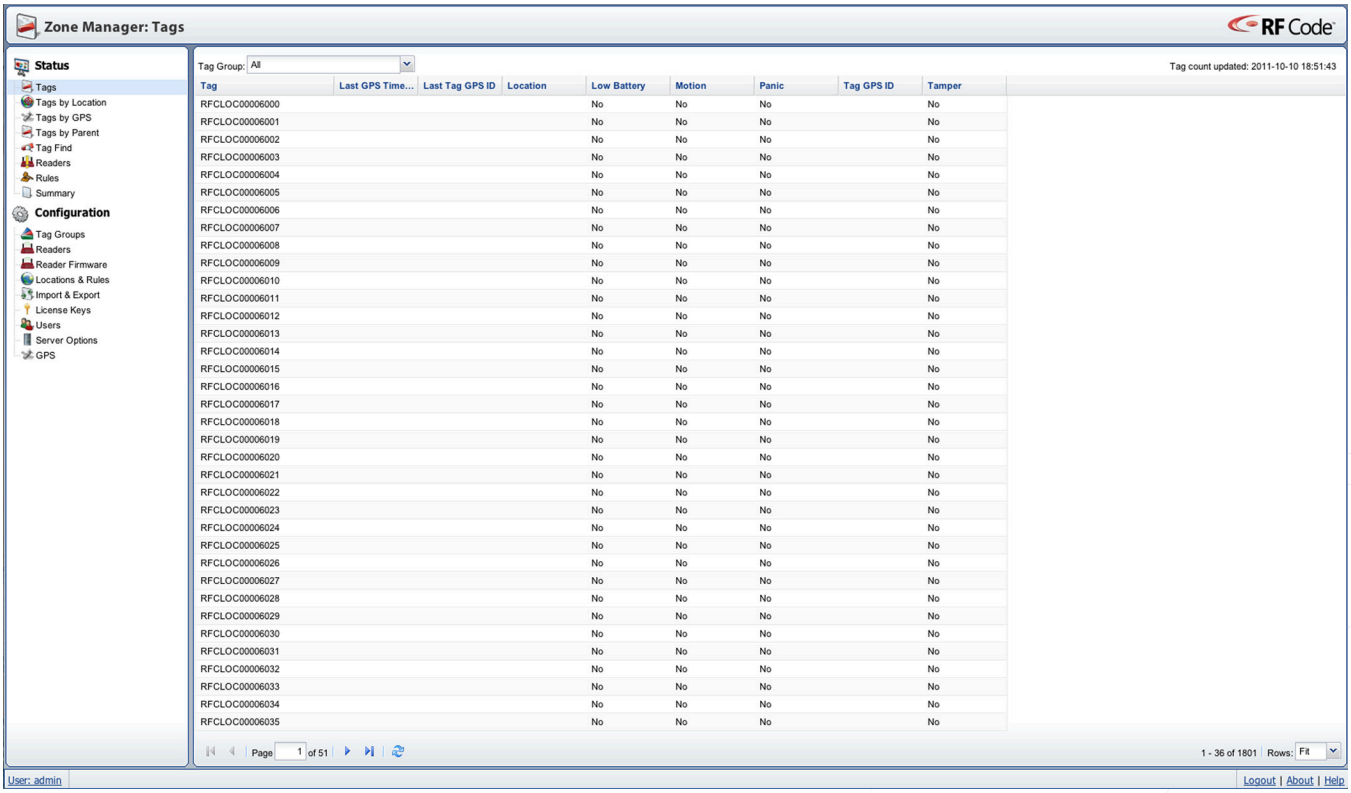
Zone Manager



RF Code™
discover. track. monitor.

User Manual

Contents

Preface 3
- Trademarks 3
- Copyright Statement 3

Zone Manager 4
- Introduction 4
- CD Contents 4
- Requirements 4
- Communication Ports 5
- Installation 5
  - Windows 5
  - Linux 5
- Architecture 5
- Zone Manager Terminology 6
- Configuration 7
- Browser User Interface 10
  - Status Menu 11
  - Configuration Menu 11
  - Help Link 14
- Software Registration 14
- Import/Export 15
- Mass Configuration Import 16

Appendix 17
- Additional Configuration Options 17
- Allocating Memory to Zone Manager 17
- Changing Web Server Ports 17
- Configuring SSL 18
  - Configuring HTTP Port for and Zone Manager 18
  - Configuring SSL for and Zone Manager 18
  - Modifying SSL 19
  - Configuring for Encryption and Authentication 20
  - Importing a 3rd party Root Certification Authority Certificate to Zone Manager 20

Warranty & Service 21
- Limited Standard Warranty Terms 21
- Standard Warranty Limitations 21
- Obtaining Service & Support 21
- RF Code Customer Support 21

Trademarks

RF Code™ 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 implementors 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 © 2008-2010 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

Introduction

Zone Manager is a rules based location engine designed to derive and report information about the location and status of RF Code active RFID tags (both asset tags and environmental sensor tags). 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, RFID middleware applications, or RTLS systems via an open web-based interface specification.

