d. If no error occurs, delete the WAS_HOME\systemApps\AtlasPortletsAdministrationReports.war directory.
- e. Go to the directory where you have copied the installed driver and make a backup copy of the \WP\portlets\AtlasPortletsAdministrationReports.war file.
- f. Open the original file with a compressed file utility and edit the WEB-INF\ibm-portal-topology.xml file for the URL value. Search for the <url-link> element and change the value to match your server's host name. Specify a host name instead of using an IP address. For example: http://myHost:9080/AtlasReportingServlet/AtlasReportsServlet?cmd=init
- g. Save the changes and close the WAR file.

- h. Recheck the WAR file to make sure the changes were saved.
- i. Copy the changed WAR file to the *WAS_HOME\systemApps* directory.
- j. Install the portlet using the following command:

```
%1\profiles\%2\bin\wsadmin -conntype NONE
-c "$AdminApp update isclite modulefile {-operation
add -contents %1\systemApps\isclite.ear\AtlasPortletsAdministrationReports.war
-contenturi
AtlasPortletsAdministrationReports.war -contextroot /AtlasPortletsAdministrationReports
-MapWebModToVH {{.* .* admin_host}} -server %3 -custom paavalidation=true}"
```

If you receive an error at this point, call IBM Support to help resolve the issue.

- k. If no error occurs, save the changes using the following command:

```
%1\profiles\%2\bin\wsadmin -conntype
NONE -c "$AdminConfig save"
```

If you receive an error at this point, call IBM Support to help resolve the issue.

- l. Start WebSphere Application Server.

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

What to do next

Check the WebSphere Sensor Events Support site for any product-related fixes.

If you need to uninstall the WebSphere Sensor Events and Location Awareness Services for WebSphere Sensor Events software, refer to “Uninstalling WebSphere Sensor Events” on page 78.

Installing Location Awareness Services for WebSphere Sensor Events

Follow the steps in this topic to install IBM Location Awareness Services for WebSphere Sensor Events on an existing installation of WebSphere Sensor Events.

Before you begin

Stop all WebSphere Application Server profiles before you run the installer.

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

Important installation tips:

- When specifying installation paths, make sure the directories contains only US English ASCII characters. Also enter only US English ASCII characters in directory paths in properties files.
- Enter a password that meets the password rules of the target machine. A password that is not valid will cause installation to fail.

1. Check your hardware and operating system and make sure that they meet the necessary requirements.
2. Make sure that you have completed all the prerequisite steps necessary for your environment. If you would like to modify the path used by the deployment wizard, follow the steps in “Changing the deployment wizard path” on page 11 before launching the installation program.
3. If you are running Terminal Server and Terminal Server Licensing, run the change user /install Windows command before starting the installation program.

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

4. Run the installation program located in the root directory of the first WebSphere Sensor Events disk for Windows.

Location Awareness Services for WebSphere Sensor Events is only supported on Windows.

WindowsSetup.exe

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

You can also run the installation program in silent mode. Refer to “Installing silently” on page 43 for further instructions.

5. Select the radio button beside the **I accept both the IBM and the non-IBM terms** statement if you agree to the license agreement and click **Next** to continue.
6. When the Welcome panel appears you can either:
 - Click **Next** to continue installing the product.
 - Or, if you would like to change the default path used for the deployment package, follow the instructions in “Changing the deployment package path” on page 10 before continuing with the next steps.
7. On the Select Tasks panel, click **Next** to install the product and to choose the database type.
8. Choose to use DB2 as either your local or remote database. If you do not have DB2 installed on your server, then the installer will install it for you if you want it installed locally. If you already have DB2 installed on your local server, then the installer will recognize that it is already there and check to make sure it meets the requirements.
9. Choose to install IBM Location Awareness Services for WebSphere Sensor Events and click **Next**. If you would like to install only WebSphere Sensor Events, refer to “Installing WebSphere Sensor Events” on page 14. If you would like to install both WebSphere Sensor Events and Location Awareness Services for WebSphere Sensor Events, refer to “Installing WebSphere Sensor Events and Location Awareness Services for WebSphere Sensor Events” on page 22.

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

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

11. On the Specify Target Computers panel for your database server, specify the target computer for DB2 database and click **Next**.
 - For a local server installation for DB2, the default value is localhost. You can either keep this value or change it.
 - If you are installing the product and DB2 on separate servers, specify the fully qualified host name, operating system, user ID, and password of the server where DB2 should be installed.
 - Optionally, use the **Test connections** button to test access to the remote target computer. Firewalls can have an adverse effect on the installation even though the connection test result is successful.
12. On the Specify Target Computers panel for WebSphere Sensor Events including Location Awareness Services for WebSphere Sensor Events, specify the target computer and click **Next**.
 - For a local server installation, the default value is localhost. You can either keep this value or change it.
 - If you are installing WebSphere Sensor Events including Location Awareness Services for WebSphere Sensor Events and their required middleware on a remote server, specify the fully qualified host name, operating system, user ID, and password of the server where it should be installed.
 - Optionally, use the **Test connections** button to test access to the remote target computer. Firewalls can have an adverse effect on the installation even though the connection test result is successful.
13. Enter your database configuration information.
 - If you already have a database server installed, enter the correct user ID and password for that database server. If you are installing DB2, enter a user ID and password to be created.

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

- If you would like the installation program to run database scripts to create tables and populate data on the database you have provided, check **Create and populate 6.2 tables** and click **Next**. This option is especially useful for remote databases, reinstallation on the same server, and clustered environments.
- If you have already created your database manually with the scripts provided, select **Do not change the database**. The database creation is required for the successful installation of WebSphere Sensor Events.

Restriction: If you install DB2 remotely on a Windows operating system, be sure that your WebSphere Sensor Events server and the remote server have the same drive letter for the DB2 installation. For

example, if you want to use drive F on your remote server for the DB2 installation, then your WebSphere Sensor Events server should also have a drive F.

14. Enter the installation directory for WebSphere MQ or accept the default installation directory and click **Next**.
15. Enter your WebSphere Application Server configuration information and click **Next**.

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

Important:

- WebSphere Application Server security is not enabled by the installer. You must set up and configure security separately.
 - If you are going to use any WebSphere Sensor Events APIs or the Print, Verify, and Ship application, make sure that the profile you choose to use has the **HTTP transport port** set to 9080.
16. Enter your IBM HTTP Server configuration information and click **Next**.
 17. Enter the installation directory for the WebSphere Application Server Web server plug-ins.

The default value in this panel creates a new **Plugins** directory in the WebSphere directory. If you choose to use an existing directory for your plug-ins, make sure that the existing directory does not already contain any files. If it does, then the installation could fail.
 18. Enter the required information for DB2 Workgroup Server Edition Client.
 19. Enter the configuration information for WebSphere Business Events.
 20. Enter the installation directory for WebSphere Sensor Events.

Reminder: If you changed the default installation path for WebSphere Application Server, make sure that you modify the installation path for WebSphere Sensor Events to match the WebSphere Application Server path.

21. Enter the configuration information for Location Awareness Services for WebSphere Sensor Events.

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

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

Click **Back** to make any changes. After you start the deployment, you have the option to click **Stop Deployment** if you need to stop the installation

before it is finished. Once all deployment tasks are complete, the Deployment Status screen indicates if the deployment was successful.

23. Insert the Location Awareness Services for WebSphere Sensor Events CD when prompted.
24. When the installation is complete, check the log files for any errors. From the Deployment wizard, you can view detailed messages or the master log. Click **Master log** and select **Save as...** to save the log file. The logs can be found in `deployment_wizard_installation_dir/logs`, where *deployment_wizard_installation_dir* is the installation location of the Deployment wizard.
`C:\Program Files\SolutionFiles\logs`
25. Click the X at the top, right-hand side of the panel to exit the wizard. The wizard displays some messages:
 - A prompt for whether you want to save changes. If you plan to run the wizard again, click **Yes**. Otherwise, click **No**.
 - A prompt for whether you wish to exit. Click **Yes** to exit the wizard.

Results

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

`C:\LAS`

What to do next

Complete the “Post-installation steps.”

Post-installation steps Before you begin

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

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

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

- AMITJ2EE
- AtlasAlertHandlerEJB
- AtlasEMailSampleServiceEAR
- AtlasEventSubscriberEAR
- AtlasImportEAR
- AtlasReportingServletEAR
- AMITJ2EE
- IBM_WSE_ALE_Application
- IBM_WSE_Admin_Console
- IBM_WSE_Bundles_Management

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

- IBM_WSE_Container_Tracking
 - IBM_WSE_Diagnostics
 - IBM_WSE_DockDoor_Receiving
 - IBM_WSE_EPCIS_Connector
 - IBM_WSE_Engine
 - IBM_WSE_Event_Monitor
 - IBM_WSE_Gateway
 - IBM_WSE_PVS_Console
 - IBM_WSE_RUC
 - IBM_WSE_RUC_BackendImpl
 - IBM_WSE_Server
 - IBM_WSE_Server_BIRT
 - IBM_WSE_Track_Trace
 - wberuntimeear
2. Enable security for WebSphere Application Server.
 3. Synchronize the DB2 server time and WebSphere Application Server time prior to running your configuration because location events use the DB2 server time for event creation, but Common Event Infrastructure (CEI) events use the WebSphere Application Server time for event creation.
 4. Configure and verify the Location Awareness Services for WebSphere Sensor Events installation.
 5. For reporting, the browser runs only on the server with WebSphere Application Server by default. To modify the target URL for the reports, follow these steps.

Note: Before running the commands, substitute the following symbolic parameters with your specific environment values.

- %1 is *WAS_HOME*, such as C:\Progra~1\IBM\WebSphere\AppServer

Tip: DOS short names are required for directories containing blanks.

- %2 is name of the profile, such as AppSrv01
- %3 is name of the server, such as server1

- a. Stop WebSphere Application Server.
- b. Uninstall the portlet with the following command:

```
%1\profiles\%2\bin\wsadmin -conntype NONE
-c "$AdminApp update isclite modulefile {-operation
delete -contenturi AtlasPortletsAdministrationReports.war -server
%3}"
```

If you receive an error at this point, call IBM Support to help resolve the issue.

