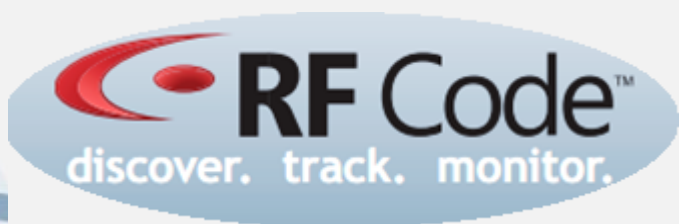


Zone Manager

Administration and Usage Manual



Publication P/N 00555 REV05

Trademarks

RF Code TM and the RF Code logo are trademarks of RF Code, Inc. All other product names are copyright and registered trademarks or trade names of their respective owners.

Information in this document is provided solely to enable system and software implementers to use RF Code products. There are no express or implied copyright licenses granted hereunder to design or fabricate any integrated circuits or integrated circuits based on the information in this document.

RF Code reserves the right to make changes without further notice to any products herein. RF Code makes no warranty, representation or guarantee regarding the suitability of its products for any particular purpose, nor does RF Code assume any liability arising out of the application or use of any product, and specifically disclaims any and all liability, including without limitation consequential or incidental damages.

The user of this system is cautioned that any changes or modifications to this system, not expressly approved by RF Code, Inc., could void the warranty.

Copyright Statement

Copyright © 2008-2013 RF Code, Inc. All Rights Reserved.

This document, as well as the hardware and firmware described therein, are furnished under license and may only be used or copied in accordance with the terms of such license. The information in these pages are furnished for informational use only, are subject to change without notice, and should not be construed as a commitment by RF Code, Inc. RF Code assumes no responsibility or liability for any errors or inaccuracies that may appear in these pages.

Every effort has been made to supply complete and accurate information. However, RF Code assumes no responsibility for its use, or for any infringements of patents or other rights of third parties, which would result.

RF Code, Inc.
9229 Waterford Centre Blvd.
Suite 500
Austin, TX 78758

www.rfcode.com

Table of Contents

Trademarks	2
Copyright Statement	2
Table of Contents	3
Introduction	5
CD Contents.....	5
Scalability	5
Minimum Hardware, Operating System, and Browser Requirements	6
Communications Ports Used by Zone Manager	6
Installation Instructions.....	7
Windows Installation Instructions.....	7
Linux Installation Instructions	7
Zone Manager Architecture	7
Zone Manager Terms and Concepts.....	8
Zone Manager Configuration	10
Overview	10
Adding Tag Groups in the Zone Manager UI	10
Adding Readers in the Zone Manager UI	11
Adding Locations and Rules in the Zone Manager UI	11
Retrieving Data from Zone Manager Programmatically	12
Browser-Based User Interface	14
Status Menu	16
Status – Tags.....	16
Status – Tags by Location	16
Status – Tags by GPS	16
Status – Tags by Parent	16
Status – Tag Find	16
Status – Readers	16
Status – Rules.....	17
Status – Summary	17
Configuration Menu.....	17

Configuration – Tag Groups.....	18
Configuration – Reader	18
Configuration – Reader Firmware.....	19
Configuration – Locations & Rules.....	21
Configuration – Import & Export	21
Configuration – License Keys.....	23
Configuration – Users.....	24
Configuration – Server Options	24
Configuration – GPS	25
Appendix	26
Tag Event and Attribute Reference	26
Advanced Reader Configuration Settings	28
Advanced Zone Manager Configuration	29
Allocating Memory to Zone Manager	29
Configuring Web Server Ports for Zone Manager.....	30
Configuring SSL for Zone Manager	30
Configuring SSL with a Digital Certificate from a Trusted Authority	31
Modifying SSL Settings	31
Configuring Zone Manager for Encryption	32
Configuring Zone Manager for Both Encryption and Authentication	33
Importing a Third-Party Root Certification Authority Certificate to Zone Manager	34
Warranty & Service	35
RF Code Support and Professional Services.....	35

Introduction

Zone Manager is a rules-based location engine that uses complex algorithms to determine the location and status of RF Code active RFID tags (both asset tags and environmental sensor tags) in order to manage the information sent by RF Code Readers. Zone Manager handles all TCP/IP communications to one or more RF Code readers and then reports information in real time to end-user software applications (e.g., Asset Manager), to RFID middleware applications, or to RTLS systems using an open web-based interface.

Because RF Code active tag beacons have the potential to be seen by multiple readers at the same time, Zone Manager uses a sophisticated rules engine to assign tags to locations based upon signal strength indicators (SSI). Locations can also be determined by IR rules in deployments that also use Room Locators or Rack Locators, or Proximity Locators and Room Locators with IR-enabled badge tags. In addition to determining tag location, Zone Manager also reports the current value of any additional sensors present on RF Code asset tags such as motion, tamper or low battery, as well as sensor readings from RF Code environmental sensor tags such as temperature, humidity, air pressure, door position, and the presence of fluid.

Zone Manager is the workhorse that continually receives and processes a continuous stream of tag and reader events from large quantities of RF Code active tags and readers. Applications can be written and integrated easily with Zone Manager to use any or all of this information in a variety of different ways such as driving business rules based on asset locations or monitoring environmental readings for critical locations. Once an application is integrated with Zone Manager to consume the information it can deliver, that application can then focus on analyzing the business data without having to have the complex state engines inherent in Zone Manager.

CD Contents

The Zone Manager CD-ROM includes the following files:

- A Windows installer executable
- A Linux RPM
- A TAR.GZ file for non-RPM Linux OS's
- This Zone Manager Admin and Usage Manual
- The Zone Manager API Reference Specification
- The Zone Manager—IBM WebSphere Interface Specification
- The Zone Manager—IBM BizTalk Installation Guide
- Sample CSV Configuration and Import Files

Scalability

As the number of tags and readers are added, the computing resources used by Zone Manager also increase. However, Zone Manager is designed for use with up to 1000 readers on a single instance and in certain circumstances can go well beyond that number. As the scope of a deployment environment grows, more memory can and should be allocated to the server that is running Zone Manager.

Minimum Hardware, Operating System, and Browser Requirements

The following are the minimum hardware and software requirements for a Zone Manager configuration with up to 50 readers with up to 10,000 tags.

- A Dual Core Intel or AMD Processor or better
- 512MB of RAM or more allocated specifically to Zone Manager
- Windows Operating System Support:
 - Windows XP
 - Windows Vista
 - Windows 2008 Server
 - Windows 2008 Server R2
 - Windows 7
 - Windows 2012 Server

NOTE: Zone Manager administrators must have Administrator Rights in the operating system.

- Linux Support and Compatibility
 - The RPM file is provided for RPM-based Linux distributions, e.g., Red Hat and CentOS.
 - The TAR.GZ file is provided for non-RPM Linux distributions.
 - Zone Manager has been tested and is officially supported on Fedora 11, but it has been used widely on various other Linux platforms, e.g., Ubuntu, SUSE, and Gentoo
- Web Browser Support (for the user interface)
 - Internet Explorer 8 and 9 (IE8 and IE9)
 - Mozilla Firefox 15+
 - Google Chrome 21+
 - Apple Safari 5.1+

Communications Ports Used by Zone Manager

Telnet Ports

- 6501 – Command and response interface
- 6502 – Tag-change events interface
- 6503 – Up Connect interface

HTTP Port

- 6580 – Command and response interface

HTTPS Port

- 6581 – Command and response interface

Installation Instructions

The following installation and configuration instructions assume that Zone Manager is being installed separately from Asset Manager, as any configuration settings written to Asset Manager are propagated in Zone Manager. Therefore, any configuration done directly in a Zone Manager instance, which is installed as part of an Asset Manager installation, will be overwritten if any changes are made in Asset Manager.

Windows Installation Instructions

To install the Windows version of Zone Manager, perform the following steps:

1. Browse to the \install\windows folder on the Zone Manager CD.
2. Double-click the setup.exe file.
3. Follow the installation wizard prompts to complete the installation.
After the installation is completed, the Zone Manager service will start.

Linux Installation Instructions

To install Zone Manager in an RPM-based Linux operating system, perform the following steps.