Because RF Code active tags can potentially 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 are determined by each reader or by the Room Locator ID information reported by IR equipped asset tags. In addition to determining tag location, Zone Manager also reports the current value of any sensors that may be present on some RF Code asset tags such as motion, tamper or low battery as well as the sensor readings from RF Code environmental sensor tags such as temperature, humidity, door position, and the presence of fluid.

A consuming application can easily be integrated with Zone Manager to utilize 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 the consuming application is integrated with Zone Manager, it can focus on utilizing the business data without having to implement complex state engines required to process the continuous reporting of tag events from large quantities of RF Code active tags and readers.

CD Contents

The Zone Manager CD-ROM contains several items to assist partners and customers with using the Zone Manager software with RF Code Readers:

- Windows installer executable
- 32 bit Linux RPM
- 64 bit Linux RPM
- TAR.GZ file non-standard Linux installs
- User Manual
- API Reference Document
- Example Deployment Guide
- Sample Configuration Files

Requirements

As the number of tags and readers are added the resources used by Zone Manager also increase. The software is designed for use with up to 1000 readers on a single instance and in certain circumstances can go well beyond that number. The minimum hardware and software requirements below are for up to 50 readers with 10,000 tags. As the scope of the deployment is grows, more memory can be allocated to the system running Zone Manager.

Minimum Requirements:

- Dual Core Intel or AMD Processor
- 512MB of RAM Available to Zone Manager
- Windows Operating System Support
  - Windows 7
  - Windows XP
  - Windows Vista
  - Windows 2003/2008 Server
  - Windows 2008 Server R2(*PV)
  - Must have Administrator Rights
- Notes on Linux Compatibility
  - RPM file provided for RedHat Based Distributions
  - TAR.GZ file provided for any Linux Distribution
  - Tested on Fedora 11, but widely used on various platforms including Ubuntu, SUSE, and Gentoo
- Web Browser Support for Configuration Interface
  - Internet Explorer Version 6, 7, 8 and 9
  - Firefox 3.6 or greater (v6 *PV)
  - Other Browsers like Google Chrome may work but are not tested.

(*PV) –Preferred version. When supporting multiple versions of a single vendor's software, the preferred version was observed to have superior performance and scalability characteristics over other versions that are supported.

Communications Ports

Telnet:
6501 – command & response interface
6502 – tag change events interface
6503 - upconnect
HTTP Port:
6580 – command & response interface
HTTPS Port:
6581 – command & response interface

Installation

Windows Installation

To install the Windows version of Zone Manager browse to the setup.exe file in the \install\windows folder of the Zone Manager CD. Double-click on the setup.exe file to start the Zone Manager installation wizard and follow the wizard's prompts to complete the installation. After the installation is completed the Zone Manager service will be started.

Linux Installation

To install the Linux version of Zone Manager the user must browse to the RPM file in the \install\linux folder of the Zone Manager CD use the following command:

rpm –ivh rfcode-zonemgr-<version-buildID>.noarch.rpm

Note This command will install the software and start the Zone Manager service. The server will be automatically configured to start at boot as well. The Zone Manager service will automatically start on boot up.

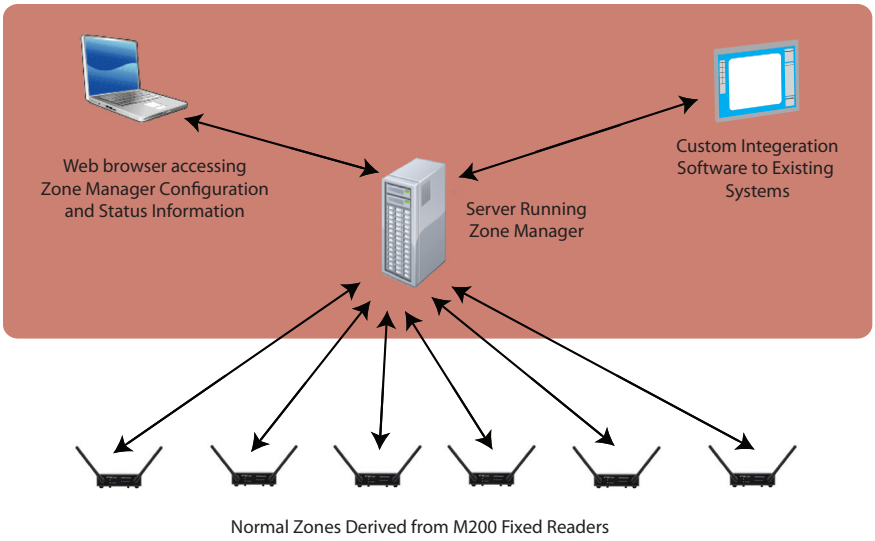
The name of the RPM file may be different depending on the version of Zone Manager being installed.