- c. If no error occurs, save the changes using the following command:

```
%1\profiles\%2\bin\wsadmin -conntype
NONE -c "$AdminConfig save"
```

If you receive an error at this point, call IBM Support to help resolve the issue.

- d. If no error occurs, delete the *WAS_HOME\systemApps\AtlasPortletsAdministrationReports.war* directory.
- e. Go to the directory where you have copied the installed driver and make a backup copy of the *\WP\portlets\AtlasPortletsAdministrationReports.war* file.

- f. Open the original file with a compressed file utility and edit the WEB-INF\ibm-portal-topology.xml file for the URL value. Search for the <url-link> element and change the value to match your server's host name. Specify a host name instead of using an IP address. For example:
http://myHost:9080/AtlasReportingServlet/AtlasReportsServlet?cmd=init
- g. Save the changes and close the WAR file.
- h. Recheck the WAR file to make sure the changes were saved.
- i. Copy the changed WAR file to the WAS_HOME\systemApps directory.
- j. Install the portlet using the following command:

```
%1\profiles\%2\bin\wsadmin -conntype NONE
-c "$AdminApp update isclite modulefile {-operation
add -contents %1\systemApps\isclite.ear\AtlasPortletsAdministrationReports.war
-contenturi
AtlasPortletsAdministrationReports.war -contextroot /AtlasPortletsAdministrationReports

-MapWebModToVH {{.* .* admin_host}} -server %3 -custom paavalidation=true)"
```

If you receive an error at this point, call IBM Support to help resolve the issue.

- k. If no error occurs, save the changes using the following command:

```
%1\profiles\%2\bin\wsadmin -conntype
NONE -c "$AdminConfig save"
```

If you receive an error at this point, call IBM Support to help resolve the issue.

- l. Start WebSphere Application Server.

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

What to do next

Check the WebSphere Sensor Events Support site for any product-related fixes.

If you need to uninstall the WebSphere Sensor Events and Location Awareness Services for WebSphere Sensor Events software, refer to “Uninstalling WebSphere Sensor Events” on page 78.



Installing a high availability system

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

About this task

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

1. Make sure that you have completed all the prerequisite steps necessary for high availability.
2. Launch the high availability post-installation script located at the root of the High Availability for IBM WebSphere Sensor Events Enterprise Edition disk.



	setupwin32.exe
	setuplinux.bin

The Welcome panel displays.

3. Click **Next**.

4. This panel shows the installation directory for the WebSphere Sensor Events high availability system.

The directory is:

	<code>IBM_RFID_HOME\HA</code>
	<code>IBM_RFID_HOME/HA</code>

Click **Next** to continue.

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

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

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

Use the **Add Member** button to add cluster members. The created member's name, node, and weight appear in the box at the bottom of the installer panel. To delete a cluster member, select the member name from the list of created members and click **Delete Member**.

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

7. Click **Next**.

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


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

	<code>IBM_RFID_HOME\HA\logs\install.log</code>
	<code>IBM_RFID_HOME/HA/logs/install.log</code>

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

9. If you see exceptions in the WebSphere Application Server SystemOut.log file on the central and node servers, follow the procedure in this technote.
10. Restart the central server and the cluster.
11. If you are using WebSphere Application Server security, enable it, and then restart the deployment manager, all node agents, and all servers.
12. Enable dynamic cache replication for all servers in the cluster.
 - a. In the WebSphere Application Server administrative console, go to **Servers** → **Application servers** → *server name* → **Container Services** → **Dynamic cache service** and check **Enable service at server startup** for each server in the cluster.
 - b. Define a new replication domain by going to **Environment** → **Replication domains** → **New**. Choose **Entire domain** when creating the new replication domain.
 - c. Navigate to **Resources** → **Cache instances** → **Object cache instances** and add the new replication to all object cache components.
 - 1) Check Enable cache replication.

- 2) Choose your cluster name for **Full group replication domain**.
 - 3) Choose **Push only** for **Replication type**.
 - 4) Set **Push frequency** to 1 seconds.
13. Configure the Data Capture and Delivery controllers for high availability.
- a. Make sure you are using Java 1.4.2 on your Data Capture and Delivery controllers.
 - b. Set the appropriate MQ user name for your operating system in the controller's Equinox script.

 **Windows** -Duser.name=MUSR_MQADMIN

 **Linux** -Duser.name=mqm

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

For example:  **Windows**

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

 **Linux**

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

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

```
com.ibm.rfid.bundle.list.url=http://IP_address:port_number/bundleadmin/GetBundle?name=http://IBM_HTTP_Server_IP_address/bundles/bundlelists/dc_core4dts.txt
com.ibm.rfid.edge.config.url=http://IP_address:port_number/bmrfdadmin/premises.s1?action=getconfig&edge=E4&version=6.1
```

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

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

14. Check to see if Data Transformation is running (started as a service) on your central server, and if so, stop it.
15. Start the Equinox runtime on the Data Capture and Delivery controllers.
16. Start the bundle loader on the Data Capture and Delivery controllers.
 - a. Find the ID of the bundle loader bundle by running the OSGi ss command.
 - b. Start the bundle loader bundle by entering start *bundle_ID* at the OSGi prompt.
17. Test the clustered configuration using the Simulated Reader in the WebSphere Sensor Events Administrative Console. Choose **R4** as your simulated test reader.

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

What to do next

If you need to create additional cluster members, follow the steps in "Installing additional cluster members" on page 43.

Manually configuring the clustered system for multiple messaging engines

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

WebSphere Sensor Events SIBus configuration overview

There are two SIBuses created with the WebSphere Sensor Events installation, AMIT and ibmsensorevent.

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

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

Adding multiple messaging engines:

About this task

These steps are specifically for the ibmsensorevent SIBus. You will also need to perform these steps for the AMIT SIBus.

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

In the next three steps, you repeat the actions in this step to define additional match criteria for the policy.

7. Click **New** and define an additional match criteria for the policy.
 - a. For **Name**, enter `WSAF_SIB_BUS`.

- b. For **Value**, enter `ibmsensorevent`.
 - c. Click **OK**.
8. Click **New** and define an additional match criteria for the policy.
 - a. For **Name**, enter `WSAF_SIB_MESSAGING_ENGINE`.
 - b. For **Value**, enter `PremisesCluster.000-ibmsensorevent`.
 - c. Click **OK**.
9. Click **New** and define an additional match criteria for the policy.
 - a. For **Name**, enter `IBM_hc`.
 - b. For **Value**, enter `PremisesCluster`.
 - c. Click **OK**.
10. Navigate back to the **SIBusClusterME001Policy** and click **Preferred servers** under **Additional Properties**.
11. Select the server name of a cluster member from the **Core group servers** and click **Add>>**.
12. Click **OK**.
13. Repeat steps 4 on page 41 through 12 to create new policies and assign each to a cluster member. Every cluster member except the central server needs a policy.
14. Create messaging engines for each cluster member.

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

 - a. Navigate to **Service integration** → **Buses** → **ibmsensorevent** → **Bus members** → **PremisesCluster**.
 - b. Click **Add messaging engine** and select **File store**.

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

 - c. Click **Next**.
 - d. For **Log directory path**, enter `${LOG_ROOT}/sibus-se`.
 - e. For **Permanent store directory path**, enter `${LOG_ROOT}/sibus-se`.
 - f. Click **Next**.
 - g. Click **Finish**.
15. Synchronize all cluster members and server configurations by navigating to **System administrator** → **Nodes** and clicking **Full Resynchronize**.
16. Restart the `PremisesCluster` cluster and the central server.
 - a. Navigate to **Server** → **Clusters**.
 - b. Select **PremisesCluster** and click **Stop**.
 - c. Once it all cluster members are stopped, click **Start**.
 - d. Navigate to **Server** → **Application servers**.
 - e. Select the central server (such as `PremisesNode`, `server1`).
 - f. Click **Stop**.
 - g. Once the central server has stopped, click **Start**.
17. Repeat all of the previous steps for the AMIT SIBus. To do this, replace every instance of "ibmsensorevent" with "AMIT" in the instructions, specifically in the console paths, SIBus name, and messaging engine names.

Installing additional cluster members

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

Before you begin

Before adding a new node, make sure to complete the prerequisite steps for the new node. Refer to steps 3 on page 8 and 4 on page 8 in “Prerequisite steps for a high availability system” on page 7.

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

Installing silently

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

About this task

Note: Silent uninstallation is not supported.

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

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

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

Windows

There are three sample response files for Windows operating systems:

- PremisesSolutionForWindowsDB2_LAS_Task.xml for WebSphere Sensor Events and IBM Location Awareness Services for WebSphere Sensor Events using DB2
- PremisesSolutionForWindowsDB2_Task.xml for WebSphere Sensor Events only using DB2
- PremisesSolutionForWindowsOracle_Task.xml for WebSphere Sensor Events only using Oracle

Linux

There are two sample response file for Linux operating systems:

- PremisesSolutionForLinuxDB2_Task.xml for WebSphere Sensor Events only using DB2
 - PremisesSolutionForLinuxOracle_Task.xml for WebSphere Sensor Events only using Oracle
2. Accept the WebSphere Sensor Events license.
 - a. Open the IRU_install.iss file located in the tasks directory of the WebSphere Sensor Events CD appropriate for your operating system.
 - b. Replace -G licenseAccepted=false with -G licenseAccepted=true.
 3. Open and update the sample response file.
 - a. Specify the target computer for the deployment tasks.
 - Search for the <targetHostname> tag and specify the target computer name within that element for each deployment task.
 - If the target computer is not localhost, search for and uncomment the <credentialsSat> element. Then, update this line with the target computer's host name, user ID, and password.

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

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

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

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

Windows C:\Program Files\SolutionFiles\logs
Linux \opt\SolutionFiles\logs

5. Launch the installer in silent mode.

Windows For Windows operating systems:

- a. Open a command line prompt.
- b. Change directory to the location of the tasks directory.
- c. Run this command.

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

Linux For Linux operating systems:

- a. Open a shell window.
- b. Change directory to the location of the tasks directory.
- c. Run this command.

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

Note: In this example, the variable, *silent_response_filename*, means the name of the sample response file. Do not include the path of the file if using these commands. If you are using a customized task file that is not in the tasks directory, then use the absolute path to the file when running the command.