1. Browse to the RPM file in the \install\linux folder of the Zone Manager CD.
2. Issue either the command in either (a.) or in (b.) below:
 - a. If this is a new installation of Zone Manager, issue this Terminal command:

```
rpm -ivh rfcode-zonemgr-{Version-BuildID}.noarch.rpm
```

where Version-BuildID is the version and build date of the rpm, e.g., 2.8_20130606_123456

NOTE: This command will install the software, start the Zone Manager service, and configure the service to start at boot.

- b. If you are upgrading from previous version of Zone Manager, issue this Terminal command:

```
rpm -Uvh rfcode-zonemgr-{Version-BuildID}.noarch.rpm
```

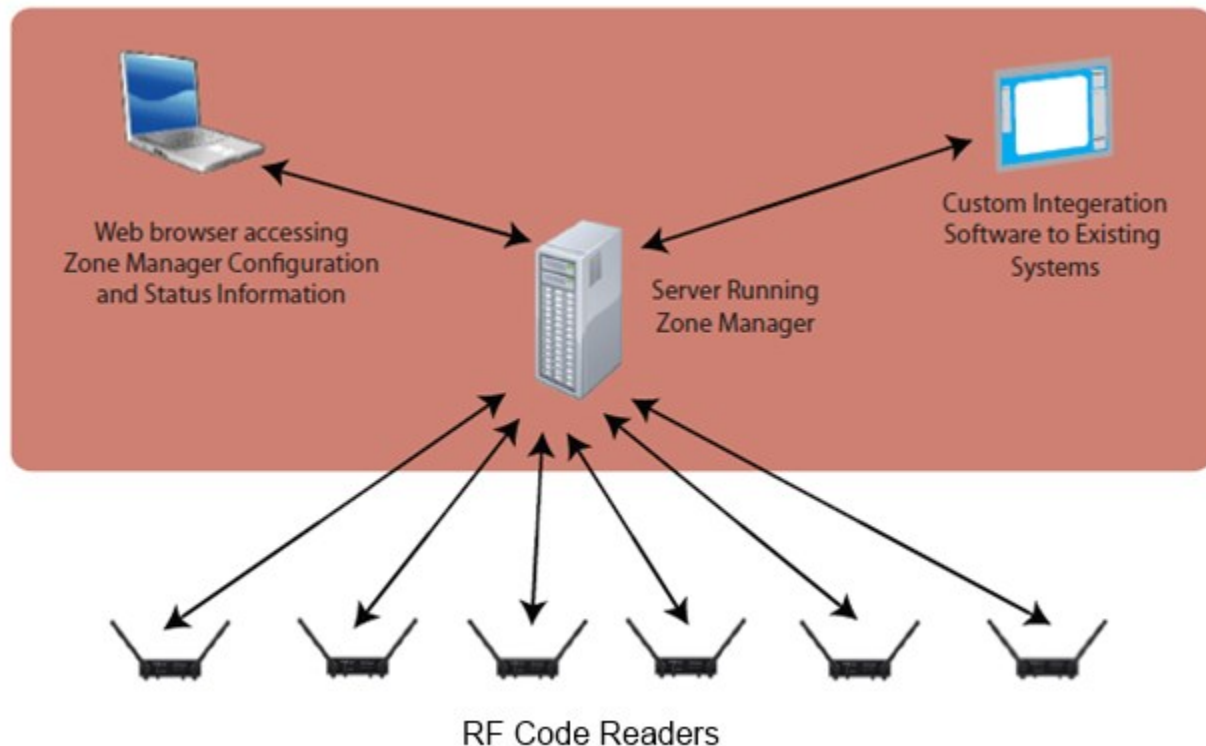
Zone Manager Architecture

Zone Manager handles all of the direct hardware interfaces for RF Code readers and tags. Zone Manager is essentially the engine designed for integration with one or more business applications through its open application programming interface (API).

RF Code fixed readers receive tag beacons and the information contained in them about the location of asset tags and the assets associated with them and about the status of the environment monitored by RF Code sensor tags and then communicate this information over an IP network to Zone Manager.

Readers and Tag Groups are configured in Zone Manager. After making Zone Manager aware of the RF Code reader and tag hardware devices that have been deployed in the production environment, an admin creates locations and rules that interpret the communications. Then, Asset Manager or another third-party end-user application can consume the data, analyze it using its own set of rules and calculations, store it for historical analysis, and generate alerts and other notifications.

Figure: Zone Manager Architecture



Zone Manager Terms and Concepts

The following terms and concepts are important to the understanding of Zone Manager.

Readers

- Readers are active RFID readers such as the RF Code M250 Reader and the RF Code M240 Reader. However, Zone Manager is also compatible with older or legacy reader models such as the M200, D200, and R200.
- Readers receive tag beacons. The information in these beacons is received on two channels, Channel A and Channel B, which correspond to the two RF antennas on the reader.
- Readers only communicate with Zone Manager using the IP protocol.
- Every reader must be added to and configured in Zone Manager.

Tags

- Tags are RF Code active tags such as the M-Series or R-Series tags.
- Each tag has a Group Code, a unique Tag ID, and a Tag Treatment Code. In combination, these are used to parse communications from hundreds or thousands of tag beacons transmitted to RF Code readers.

Tag Groups

- Tag Groups are group codes and corresponding tag treatment codes needed by Zone Manager to interpret tag events correctly.
- Tag Groups must be configured in Zone Manager.
- Tag Groups must exist for all asset and sensor tags in the production environment you are managing and monitoring.

Locations

- Locations are logical definitions (i.e., “places” or “areas”) in Zone Manager that correspond the physical deployment environment.
- In its most basic form, a Location in Zone Manager is a label name.
- Locations are structured in a Location Hierarchy.
- Location names need to be specific enough to distinguish them from one another, e.g., two rows could each have a “Rack 1,” so while possibly evident in the Location Hierarchy, when querying Zone Manager, the specific Location needs to be discernible, so it is best to use nomenclature such as the following for these two different racks: *R1-Rack-1* and *R2-Rack-1*.

Location Hierarchies

- The Location Hierarchy represents the environment being monitored and in which assets are being managed.
- The Location Hierarchy defines parent-child relationships between individual Locations.
- The following top-to-bottom (physically largest-to-smallest) hierarchy represents that Rack 5 (*DCA-R13-Rack-5*) is in Row 13 (*DCA-Row-13*), which is in Data Center A (*Data-Center-A*):
Data-Center-A – DCA-Row-13 – DCA-R13-Rack-5

Rules

- Rules are essentially algorithms that are used to determine the location of tags.
- Zone Manager uses the logic in the algorithms such that when parameters are met, a confidence value is calculated and the location (zone) a tag is determined.
- If no rules match, then the tag location is considered to be unknown.
- By far the two rules that are used most often are the following:

- **Match by Simple SSI** – This rule compares tag signal strengths to the Minimum and High Confidence SSI Thresholds set for readers and reported by one or both of the reader radio channels that have been configured for the rule.
- **Match by IR Locator** – This rule compares the *irlocator* attribute (of those tags that support it) with a specific value (the ID of the IR Locator device).

Zone Manager Configuration

Overview

After completing the installation, perform the following tasks to configure a basic functional instance of Zone Manager. The following sections of this document describe how to perform these tasks using the browser-based user interface (UI) accessible at the following URL: <http://localhost:6580>

NOTE: All configurations done with the browser-based UI can also be accomplished programmatically using functions described in the Zone Manager API Specification, which is available on the Zone Manager CD and from the RF Code Support website: <http://support.rfcode.com>.

After you have accessed the User Interface, configure Zone Manager to bring it to a basic functional state. The following sections are presented in the suggested order of operation:

1. Add one or more Tag Groups.
2. Add one or more Readers.
3. Add one or more Locations.
4. Add one or more Rules.

After you have configured at least a minimal instance of Zone Manager, you can then retrieve data from it. This process is covered later in the [Retrieving Data from Zone Manager Programmatically](#) section.

Adding Tag Groups in the Zone Manager UI

In the Configuration Menu, add the tag groups for the RF Code Active RFID tags that you wish to read.

Tag groups require a treatment code and group code to be read properly. The Treatment Code and the Group Code (as well as the unique Tag ID) are printed on the tag label. The arbitrary Tag Group ID is defined by the user and can be any string, as long as it is unique and it uses standard characters.

Figure: RF Code Active RFID Tag Group Code, Tag ID, and Treatment Code



Adding Readers in the Zone Manager UI

After you add tag groups, any reader that is added will automatically begin reading tags that belong to these groups.