If you are upgrading from previous version of Zone Manager use the following command:
rpm –Uvh rfcode-zonemgr-1.0.0-20071212_153937_P.noarch

Architecture

When utilizing Zone Manager as part of a custom solution, RFCode fixed readers are deployed where tags must be read and then placed on an IP network. Zone Manager is then installed on either a Windows or Linux based server. Using a web browser, the readers are added to Zone Manager either by adding their IP address to Zone Manager, or by us- ing the reader "up-connect" feature. Additional configuration using a web browser is then needed to create locations, rules and tag groups. Finally a consuming application or middleware is then pointed at the Zone Manager and can then query for tag data or subscribe for updates.

Figure 1: Zone Manager Architecture



Zone Manager Terminology

Listed below are a list of Zone Manager terminology and concepts that are used in the Zone Manager software:

Reader:

- RF Code readers such as the M200, D200, R200.
- Zone Manager only supports IP connections to readers.
- Each reader must be defined (created), then setup (IP address, plus additional parameters).

Tag:

- RF Code active tags such as the M-Series or R-Series tags. Each tag has a unique ID and a group code.

Tag Groups:

- Are the list of tag group codes and corresponding tag treatment codes needed by Zone Manager to interpret tag events correctly.
- All unique tag group codes must be properly configured in Zone Manager.

Locations:

- Define "places" or "areas" inside Zone Manager.
- In its most basic form, a Location is merely a label name.

Location Hierarchies:

- Defines location parent-child relationships.
- This allows Zone Manager to have a Location path such as "Tag 1 is in Rack 5 which is in Row 13 in Data Center A".

Location Attributes:

- Locations can also be defined with additional user defined attributes such as a city name, or a rack type, etc..
- Location Attributes can be defined at any level in the location hierarchy. All children inherit the attributes of their parents.

  Example:
  - ◊ A location called "Data Center A" is created as the top level location (no parent) with a user defined attribute of "city=Austin"
  - ◊ A location called "Row 1" is created with "Data Center A" as its parent with a user defined attribute of "rack type=IBM"
  - ◊ A location called "Rack 3" is created with "Row 1" as its parent with no user defined attributes
  - ◊ A query of all tags in location "Rack 3" would return a list of those tags and all attributes of those tags. The response would look like the following:

    RFCRCK00000012 locationzone=Rack 3, city=Austin, racktype=IBM

Rule Types:

- Rule algorithms that are available for use to build location rules.
- Currently there are three types of rules included with Zone Manager that are commonly used:
  - ◊ SimpleSSIRule - which thresholds on the strongest SSI reported from a set of one or more radio channels associated with the rule
  - ◊ AverageSSIRule - which thresholds on the average SSI reported from a set of one or more radio channels associated with the rule, and requires ALL listed channels to be able to read the tag
  - ◊ IRLocatorRule - which compares the 'irlocator' attribute of tags supporting it with a specific value, and can optionally require that one of a set of channels be able to read the tag

Rules:

- Logic used by Zone Manager that when parameters are met, determines which location (zone) a tag is located in.
- If no rules match, then the tag location is considered unassigned.

Configuration

After installing Zone Manager the following tasks need to be accomplish for a minimal working installation. These tasks may be done using the **Configuration User Interface** by using a web browser at the url:

http://localhost:6580

It is important to note that all configuration done via the user interface can also be accomplished programmatically using functions described in the Zone Manager API document. Once you have accessed the User Interface, the following is a suggested order of configuration steps needed to bring the software up to a basic functional state.

1. **Add Tag Groups**

   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. In most cases both the treatment code and group code are printed on the tag label itself. The ID is user defined and can be anything the user wishes as long as it is unique and an allowed character set.