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

Windows C:\Program Files\SolutionFiles\logs
Linux \opt\SolutionFiles\logs

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

Installing using Tivoli Provisioning Manager for Software

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

Before you begin

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

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

1. Check your hardware and operating system and make sure that they meet the necessary requirements.
 2. Install Tivoli Provisioning Manager for Software using the instructions in the Tivoli Provisioning Manager for Software documentation.
 3. Discover your endpoints (one for each WebSphere Sensor Events server) for Tivoli Provisioning Manager for Software.
 4. Install the common agent on each endpoint server. If you are installing DB2, make sure to set the common agent as LOCAL_SYSTEM on the client server.
 5. Set up Tivoli Provisioning Manager for Software to install the prerequisite software for WebSphere Sensor Events.
 - a. Copy the contents of the TPM directory from the second disk for WebSphere Sensor Events for Windows operating systems to the Tivoli Provisioning Manager for Software server's C: drive.
 - b. Copy the WASEC61 directory from the second WebSphere Sensor Events disk to C:\IBM\SIF\isp\windows\cdimages\WASEC61.
 - c. Extract *disk_root\bin\com\ibm\jsdt\webserver\tree\ihswin.xx.jar* from the first WebSphere Sensor Events disk to C:\IBM\SIF\isp\windows\cdimages\WASND61.
 - d. Extract *disk_root\bin\com\ibm\jsdt\webserver\tree\waswin.xx.jar* from the first WebSphere Sensor Events disk to C:\IBM\SIF\isp\windows\cdimages\WASND61.
 - e. Extract *disk_root\bin\com\ibm\jsdt\webserver\tree\db2win.xx.jar* from the first WebSphere Sensor Events disk to C:\IBM\SIF\isp\windows\cdimages\DB2WSE95.
- Note:** If you are installing DB2, the provided response file uses the DB2 user name, db2admin, and the password, Passw8rd. The response file is located at *disk_root\TPM\IBM\SIF\isp\windows\bin\DB2WSE95FP3A\SifInstall_DB2WSE95.rsp*
- f. Extract *disk_root\bin\com\ibm\jsdt\webserver\tree\mqwin.xx.jar* from the first WebSphere Sensor Events disk to C:\IBM\SIF\isp\windows\cdimages\MQ6.
 - g. Extract *disk_root\bin\com\ibm\jsdt\webserver\tree\mq6rp2fp5win.xx.jar* from the first WebSphere Sensor Events disk to C:\IBM\SIF\isp\windows\cdimages\MQ602FP5.

6. Open the software packages in the Software Package Editor. You can launch Software Package Editor through Java Web Start or in an Eclipse environment.
7. Create the software package block by selecting **File → Save → Save to repository** and choosing **LocalFileRepository**.

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

Table 2. Data packages for Windows

Package name	Package description
Base61WinD	This package contains the directory structure and utilities that must be installed before the following packages.
Mq6WinD	Contains the installable image of WebSphere MQ 6.0
Mq602Fp5WinD	Contains WebSphere MQ 6.0.2 Fix Pack 5, which brings the product level to 6.0.2.5
Db2Wse95WinD	Contains the installable image of DB2 Workgroup Server Edition 9.5 Fix Pack 3a
WasNd61WinD	Contains the installable image of WebSphere Application Server 6.1.0.23 (includes IBM HTTP Server 6.1 and the Web Services plug-in for 6.1)
WasEc61WinD	Contains the installable image of WebSphere Application Server 6.1 Edge Components

Table 3. Installation packages for Windows

Package name	Package description
Mq6WinI	Installs WebSphere MQ 6.0
Mq602Fp5WinI	Installs WebSphere MQ 6.0.2 Fix Pack 5, which brings the product level to 6.0.2.5
Db2Wse95WinI	Installs DB2 Workgroup Server Edition 9.5 Fix Pack 3a
WasNd61WinI	Installs WebSphere Application Server 6.1.0.23 (includes IBM HTTP Server 6.1 and the Web Services plug-in for 6.1)
WasEc61WinI	Installs WebSphere Application Server 6.1 Edge Components

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

For example, if you want to install DB2 Workgroup Server Edition 9.5 Fix Pack 3a remotely, distribute and install the packages in the following sequence.

- a. Base61WinD
- b. Db2Wse95WinD
- c. Db2Wse95WinI

To install WebSphere MQ 6.0.2.5 remotely, distribute and install the packages in the following sequence.

- a. Base61WinD

- b. Mq6WinD
- c. Mq602Fp5WinD
- d. Mq6WinI
- e. Mq602Fp5WinI

To install WebSphere Application Server 6.1.0.23, IBM HTTP Server 6.1, and the Web Services plug-in for 6.1 remotely, distribute and install the packages in the following sequence:

- a. Base61WinD
 - b. WasNd61WinD
 - c. WasNd61WinI
9. If you would like to change your DB2 password from the defaults used in the DB2 installation, follow these steps:
 - a. Navigate to **Start → Administrative Tools → Computer Management → Local Users and Groups → Users** on your Windows server.
 - b. Right-click **db2admin** and choose **Set Password**.
 10. Follow the steps provided in “Installing WebSphere Sensor Events” on page 14.

What to do next

If you need to uninstall the WebSphere Sensor Events software, refer to “Uninstalling WebSphere Sensor Events” on page 78.

Installing the Sensor Data Services for WebSphere Remote Server

Follow the steps in this topic to install Sensor Data Services for WebSphere Remote Server or Sensor Data Services for WebSphere Central Site.



About this task

The Sensor Data Services for WebSphere Remote Server installs WebSphere Sensor Events on top of an existing WebSphere Remote Server 6.2 or 6.2.1 installation.

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

1. Check your hardware and operating system and make sure that they meet the necessary requirements.
2. Make sure that you have completed all the prerequisite steps necessary for your environment and that you have already have an existing installation of WebSphere Remote Server.
3. Install the prerequisite software fix packs and feature packs for WebSphere MQ, DB2 Workgroup Server Edition, and WebSphere Application Server.
 - WebSphere MQ 6.0.2.5 - available for download at: <http://www.ibm.com/support/docview.wss?rs=171&uid=swg27007069>
 - DB2 Workgroup Server Edition 9.5 Fix Pack 3a- available for download at: <http://www.ibm.com/support/docview.wss?rs=71&uid=swg21287889>
 - WebSphere Application Server 6.1.0.23 - available for download at: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27007951>
 - WebSphere Application Server 6.1 Feature Pack for Web Services - available for download at: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27008534>

4. Verify that you have properly installed WebSphere Application Server before installing the Sensor Data Services for WebSphere Remote Server.
5. Install WebSphere Business Events 6.2 and the required fix pack.
The WebSphere Business Events 6.2 Fix Pack 1 is available for download at:
http://www.ibm.com/support/docview.wss?rs=3458&context=SSTNLG&context=SSQR57&dc=D600&uid=swg21381218&loc=en_US&cs=UTF-8&lang=en
6. Create the database.
7. Run the installation program located in the root directory of the Sensor Data Services for WebSphere Remote Server CD appropriate for your operating system.

	setupwin32.exe
	setupLinux.bin

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

8. Choose the language for your installation.
9. In the installation wizard Welcome panel, click **Next** to continue.
10. Click the radio button beside the **I accept both the IBM and the non-IBM terms** statement if you agree to the license agreement and click **Next** to continue. After you accept the licensing terms, the installation wizard checks for the product prerequisites.
11. Select the installation directory for WebSphere Sensor Events.
12. The installation wizard prompts you to select either a **Typical** or **Custom** installation.

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

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

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

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

13. Choose a database type, either DB2 or Oracle, and click **Next**.
14. 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**.
15. 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 Sensor Events APIs or the Print, Verify, and Ship application, set the **HTTP transport port** to 9080 when you create the profile.

16. 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 Sensor Events installation.
 - If you do not have WebSphere Application Server security enabled, then you may proceed without filling in an administrator ID and password.
17. Enter your Web server information or accept the defaults provided and click **Next**.

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

18. Browse to your WebSphere MQ installation directory and click **Next**.
19. If you did not choose to install the Bundle Repository Server with WebSphere Sensor Events, a panel prompts you to enter your Bundle Repository Server information.
20. Browse to the location of the IBM Tivoli License Compliance Manager inventory file. The file is in the TIVREADY path at the root of the product disk.
21. A summary panel displays your installation selections. Click **Install** to continue the installation process.
22. 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	<code>IBM_RFID_HOME\logs\install.log</code>
 Linux	<code>IBM_RFID_HOME/logs/install.log</code>

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

Results

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

- WebSphere Sensor Events in this default location:

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

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

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

Post-installation steps



Before you begin

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



1. Make sure that the `cache.refresh.interval` property for the System Agent has been met before trying to access the WebSphere Sensor Events server.

Note: This property is configurable for time delays at startup and after updates. The default value is 60 seconds. Be aware of this delay because if an application tries to query the agent property information within that first minute, it cannot be successfully retrieved.

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

	C:\Program Files\IBM\WebSphere\AppServer
	/opt/IBM/WebSphere/AppServer

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

3. Make sure that the correct file paths are specified for the edge alerts and heartbeat log files in the SystemAgent.
See Log file locations and settings for the default installation locations of the edge alerts and heartbeat log files.
4. Make sure that the delete filter for Data Capture and Delivery is set correctly in the SystemAgent. See Setting the delete filter for Data Capture and Delivery.
5. Make sure that the DC Queue Manager is running.
 -  Open the WebSphere MQ explorer and look for IBM.DC.QM in the Queue Managers folder. If there is a green arrow next to the queue manager, then it is running.
 -  Run the command `dspmqr` in `/opt/mqm/bin`. This command tells you the current status of a queue manager.

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

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:

- AMITJ2EE
- IBM_WSE_ALE_Application
- IBM_WSE_Admin_Console
- IBM_WSE_Bundles_Management

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

- IBM_WSE_Container_Tracking

- IBM_WSE_Diagnostics
 - IBM_WSE_DockDoor_Receiving
 - IBM_WSE_EPCIS_Connector
 - IBM_WSE_Engine
 - IBM_WSE_Event_Monitor
 - IBM_WSE_Gateway
 - IBM_WSE_PVS_Console
 - IBM_WSE_RUC
 - IBM_WSE_RUC_BackendImpl
 - IBM_WSE_Server
 - IBM_WSE_Server_BIRT
 - IBM_WSE_Track_Trace
 - wberuntimeear
7. Open the WebSphere Sensor Events Administrative Console to verify that it is accessible.
 8. Check for errors in the WebSphere Application Server and WebSphere Sensor Events log files. Refer to Log file locations and settings for information about where to find the log files.
 9. Open the config.ini file in the *IBM_RFID_HOME\dts\configuration* directory and update the server IP address, port number, bundle list file, and Data Capture and Delivery controller, as necessary.