To add a reader, simply add the IP address or hostname of the reader to Zone Manager under the Reader Configuration Menu.

In the normal mode of operation, Zone Manager contacts the reader using the IP address or hostname configured for the reader in Zone Manager. However, when the reader (instead of Zone Manager) must initiate the connection, you can use Up Connect.

NOTE: To use Up Connect, you must give the reader an Up Connect ID and a login password. This is done by using the Reader Configuration Utility (RCU) or the browser-based reader web console. For more information, please refer to the Reader Configuration Utility User Manual and other documents and knowledge base articles on the RF Code Support website: <http://support.rfcode.com>.

NOTE: The reader ID and login password must also be configured in Zone Manager and must match exactly to what was assigned to the reader using the RCU. The IP address of the reader must be configured in Zone Manager as well.

After adding a reader you will see tags in the Status views, but they will not be tied to a location.

Adding Locations and Rules in the Zone Manager UI

In the Location & Rules section of the configuration menu, a rule and a location must be added in order to bind the tags that are read by the reader to a specific location.

To add a location and a rule, perform the following steps:

1. Click **New Location**.
2. Enter a **Name** for a location.
3. Using the Location that was just created, click **New Rule**.
4. Give the rule a unique identifier.
RF Code recommends LOCATIONNAME_RULE as a naming convention.
5. Choose **Match by Simple SSI** rule and add both **Channel A** and **Channel B** of at least one reader to the rule.

NOTE: The drop-down Rule menu includes a number of different rules. Match by SimpleSSI and Match by IR Locator are by far the most common and useful of the rules available. The SimpleSSI rule matches the best read by any antenna channel that sees a tag. The IR locator rule matches location to the ID of the Room Locator, Rack Locator, or Proximity Locator that an IR tag receives. Matching by IR Locator gives more precision to tag location but requires the use of an IR Locator (Room, Rack, or Proximity) and IR-enabled RFID tags.

6. Click **Save Changes**.
Tags in the Status View will appear in the newly created location.

NOTE: Experimenting with the SSI Minimum rule will allow you to adjust the range within which tag beacons are received and the tag location is determined. The High Confidence SSI Threshold can help to determine location more precisely in the case where when more than one reader sees the same tag.

Retrieving Data from Zone Manager Programmatically

While the Zone Manager API Specification contains a complete reference to all of the parameters you can use to get data from and put data into Zone Manager, through the use of only a few simple parameters you can get a good general picture of your assets and/or environment after Zone Manager has been configured. The following explanations of basic query parameters are universal, but the specific examples below are for use with HTTP commands in a browser; as such, they resemble website address URLs. In fact, the first part of the command is the URL that you used to access the user interface in order to configure Zone Manager. However, the full command is a query (and in certain specific instances, commands can also be used create, update, or delete tags, readers, or other configurations within the Zone Manager environment). The queries you can issue to Zone Manager are issued to the specific Zone Manager instance that is located at the URL that comprises the beginning of the command.

Basic Query Parameters

Using only the three following parameters, you can build a basic yet powerful HTTP query to return a wealth of information about your Zone Manager environment.

tagupdates

The **tagupdates** parameter tells Zone Manager to return current state(s) of every tag and reader in the environment.

init

The **init** parameter starts a session for communicating with Zone Manager. Set the **init** parameter to true (**init=true**) in the HTTP query when you first query Zone Manager.

NOTE: Zone Manager must be queried at least once every two minutes or the session will expire; if this happens, you must start a new session by setting **init=true** again in the next query.

NOTE: After opening the session by setting the **init** parameter, all future queries in the session will retrieve only changes in tag or reader states.

sid

The **sid** parameter is the Session ID. Zone Manager uses the Session ID to distinguish collections of tag and reader events from one another.

NOTE: The **sid** can be any arbitrary integer, but it is important for each session to have its own unique ID so that tag events are associated with and reported by each session separately. Otherwise, querying Zone Manager could result in incomplete and/or inaccurate data as a query to one session with the same ID as another will return only those events that haven't been queried by and reported the other session.

Basic HTTP Queries

Your initial query to Zone Manager should look like the following:

http://localhost:6580/rfcode_zonemgr/zonemgr/api/tagupdates?_sid=5&_init=true

NOTE: This returns the current (initial) state of the tags and readers in your environment.

Subsequent queries can omit the **init** parameter and should look like the following:

http://localhost:6580/rfcode_zonemgr/zonemgr/api/tagupdates?_sid=5

NOTE: This query will return any changes that have occurred since the initial state.

Alternate Formats for Query Results

When you query Zone Manager with HTTP commands, the default format for the results presented in the browser is CSV. However, you can also choose to have the data returned as either JSON or XML formatted data. This is done by appending one of two alternate file type extensions to the tagupdates command in the query.

JSON — http://localhost:6580/rfcode_zonemgr/zonemgr/api/tagupdates.json?_sid=5

XML — http://localhost:6580/rfcode_zonemgr/zonemgr/api/tagupdates.xml?_sid=5

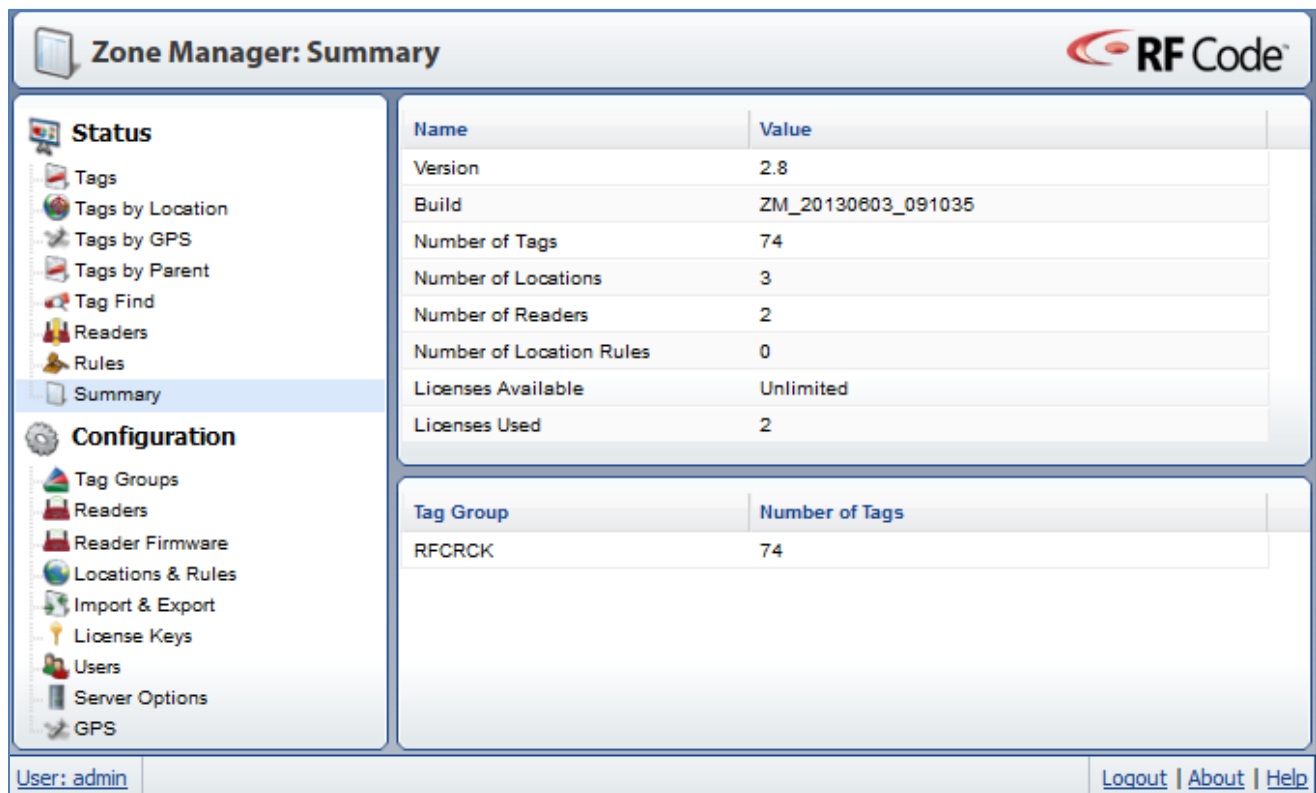
Browser-Based User Interface


This Zone Manager user interface is a browser-based UI for configuring and viewing RF Code Reader and Tag settings. As previously discussed, Zone Manager can also be configured using Telnet or HTTP commands.