Figure 2 RF Code Active RFID Tag Labeling



2. **Add Readers**

   Once tag groups are added, any reader that is added will automatically begin reading tags. To add a reader simply add the IP address or hostname of the reader to Zone Manger under the **Reader Configuration Menu**.

   In a normal mode, Zone Manager contacts the reader on the basis of the IP address or hostname set in the reader configuration dialog, but in some cases another method of connectivity is required. In cases where the reader must initiate the connection, *up-connect* is used. The ID of the reader and a login password must be defined for an up-connected reader. Also, the up-connected reader must have the ID and login password entered along with the IP address of the Zone Manager server. This is performed by using the Reader Configuration Utility (please refer to the Reader Configuration Utility User Manual for more information). After adding a reader you will see tags in the **Status views**, but they will not be tied to a location.

3. Add a Location and a Rule

In the **Location and 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. Click on **New Location** and enter a name for a location.

Using the Location that was just created selected, click on **New Rule**. You must name the rule with a unique identifier. RF Code recommends *LOCATIONNAME_RULE* as a naming convention.

The drop down 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 based on the best read by any antenna channel that sees a tag. The *IR locator rule* matches a location based on the Room Locator ID that an IR tag receives.

Use the *Simple SSI rule* and add both the A and B channels of the reader to the rule. After saving the rule, tags in the **Status View** should appear in the newly created location. Experimenting with the *SSI Minimum rule* will allow you to adjust the range of the location. *SSI Threshold* (High Confidence) will come into play when more than one reader see the same tag.

4. Getting Data Programmatically

The API Document has many methods of getting data into and out of Zone Manager. However, a complete solution can be built on just a few commands . For web based data exchange the "tagupdates" URL will accomplish most everything one can need. When using the tag updates URL the first usage should get all the current states of every tag and reader. From that point on usage will retrieve only changes in state.

For the initial query use

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

The sid=5 gives the session an ID. With this Zone Manager can keep track of what tag data each session has received and act accordingly. The number value can be changed to any number, but it is important that if multiple applications are using tag updates that they use different numbers. Otherwise they could lose tag updates. The init=true returns a full list of every tag and its state on Zone Manager.

For each additional query use

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



This will return any changes from the initial state. This query must be issued at least once every two minutes, otherwise the session will expire and init=true must be resent.

The data can be returned in different formats as well:

XML

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

CSV

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

JSON

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

In addition to Location, RF Code Active RFID Tags also support a number of features. Below is a list of features that RF Code Tags support.

Tag reports all have an event type associated with them. The following are tag events may occur.

Tag Event	Description	Notes
Create	The first time a tag is reported on the updates channel.	In _init=true tags will all be reported as Create even though they will have been on the Zone Manager prior to the request. After the _init, 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. The type and number of attributes that your Zone Manager reports will be dependant on the type of tag populations configured in Zone Manager.

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)
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 ways to retrieve data from Zone Manger see the Zone Manager API Specification.

Browser User Interface

Note

To assist you in using the Zone Manager software, a browser-based UI is available. and can be accessed by opening an Internet Browser (i.e. Mozilla Firefox or Internet Explorer) and typing in the URL:

http://hostname:6580/rfcode_zonemgr/

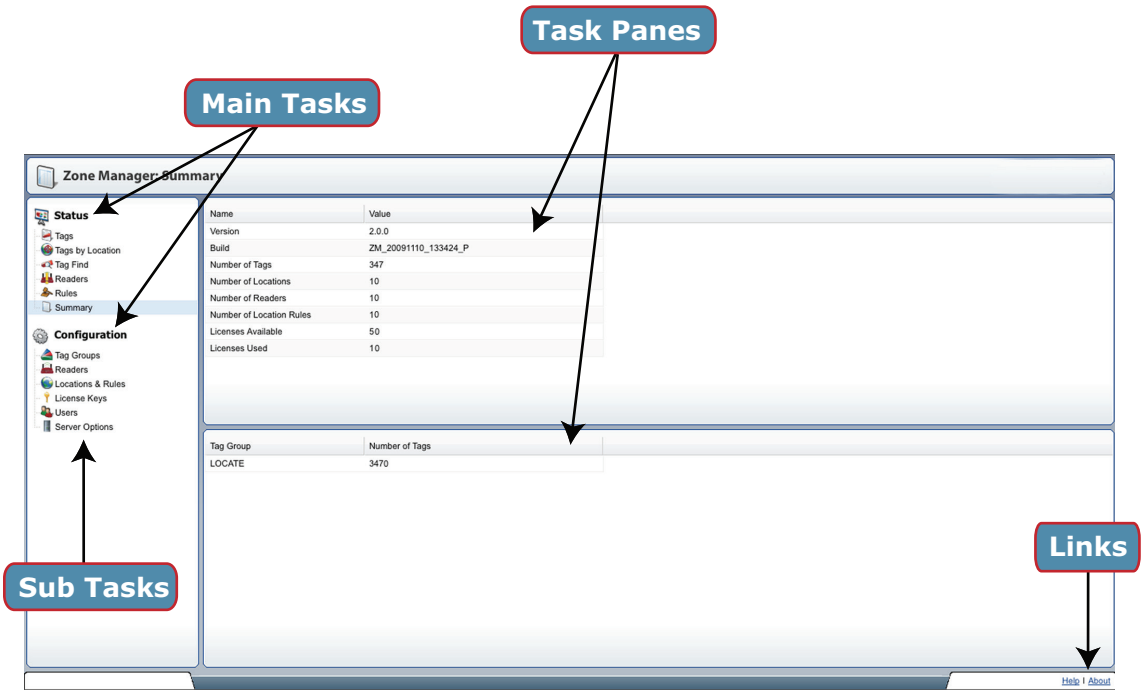
This Zone Manager user interface is for configuring and viewing RF Code Reader and Tag settings. Zone Manager can also be configured using the Telnet or HTTP command interfaces mention above. Below are brief descriptions of the Zone Manager browser-based user interface:

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

- Status
- Configuration

The Zone Manager UI is divided into two main regions, or panes. The left side is the navigation pane where the tasks and sub-tasks are located. To the right of this is the task pane which contains several varying task panes depending on the main and sub-task selected. The Zone Manager UI also contains an information bar on the bottom of the screen, which contains a link to information about the software and a link to the Help file.

Figure 3 Zone Manager UI



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*. *Tags* will provide a status view of all the tags that are recognized by the Zone Manager system. If Locations have been configured, the *Tags by Location* sub-task will allow the user to see the list of tags that are being reported in a particular location. 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. 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 tag (in this case PDU tag) by the Tag ID and will populate the search field with the various children tags (in this case, PDU data points). The *Tags 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. The *Readers* sub-task will allow the user to see the status of all Readers that are configured in Zone Manager. The *Rules* sub-task provides a list of all of the Rules that have been configured for the Zone Manager. Finally, the *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 sub-tasks available: *Tag Groups, Readers, Reader Firmware, Locations & Rules, License Keys, Users, Import/Export, Server Options and GPS*.

The **Tag Groups sub-task** is used to configure the Tag Groups for the Zone Manager as mentioned in Configuration step 1 above. The Readers sub-task is used to configure the Readers for the Zone Manager as mentioned in Configuration step 2. Below is further explanation of the settings that are available for configuration in the **Readers sub-task**.

Reader Information Input Task Pane: 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 you would like the configure the Reader for.

Reader Information Input Task Pane: Control

- Enabled - If you would like your reader to go active and receive and transmit tag data once you configure it, this box should be checked.

Reader Information Input Task Pane: 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).

Reader Information Input Task Pane: Authentication

- User ID - Enter a user ID for the reader.
- Password/Confirm Password - Enter a password and confirm the password.

Reader Information Input Task Pane: Up-Connect Settings

- Up Connection Enabled - If you are configuring an "Up-Connection Reader" that you would like to go active and receive and transmit tag data once you configure it, this box should be checked. (Please refer to the Reader Configuration Utility User Manual for more information)
- Up Connection Reader ID - The ID that was assigned when you configured your reader as an up-connection reader using the Reader Configuration Utility should be entered in this field.
- Up Connection Password - If you assigned a password when you configured your up-connection reader with the Reader Configuration Utility, you will need to enter and confirm the password for use with Zone Manager.

Reader Information Input Task Pane: Position Settings

- Position Source - This field is left at None, if your reader will not use a GPS location. Select Static Position and provide coordinates if you would like to set a static GPS location for the reader. Select Reader GPS if your reader will be connected to a GPS device, to allow for reporting GPS coordinates. Selecting this option will enable GPS Settings to be configured to filter GPS data.

Reader Information Input Task Pane: Advanced

- 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 <min-ssi-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 Box - 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 Box - enables the reader to report whichever channel gets the strongest signal from the tag. This is good for reducing bandwidth consumption.

Reader Information Input Task Pane: Reader Partitioning

- 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.

Reader Information Input Task Pane: 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.

Reader Information Input Task Pane: 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.

The **License Key sub-task** is accessed to input the user license code that you were provided with upon purchase of the Zone Manager software. To input the license key code, simply click the **+** button, enter in the key as it appears on the License Key Card and click the **OK** button. The License Key and its expiration date will appear as well as the license key information such as the number of licenses available and used.