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

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

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

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

com.ibm.rfid.edge.config.url=http://IP_address:port_number/ibmrfidadmin/premises.s1?action=getconfig&edge=E2&version=6.1

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

Note: This step and the next one help you associate WebSphere Sensor Events to a local Data Capture and Delivery device that you can use to verify your installation. In a production environment you should use remote Data Capture and Delivery controllers. See “Installing a remote Data Capture and Delivery controller” on page 61 for details on how to install them.

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

The default is the localhost address, 127.0.0.1.

PREFIX http://IP_address/bundles/

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

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

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

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

- 1) Run this command.

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

```
sc config IBMWebSphereSensorEventsDTService depend=
"MQSeriesServices/IBMHTTPServer6.1/IBMwas61Service - PremisesNode"
```

- 2) Go to **Start → Control Panel → Administrative tools → Services**.
- 3) Select **IBM WebSphere Sensor Events DT Service**, right-click and select **Properties → Dependencies**.

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

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

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

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

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

12. Restart the Data Transformation service manually.

- **Windows** For Windows operating systems, run the `dts.bat` file in the `IBM_RFID_HOME/dts` directory.
- **Linux** For Linux, run the `dts.sh` file in the `IBM_RFID_HOME/dts` directory.

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

13. Check the log files for any failures in loading the bundles.
14. Tune your database to improve performance.

15. If you are using the Print, Verify, and Ship example usage scenario, edit the contents of the pvsapp.properties file to point to the correct directory and host name for your IBM HTTP Server. Specifically, modify the following properties: premises.hostname, report.location.csv, and report.location.csv.url. The pvsapp.properties file is located in the \installedApps\profile_cell_name\IBM_WSE_PVSConsole.ear\ibmrfd_premises_pvsapp.war\config\ directory.
16. If you are using the Print, Verify, and Ship example usage scenario, enable ALE.
 - a. Open the WebSphere Application Server administrative console.
 - b. Navigate to **Resources** → **JMS** → **Activation specifications** → **ALEWrapperAS**.
 - c. Change the text in the **Message selector** field to ibmse='RfidInventory/TagReport' OR ibmse='RfidInventory/TagAggregationReport' OR ibmse LIKE '%/report/TagReport' OR ibmse LIKE '%/report/TagAggregationReport'.
17. If you are planning to use the Container Tracking use case, modify the message selector.
 - a. Open the WebSphere Application Server administrative console.
 - b. Navigate to **Resources** → **JMS** → **Activation specifications** → **IBMCTTagReadAS**.
 - c. Change the text in the **Message selector** field to ibmse='RfidInventory/TagReport' OR ibmse='RfidInventory/TagAggregationReport' OR ibmse LIKE '%/report/TagReport' OR ibmse LIKE '%/report/TagAggregationReport'.
18. Restart WebSphere Application Server.
19. Verify the WebSphere Sensor Events installation. Choose **R2** as your simulated test reader.
20. If you plan to use WebSphere Business Events and you changed the default installation location for WebSphere Business Events, or you changed the default installation location for WebSphere Application Server, then you must set the following environment variables before running the WebSphere Business Events cmdln connector (cmdln script) or starting the WebSphere Business Events connectors (connectors script):
 - WBE_HOME - set this to the installation directory.
For example, for Windows operating systems:
set WBE_HOME=C:\Program Files\IBM\WBE62
For Linux operating systems:
export WBE_HOME=/opt/IBM/WBE62
 - WBE_WAS_HOME - set this to the WebSphere Application Server Network Deployment installation location. This is only needed if the default WebSphere Application Server installation location was not used.

See the WebSphere Business Events Information Center for more information.

What to do next

Check the WebSphere Sensor Events Support site for any product-related fixes.

If you need to uninstall the WebSphere Sensor Events software, refer to “Uninstalling WebSphere Sensor Events” on page 78.

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 Sensor Events 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 Sensor Events. Instructions for downloading the Tivoli License Compliance Manager are documented in the Tivoli License Compliance Manager information center.

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

`IBM_RFID_HOME\TIVREADY`

Installing the toolkits

Use the topics below to install the toolkits shipped with WebSphere Sensor Events.

Installing WebSphere Sensor Events Toolkit

Use these steps to install the WebSphere Sensor Events Toolkit.

Installing the toolkit on Rational Application Developer for WebSphere Software 7.5.1

1. Check your hardware and operating system and make sure that they meet the necessary requirements.
2. Install this WebSphere Application Server fix to the WebSphere Application Server 6.1 runtime that is installed in Rational Application Developer for WebSphere Software at C:\Program Files\IBM\SDF\runtimes\base_v61:
<http://www.ibm.com/support/docview.wss?uid=swg24023075>
3. Start Rational Application Developer for WebSphere Software using a new workspace directory.
4. From the menu select **Help** → **Software Updates**.
5. Select the **Available Software** tab.
6. Click **Add site ...** and select the directory containing the toolkit update site.
7. Expand the new local site to find **IBM WebSphere Sensor Events Toolkit**.
8. Select the toolkit.
9. Click **Install ...** and select the feature.
10. Click **Next**.
11. Accept the license agreement and click **Next**.
12. In the Installation window, click **Finish** to install the plug-in into the default location.

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

13. When the installation completes, click **Yes** when prompted to restart the workbench.
14. Download and install the WebSphere Sensor Events Toolkit help plug-in. You can find the downloadable help plug-in on the Library page:
<http://www.ibm.com/software/integration/sensor-events/library/>
15. If you see any errors after installation, refer to the troubleshooting tips in the WebSphere Sensor Events Toolkit help.

Installing the toolkit on Rational Application Developer for WebSphere Software 7.5.3

1. Check your hardware and operating system and make sure that they meet the necessary requirements.
2. Install this WebSphere Application Server fix to the WebSphere Application Server 6.1 runtime that is installed in Rational Application Developer for WebSphere Software at C:\Program Files\IBM\SDF\runtimes\base_v61:
<http://www.ibm.com/support/docview.wss?uid=swg24023075>
3. On the WebSphere Sensor Events Toolkit disk, find the
\\ibmrfd_toolkit_update_site\plugins\
com.ibm.rfid.premises.toolkit.plugin_6.2.0.200906051229.jar file.
4. Within that JAR file, find and extract the rfid_premises_toolkit.zip file to the root of the C directory.
5. Start Rational Application Developer for WebSphere Software using a new workspace directory.
6. Select **File** → **Import** → **Other** → **Project Interchange** and import all projects from the C:\rfid_premises_toolkit.zip file.
7. Accept the license agreement and click **Next**.
8. In the Installation window, click **Finish** to install the plug-in into the default location.

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

9. When the installation completes, click **Yes** when prompted to restart the workbench.
10. Download and install the WebSphere Sensor Events Toolkit help plug-in. You can find the downloadable help plug-in on the Library page:
<http://www.ibm.com/software/integration/sensor-events/library/>
11. If you see any errors after installation, refer to the troubleshooting tips in the WebSphere Sensor Events Toolkit help.

What to do next

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

If you need to uninstall the WebSphere Sensor Events Toolkit software, refer to “Uninstalling the WebSphere Sensor Events Toolkit” on page 80.

Installing IBM Data Capture and Delivery Toolkit for WebSphere Sensor Events

Use these steps to install the IBM Data Capture and Delivery Toolkit for WebSphere Sensor Events.

1. Check your hardware and operating system and make sure that they meet the necessary requirements. Also make sure that an Internet connection is available.
2. Start Eclipse.
3. From the menu select **Help** → **Software Updates**.
4. Select the **Available Software** tab.
5. Click **Add site**
6. Click **Local** and navigate to your local directory containing the toolkit update site for IBM Data Capture and Delivery Toolkit for WebSphere Sensor Events. Then click **OK**. The update site is located on the CD containing the toolkits in the update directory.
7. Click **OK**.
8. Expand the new local site and check the category for **IBM Data Capture and Delivery**. Leave **Uncategorized** unchecked.
9. Click **Install**
10. Click **Next**.
11. Accept the license agreement and click **Finish**.
12. Click **Yes** when prompted to restart the Eclipse SDK.
13. When Eclipse has restarted, you can import the sample agents and launch configurations for IBM Data Capture and Delivery Toolkit for WebSphere Sensor Events by selecting **File** → **New** → **Project** → **IBM WebSphere Sensor Events Toolkits** → **Data Capture and Delivery Toolkit** and click **Next**.
14. Select **Data Capture**.
15. Click **Finish** to install the toolkit project in the current workspace.

What to do next

If you need to uninstall the IBM Data Capture and Delivery Toolkit for WebSphere Sensor Events software, refer to “Uninstalling the IBM Data Capture and Delivery Toolkit for WebSphere Sensor Events” on page 80.

Configuring the IBM Data Capture and Delivery Toolkit for WebSphere Sensor Events

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

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

The following launch configurations are included in the toolkit:

DataCapture-FullSim

Launches both the Simulated Reader and the simulated WebSphere Sensor

Events on one machine. This configuration launches the I/O Simulator, the Sensor Events Simulator, and the Sensor Events Simulator Status Window interfaces.

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

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

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

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

DataCapture-RdrSim

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

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

DataCapture-LLRP

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

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

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

DataCapture-SensorEventsSim

Launches a simulated WebSphere Sensor Events. The Sensor Events Simulator interface and Sensor Events Simulator Status Window interface are also launched.

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

Launching the Simulated Reader and simulated WebSphere Sensor Events on the local system

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

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

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

This section describes how to configure the Simulated Reader and I/O Simulator interface when you are connecting it to a WebSphere Sensor Events (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:

```
sensor_events_ip_address put_sensor_events_hostname_here
```

For `sensor_events_ip_address`, enter the WebSphere Sensor Events IP address. All instances of `"put_sensor_events_hostname_here"` in the configuration file will be replaced with this IP address.