The URL of the browser-based UI is: http://hostname:6580/rfcode_zonemgr/

The Zone Manager UI functions focus on tasks for managing the system infrastructure and displaying system data. It is used by an administrator to set up a system structure for the purpose of discovering, monitoring and tracking tagged assets. The Zone Manager UI provides two main task menus:

- Status
- Configuration



Zone Manager: Summary 

Status

- Tags
- Tags by Location
- Tags by GPS
- Tags by Parent
- Tag Find
- Readers
- Rules
- Summary

Configuration

- Tag Groups
- Readers
- Reader Firmware
- Locations & Rules
- Import & Export
- License Keys
- Users
- Server Options
- GPS

Name	Value
Version	2.8
Build	ZM_20130603_091035
Number of Tags	74
Number of Locations	3
Number of Readers	2
Number of Location Rules	0
Licenses Available	Unlimited
Licenses Used	2

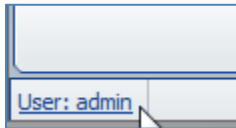
Tag Group	Number of Tags
RFCRCK	74

User: admin Logout | About | Help

The Zone Manager UI is divided into window panes. Typically, the left pane is the navigation pane where the tasks and sub-tasks are located and the right pane or panes contain various configuration options for the respective tasks. The Zone Manager UI also contains an information bar on the bottom of the screen, which contains four links: [User](#), [Logout](#), [About](#), and [Help](#).

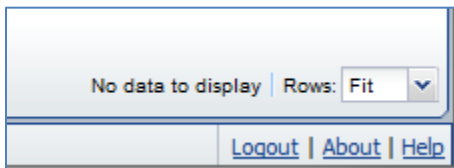
User Link

The User link at the far left of the bottom navigation bar shows who is logged into the user interface.



If you click the link, you are prompted with a Password Change pop-up window that lets you change your password. If you want to keep your current password, simply click the Cancel button.

At the far right of the bottom navigation links are the other three links.



Logout Link

The Logout link simply logs you out of the UI browsing session. Alternatively, you can close the browser or browser tab; however, the Zone Manager session will still remain active for a limited time if you do not click the Logout link to end it.

About Link

The About link provides information about the Zone Manager version that is installed.

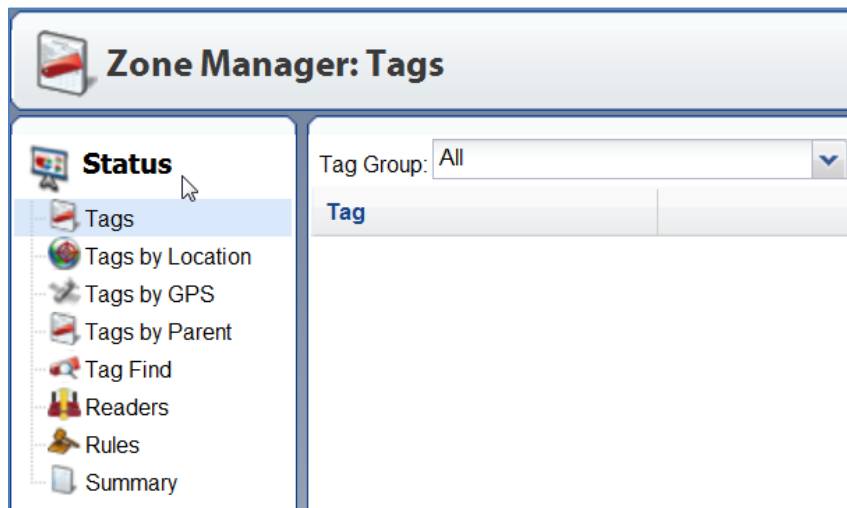
Help Link

The Help link opens this PDF document (*The Zone Manager Administration and Usage Manual*).

NOTE: For additional details about Zone Manager communication and protocols, refer to the Zone Manager API Specification, which is available on the Zone Manager CD and from RF Code Support at <http://support.rfcode.com>.

Status Menu

This is the first of two main task menus available in the Zone Manager Browser User Interface.



It has eight sub-tasks available: Tags, Tags by Location, Tags by GPS, Tags by Parent, Tag Find, Readers, Rules, and Summary.

Status – Tags

Tags will provide a status view of all the tags that are recognized by the Zone Manager system.

Status – Tags by Location

If Locations have been configured, this sub-task shows a list of tags that are being reported in any particular location if you click on that Location in the Location Hierarchy.

Status – Tags by GPS

If the Reader has an attached and configured GPS device, the Tags by GPS sub-task will allow the user to see the list of tags and their location and their broadcast latitude-longitude coordinates.

Status – Tags by Parent

The Tags by Parent sub-task is used with the RF Code PDU Sensor Tags. This feature allows the user to search for a parent PDU tag by the Tag ID and will populate the search field with the various children tags, i.e., the PDU data points.

Status – Tag Find

The Tag Find sub-task will allow the user to search for a specific tag by the tag ID or a group of tags by the *groupcode*.

Status – Readers

The Readers sub-task will allow the user to see the status of all Readers that are configured in Zone Manager.

The first five Reader Status attributes are Status, Reader ID, Hostname, Noise (Ch. A), and Noise (Ch. B).

Zone Manager: Readers					
Status	Reader ID	Hostname	Noise (Channel A)	Noise (Channel B)	
ACTIVE	\$zReaderM250_44abfc5c5fd7f779	192.168.1.129	-113	-113	
ACTIVE	\$zReaderM250_61fca1feaf330f2	192.168.1.101	-106	-103	
ACTIVE	\$zReaderM250_835f4dff5b1fd118	10.1.9.127	-99	-99	
ACTIVE	\$zReaderM250_7908de183d89b979	10.1.9.112	-100	-96	
ACTIVE	\$zReaderM250_a0dcf96ca2930688		-92	-93	
ACTIVE	\$zReaderM250_52c92262a00cca3	192.168.1.129	-89	-91	
DISCONNECTED	\$zReaderM250_540af305fbd1370	192.168.1.129	0	0	

The rest are Event Rate (Ch. A and Ch. B), Tag Capacity Used, Firmware Version, Connected Address, Connection Encrypted, and GPS.

Event Rate (Channel A)	Event Rate (Channel B)	Tag Capacity Used (%)	Firmware Version	Connected Address	Connection Encrypted	GPS Status
157	157	0	1.2.3	10.1.9.103	true	
152	150	0	1.3.0	10.1.9.117	true	

Status – Rules

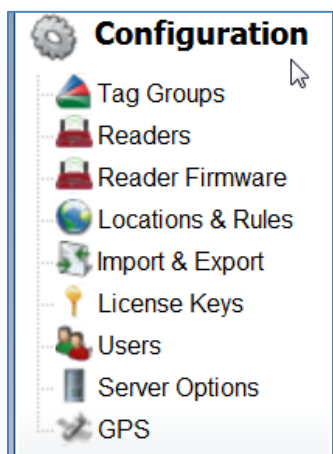
The Rules sub-task provides a list of all of the Rules that have been configured for the Zone Manager.

Status – Summary

Summary sub-task will provide the user with an over view of the complete status of all of the Readers, Locations, Rules, Tags, and Licenses that have been configured for the Zone Manager, as well as the version and build number of the installed Zone Manager software.

Configuration Menu

The second of the main task menus available in Zone Manager is the Configuration Menu.



This menu has nine subtasks available: Tag Groups, Readers, Reader Firmware, Locations & Rules, License Keys, Users, Import/Export, Server Options and GPS.

Configuration – Tag Groups

The Tag Groups sub-task is used to configure the Tag Groups for the Zone Manager as discussed in Zone Manager Configuration Step 1.

Configuration – Reader

The Readers sub-task is used to configure the Readers for the Zone Manager as discussed in Zone Manager Configuration Step 2. Below is further explanation of the settings that are available for configuration in the Readers sub-task.

Basic Information

ID - Create an ID for the reader.