The **Users sub-task** can be accessed to configure user settings for the Zone Manager software. By default, the Zone Manager software is installed without any user accounts 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. There are three levels available, Administrator, Config View, or Event view. If you choose to create user accounts, the first user account created MUST BE an administrator account. That administrator can then configure accounts and permission levels for other users. An Administrative user will have full access to both the Configuration and Status menus and sub-tasks. A user that is assigned the Config View user role will have "view-only" access to the Configuration Menu and sub-tasks and will also have access to the Satus Menu and sub-tasks. A user that is assigned Status View will only be able to view and access the Status menu and sub-tasks.

The **Server Options sub-task** allows the user to configure various advanced options for a separate database that can be used with the Zone Manager software. These advanced features are described in the following:

- An Up-Connection feature is available to allow for communication with a consuming application if you are setting up a Zone Manager that is behind a firewall. Up-Connection settings are configured by clicking the **Enabled** check box and entering in the required information and finally clicking on the **Save Changes** button. The Up-Connection Zone Manager ID and password can be any combination of alpha or numeric values you choose.
- Zone Managers have the capability to store (on a local hard drive) tag events if the connection to the Zone Manager is interrupted and then forward the stored events 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 worth of data events that will be captured and stored until the reconnection.
- For the Expected Location Bias setting you can specify the confidence factor that you would like added to the expected locations rule.
- The Zone Manager software allows for IBM Premises server integration. To configure IBM Premises settings check the Enabled box to enable integeration. Also, enter the required information for the following settings:

  IBM Premises Hostname - Enter the IP address of your IBM Premises server.
  - » IBM Premises Port - Enter the port number over which to communicate with your Premises server.
  - » IBM Premises Source ID - Assign an alphanumeric ID for Zone Manager.

- When you have entered your desired configuration settings for the Server Options sub-task, click the **Save Changes** button.

The **Locations & Rules sub-task** is used to configure the Locations & Rules for the Zone Manager as mentioned in Configuration step 3.

Zone Manager has a **Reader Firmware upgrade sub-task** available that will allow for upgrading individual or multiple RF Code Readers at once. To upgrade a RF Code Reader's firmware using Zone Manager, navigate to **Configuration > Reader Firmware**. Zone Manager version 2.1 or later is bundled with the latest reader firmware at the time of release. For future reader firmware upgrade assistance using this task please contact RF Code support:

E-mail: support@rfcode.com
Voice: 512.439.2244 or toll-free at 866.830.4578



It is vital these updates be obtained directly from RF Code or its authorized source, since these files define the operation of the Reader and if defective, the files will render the Reader inoperable. The Reader Firmware updates can be obtained from the RF Code website:

http://www.rfcode.com/Resources/Library/Library.html

The **GPS sub-task** enables the user to adjust the global GPS settings for all GPS devices that are connected to Readers. Select and input desired global GPS settings. Click the **Save Changes** button to save the settings. Below is further explanation of the settings that are available for configuration in the **GPS sub-task**.

Global GPS Defaults: GPS Data Reporting

- LAT - Latitude
- LON - Longitude
- EPE - Estimated Position Error
- SPD - Speed
- ALT - Altitude

Global GPS Defaults: Minimum GPS Update Period

- Input the minimum time period required for GPS data updates. The Asset Manager default is set for 30 seconds.

Global GPS Defaults: Minimum Horizontal Change

- Input the minimum distance required for horizontal change for GPS data updates. The Asset Manager default setting is 10 meters (32.8 feet).

Global GPS Defaults: Minimum Vertical Change

- Input the minimum distance required for vertical change for GPS data updates. The Asset Manager default setting is 100 meters (328.1 feet).

Help Link

This tab provides links to this document (ZoneManager_UserManual.pdf). If you would like more in-depth information regarding the use of the Zone Manager software, please access the Zone Manager API Specifications document that is located on your Zone Manager CD.

Software Registration

Please be sure to register with RF Code to get updated documentation and information regarding upgrades:

http://www.rfcode.com/registration

Import/Export

In order to simplify configuration of large numbers of readers, a Configuration Import/Export task has been designed. 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 "R200".
- **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 asssumed 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.



Please refer to the Zone Manager API Specification document on the CD for updated information regarding column names.

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, use the value "<blank>".

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 "R200, M200, 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.