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

```
<property key="matrix.properties" value="file:BDDR.properties"/>
<!--<property key="matrix.properties"
value="http://put_sensor_events_hostname_here/bundles/BDDR.properties"/>-->
```
 - b. Copy `com.ibm.rfid.resource.toolkit/Matrices/BDDR.properties` from the workspace to the root runtime directory. By default the root runtime directory is the Eclipse installation root, which is the directory location for the `eclipse.exe` file.
3. From within Eclipse, click **Run** → **Open Run Dialog...**
4. Browse to and select **DataCapture-RdrSim**. It is located under **OSGi Framework**.
5. Click **Run**.

What to do next

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

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

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

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

Launching the LLRP Reader while connecting to a remote WebSphere Sensor Events or Sensor Events Simulator

This section describes how to configure the LLRP Reader when you are connecting it to a WebSphere Sensor Events (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:

```
sensor_events_ip_address put_sensor_events_hostname_here
```

For *sensor_events_ip_address*, enter the WebSphere Sensor Events IP address. All instances of "put_sensor_events_hostname_here" in the configuration file will be replaced with this IP address.

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

```
<property key="matrix.properties" value="file:BDDR.properties"/>
<!--property key="matrix.properties"
value="http://put_sensor_events_hostname_here/bundles/BDDR.properties"/>-->
```
 - b. Copy `com.ibm.rfid.resource.toolkit/Matrices/BDDR.properties` from the workspace to the root runtime directory. By default the root runtime directory is the Eclipse installation root, which is the directory location for the `eclipse.exe` file.
3. From within Eclipse, click **Run** → **Open Run Dialog...**
4. Browse to and select **DataCapture-LLRP**. It is located under **OSGi Framework**.
5. Click **Run**.

What to do next

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

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

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

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

Launching the Sensor Events Simulator

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

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

Adding additional XML configuration files to the Sensor Events Simulator

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

1. Copy the new configuration file to the Configurations directory within the `com.ibm.rfid.resource.toolkit` project. For example, `com.ibm.rfid.resource.toolkit/Configurations/edge-samsys.xml`.

2. Add a new, unique property to the `com.ibm.rfid.premises.simulator.servlet.properties` file within the `com.ibm.rfid.premises.simulator.servlet.bundle` package of the `com.ibm.rfid.premises.simulator.servlet` project, which maps the new configuration file to a Data Capture and Delivery controller ID. For example, `E2=edge-samsys.xml`.
3. Restart the Sensor Events Simulator.

Verifying the installation

This topic provides instructions for how to verify that WebSphere Sensor Events was installed successfully.

About this task

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

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

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

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


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


1. Complete the “Post-installation steps” on page 18.
2. Restart WebSphere Application Server.
3. Open the WebSphere Sensor Events Administrative Console. The Welcome page displays.
4. Select **Simulated Reader** from the left navigation pane.
5. On the Simulated Reader console page, select a reader from the menu.


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

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

The following icons represent the status of the reader:

-  - The reader is off, but available.

-  - The reader status is unavailable.

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

You should see tag information appear in the output box.

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

Installing a remote Data Capture and Delivery controller

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

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

Installing the bundle loader and a bundle list

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

The bundle list file format

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

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

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

This is an example of the file format:

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

The bundle list location

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

- At startup it checks for the Configuration Admin (ConfigAdmin) service, which is an OSGi Managed Service. If the ConfigAdmin service is available and the bundle loader receives a configuration object it will look for the URL there.

- If either the ConfigAdmin is not available or the configuration object is empty, the bundle loader looks for a system property which is either set in the config.ini file or through a Java command line argument.
- If the bundle loader cannot find the list in the system property, then it looks at a default location in the file system for the ibm-rfid-bundle-list.txt bundle list.

After successfully receiving the bundle list, the bundle loader runs the commands in the list to install the bundles. This process is stored in the ConfigAdmin object as a result property (for example, value="working"). After this task is completed, the bundle loader saves the final result (as a success or a failure) in the result property. Then, when the bundle loader is restarted or when the configuration changes, the bundle loader looks in the result value to determine if it should download additional bundles.

Installing the bundle loader and bundle list

About this task

Use these steps to install the bundle loader and a bundle list. For reference, see the tools/remotedC.zip sample packaged with the IBM Data Capture and Delivery Toolkit for WebSphere Sensor Events.

Note: The sample config.ini uses 127.0.0.1 for the IP address of the WebSphere Sensor Events. Change the value to the actual IP address if using the sample config.ini for a remote Data Capture and Delivery install.

1. Install Equinox on the server that will run the bundle loader.
Equinox is packaged in the equinox folder of the IBM Data Capture and Delivery Toolkit for WebSphere Sensor Events disk.

Note: Other OSGi implementations are also supported, but this document only covers the Equinox implementation.

2. Create a configuration directory in the eclipse path in Equinox. For example, C:\equinox\eclipse\configuration.
3. Create a config.ini file in the configuration directory and add these lines to it:

```
com.ibm.rfid.bundle.list.url=http://IP_address:port_number/bundleadmin/GetBundle?name=http://IBM_HTTP_Server_name/bundles/bundlelists/dc_core.txt
com.ibm.rfid.edge.config.url=http://IP_address:port_number/ibmrfdadmin/premises.s1?action=getconfig&edge=E3&version=6.1
```

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

The second line of code configures Data Capture and Delivery to use the E3 controller, which is shipped as a sample remote controller with WebSphere Sensor Events. The E3 controller loads the Simulated Reader to help verify your configuration before testing with a real reader.

4. Start the Equinox runtime.

Note:

- Be sure the Data Transformation service is running on the server (dts.bat).
- In the case of Data Transformation, the bundle loader bundle is loaded, but not started. It must be started manually.
- The bundle lists are slightly different for Data Transformation (for example, dc_core.txt and dc_core4dts.txt). Be sure that you reference the correct bundle list version based on whether you are loading the list into a remote Data Capture and Delivery controller

(dc_core.txt, dc_rdrsim.txt) or into Data Transformation (dc_core4dts.txt, dc_rdrsim4dts.txt).

5. Start the bundle loader.
 - a. Find the ID of the bundle loader bundle by running the OSGi ss command.
 - b. Start the bundle loader bundle by entering start *bundle_ID* at the OSGi prompt.

Once the core Data Capture and Delivery bundles are loaded, Data Capture and Delivery pulls its configuration from WebSphere Sensor Events (using the com.ibm.rfid.edge.config.url= property). If this configuration includes an update to the bundle list URL, then the bundle loader attempts to load that additional list of bundles.

This is one method of installing multiple bundle lists into a Data Capture and Delivery controller. Data Transformation is set up with E2 to run the reader simulator. The Data Transformation config.ini file points to dc_core4dts.txt file to load the core bundles, and the Data Capture and Delivery configuration then points to the dc_rdrsim4dts.txt file to then load the reader simulator. For additional methods for installing bundle lists, refer to “Installing additional bundle lists.”

6. Test the configuration using the Simulated Reader in the WebSphere Sensor Events Administrative Console. Choose **R3** as your simulated test reader.
7. Create a new remote Data Capture and Delivery controller based on the E3 sample and use it with your real reader.

Installing additional bundle lists

Once the bundle loader is running, you can use it to load additional bundles. There are several methods you can use to load the bundles.

One way to load additional bundles is to add an additional bundle list in the config.ini file of Equinox, and then restart Equinox. The configuration file contains a comma-separated list of bundle lists. When the bundle loader is restarted, it reads the updated configuration and loads the bundles in the new bundle list specified in the config.ini file.

To do this in a production system with a remote Data Capture and Delivery controller, use the WebSphere Sensor Events Administrative Console to update the com.ibm.rfid.bundle.list.url property in the bundle loader agent. Then navigate to **Controllers** in the left navigation pane of the console and click the controller you are using. Click the **Reload Configuration** button to reload your controller’s configuration. This triggers the Data Capture and Delivery controller to reload its configuration, including the new bundle list URL, which causes the Bundle Loader to download the new bundle list.

To install additional bundle lists within the IBM Data Capture and Delivery Toolkit for WebSphere Sensor Events, modify the edge XML used to configure the Data Capture and Delivery bundles by adding a block to the XML that configures the bundle loader. Then you can force a reload of the edge configuration (possibly by restarting the edge configuration bundle) so that the bundle loader picks up the new configuration. The following is an example of the XML used to modify the bundle loader URL property:

```
<configuration pid="com.ibm.rfid.bundle.loader">
  <properties>
    <property key="bundleListURL" value="file:///bundlelist2.txt"/>
    <property key="clearCache" value="false"/>
  </properties>
</configuration>
```

For more information on configuring Data Capture and Delivery, see *Managing your configuration*.

Using wildcards with the bundle loader

If the bundle loader uses the Bundle Repository Server on WebSphere Sensor Events to read the bundle list, then you can use a form of wildcarding for the bundle names in the bundle list.

By default, wildcarding is turned off, so the bundle names in the bundle list must be an exact match to the bundles you want to load. To turn on wildcarding, follow these steps:

1. Set the `com.ibm.rfid.bundle.server.fullname` property in the `bundleserver.properties` file to `true`.
The `bundleserver.properties` file is located in the `IBM_RFID_HOME/dms/properties` directory.
2. Restart WebSphere Application Server, if it has already been started, in order for the change to take effect.

If wildcarding is turned on, then the Bundle Repository Server matches the name of each bundle in the bundle list to the bundles in its bundles directory. If it finds an exact match, then it uses the bundle that matches. If there is no match, then the Bundle Repository Server places a wildcard character on the end of the bundle name and returns the first bundle in alphabetic order that matches that pattern.

Defining the network topology

After the required software is installed on WebSphere Sensor Events, the next step in installing your solution is to define the RFID network topology.

Before you begin

Before beginning this process, ensure that you:

- Obtain the IP addresses and port numbers of the tag readers and tag printers in the network.
- Obtain the MAC addresses of the Data Capture and Delivery controllers in the network.

About this task

The RFID network topology contains important information about the devices in your network. This information is stored in a configuration database on WebSphere Sensor Events. The Data Capture and Delivery controller retrieves the configuration and uses it to set all of the bundle parameters including the Controller Manager and Digital I/O Manager. The following information is stored in the network topology:

- Agents and configuration properties
- Device IDs and configuration information for devices, such as tag readers and tag printers
- Location IDs for each store location, including dock door IDs
- Data Capture and Delivery controller IDs and configuration information

Use the WebSphere Sensor Events Administrative Console to create and edit the topology definition.

