
ID.ALLOGY Inc.

ID.ALLOGY Inc. RFID Project

QtrMaster Usage Guide

Version: V1.0



1309 CARLING AVENUE
OTTAWA, ONTARIO K1Z 7L3
TEL: 613-722-3232

WWW.BITHEADS.COM

Table of Contents

1. QtrMaster Overview	3
2. Deployment and Configuration	3
2.1. Configuring QtrMaster	4
3. Data Overview	6
4. Web Portal Overview	6
5. Handheld Overview	9
6. Data Import Process	10
6.1. People	10
6.2. Items	11
6.3. Tags	11
6.4. Bulk Import of Items Using Barcodes	12
7. Inventory Audit	13
8. Scheduling Item Events	13

1.QtrMaster Overview

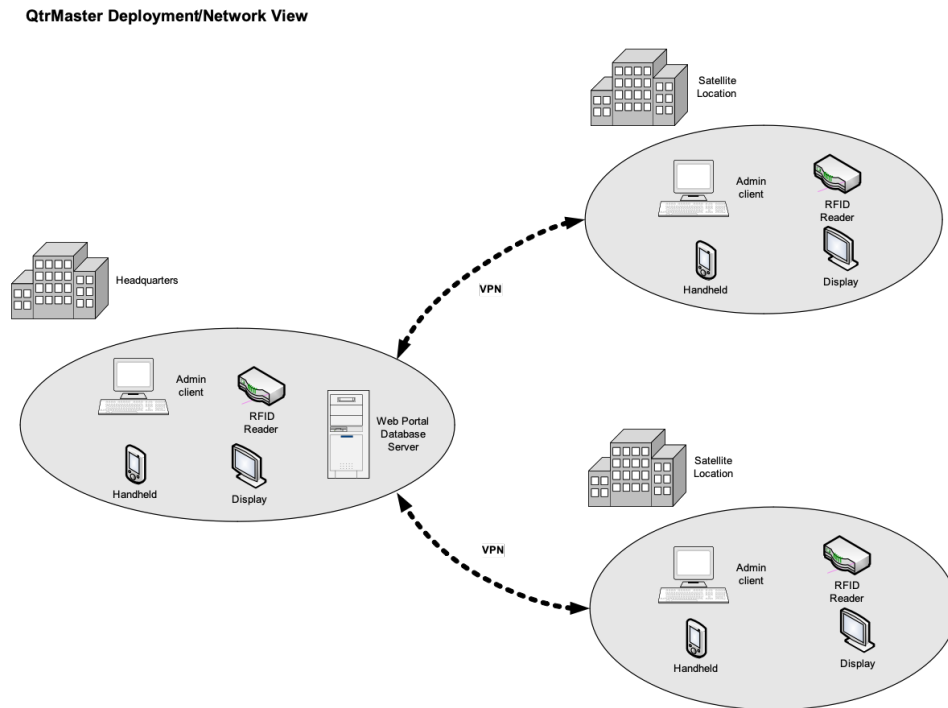
QtrMaster is a revolutionary asset tracking solution that uses RFID technology to capture the egress and return of assets and personnel from an inventory storage location. It allows personnel to simply walk in and out of a storage location, with their required items, without having to manually scan or “sign out” the items in question.

Using the RFID tags carried by the personnel and attached to the items, the system creates a “loan record” for each item in a central database that can be monitored and audited. When the item is returned, the record is updated accordingly.

The system is also able to monitor and track required maintenance operations, and will notify the appropriate resources when an item is due for scheduled maintenance.

2.Deployment and Configuration

QtrMaster can be installed at a single location, but also supports consolidating information from multiple locations into a single database. The system allows you to configure multiple locations and assign each item to a particular location. It will alert the appropriate resources if items are returned to a different location from which they were originally assigned.



2.1. Configuring QtrMaster

Configuring QtrMaster is a straight forward process. The key issue is to ensure all components are on the same network, and if using host names instead of IP addresses, that all devices can properly resolve any domain names being used. If the installation requires multiple locations, each location must also be able to see the QtrMaster server. This is usually achieved using a Virtual Private Network (VPN) to ensure a secure stable connection.

Once the web server portion has been installed, the IP address should be noted, as this will be used by the readers and handheld to communicate with the server.

The address of the server must be added to reader configuration as well as to the handheld. The IP address is added to a configuration file that is loaded into the PII4 device using an SD card. The reader is expected to communicate over port 3002 (ie. 198.168.300.100:3002). The server address is added to the handheld application via the settings screen. The handheld uses the default port to communicate with the server.