Note

- The minimal CSV file columns to define a reader, an associated location, and a default AverageSSIRule rule tying the two would include the following columns:

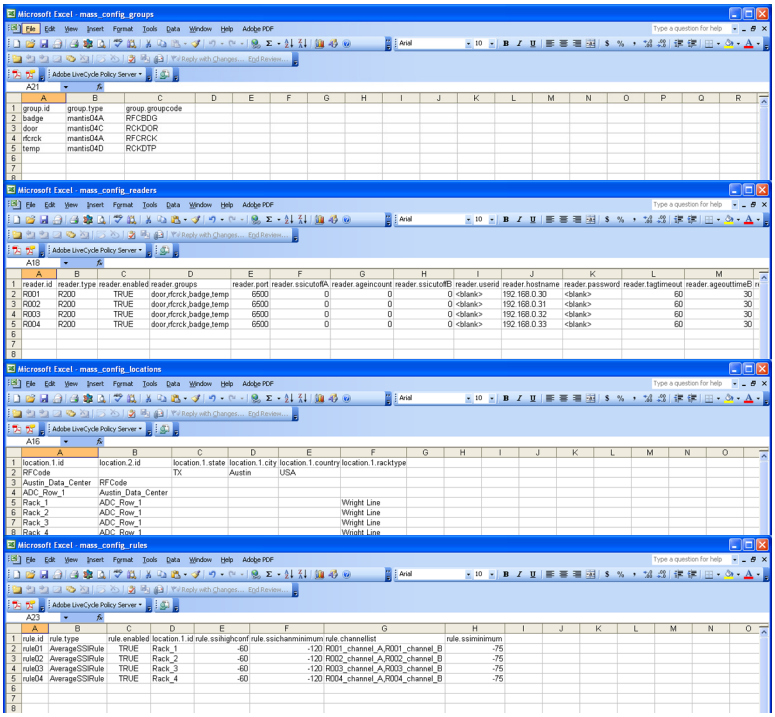
"reader.id","reader.hostname","location.1.id"

- 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 by simply adding another location level column:

"reader.id","reader.hostname","location.1.id","location.2.id"

- The imported CSV files can be updated and imported again to update the created objects (or to create new ones).
- Column names ARE case sensitive, but can have the first letter capitalized (as some spreadsheet tools insist on capitalizing column names). So, "reader.id" and "Reader.id" are acceptable, but "READER.id" is not.
- Using spaces in the column titles will cause an error, therefore they must be named Rack_1 as opposed to Rack 1.
- Having 2 attributes with the same name will also cause an error.
- It is recommended that these Mass Configuration Import files are created as four separate files that are grouped and named according to column name type (groups.csv, readers.csv, locations.csv, rules.csv).

Figure 3 Sample Mass Configuration Import Files



TIP

Please refer to the mass_config sample csv files that are provided with your CD in the \samples directory as an example for your configuration.

Additional Configuration Options

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.



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 exceed 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.

Changing Web Server Ports

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 Manger can be directed to run on these ports instead of the default ones. To do this, the service must be shutdown and the system.properties file modified. The port parameters are then set to 80 and 433 (or whatever port is wished) and the service restarted.

```
http.port=80
https.port=443
```

Once the service is restarted Zone Manager will run on the new port settings, however on localhost, port 6580 will continue to be available to configure the server. This will allow the desktop and start menu icons to continue working.

Configuring SSL

Configuring HTTP port for Zone Manager

By default, Zone Manager uses port 6580 for HTTP and port 6581 for HTTPS communications. Please refer to **Changing Web Server Ports.**

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

Configuring Zone Manager to use SSL involves three steps:

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

Other optional steps include:

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.

Configure SSL using a digital certificate from a trusted authority
Familiarity with the web server setup for Zone Manager is helpful for understanding how to set up SSL.

Zone Manager are Java (see http://java.sun.com) web applications that run in the Jetty (see http://docs.codehaus.org/display/JETTY/Jetty+Wiki) web application server. Since Jetty is the web server, it's configuration must be modified to run in SSL mode. Although Jetty's SSL support can be accomplished in several ways, only configuration using Sun's "keytool" program will be described here.

The Java runtime environment used by Jetty can be found at {Zone Manager Install Dir}/jre
Sun's "keytool" program can be found at {Zone Manager Install Dir}/jre/bin
The Jetty web application server can be found at {Zone Manager Install Dir}/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 will be described below. More detailed instructions can be found at http://docs.codehaus.org/display/JETTY/How+to+configure+SSL.