1. Open the WebSphere Sensor Events Administrative Console.. The Welcome page displays.
2. Create or download agents and configure their properties.
3. Define each device in the network.
4. Define location information (stores and dock doors) in this network.
5. Enter the Data Capture and Delivery controller IDs for the Data Capture and Delivery devices in the network.

Results

The network topology is created.

Installing the WebSphere Application Server log file adapters

Follow the instructions below to install the WebSphere Application Server log file adapters on WebSphere Sensor Events using the Tivoli Enterprise Console.

About this task

The WebSphere Application Server log file adapters enable you to view exceptions that occur on WebSphere Sensor Events from the Tivoli Enterprise Console. You must first load the adapters into the Tivoli Enterprise Console, and then distribute them to your WebSphere Sensor Events servers. The adapters then run as services on WebSphere Sensor Events, 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 WebSphere Sensor Events 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 Sensor Events 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 Sensor Events. After distribution, a new service should be listed in the Windows Services Manager, with an ID equal to the Identifier Name given to the ACP entry.

What to do next

Now, the log file adapter should be monitoring the log file entered into the wasjava.conf file. Exceptions logged to the WebSphere Application Server log file are changed to an instance of the Was_Java_Exception class and sent to the Tivoli Enterprise Console Event Server.

Installing the edge controller heartbeat log file adapters

Follow these instructions to install the edge controller heartbeat log file adapters on one or more WebSphere Sensor Events using the Tivoli Enterprise Console.

About this task

The edge controller heartbeat log file adapters enable you to view the status of edge controllers and tag readers from the Tivoli Enterprise Console. You must first load the adapters into the Tivoli Enterprise Console, and then distribute them to your WebSphere Sensor Events servers. The adapters then run as services on WebSphere Sensor Events, 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 WebSphere Sensor Events 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:
 - 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 Sensor Events 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 Sensor Events. After distribution, a new service should be listed in the Windows Services Manager, with an ID equal to the Identifier Name given to the ACP entry.

What to do next

At this point, the log file adapter should be monitoring the log file entered into the tecad_win.conf file. Exceptions logged to the WebSphere Application Server log file will change to an instance of the Was_Java_Exception class and be sent to the Tivoli Enterprise Console Event Server.

Configuring security for WebSphere Application Server

Use scripts provided to enable or disable security for WebSphere Application Server with WebSphere Sensor Events or IBM Location Awareness Services for WebSphere Sensor Events.

Enabling security

Scripts are provided to enable WebSphere Application Server security for WebSphere Sensor Events and for Location Awareness Services for WebSphere Sensor Events. You can also use these scripts to disable security at a later time.

The following are a few key concepts that you should understand about WebSphere Application Server security for WebSphere Sensor Events and for Location Awareness Services for WebSphere Sensor Events:

- A WebSphere Application Server administrative user has administrative access to the WebSphere Application Server administrative console. There can be more than one user who is a WebSphere Application Server administrative user. See Authorizing access to administrative roles in the WebSphere Application Server Information Center for more information.
- You must create an administrative operating system user for WebSphere Sensor Events. The WebSphere Sensor Events administrative user either has to be user name in the `ibmrfid` group. The WebSphere Sensor Events administrative user has administrative rights to the WebSphere Sensor Events Administrative Console. This user can also be a WebSphere Application Server administrative user, if you decide to set up your users and authorization in that way.
- Location Awareness Services for WebSphere Sensor Events needs a WebSphere Application Server administrative user when you enable security, but this user does not have to be the same WebSphere Application Server administrative user that WebSphere Sensor Events uses.
- “Enabling security for WebSphere Sensor Events”
- “Enabling security for Location Awareness Services for WebSphere Sensor Events” on page 69

Enabling security for WebSphere Sensor Events Before you begin

The `ws_security` script enables WebSphere Application Server security. Before running the `ws_security` script, ensure the following:

- A local user exists
- Or a local user group exists and has users in it

You will set a local user as the WebSphere Application Server administrative user so that after WebSphere Application Server security is enabled, you can sign on to the WebSphere Application Server administrative console as an administrator. If you want your WebSphere Application Server administrative user to have administrator access to the WebSphere Sensor Events Administrative Console as well, then that user must be in the `ibmrfid` group.

1. Navigate to the security directory:

```
Windows IBM_RFID_HOME\premises\install\security\
Linux IBM_RFID_HOME/premises/install/security/
```

2. Run the following command:

```
ws_security enable userid password
```

- `userid` = Local OS user ID

This is the user ID of the WebSphere Application Server administrator. This user must belong to the group called `ibmrfid` if you want the user to have administrative access to the WebSphere Sensor Events Administrative Console. The WebSphere Application Server administrator ID cannot be the same as the name of your server because the repository sometimes returns

server-specific information when querying a user of the same name. For more information, refer to the Local operating system settings topic in the WebSphere Application Server Information Center.

If you have installed Location Awareness Services for WebSphere Sensor Events, a WebSphere Application Server administrative user ID also has to be set in `atlas.config.bat` file under WASADMIN.

- `password` = Local OS password.

This is the password of the WebSphere Application Server administrator.

If you have installed Location Awareness Services for WebSphere Sensor Events, a WebSphere Application Server administrative password also has to be set in `atlas.config.bat` file under WASPSWD.

3. Restart WebSphere Application Server.

Enabling security for Location Awareness Services for WebSphere Sensor Events

Complete the following steps to configure security for WebSphere Application Server when you have Location Awareness Services for WebSphere Sensor Events installed. Enabling security in WebSphere Application Server provides security for the Spatial Management Client and portlets.

About this task

Note: You should not perform the steps if Location Awareness Services for WebSphere Sensor Events is not installed.

1. If you have not already done so, follow the steps to run the `ws_security` script and enable security for WebSphere Application Server.
2. Navigate to the root installation directory of Location Awareness Services for WebSphere Sensor Events (such as, `C:\LAS`).
3. Edit the `las.config.properties` file and define the values for the WebSphere Application Server administrator and the message queue user.

```
#-----  
# wasadmin      WAS admin.  
# waspswd       Password for WAS admin.  
#-----  
settings.7.name=wasadmin  
settings.7.value=newUser  
  
settings.8.name=waspswd  
settings.8.value=newUser  
  
#-----  
# meuser        Message Queue user.  
# mepswd        Password message queue user.  
#-----  
settings.9.name=meuser  
settings.9.value=newUser  
  
settings.10.name=mepswd  
settings.10.value=newUser
```

The script expects that WebSphere Application Server security is already enabled. The values for `wasadmin` and `waspswd` should reflect the WebSphere Application Server administrative user ID and password, respectively. These values can match the user ID and password that you used previously with the `ws_security` script, or they can match the ID and password for another WebSphere Application Server administrative user that you have set.

4. Open a command prompt and change to the `LAS_HOME\WAS\scripts` directory.

5. Type `ATLAS_MAIN -security enable` at the command-line prompt.
The script completes the following actions:
 - Creates the following groups on the operating system: `lassmcadministgrp`, `lasmonitorgrp`, `lasoperategrp`, `lasadministgrp`, `laslocategrp`, `lasregistrategrp`, `lasconfiguregrp`, and `lascustomizegrp`.
 - Creates the user `lasoveradmin` with password `lasoveradmin`. This superuser can run Location Awareness Services for WebSphere Sensor Events functions in the WebSphere Application Server administrative console. Use the `lasoveradmin` superuser for testing or proof-of-concept environments only. The `lasoveradmin` user should not be used in production environments.
 - Applies security settings.
6. Restart WebSphere Application Server.
7. Edit the `LAS_HOME\AtlasIntegrator\Data_Export.properties` file to specify the real host name of your server instead of `localhost`.
8. Verify that security is running by logging into the WebSphere Application Server administrative console. If security is enabled, you are prompted for your WebSphere Application Server user ID and password. A random user ID is no longer accepted.

What to do next

Follow the steps in “Configuring security for the Control Processing portlet” on page 74.

Disabling security

Use the instructions in this topic if you have enabled WebSphere Application Server security for WebSphere Sensor Events or for Location Awareness Services for WebSphere Sensor Events and would like to disable it.

Since WebSphere Sensor Events and Location Awareness Services for WebSphere Sensor Events share the same WebSphere Application Server administrative console, if you disable security for WebSphere Sensor Events, then security is also disabled for Location Awareness Services for WebSphere Sensor Events. Be sure to follow the instructions in “Disabling security for WebSphere Sensor Events and Location Awareness Services for WebSphere Sensor Events” on page 71 to properly disable security when you have both software packages installed.

- “Disabling security when only WebSphere Sensor Events is installed”
- “Disabling security for WebSphere Sensor Events and Location Awareness Services for WebSphere Sensor Events” on page 71

Disabling security when only WebSphere Sensor Events is installed

Before you begin

These instructions are for disabling WebSphere Application Server security when you have only WebSphere Sensor Events installed. If you have both WebSphere Sensor Events and Location Awareness Services for WebSphere Sensor Events installed, follow the instructions in “Disabling security for WebSphere Sensor Events and Location Awareness Services for WebSphere Sensor Events” on page 71.

1. Navigate to the security directory for WebSphere Sensor Events:

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

2. Run the following command:


```
ws_security disable userid password
```

 - *userid* = Local OS user ID. This is the user ID of the WebSphere Application Server administrator.
 - *password* = Local OS password. This is the password of the WebSphere Application Server administrator.
3. Restart WebSphere Application Server.

Disabling security for WebSphere Sensor Events and Location Awareness Services for WebSphere Sensor Events

If you have installed Location Awareness Services for WebSphere Sensor Events, complete the following steps to disable security for AtlasBus. Completing these steps ensures that you can import data into Location Awareness Services for WebSphere Sensor Events after turning off security.

1. Open the WebSphere Application Server administrative console and log in with your WebSphere Application Server administrative user ID and password.
2. Select **Security** → **Bus Security** → **AtlasBus**.
3. Under **Additional Properties** select **Security**.
4. Clear the check box beside **Enable bus security**.
5. Choose to enable all transport chains. This step enables AtlasIntegrator to connect to the AtlasBus on a non-secure port.
6. Click **OK**.
7. Save the configuration.