QTRMaster will have the following folder structure when installed:

<root of your install>

- / certs
- / config
- / dbdata
- / itemsimg
- / license
- / peopleimg

These folders hold the following information:

/ **cert** - this folder is used to store the SSL certificates if HTTPS is to be used. See *AppConfig.json* below.

/ **config** – this folder contains the file *AppConfig.json*. The content of this file is as follows:

```
JavaScript
{
  "ItemCategoryController" : {
    "imagePath": "/public/itemsimg",
    "imageUrl": "http://qtrmaster.my-company.local:3000/itemsimg/"1,
    "destinationField": "picture",
    "generateFileName" : true2
  },
  "PersonController" : {
    "imagePath": "/public/peopleimg",
    "imageUrl": "http://qtrmaster.my-company.local:3000/peopleimg/"3,
    "destinationField": "picture",
    "generateFileName" : true2
  },
  "ConfigController": {
    "imagePath": "/public/img",
    "imageUrl": "http://qtrmaster.my-company.local:3000/img/"4,
    "destinationField": "picture",
```

```
"generateFileName" : false2
},
"Api" : {
  "serverAddress":"http://qtrmaster.my-company.local"5,
  "port": 30005b,
  "cert":"/var/certs/bqtrmaster.my-company.local.crt"6,
  "key":"/var/certs/qtrmaster.my-company.local.key"7,
  "auditdir":"../",
  "tokenExpires":18008
},
"PersonLookup" : {
  "nobodyId":"1"9
},
"Terminal" : {
  "server": "server",
  "port":3001,
  "pem":"/var/RFIDLoan-CA.pem"10,
  "cert":"/var/certs/qtrmaster.my-company.local.crt"6,
  "key":"/var/certs/qtrmaster.my-company.local.key"7
},
"Nodemailer": {
  "host": "smtp.my-company.local"11,
  "port": 25,
  "secure": false,
  "ignoreTLS" : true
},
"ReaderServiceHost": "reader"12
"Scheduler": {
  "jobs": [
    {
      "name":"Maintenance",
      "url": "http://server/maintenance_check"13,
      "sched": "0 0 23 * * *"
    },
    {
      "name":"LateReturns",
      "url": "http://server/loan_check"13,
      "sched": "0 */1 * * * *"
    }
  ]
}
}
```

¹ The URL that the browser (Dashboard) and terminal can use to retrieve and display items image.

² Flag to indicate if you want the images name to be anonymized upon upload to server.

³ The URL that the browser (Dashboard) and terminal can use to retrieve and display people image.

⁴ The URL that the browser (Dashboard) and terminal can use to retrieve and display brandings image.

⁵ The URL to access the Dashboard. This will be used by the Terminal when the user enters Reasons when items are missing.

^{6,7} The Certificate and Private Keys for SSL support on the Dashboard URL. The folder (/var/certs/) should not be changed, only the file name should be adjusted.

- ⁸ The length of a user session in the Dashboard in seconds.
- ⁹ The id of the person to use when a scan fails to detect a person type tag, so that the loan or returns get associated.
- ¹⁰ If using self-signed certificate, this will be used by the server to accept connection to the Terminal service. If the cert is not self-signed, this line should be removed.
- ¹¹ The STMP mail server details here - see <https://nodemailer.com/smtp/>
- ¹² The host name of the reader service.
- ¹³ The URL to trigger for maintenance checks and late returns, only adjust the http or https part as required, leave the rest as is.

3.Data Overview

The primary data entities within QtrMaster are administrators, devices, people, locations, item categories, and items.

Administrators are the actual users of the portal, and require login accounts to access the functionality they require. These users belong to predefined roles: administrators, auditors, observers and maintenance. Administrators have full access to all of the functionality and information within the portal. You must be an administrator to create other user accounts. If an administrator wants to receive notifications, they must also have a “people” record created.

Devices include the RFID readers and each handheld that is in use at the required locations. For security purposes, the devices must be registered with the portal to be properly authenticated for use.

People are the instances of the users who have an RFID tag associated with them for the purposes of tracking the usage of items. People records should have an image associated with it to be displayed by the terminal when items are borrowed from the storage location.

Locations are where items are stored, and more importantly, where an instance of an RFID reader and terminal are located. There can be multiple locations for a single QtrMaster installation. All items in the system must belong to a location, but can only belong to a single location.