Tag Groups - Select either All Tag Groups setting or Tag Groups and select the specific Tag Groups for which you would like to configure the Reader.

Control

Enabled – If you want a properly configured reader to be active so that it can receive tag data and then transmit the data to Zone Manager, this box must be checked.

Network Settings

Hostname - Enter the IP address of your reader in this field.

Port - Enter the port number over which to communicate with your reader (by default this is 6580).

Authentication

User ID - Enter a user ID for the reader.

Password/Confirm Password - Enter a password and confirm the password.

Up Connect Settings

Up Connection Enabled - If you are configuring Up Connect, it needs to be enabled in order for reader to send tag data “upstream” to Zone Manager after it has been properly configured. (Please refer to the Reader Configuration Utility User Manual for more information)

Up Connection Reader ID – Enter the ID that was assigned when you configured your reader for Up Connect using the Reader Configuration Utility (RCU).

Up Connection Password - If you assigned a password when you configured Up Connect for the reader with the Reader Configuration Utility, you will need to enter and confirm the same password for use with Zone Manager.

Position Settings

Position Source – Configure this setting to use GPS with your readers.

None – Leave the default setting of **None** if your reader will not use a GPS location.

Static Position – Select Static Position and provide coordinates if you would like to set a static GPS location for the reader.

Reader GPS – Select Reader GPS if your reader will be connected to a GPS device. You can then further configure GPS settings under the Configuration > GPS menu options.

Advanced

NOTE: The advanced reader configuration settings are discussed in the Appendix; if not used properly, they can seemingly cause tag transmissions and/or locations to be misidentified or prevented from being determined at all. Do not change these settings without first contacting RF Code Support.

Reader Partitioning

NOTE: The Reader Partitioning settings should only be changed at the direction of RF Code Support.

Reader Partition Count - This indicates the number of portions the tag ID range will be divided into. The value must be from 1 to 32, and must be greater than Reader Partition Index. The default is 1.

Reader Partition Index - This indicates which portion of the range of tag IDs the reader will observe (specifically, what the remainder must be when the tag ID is divided by Reader Partition Count). The value must be from 0 to 31, and must be less than Reader Partition Count. The default is 0.

Reader Partition Rotation Time - This specifies the amount of time that the reader is reset to observe tag IDs of the next partition index. The default is 0, which will not reset the reader to observe tag IDs of the next partition index.

Diagnostics

Noise Threshold - This is the threshold for Zone Manager to send an alert for excessive RF noise in the system, as detected by the reader ("D" command for noise level). If the noise is excessive, the reader performance is compromised.

Tag Event Rate Threshold - This is the threshold that will determine high reader event activity.

Serial Port

Serial Baud Rate - Enter the recommended baud rate for the serial device. This should be indicated with the literature that came with the device.

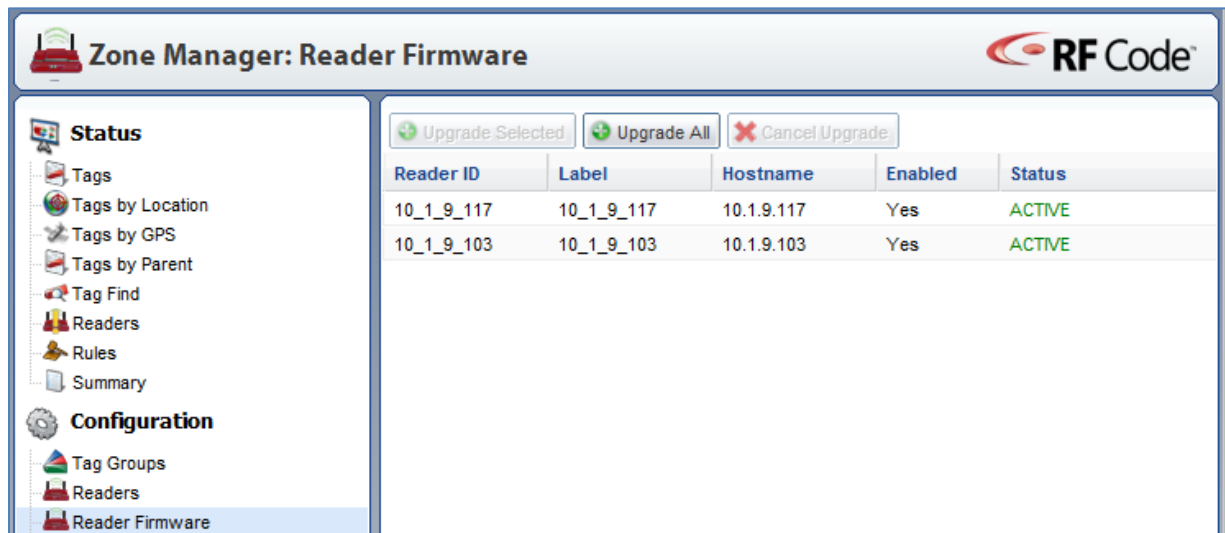
Serial Driver - Choose the serial driver parameters used to communicate with the serial device. This will be indicated with the device literature.

Configuration – Reader Firmware

The Reader Firmware upgrade sub-task lets you upgrade a single individual reader or multiple RF Code Readers at the same time.

To upgrade the firmware of an RF Code Reader through the Zone Manager user interface, perform the following steps:

1. Navigate to **Configuration > Reader Firmware**.



2. From the list of readers that have been added to Zone Manager, look for those with something other than Up to date in the Firmware Available column.

Reader ID	Label	Hostname	Enabled	Status	Firmware Version	Firmware Available
10_1_9_117	10_1_9_117	10.1.9.117	Yes	ACTIVE	1.3.0	Up to date
10_1_9_103	10_1_9_103	10.1.9.103	Yes	ACTIVE	1.2.3	1.3.0

3. If you see any that are not up to date, highlight the row corresponding to the reader to be upgraded and click the **Upgrade Selected** button, which will now be active.

NOTE: If the Firmware version listed in the Firmware Information pane is not the most recent, go to RF Code Support and download the latest firmware for your reader:
<http://support.rfcode.com/customer/portal/articles/716055>.

NOTE: After downloading and saving the newer firmware, click the **Browse** button in the bottom right Firmware Information pane, and then click the **Upload** button. After you have saved the firmware package locally, follow the steps above to upgrade the reader firmware.

NOTE: For assistance with the upgrade, please contact RF Code Support.

NOTE: It is vital that any firmware updates be obtained directly from RF Code (or through an authorized source). If you use firmware from any other source, you will render the reader inoperable.

Configuration – Locations & Rules

The Locations & Rules sub-task is used to configure the Locations and Rules for Zone Manager.

Configuration – Import & Export

In order to simplify configuration and addition of a large numbers of readers, you can use the Import & Export task.

This task is designed particularly for the common pattern of one reader per location (i.e. rack), with one rule associating tags seen by that reader with that location. This feature uses simple form CSV-formatted spreadsheets for importing, defining one or more readers, locations, and rules binding them. The import is performed by accessing the Configuration > Import/Export sub-task. Under the Import Configuration, select the CSV configuration files you would like to import and click Upload. The export task is performed by clicking on the button for the particular configuration that you want to export (tags.csv, readers.csv, locations.csv, rules.csv) and choosing a location to save the file. Below is a list of column names in the first line of the CSV file that are to be used to control the requested operations, and must be formatted as follows:

group.id - Defines the ID of the grouped object.

group.type - Defines the type of group that is being created according to tag treatment code.

group.groupcode - Defines the groupcode of a tag or tags.

reader.id - Defines the ID of the reader object. This will be created if it is not defined.

reader.type - Defines the type of reader object (only used if created). The default is “R250.”

reader.enabled - Defines the activation state to set for reader (default is true (active)).

reader.<attrib> - Provides a value for the field <attrib> of the indicated reader:

reader.id - Must be defined in order for this to work.

reader.groups - Provides a list of tag group IDs to be associated with the reader. If set to ‘*’, all existing tag groups will be added. If not provided, all existing tag groups will be added when the reader is created (but not for updates).

location.<N>.id - Defines the ID of the Nth object in the location path for the given position. N=1 is the location corresponding to reader, N=2 is that location’s parent, etc.

location.<N>.<attrib> - Provides a value for the field <attrib> in the location identified by location.<N>.id (which must be defined).

rule.id - Defines the ID of a location rule relating the reader’s channels to the location.1.id location (by default, given reader.id and location.1.id are defined). If not provided, but reader.id and location.1.id are defined, rule.id is assumed to be “<reader.id>_<location.1.id>_rule”.

rule.type - Defines the rule type. If undefined, “AverageSSIRule” is assumed.

rule.enabled - Defines the rule activation state. The default is “true” (active).

rule.<attrib> - Defines the value of the field <attrib> in the rule.