8. Navigate to the security directory for WebSphere Sensor Events:

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

9. Run the following command:


```
ws_security disable userid password
```

 - *userid* = Local OS user ID. This is the user ID of the WebSphere Application Server administrator.
 - *password* = Local OS password. This is the password of the WebSphere Application Server administrator.
10. Restart WebSphere Application Server.

Configuring Location Awareness Services for WebSphere Sensor Events

These topics describe how to configure IBM Location Awareness Services for WebSphere Sensor Events.

Configuring the database

Use this topic to modify the database for IBM Location Awareness Services for WebSphere Sensor Events.

Manually importing the sample data

This topic describes how to manually import the sample data if you did not choose to import it during installation.

Importing sample data for S-1 group languages:

About this task

If your language is in the S-1 group, complete the following steps to predefine sample values.

1. Change directory to the *LAS_HOME*\DB2\sampleData directory.
If your DB2 server is remote, copy the DB2 directory to the database server and complete these instructions on that server.
2. Run this command, where %DB2ADMIN% is your DB2 administrative user ID and %DB2PSWD% is the corresponding password:

```
db2cmd /c /w /i ATLASDB_SampleDataImport.bat %DB2ADMIN% %DB2PSWD%
```
3. To activate rules, change to the *LAS_HOME*\tools4rules directory and run the runCEPRulesDeploymentTool.bat file.

Importing sample data for languages not in the S-1 group:

About this task

If your language is not in the S-1 group, complete the following steps to predefine sample values.

1. Navigate to the *LAS_HOME* directory.
2. Verify that your DB2 user ID and password settings are correct in the SetUser.bat file.
3. Change directory to the *LAS_HOME*\DB2\sampleData directory.
If your DB2 server is remote, copy the *LAS_HOME* directory to the database server and complete these instructions on that server.
4. Run this command:

```
db2cmd /c /w /i ATLASDB_IMPORT_S2D.bat
```
5. To activate rules, change to the *LAS_HOME*\tools4rules directory and run the runCEPRulesDeploymentTool.bat file.

Installing the Spatial Management Client

This topic contains the steps for installing the Spatial Management Client.

Before you begin

Make sure that you installed the prerequisites for the Spatial Management Client. See “Hardware and software requirements” on page 4.

1. Make sure you installed Adobe SVG viewer on the system where you will run the user interface. You can download the Adobe SVG viewer from <http://www.adobe.com/svg/viewer/install/main.html>.
2. Make sure your browser is configured to run Active X plug-ins:
 - a. Open your browser.
 - b. Select **Tools** → **Internet Options**.
 - c. On the **Security** tab, select a zone to change security settings.
You can choose one of several zones, depending on how you access the Spatial Management Client. For example, if you access the Spatial Management Client using the host name in the URL, then you would modify the **Internet** zone settings. If you use localhost in the URL, then you would modify the **Local intranet** zone settings. If you have added the Spatial Management Client URL to the **Trusted sites**, then you would modify security settings in that zone.

Be sure to select the zone where WebSphere Application Server and IBM HTTP Server are running. Make sure that both domains match the same zone.

- d. In the zone you choose, click **Custom level**.
- e. Make sure the following settings are correct and click **OK**:
 - **ActiveX controls and plug-ins:**
 - Click **Enable** for **Automatic prompting for ActiveX controls**.
 - Click **Enable** for **Binary and script behaviors**.
 - Click **Prompt** for **Download signed ActiveX controls**.
 - Click **Disable** for **Download unsigned ActiveX controls**.
 - Click **Enable** for **Initialize and script ActiveX controls not marked as safe**.
 - Click **Enable** for **Run ActiveX controls and plug-ins**.
 - Click **Enable** for **Script ActiveX controls marked safe for scripting**.
 - **Downloads:**
 - Click **Enable** for **Automatic prompting for file downloads**.
 - Click **Enable** for **File download**.
 - Click **Enable** for **Font download**.
 - **Miscellaneous:**
 - Click **Enable** for **Access data sources across domains**.
 - Click **Enable** for **Allow META REFRESH**.
 - Click **Disable** for **Allow scripting of Internet Explorer Web browser control**.
 - Click **Disable** for **Allow script-initiated windows without size or position constraints**.
 - Click **Prompt** for **Allow Web pages to use restricted protocols for active**.
 - Click **Prompt** for **Display mixed content**.
 - Click **Disable** for **Don't prompt for client certificate selection when no certificates or only one certificate exists**.
 - Click **Enable** for **Drag and drop or copy and paste files**.
 - Click **Prompt** for **Installation of desktop items**.
 - Click **Prompt** for **Launching applications and unsafe files**.
 - Click **Prompt** for **Launching programs and files in an IFRAME**.
 - Click **Enable** for **Navigate sub-frames across different domains**.
 - Click **Enable** for **Open files based on content, not file extension**.
 - Click **Medium safety** for **Software channel permissions**.
 - Click **Enable** for **Submit nonencrypted form data**.
 - Click **Disable** for **Use Pop-up Blocker**.
 - Click **Enable** for **Userdata persistence**.
 - Click **Enable** for **Web sites in less privileged web content zone can navigate into this zone**.
 - **Scripting:**
 - Click **Enable** for **Active scripting**.
 - Click **Enable** for **Allow past operations via script**.
 - Click **Enable** for **Scripting of Java applets**.

- **User Authentication:**
 - Click **Automatic login only in Intranet zone for Logon**.
3. Open `http://host_name_or_IP_address/Tracking GUI/AtlasPrefsAdmin.html` and verify that your preferences are set correctly:
 - **Host** - Enter the IP address or fully qualified host name of your Location Awareness Services for WebSphere Sensor Events server.
 - **Port** - Enter the port number that WebSphere Application Server listens on.
 - **Poll interval:** Enter a value to indicate the rate in milliseconds that tag data is requested from the server.

Note: Changing this value does not affect the frequency at which a tracked item's position is reported to the system. It only affects the frequency with which the GUI is updated.

- **Number of clustering grid rows and columns:** Define the number of grids to use for clustering tags. If you have many tags on the screen, overlapping tags can occur. If clustering is set to a value greater than 0, overlapping tags are shown as a cluster icon. This cluster icon can be clicked to open a window showing all tags in the cluster. Ten of those tags can be individually selected.

The number of grid rows defines how large the grid will be, which is covered by a cluster. For example, a value of 20 means a grid of 20 rows and columns, where all tags in one cell are shown as part of the cluster. A value of 0 turns off clustering, meaning you cannot influence the order of tags from back to front or select individual tags.

- Click **Save Installation Changes** to save your changes to the preferences. These preference settings will apply each time the user logs in to the Spatial Management Client.

4. Open the Spatial Management Client using one of the following URLs:
 - `http://host_name_or_IP_address/Tracking GUI/AtlasAdmin.html` (administration version)
 - `http://host_name_or_IP_address/Tracking GUI/AtlasMonitor.html`

Note: The variable *host_name_or_IP_address* indicates the fully qualified host name or IP address of the machine on which IBM HTTP Server is installed, which is also the Location Awareness Services for WebSphere Sensor Events server. The default port number is 80; however, if a different port number is used, you must specify the new port number (*host_name_or_IP_address:port_number*).

For more information about the Spatial Management Client, see the topics on starting the Spatial Management Client.

5. Ensure that application `db2AssetMgmtEAR` has been installed and is started in your WebSphere Application Server.

Configuring security for the Control Processing portlet

Complete these steps to enable security for the Control Processing portlet.

Before you begin

Important: You must enable security for WebSphere Application Server before completing these steps.

About this task

Each time a new user logs into the WebSphere Application Server administrative console to use Location Awareness Services for WebSphere Sensor Events, they must perform the following step in the Control Processing portlet.

The user must be a member of the `lasoperategrp` or an equivalent group for these steps to work.

1. Navigate to **Control Processing**.
2. Click **Refresh List**.
3. Click **Edit** (the wrench icon) in the upper right corner.
4. For each entry, enter the user name and password of the current user.
5. Click **Save**.

Using the sample subscriber and notification programs

This topic describes how to use the two sample subscriber programs that are shipped with Location Awareness Services for WebSphere Sensor Events: sample mail service program and sample alert events subscriber program.

About this task

The sample subscriber and notification programs are referenced in the sample data and can be used to verify your installation. If you do not want to use them, you can deactivate them.

1. In the `http_root\htdocs\en_us\wsdl\EmailHandler.wsdl` and `http_root\htdocs\en_us\wsdl\LasCeiMessageWrapper.wsdl` files, make sure that the `host_name: portnumber` key value pair reflects the real `WC_defaulthost` port. The sample includes 9080 as the port number.

The `LasCeiMessageWrapper.wsdl` file provides a sample API to analyze the Location Awareness Services for WebSphere Sensor Events CEI events. The source code is included as a sample in the `LASCEIWrapper.jar` file. Using the Notification Channels portlet, you can define a new channel using the existing `LasCeiMessageWrapper.wsdl` file. Then, every time an event for the given filter criteria occurs, the `handleEvent` method of the `CeiMessageWrapper` class is called within the `LASCEIWrapper.jar` file.

2. In the Mail Server portlet, configure your mail server:
 - a. Open the WebSphere Application Server administrative console and click **Rules/Alerts → Mail Server**.
 - b. On the Mail Host Configuration page, click **Add**.
 - c. In **Host Address**, enter the IP address or fully qualified host name of your mail server.
 - d. In **Port**, enter the port number.
 - e. In **Default Sender**, enter your e-mail address.
 - f. In **Default Subject**, enter a default subject line to send with the notification.
 - g. Click **Save** to save your settings.
3. In the Mail Receiver portlet, specify receiver information for users who should receive notification of specific events:

Note: Times are relative to times on the database server. The machines that host the database server and WebSphere Application Server must be set to the same time zone.

- a. Open the WebSphere Application Server administrative console and click **Rules/Alerts → Mail Receiver**.
- b. Click **Add New Mail Receiver**.
- c. In **Receiver Name**, enter the name of a receiver.
- d. In **Receiver Address**, enter the e-mail address of a receiver.
- e. In **Week Days**, select the days of the week when the receiver should be notified of events.
- f. In **Start Time**, enter the time when the receiver should start receiving notification each day.
- g. In **End Time**, enter the time when the receiver should stop receiving notification each day.
- h. In **Alert Types**, select the type of alerts that the receiver should be notified about.
- i. In **Mail Host**, select the mail server to associate with the receiver.
- j. Click **Save** to save your settings.