Item Types define the high level description of a class of items. The item type contains the description and image of the item class. This image is what is displayed by the terminal when an item is borrowed from storage.

An item is the physical item that is borrowed and tracked from a storage location. Along with the associated RFID tag, there is typically an additional unique identifier, such as a serial number and/or barcode tag. An item can only belong to one item type, and one location. However, for redundancy, an item can have multiple RFID tags.

4.Web Portal Overview

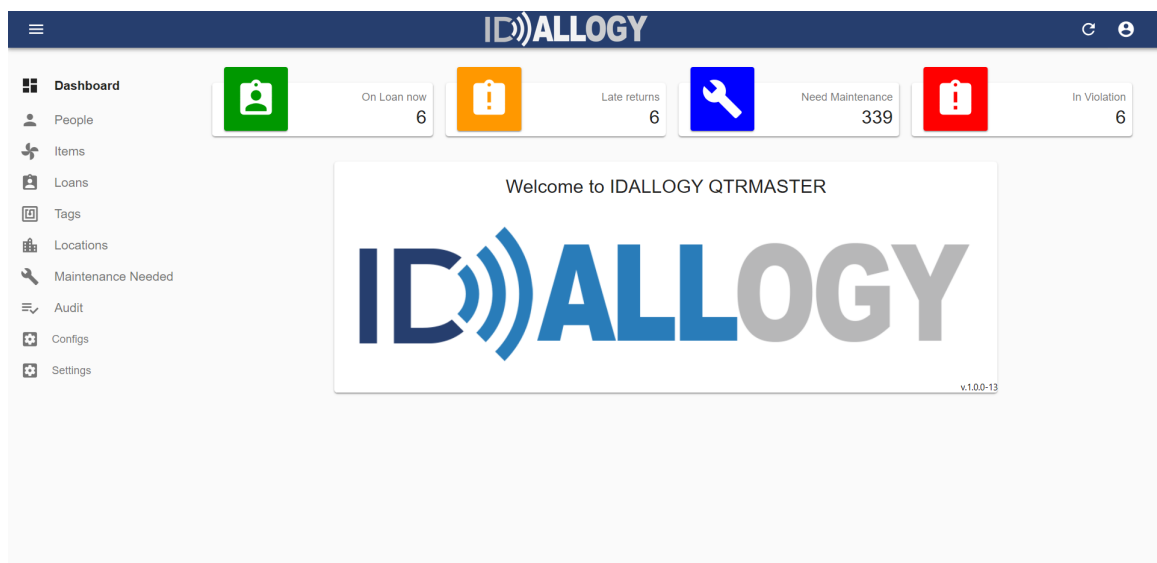
The web portal is the primary interface into QtrMaster. It is used to add information into QtrMaster, such as users, locations and items, and it is also used to review the loan records and maintenance schedules for the actual items. It is designed to work with most standard browsers, such as Edge, Chrome and Firefox.

The portal comes pre-configured with an administrator account called “qtrmaster” with a password of “password”. Use this account to create your own administrator account. For security, change the password on the “qtrmaster” account by clicking on the profile icon on the top right of the screen, and **be sure to record the new password**. There are four primary administrator types within the portal:

- Administrator – has full access to all of the functionality within the portal.
- Auditor - Can perform Audit and review Audit in the dashboard.
- Observer - Can only view data related to items loans, locations, and people.
- Maintenance - Can view and perform maintenance tasks on items.

Create a new administrator account by clicking on **Settings->Administrators** and clicking on the **+CREATE** button. You will be prompted for the Username, Password and the type of administrator account to create.

Upon login, you are presented with the QtrMaster Dashboard, and a set of menu items that correspond with the functionality you are permitted to execute based on the role associated with your credentials. You are also presented with a quick snapshot of the status of items that are currently on loan, or are in need of service maintenance.



You can customize the portal and handheld device by adding your department's logo to the system from the **Settings->Brandings** page.