NOTE: For additional information about column names, refer to the Zone Manager API Specification.

If the value of a given field is blank for a given row, the field is ignored for that row (versus being used to set an attribute to blank, for example). To delete an attribute, the value must be set to the string "<null>". To set it to a blank string, assign <blank> as the value.

The general flow of execution for each line is as follows:

1. If reader.id is provided, a reader with that ID is created, if needed, use the reader.type value (or "R250, etc." otherwise).
2. If any reader.<attrib> values are defined, they are set for the reader.
3. If the reader.groups field is provided, the listed tag groups are added to the reader. If reader.groups is not provided AND the reader was newly created, all currently defined tag groups are added to the reader.
4. If the reader was newly created, it is activated (unless reader.enabled is defined and set to false). If reader.enabled is defined, the reader's activation state is updated accordingly.
5. For each location.<N>.id defined, starting at the highest value of <N>, a location with the given ID is created, if needed, and set to have the location.<N+1>.id as its parent (if defined). Any location.<N>.<attrib> values are set for each location.
6. If reader.id is defined AND location.1.id is defined, a location rule is created (if needed). If rule.id is defined, the value is used as the ID. If not, the ID is assumed to be "<reader.id>_<location.1.id>_rule". If created, the rule type is "AverageSSIRule", unless rule.type was provided. The channellist for the rule is assumed to be "<reader.id>_channel_A,<reader.id>_channel_B", unless rule.channellist is set. Other rule.<attrib> values are used to set rule settings. If created, the rule is activated (unless rule.enabled is defined and false). If rule.enabled is set, the rule activation is updated appropriately.

Import Examples, Guidelines, and Notes

The following are two examples of import file configuration:

- The minimal configuration of a CSV file to define a reader, an associated location, and a default AverageSSIRule rule that ties the two together, would need to include only the following columns: **reader.id** | **reader.hostname** | **location.1.id**
- A simple two-tier location hierarchy, with each reader's location having a parent location (i.e. A room containing each of the racks), can be defined simply by adding another location level column for the parent: **reader.id** | **reader.hostname** | **location.1.id** | **location.2.id**

NOTE: For other examples of import file configuration, refer to the mass_config sample CSV files that are provided in the \samples directory on the Zone Manager CD.

Please heed the following guidelines and notes when configuring import files:

- Imported CSV files can be updated and imported again in order to update the created objects (or to create new ones).
- Column names are **case sensitive**, but the first letter of the column name can be capitalized (to accommodate those spreadsheet tools that insist on capitalizing column names). So, both **reader.id** and **Reader.id** are acceptable, **but not READER.id**.
- Using spaces in a column title will cause an error; therefore, omit spaces and use underscores or hyphens instead, e.g., **Rack_1** or **Rack-1** and **not Rack 1**.
- Having two (2) attributes with the same name will cause an error.
- Create Mass Configuration Import files as four separate files, separated as follows: **groups.csv**, **readers.csv**, **locations.csv**, **rules.csv**.

Configuration – License Keys

The License Keys sub-task is used to enter the RF Code Zone Manager license key that you were provided.

To enter the license, perform the following steps:

1. Click the **Add** button.
2. Enter the key as it appears on the License Key Card.
3. Click the **OK** button.
The License Key and its Expiration Date will appear in the top right pane and the number of Licenses in Use, Total Licenses, and Available Licenses will appear in the bottom right pane.

Configuration – Users

The Users sub-task is used to configure user account settings for accessing the Zone Manager user interface. By default, Zone Manager is installed with only the admin user account configured. You can grant or restrict access to the Zone Manager by using the Users configuration sub-task to create user accounts with various permission levels.

To create a user account, perform the following steps:

1. Click the **New** button.
2. Give the user account a name or identifier in the **ID*** field.
3. Give the user a **Password** and then enter it again in the **Confirm Password** field.
4. Assign a role to the user account by choosing one of the three available choices in the **Roles*** drop-down menu.

NOTE: There following three Roles are available:

Administrator – An Administrator has full access to both the Configuration and the Status menu and everything within each of them.

Config View – A user assigned the Config View user role will have “view-only” access to both the Configuration Menu and sub-tasks and the Status Menu and sub-tasks.

Status View – A user assigned Status View will only be able to view and access the Status menu and sub-tasks.

Configuration – Server Options

The Server Options sub-task lets you configure various advanced options used with Zone Manager.

Up Connect

Up Connect is available to allow for communication with a consuming application if you are setting up a Zone Manager that is behind a firewall.

The following Up Connect fields and settings can be configured:

- **Enabled** – This checkbox must be checked to enable Up Connect in Zone Manager.
- **Hostname** – This is the hostname of the Zone Manager server.
- **Port** – This is the communications port that will be used by Up Connect. The default value is 6580.
- **SSL** – If you want to encrypt communication within Up Connect, choose **SSL – No Verification** and if you want to enforce greater security in the communication channel, choose **SSL Verify Certificate & Hostname**. If you do not want to use SSL, leave the default setting of **Do not use SSL**.
- **Zone Manager ID** – The **Zone Manager ID** can be any alphanumeric string you choose.
- **User ID** – Enter the User ID
- **Password** – Assign the user a password.
- **Confirm Password** – Enter the same password again.

Event Store & Forward

Zone Manager offers the ability to store tag events on a local hard drive so that if the connection to the Zone Manager is interrupted, then these locally stored events can be forwarded when the connection is restored. This capability is only limited by the amount of hard drive space available. To configure this feature, enter in the maximum number of hours of data events that will be captured and stored until the reconnection. If you choose to use this feature, you will need to monitor your drive space over time and make the necessary calculations to ensure you have adequate storage available for Zone Manager; for a general calculator, you can refer to the following RF Code Support Knowledge Base article:

<http://support.rfcode.com/customer/portal/articles/760679>.

Expected Location Bias

NOTE: This advanced setting should only be used at the direction of RF Code Support.

IBM® WebSphere® Sensor Events

NOTE: These fields are used specifically for configuring Zone Manager for use with IBM WebSphere. If you use IBM WebSphere, refer to the Zone Manager-IBM WebSphere Events Interface Specification PDF and contact RF Code Support for assistance.

Configuration – GPS

The GPS sub-task lets you adjust the global GPS settings for all GPS devices that are connected to RF Code Readers. The settings below are available for configuration.

GPS Data Reporting

The following options are available for what aspects of GPS you want to view and use in reports:

- lat-lon
- lat-lon-epe
- lat-lon-spд
- lat-lon-spд-epe
- lat-lon-alt
- lat-lon-alt-epe
- lat-lon-alt-spд
- lat-lon-alt-spд-epe

[lat = latitude, lon = longitude, epe = Estimated Position Error, spд = speed, alt = altitude]

Minimum GPS Update Period

Enter the minimum time period required for GPS data updates. The default setting is 30 seconds.

Minimum Horizontal Change

Enter the minimum distance of horizontal change required for GPS data updates.

The default setting is 10 meters (32.8 feet).

Minimum Vertical Change

Enter the minimum distance of vertical change required for GPS data updates.

The default setting is 100 meters (328.1 feet).

Appendix

Tag Event and Attribute Reference

In addition to Location, RF Code Active RFID Tags can report a wealth of additional information. Tags report to readers when one of three possible events occurs. These events and the tag attributes that are reported are presented in the following tables.

Tag Event	Description	Notes
Create	The first time a tag is reported on the <i>updates</i> channel.	In <i>_init</i> =true tags will all be reported as Create even though they will have been on the Zone Manager prior to the request. After the <i>_init</i> , Create indicates a newly found tag.
Update	An update occurs whenever an attribute changes on a tag that was previously reported by Create on the updates channel.	The attribute that changed is listed. A list of attributes is included below. Location is also considered an attribute.
Delete	When a tag is no longer seen by any readers in Zone Manager's scope, a delete event occurs.	No further information on the deleted tag will be available until it is seen again during a create event.