Modify SSL Settings

Configure the {Zone Manager Install Dir}/conf/system.properties file:

- Open the file in a text editor. In the file you will see a number of properties (key=value pairs).
- To modify SSL settings add the following properties
  - » https.port: Sets the port used for SSL communications
  - » https.keyStorePassword: Refers to the password of the keystore.
  - » https.certPassword: Refers to the password of the SSL certificate
- To deactivate the regular non-SSL HTTP port so that communications to Zone Manager can only occur securely, simply remove the "http.port" property if it exists.

Encryption-Only Configuration

Note that Zone Manager installs its own self-signed certificate at install time. 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 Dir*}/*jre/bin/keytool*) to create a self-signed digital certificate. In order to launch keytool, the following parameters must be provided:
   - **-genkey** (tells keytool to create a new key)
   - **-keystore** {*Zone Manager Install Dir*}/*jetty/keystore* (tells keytool where to save the created key and keystore)
   - **-alias** string (A name to distinguish the key by)

   For Example (running keytool in the Zone Manager installation directory):

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

The above generates a key in DSA algorithm. Some Certificate Authorities require using RSA key algorithm. Use –keyalg to specify key algorithm.

For Example:

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 generated key's alias 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 the password set for the keystore, otherwise enter the password you previously set for the keystore)
Re-enter new password: (This will only be asked if this is the first time using keytool for this keystore)
What is your first and last name? (Enter your first & last name)
What is the name of your organizational unit? (i.e. 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. After this you will be prompted to confirm that the information you entered is correct. After pressing Y {enter} the digital certificate will be prompted for a password for your new certificate, then 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 Dir}/conf/system.properties file. 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 still have an encrypted stream of data between the browser and the server, but without obtaining a signed certificate from a trusted authority (see next section for instructions on getting a signed certificate) SSL authentication rules will not be enforced.

Configuring For 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, the first step is to have keytool create a CSR (Certificate Signing Request). The process for creating a CSR is very similar to the process described in step #1 above for creating a self-signed certificate, except that instead of passing the -genkey command to keytool, you pass the -certreq command and specify the -file {filename} that should be used for the output file. For example:

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

This will create a file called rfcode.csr under 'conf' directory in Zone Manager installation path. Once this file is created, please follow the instructions of the trusted certificate authority that you wish to sign your certificate. These instructions will include sending them the .csr file to be signed.

When the certificate authority issues a certificate based on the CSR request, a file in PEM format will be returned that must be imported into the server keystore. First save the certificate in 'conf' directory in Zone Manager installation path and use keytool to import certificate as follows:

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

Once the digitally signed certificate is installed in the keystore, follow step #2 above to turn on SSL support in jetty then restart the Zone Manager service.

With a digitally signed certificate from a trusted authority, step #3 above should be irrelevant and your browser should naturally use the certificate without complaint.

Importing a 3rd party Root Certification Authority Certificate to Zone Manager

The Java library that comes with Zone Manager by default includes well-known 3rd party Root CA Authorities as mentioned in the **Configuring For Encryption and Authentication section**. If the SSL certificate of the target web server is included in Java library, this step does not apply. In the case where an SSL certificate installed on the target web server is not issued by any authorities in Java library, you may manually import Root CA certificate for that authority to Java library in Zone Manager:

jre\bin\keytool -importcert -file <Root CA certificate file> -keystore jre\lib\security\cacerts



Re-importing a Root CA certificate is required if Zone Manager is upgraded to the next version.

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.

Obtaining Service & Support

For in-warranty service, customers have several options. Customers having difficulty with RF Code products should attempt to solve those problems through RF Code's Technical Support Problem Escalation Process:

First, contact the RF Code representative or other distributor from whom the RF Code product was purchased for information on how to obtain local support.

Second, contact the RF Code Customer Support via e-mail.

Third, contact the RF Code Customer Support via the Support Line.

For product returns, the support engineer will give you a return material authorization (RMA) number. No returns will be accepted without an RMA number. If the warranty expired, there is a charge for repair or replacement per RF Code's out-of-warranty policy. For full details of the RF Code RMA policy, please review the "RF Code Warranty, RMA, and Extended Warranty Policy" document.

RF Code Customer Support

RF Code Customer Support gives entitled customers and partners the ability to contact RF Code about installation and usage-related questions as well as make defect inquiries about eligible products that are covered under RF Code warranty agreements. A team of technical specialists can be contacted electronically or via phone.

The Support Line is available to provide General Support during normal business hours: Monday through Friday, 8:00 am to 5:00 pm Central time, excluding national holidays.

E-mail: support@rfcode.com
Support form: http://www.rfcode.com/Resources/Support/Support-Request.html
Voice: 512.439.2244 or toll-free at 866.830.4578