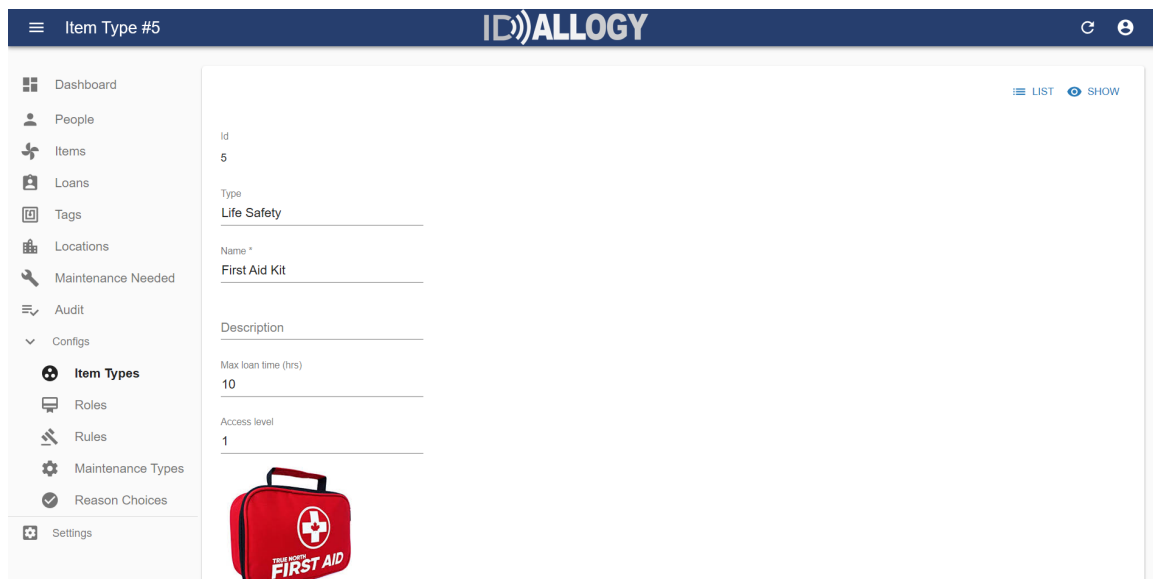
Select the "People" menu item to add a person to the database or to get a list of people currently in the database and their associated tag if they have been assigned one. Before adding a person, ensure that Roles have been defined from the **Configs->Roles** menu item. Roles can be defined as you see fit for your organization, and supervisors for individuals can be selected from the list of people in the database if required. Access levels are associated with Item Types. Users with an Access Level lower than that set for an Item Types are flagged when trying to borrow that item. For instance, if an item (such as a C8) has an access level of 8, only people with access levels of 8 or higher can borrow that item.

Clicking on an existing person to view the detail screen or update the existing information. Ensure that you add a picture of the person so that it displays on the monitor when the person borrows an item. From the detail screen, you can also view the Loans history for this person, and any Notifications that may have been sent by clicking on the tabs in the detail page. If a person is to receive notifications, a Notification Identity must be created that includes the minimum severity level and the email address for notification purposes. **If an administrator needs to receive notifications, they must also have a People record created to define the notification information.**

Select the “**Locations**” menu item to view the list of locations records in the database, or to create a new location. Locations are typically associated with an RFID reader, and are normally where Items will be stored. In order to add items to the database, there has to be at least one location record defined, as each item must be associated with a location.

Before adding Items, you must create a set of Item Types and create a Location for that item. Select **Configs->Item Types** to create the set of item types that are available to be loaned. Access Level is related to the Access Level associated with the users. Users can only borrow items that have an access level equal to or lower than the access level set in their profile.

Ensure that you add a picture of the item so that it displays properly on the monitor when a person borrows that item. See the sample Item Types screen below:



Select the “**Items**” menu item to get a list of items currently in the database. You may also manually add an item from this menu item. You must create the Item Type before creating individual items of that type. Click on an existing item to view and edit the detail information for an item, or to view the loans history and maintenance record for that item. When creating an item, you can specify the type, location, description, and associated identifiers, such as serial numbers or barcode value. The Reason fields are typically used to provide additional information regarding loan incidents after the item has been borrowed.

Select the “**Loans**” menu item to get a list of current and past loans records in the database. Clicking on a specific loan record presented the detailed view, where you can manually mark an item as returned.

Select the “**Tags**” menu item to view a list of current tags and their associated to either people or items. If necessary, you may also manually add a new tag from this menu item.

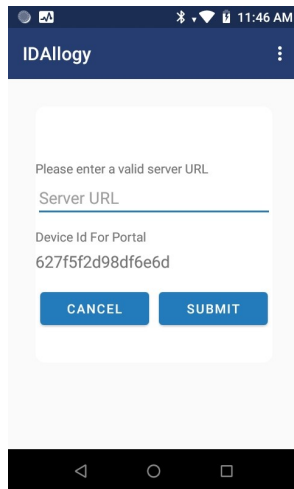
Configs->Rules defines the set of rules that are applied to Items during a loan. QtrMaster comes preloaded with a set of rules already defined. It is strongly recommended that these rules do not get changed. You may create additional rules as you see fit for your particular situations. The rules are applied based on one of four types: all scans, incoming scans, outgoing scans, or on a schedule.