The following is a list of tag attributes that Zone Manager may report. Both the type and number of attributes reported by Zone Manager are dependent upon the type and number of tag populations that are configured. Different asset and sensor tags report different information.

Attribute	Description	Type	Value Type/Range
id	The tag ID.	string	A combination of group code and tag number
type	The type of object being reported on for a tag. This will be "tag".	string	location, tag, reader
motion	Motion detected by tag.	Boolean	true (motion detected) false (none detected)
tamper	Attempt to tamper with tag or remove tag detected.	Boolean	true (tamper detected) false (none detected)

Attribute	Description	Type	Value Type/Range
lowbattery	Low battery condition detected by tag.	Boolean	true (low battery voltage) false (normal battery voltage)
panic	Panic/alarm button depressed on tag.	Boolean	true (button activated) false (button not activated)
dooropen	Door switch on tag reporting opened door.	Boolean	true (door open) false (door closed)
lockopen	Lock open (unlocked) reported by tag.	Boolean	true (lock open) false (lock not open)
lockclosed	Lock closed (locked) reported by tag.	Boolean	true (lock closed) false (lock not closed)
irlocator	IR locator code detected by tag	string	000 – no locator detected 001-757 – locator code detected 0001-9999 – IR series 2 locator code detected
motioncount	Number of motion events detected.	integer	
lockcount	Number of lock/unlock events detected.	integer	
userpayload	Custom numeric payload.	integer	0-65535 - for use with custom engineered tags
temp	Temperature measured by tag.	double	Value in degrees Centigrade.
humidity	Humidity measured by tag.	double	Value in percent relative humidity.
pressure	Pressure measured by tag.	double	Value in pounds per square inch (psi).
dryopen	Dry contact input on tag reporting opened switch/circuit	Boolean	true (switch open) false (switch closed)
dewpoint	measured by tag	double	Value in degrees Centigrade.

NOTE: There are many more options for retrieving tag data from Zone Manager. For example, the tagupdates channel is also implemented on a telnet style interface at port 6502. For more information on alternative ways to retrieve data from Zone Manager, refer to the Zone Manager API Specification.

Advanced Reader Configuration Settings

NOTE: If not used properly, these advanced reader configuration settings can seemingly cause tag transmissions and/or locations to be misidentified or prevented from being determined at all. Do not change these settings without first contacting RF Code Support.

SSI Change Threshold - <min-ssi-change> is a parameter that allows messages that report small SSI value changes to be treated as “unchanged”. Any message where all the SSI values reported are <minssi-change> or less dBm different from the previously reported message will be considered to have not changed. The default value, 0, considers any change in SSI as significant.

SSI Cutoff (Channel A, B) - Sets the channel SSI threshold to the respective –dBm (fixed threshold value). RF Code reader limitation is 41 to 115. This feature is used to reduce the effective read range of a reader. For example: Z,68,102 <cr> sets channel A threshold to –68 dBm and channel B threshold to –102 dBm. On channel A tags that are at -68 dB or less are not reported, and on Channel B tags that are at -102 dB or less are not reported.

Tag Age-Out Time - <tag-timeout> is the number of seconds since the last successful message read from a tag before the tag is considered “lost”. The allowed values range from 10 to 32767. The default value is 256 seconds. If the value is set to 0, the tag timeout is infinite. A tag that has not been seen by a reader for “n” seconds will be reported as not present.

Tag Age-Out Time (Channel A, B) - This field functions the same as Tag Age-Out Time, but is Channel specific. One of your reader channels would be set to a shorter time as in Tag Age-Out Time.

Tag Age-Out Time (Reader Offline) - is the length of time to keep tags in the system if a reader goes offline. “n” seconds after a reader goes offline the tags that had been reported by this reader will be reported as not seen anymore.

Tag Age-In Count - <age-in-count> is an optional parameter used to tell the reader to not report messages from a tag until <age-in-count> messages have been received from that tag. This allows the option of ignoring tags that may appear for a short period of time (for example, due to a tag isolation box being opened for a few seconds).

Channel Bias (Channel A, B) - This setting allows for a compensation offset value to be added when different gain antennae are used. For the rack solution for example a very low gain antennae is used inside the rack, but high gain antennae are used for zone level coverage. To be able to report tags within a rack without having the zone reader (with the higher gain antenna) take possession of it, there is a need to add some value (bias) to the rack reader for the tag to appear stronger inside the rack.

Report Tag Controller Events Box - enables Zone Manager to receive Tag Controller Compatible Tag information from the reader.

Join Reader Channels - enables a reader's channel A and B into a single logical channel, by combining the raw samples into a single sample stream

Merge Reader Channels - enables the reader to report whichever channel gets the strongest signal from the tag. This is good for reducing bandwidth consumption.

Advanced Zone Manager Configuration

The `system.properties` file contains configuration directives for the software such as web server ports configuration, SSL keystore and certificate password, and Memory Allocation Configuration when the service is started. Changes made to {Zone Manager Install Directory}\conf including this file are preserved when Zone Manager is upgraded.

Additionally directives can be modified and added by hand that will change the behavior of the software. It may be beneficial to have {Zone Manager Install Directory}\conf included in the regular backup regimen of the server. All other unique information for Zone Manager other than what is contained in this file is stored {Zone Manager Install Directory}\zonemgr.datadir.

NOTE: The SSL key is stored in the {Zone Manager Install Directory}\conf directory.

Allocating Memory to Zone Manager

By default the amount of memory that is allocated to the Zone Manager software is configured for medium sized deployments. For the vast majority of installations this amount of memory is sufficient, but if the number of tags exceeds roughly 30,000 or tags can be seen by a large number of readers at one time, additional memory may be needed to maintain good performance characteristics. Simply adding physical memory to the server that runs Zone Manager may help if swapping is experienced but to fully utilize the free memory the software must be told that it is allowed to use more memory than the default.

To change the amount of memory being used by Zone Manager edit `system.properties` file and change the value of the memory directive. The following example sets the memory footprint to 1GB or 1024MB of memory.

```
wrapper.java.maxmemory=1024
```

The maximum amount of memory that can be allocated to Zone Manager on a 32-bit operating system is 1700MB, but depending on your version of Windows, the operating system may limit the amount of physical memory that can be addressed. In most cases CPU will become the performance bottleneck after around 2GB of RAM is allocated.

Since the location engine must be single threaded, this will look like a single core on the server being fully utilized while other cores are nowhere near capacity. The only way to continue scale at this point is to install a second Zone Manager. This type of condition is generally experienced at around 600,000 tag links or roughly 300,000 tags being seen at one time by an average of two channels each.

Configuring Web Server Ports for Zone Manager

Zone Manager will utilize port 6580 for HTTP traffic and port 6581 for SSL traffic on a new installs. Most web servers run HTTP on port 80 and SSL on port 443, but Zone Manager uses different ports to avoid potential conflicts with existing web server installs. If the server that Zone Manager is running on does not have a web server already using these ports, then Zone Manager can be directed to run on these ports instead of the default ones.

To modify the default HTTP and HTTPS ports, perform the following steps.

1. Shut down the service.
2. Edit the system.properties file and set the port parameters to 80 and 433 (or whatever port is wished).
3. Restart the service.

NOTE: After the service is restarted, Zone Manager will run on the new port settings. However, on localhost, port 6580 will continue to be available for configuring the server through the user interface; the desktop and start menu icons will continue working.

Configuring SSL for Zone Manager

By default, Zone Manager is installed with a self-signed SSL certificate. The self-signed SSL certificate will be created only if the keystore file, {Zone Manager Install Path}\conf\keystore, does not exist. On upgrade, the keystore file will be created if it does not already exist but the HTTPS port will not be turned on.

On the initial install, the self-signed certificate will be created and both the HTTP/HTTPS ports will be enabled.

The default self-signed certificate has the following properties:

- The default keystore password is: rfcode
- The default self-signed certificate password is: rfcode
- The self-signed certificate is valid for 10 years of the installation time.

In the case where users wish to renew the self-signed SSL certificate or obtain a digital certificate signed by a trusted authority to Zone Manager, the following guidelines should be followed

To configure Zone Manager to use SSL, perform the following steps:

1. Obtain a digital certificate and install in on the server.
2. Modify server settings to run SSL using the certificate.