Deactivate the sample programs

About this task

If you do not want to use the sample programs, perform the following steps:

1. In the Notification Channels portlet, remove the channels related to the programs that you want to deactivate:
 - a. Open the WebSphere Application Server administrative console and click **Rules/Alerts → Notification Channels**.
 - b. Select the check box next to the sample programs to remove and then click **Delete Selected**.
2. In the Notification Program Manager portlet, remove the entries for the programs that you want to deactivate:
 - a. Open the WebSphere Application Server administrative console and click **Rules/Alerts → Notification Programs**.
 - b. Select the check box next to the sample programs to remove and then click **Delete Selected**.

Verifying your installation

This topic explains how to verify your installation by verifying the Spatial Management Client and the subscriber programs.

Verifying the Spatial Management Client

This topic provides steps for verifying the Spatial Management Client installation.

Before you begin

Before verifying the Spatial Management Client installation, make sure you have performed the following tasks:

- Installed the Spatial Management Client and set your preferences in the Preferences Administration GUI. See step 3 on page 74 in “Installing the Spatial Management Client” on page 72.
 - Adapted the hub data to the needs of the application and pointed to the correct server IP address and event provider hubs or controllers.
1. Follow the steps in “Configuring security for the Control Processing portlet” on page 74.

2. In the Control Processing portlet, start the tag processing servlet:
 - a. Open the WebSphere Application Server administrative console and click **Control Processing**.
 - b. Select the WebSphere Application Server that is related to your installation and click **Start Selected**.
3. Start the Spatial Management Client by opening the following URL: `http://fully_qualified_host_name/Tracking GUI/AtlasMonitor.html`, where *fully_qualified_host_name* is the fully qualified host name of the system where you installed IBM HTTP Server and the Spatial Management Client.
4. Define your preferences in the Location Awareness Services for WebSphere Sensor Events Preferences Administration GUI. Start the GUI by opening the following URL: `http://fully_qualified_host_name/Tracking GUI/AtlasPrefsAdmin.html`. See Preferences Administration GUI for more information.

Note: It is only necessary to define your preferences once per installation and user.

5. Under **ZONES**, select **All** from the **Visible** drop-down menu to see all defined zones. The location entitled **Matrix** has been predefined in the database and you should see five sample zones for this location.
6. Under **ALERTS**, select **Yes** from the **Hide** drop-down menu to hide all alerts or select **No** to view all alerts.
7. Start the hub simulator:


```
location_of_hub_simulator\HubSim.bat
```

The variable *location_of_hub_simulator* indicates the directory where the hub simulator is located. It must be a subdirectory of the directory in which `atlas.config.bat` file is located. For example, `C:\LAS\HubSimulator`.
8. View the simulated resources and events.

Tip: If a tag icon is red, click the icon to see tag and alert details. Click **Acknowledge** to acknowledge the alert and the icon is no longer red. If you click the tag a second time to see details, the alert information for the tag is no longer visible.

Verifying the subscriber programs

This topic describes how to verify the subscriber programs.

Before you begin

Before verifying the subscriber programs, make sure you have performed the following tasks:

- Verified the Spatial Management Client successfully. See “Verifying the Spatial Management Client” on page 76.
- Installed the subscriber and sample notification programs and configured the mail server and receivers. See “Using the sample subscriber and notification programs” on page 75.
- When tag 00000007 enters the myAlarm zone in the Matrix area, an alarm is generated.
- Verify that an e-mail is sent to the receiver you defined.
- Verify that a line is written in the `sampleArchive.txt` and `sampleProtocol.txt` files.

Configuring InfoSphere Traceability Server

If you are using InfoSphere™ Traceability Server as your EPCIS-compliant repository, follow the steps in these topics to configure it.

Before you begin

Download the XML files you will need to complete these steps from here:
ftp://ftp.software.ibm.com/software/websphere/rfid/support/6.2/wse_62_its_config.zip

1. Copy the `EPCISDocumentMetaData.xml` file to the `INFOSPHERE_HOME/etc` path.
2. Run the `INFOSPHERE_HOME/bin/deployMetaData.sh` script.
3. Copy the `actionValues.xml` file and the `coreBusinessVocabularyDraft.xml` file to the `INFOSPHERE_HOME/bin` path.

4. Run this command:

```
import-masterdata.sh -load actionValues.xml coreBusinessVocabularyDraft.xml
```

What to do next

Follow these steps in these topics:

- Configuring WebSphere Sensor Events and InfoSphere Traceability Server to communicate on remote machines
- (Optional) Enabling the global security feature in WebSphere Application Server

Uninstalling the product

Use the following topics to uninstall the product.

Uninstalling WebSphere Sensor Events

This task describes how to uninstall WebSphere Sensor Events and its related products and components.

About this task

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



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

You need to uninstall the products in the reverse order of their installation:

1. Asset Inventory Management Services for WebSphere Sensor Events, if you chose to install this component
2. IBM Location Awareness Services for WebSphere Sensor Events, if you chose to install this component
3. WebSphere Sensor Events
4. WebSphere Business Events

5. IBM HTTP Server
6. WebSphere Application Server Network Deployment
7. WebSphere MQ
8. DB2 Workgroup Server Edition systems, if you chose to install the database

If you are uninstalling Sensor Data Services for WebSphere Remote Server, follow the steps to uninstall WebSphere Sensor Events (steps 3 through 7).

1. If you installed Location Awareness Services for WebSphere Sensor Events, remove its installation directory and the IBM HTTP Server `htdocs\en_us\Tracking GUI` directory.
2. If you installed Asset Inventory Management Services for WebSphere Sensor Events, follow the steps in Uninstalling Asset Inventory Management Services for WebSphere Sensor Events to remove it.
3. If you have WebSphere Application Server security enabled, disable it. The uninstaller cannot run properly with security enabled.
4. Ensure that WebSphere Application Server and WebSphere MQ are running, and that the Data Transformation service is not running.
5. Start the uninstallation wizard, and follow the instructions on the panels.
 -  **Windows** `IBM_RFID_HOME_uninst\uninstaller.exe`
You can also use one of the following options:
 - Navigate to **Start → All Programs → IBM WebSphere Sensor Events V6.2 → Uninstall Sensor Events**.
 - Use the **Add or Remove Programs** application on Windows by clicking **Start → Control Panel → Add or Remove Programs**.
 -  **Linux** `IBM_RFID_HOME/_uninst/uninstaller.bin`
6. A summary panel displays your uninstallation selections. Click **Uninstall** to continue the uninstallation process.
7. When the uninstallation is complete, another summary panel displays the uninstallation status. Click **Finish** to exit the uninstaller wizard.
8. Uninstall ObjectGrid for WebSphere Business Events.
9. Uninstall WebSphere Business Events.
10. Uninstall the Web server plug-ins for WebSphere Application Server.
11. Uninstall IBM HTTP Server.
12. Uninstall the Web Services Feature Pack for WebSphere Application Server.
13. Uninstall WebSphere Application Server Network Deployment.
14. Uninstall WebSphere MQ for Windows or Linux systems.
15. Uninstall the WebSphere Eclipse Platform.
16. Uninstall DB2 Workgroup Server Edition for Windows or Linux systems.



Uninstalling a high availability system

This task describes how to uninstall your high availability WebSphere Sensor Events system.

About this task

The high availability uninstaller restores your topology to a single WebSphere Sensor Events.

Note: The information in this topic only applies to the version of WebSphere Sensor Events that is available with a WebSphere Sensor Events Enterprise Edition license.

1. If you have WebSphere Application Server security enabled, disable it. The uninstaller cannot run properly with security enabled.
2. Restart the deployment manager, all node agents, and all servers.
3. Start the uninstallation wizard, and follow the instructions on the panels.
 -  `IBM_RFID_HOME\HA_uninst\uninstaller.exe`
 -  `IBM_RFID_HOME/HA/_uninst/uninstaller.bin`
4. A summary panel displays your uninstallation selections. Click **Uninstall** to continue the uninstallation process.
5. When the uninstallation is complete, another summary panel displays the uninstallation status. Click **Finish** to exit the uninstaller wizard.
6. To remove your single WebSphere Sensor Events, following the instructions in “Uninstalling WebSphere Sensor Events” on page 78.

Uninstalling the toolkits

Use the topics below to uninstall the toolkits.

Uninstalling the WebSphere Sensor Events Toolkit

This task describes how to uninstall the WebSphere Sensor Events Toolkit.

1. Start Rational Application Developer for WebSphere Software.
2. Navigate to **Help** → **Software Updates**.
3. Click the **Installed Software** tab and select **IBM WebSphere Sensor Events Toolkit**.
4. Click **Uninstall**
5. Click **Finish**.
6. When prompted, click **Yes** to restart Rational Application Developer for WebSphere Software.

Uninstalling the IBM Data Capture and Delivery Toolkit for WebSphere Sensor Events

This task describes how to uninstall IBM Data Capture and Delivery Toolkit for WebSphere Sensor Events.

1. Start Eclipse.
2. Navigate to **Help** → **Software Updates**
3. Click the **Installed Software** tab and select **IBM Data Capture and Delivery Toolkit**.
4. Click **Uninstall**.
5. Click **Finish**.
6. Click **Yes** when prompted to restart the Eclipse SDK.

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

Sensor Events

WebSphere Sensor Events Installation Guide

Version 6.2.0

We appreciate your comments about this publication. Please comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. The comments you send should pertain to only the information in this manual or product and the way in which the information is presented.

For technical questions and information about products and prices, please contact your IBM branch office, your IBM business partner, or your authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you. IBM or any other organizations will only use the personal information that you supply to contact you about the issues that you state on this form.

Comments:

Thank you for your support.

Submit your comments using one of these channels:

- Send your comments to the address on the reverse side of this form.
- Send a fax to the following number: 1-800-227-5088 (US and Canada)

If you would like a response from IBM, please fill in the following information:

Name

Address

Company or Organization

Phone No.

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 9BSA
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