Configs->Maintenance Types allows you to configure required maintenance for your items. Maintenance is applied to an Item Type, so you must define your Item Types before creating Maintenance Types. An item will be flagged for maintenance based on the frequency of usage as defined in the maintenance type record. The maintenance type record contains a Frequency and Frequency Multiplier that can be used in combination to get required values. For example, if an item requires maintenance after 5 loans, select a Frequency of “Loan count”, and a Frequency multiplier of 5.

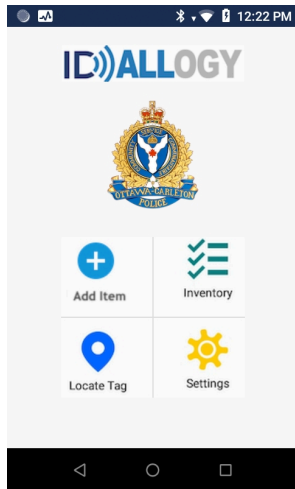
Configs->Reason Choices allows you to define a set of reasons that can be displayed on the loan terminal when an item has not been returned by a user. The reason choices can be presented in the order defined by the Sort value. The Message is the actual text displayed on the Terminal, and is also stored with the Item record, along with any additional text added by the user at loan return time.

5.Handheld Overview

The Handheld device uses a custom application for scanning and inventory audit functionality. Each device must be registered with the portal using the Device Id displayed from the application. Log into the portal using an administrator account and go to **Settings->Scanners** to add a handheld device to the system.



Once the device has been registered using the web portal interface, the web portal IP address must then be added to the handheld application. It can be updated from the settings screen if the server URL changes. You must login to the handheld application using an account that has been configured with Administrator privileges. Upon login, you are presented with a dashboard that looks similar to the following image:



Select Add Item to add individual items or to associate bar codes to RFID tags and upload a list to the server.

Select Inventory to perform an inventory audit for a particular location.

Select Locate Tag to find an individual item based on the RFID tag identifier.

Select Settings to update the URL for the server if it has changed.

6.Data Import Process

The ID.Allogy RFID Data Import Process is designed to allow users to import information into the ID.Allogy database from an existing inventory that has already been categorized. Typically, this existing inventory has been managed using bar codes or other external identification system.

The intent of the data import process is to provide for batch importing of information that resides in external files. The supported data entities are Tags, Items and People. To maintain proper referential integrity within the database, Items and People information must be imported before Tag information.

The end user is responsible for defining the external process that associates an RFID tag with an item or a person.

The suggested process is to create the People and Items data files, by exporting the required information from the existing inventory or HR platforms. It is important to ensure that each item or person has a unique identifier associated with them. This identifier must not already exist in the ID.Allogy database.

A separate corresponding Tags file must be created that maps the tag to the list of people, and list of items. The process for creating this relationship is up to the end user, and will differ from location to location.

Once these files are created, they are to be copied to the server, where an administrator can import the information using the web portal from the **Settings->Imports** area. **The files must be imported in the correct order, with People or Items being imported before the corresponding tags file.**

6.1.People

The structure of the file that contains People information that is being imported into the system is as follows:

```
## People
```csv
name, refNumber, picture, roleName, unit, zone, accessLevel
"Zac Johnson", "123456", "", "Patrol", "Unit1", "Downtown", 5
"John R Smith", "223345", "", "Patrol", "Unit1", "Downtown", 5
"Jane Doe", "876542", "JaneDoe.jpg", "SWAT", "Unit1", "Downtown", 6
"John Smith", "77665541", "JohnSmith.jpg", "Supervisor", "Unit1", "Downtown", 10
```

\* roleName: name of the role for this person, must exist in role table.

\* images should be located in the image folder indicated in the "PersonController" section of the *AppConfig.json* file.

## 6.2.Items

The structure of the file that contains Item information that is being imported into the system is as follows:

```
Items
```csv
name, description, itemcategoryName, locationName, serial
"Hand Radio", "", "Radio", "Head Office", 234231
"Hand Radio", "", "Radio", "Head Office", 235533
"C8 Rifle", "", "C8", "Head Office", 3W423231
"C8 Rifle", "", "C8", "Head Office", 3W423334
```

* itemcategoryName: category name for this item, must exist in the item type table.