The following two additional steps are optional:

3. Turning off the non-SSL HTTP port on the server.
4. Add a security exception to any browsers that may access the server (for self-signed certificates).

Digital certificates provide several features that help accomplish two purposes:

- Encryption – using public/private key pairs.
- Authentication – using digital signatures.

Configuring Zone Manager can be done in one of two ways in order to accomplish either encryption-only security or encryption plus authentication security.

Configuring SSL with a Digital Certificate from a Trusted Authority

Understanding the embedded technologies in Zone Manager is helpful for understanding how to set up SSL.

Zone Manager is a Java-based web application that runs in the Jetty (see <http://docs.codehaus.org/display/JETTY/Jetty+Wiki>) web application server. Since Jetty is the web server, its configuration must be modified to run in SSL mode. Although SSL support for Jetty can be accomplished in several ways, this manual only describes using the Oracle **keytool** program.

- The Java runtime environment (**jre**) used by Jetty can be found at {Zone Manager Install Directory}/jre
- **keytool** can be found at {Zone Manager Install Directory}/jre/bin
- The Jetty web application server can be found at {Zone Manager Install Directory}/jetty

Overview of Sun Microsystems' "Keytool" Program

keytool can be used to create digital certificates, import digital certificates, create and manage keystores, and create and manage truststores. Basic usage instructions are described in the following sections. More detailed instructions can be found at the following website (among others):

<http://docs.codehaus.org/display/JETTY/How+to+configure+SSL>

Modifying SSL Settings

To modify SSL settings, perform the following steps:

1. Browse to {Zone Manager Install Directory}/conf
2. Open the `system.properties` file in a text editor.
3. Add the following properties (key=value pairs)
 - `https.port`
This key=value pair sets the port used for SSL communications.
 - `https.keyStorePassword`
This key=value pair refers to the password of the keystore.
 - `https.certPassword`
This key=value pair refers to the password of the SSL certificate.

NOTE: To deactivate the regular non-SSL HTTP port so that communications to Zone Manager can only occur securely, remove the `http.port` entry (if it exists).

Configuring Zone Manager for Encryption

Zone Manager installs its own self-signed certificate during the initial installation routine. If you wish to install your own self-signed certificate, then use the following steps to configure the server for encryption-only SSL:

1. Use the `keytool` command (`{Zone Manager Install Directory}/jre/bin/keytool`) to create a self-signed digital certificate.

NOTE: In order to use **keytool**, you must provide the following parameters:

- **-genkey**
This parameter tells **keytool** to create a new key.
- **-keystore {Zone Manager Install Directory}/jetty/keystore**
This parameter tells **keytool** where to save the created key and keystore.
- **-alias {name}**
This parameter gives the new key a name.

From the Zone Manager installation directory, issue the following command:

```
jre\bin\keytool -genkey -keystore conf/keystore -alias rfcode
```

The command above generates a key in a DSA algorithm.

Some Certificate Authorities require using RSA key algorithm. The `-keyalg` switch is used to specify key algorithm.

```
jre\bin\keytool -genkey -keystore conf/keystore -keyalg RSA -alias rfcode
```

This command will launch **keytool** to create a new self-signed digital certificate in the keystore file specified (the keystore file will be created if it does not yet exist) and the alias of the generated key will be `rfcode`.

Once launched, **keytool** will ask a series of questions as follows:

- **Enter Keystore Password:** (If this is your first time using **keytool** for this keystore, then the password you enter will be set as the password for the keystore. If the password has already been set for the keystore, then enter the password that was set.)
- **Re-enter new password:** (This will only be asked if this is the first time you are using **keytool** for this keystore.)
- **What is your first and last name?**
- **What is the name of your organizational unit?** (I.e. the department name, etc.)
- **What is the name of your organization?** (I.e. company name, etc.)
- **What is the name of your City or Locality?**
- **What is the name of your State or Province?**

- **What is the two-letter country code for this unit?**
- 2. To confirm that the information you entered is correct, press the [Y] key and then [Enter].
The digital certificate will be prompted for a password for your new certificate and the certificate will be created in the keystore you specified.
- 3. Using your web browser, navigate to the Zone Manager server using the port specified in the {Zone Manager Install Directory}/conf/system.properties file.

NOTE: Because your digital certificate has not been signed by a trusted authority, your browser will likely ask you for a security exception before allowing you to use the site. If you grant this security exception, you will have an encrypted stream of data between the browser and the server, but without obtaining a signed certificate from a trusted authority, SSL authentication rules will not be enforced.

NOTE: To obtain a signed certificate, refer to the following section: [Configuring Zone Manager for Both Encryption and Authentication](#).

Configuring Zone Manager for Both Encryption and Authentication

If authentication is desired in addition to encryption, your digital certificate must be digitally signed by a well-known certificate authority. Each web browser or other SSL client commonly maintains a list of well-known authorities such as AddTrust, Entrust, GeoTrust, RSA Data Security, Thawte, VISA, ValiCert, VeriSign, beTRUSTed, among others.

In order to get a digital certificate signed by a trusted authority, use **keytool** to create a certificate signing request (CSR).

The process for creating a CSR is very similar to the process for creating a self-signed certificate, except that instead of passing the **-genkey** command to **keytool**, you pass the **-certreq** command and use the **-file** parameter {and then the name the output file that the commands will create}:

```
jre\bin\keytool -certreq -keystore conf/keystore -alias rfcode -file conf/rfcode.csr
```

This command creates a file called **rfcode.csr** in the **conf** directory.

Then, follow the instructions of the trusted certificate authority that will sign the certificate, which will include sending the **.csr** file to them to be signed.

When the certificate authority issues a certificate based on the CSR request, a file in PEM format will be returned. You must then import the PEM file into the Zone Manager server keystore, i.e. save the certificate in the **conf** directory. Then, use **keytool** to import certificate with the following command:

```
jre\bin\keytool -keystore conf/keystore -import -alias rfcode -file conf/rfcode.crt -trustcacerts
```

Once the digitally signed certificate is installed in the keystore, turn on SSL support in Jetty and then restart the Zone Manager service.

With a digitally signed certificate from a trusted authority installed, your browser should use the certificate without complaint.

Importing a Third-Party Root Certification Authority Certificate to Zone Manager

The Java library that comes with Zone Manager by default includes well-known third-party Root CA Authorities as mentioned in Configuring Zone Manager for Both Encryption and Authentication. If the SSL certificate of the target web server is included in Java library, the following command is unnecessary. However, if the SSL certificate installed on the target web server is not issued by any authorities in the Java library, you can manually import a Root CA certificate for that authority to the keystore in Zone Manager with the following command:

```
jre\bin\keytool -importcert -file <Root CA certificate file> -keystore conf\keystore
```

NOTE: When you upgrade Zone Manager, you do not need to re-import the Root CA certificate.

Warranty & Service

Limited Standard Warranty Terms

RF Code warrants its products to be free from defects in materials and workmanship for a period of 1 year (12 months) for hardware and software from the date of purchase from RF Code. Its obligation under this warranty is limited to repairing or replacing, at its own sole option, any such defective products. This warranty does not apply to equipment that has been damaged by accident, negligence, or misapplication or has been altered or modified in any way. This warranty applies only to the original purchaser (end-user) and is non-transferable.

Standard Warranty Limitations

Except as provided herein, the entire liability of RF Code and its suppliers under this limited warranty will be that RF Code will use reasonable efforts to repair or replace, without charge, all defective Products returned to RF Code by a Customer, as more particularly described in the End User Warranty. Except for the express warranties STATED HEREIN, RF Code makes no other representations or warranties and RF Code hereby disclaims all other warranties, express, implied, statutory, or otherwise, including without limitation, any warranty of merchantability, non-infringement of third party intellectual property rights, fitness for a particular purpose, performance, satisfactory quality, or arising from a course of dealing, usage or trade practice.

RF Code Support and Professional Services

For additional information about functionality that is not described in this document or is not clear in this document, for help with various technical issues, or for access to utilities, files, and other technical documents, please search the RF Code Support website and then contact RF Code Support.

To access the RF Code Support website, go to:

<http://support.rfcode.com>

If some feature is not inherent in the system, please contact RF Code Professional Services to discuss your specific needs.

For more information about RF Code Professional Services, refer to:

<http://www.rfcode.com/Resources/professional-services.html>.