* locationName: location name for this item, must exist in location table.

6.3.Tags

The Tags file contains the association between an RFID tag and either a person, or an item. The "refnumber" field will typically be a badge or employee number for "people", and the "itemSerial" will be a serial number or a bar code for "items".

The structure of the file that contains Tags information that is being imported into the system is as follows:

```
## Tags
```csv for items
```

id, type, itemName, itemSerial

## Sample for items

"E123453453543455", "Flex Wing", "Portable Radio", "AB1267GF86"

"E725264074636793", "Flex Wing", "First Aid Kit", "GY6253890"

```csv for People

id, type, personName, refnumber

Sample for people

"E267394528347254", "Flex Wing", "John R Smith", "1236765"

"E862543648294745", "Flex Wing", "John Smith", "HR15645"

"E474637499264578", "Flex Wing", "Jane Doe", "ADG87642"

* id: the Tag unique id a.k.a. EPC (required)

* type: a text description of the tag type (optional)

* itemName: the name of the item associated with this tag (optional)

* itemSerial: the serial number of the item associated with this tag (optional)

* personName: the name of the person associated with this tag (optional)

NOTE: If association of items or person is to be done tags must be imported after People and Items.

6.4.Bulk Import of Items Using Barcodes

An existing inventory that is tagged using barcodes can be imported into QtrMaster using the following process:

- Create an items file that identifies each item, using the existing barcode as the unique identifier. Ensure that itemcategoryName and locationName already exist in the database.
- Login to the server with administrator privileges and import the items file from the **Settings->Imports** menu
- Using the handheld, scan each item barcode and associate an RFID tag with each item, affixing the tag to the item as part of the process.
- When all of the items have been tagged with an RFID tag, and the barcode has been associated with the tag, submit the information to the server to be processed.
- Login to the server with administrator privileges and select **Settings->Provisions** from the menu.
- You are presented with a list of Manual and Barcode uploads. Click on the required Barcode record.
- Each item will indicate its status, as well as the ability to import items that are ready for import. You may import individual items, or choose the import the entire list.

7.Inventory Audit

An administrator may perform an inventory audit using the handheld application. The intent of this process is to ensure that the database accurately reflects the current status of all items that are in the storage location. It is assumed that server access is available to the handheld, either via wifi or direct Ethernet connection to the correct network.

The handheld device communicates with the central server via http. The application has a configuration screen that allows the user to enter the URL that points to the QtrMaster server. Use the “connection test” feature on the handheld to ensure that the server address has been properly entered into the settings.

Upon launching the handheld application, the user will be prompted to login, and the application will verify that the user has authority to perform an inventory audit. Once the user is authenticated, select Inventory from the dashboard. The application will request a list of locations from the server, which can then be used to identify which location is being audited. After the user selects a location from the list, the application will download a list of all items for the selected location and notify the user once the list has been loaded onto the handheld.

The user can then use the handheld to begin scanning all of the items in the room. Once all of the items have been scanned, the user selects “verify inventory”. The handheld will then compare the list of items scanned against the list of items loaded from the server for that location. It will identify which items are in the database, but not at the location, and which items are at the location, but not in the database. It will also indicate which items are currently known to be out with an active user.

For each of those items in the database but not at the location, the user will have the option of performing a single item scan of the location to try and find the item. The application will request the item detail information from the server to assist in locating the item (i.e. radio, flashlight, pistol, etc.).

For those items at the location, but not in the database, the user will have the option of provisioning them into the database. The application will present a form that allows the user to input the item information, along with the RFID Tag ID, and save it on the server.

Once processing of all the items in the list is complete, the user can then mark the inventory audit as complete. This will create an inventory audit record on the server, along with the pertinent information about the audit.

8.Scheduling Item Events

Items can be scheduled for maintenance events, as well as have loan deadlines associated with them. The system automatically checks for scheduled maintenance once a day, and checks for loan expiries every hour.

To schedule a loan expiry, navigate to the item type detail by clicking on **Configs->Item Types** and selecting the item type in question, or create a new Item Type. Click on the Edit button, and update the Maxloantime field to the number of days an item can be borrowed.

To schedule a maintenance event, select **Configs->Maintenance Types**, and create or select an existing maintenance record. Maintenance events are creating for existing Item Types. Set the frequency and frequency multiplier based on your specific needs.