



## INTEGRITI MOBILE READER COMMUNICATIONS HANDLER

*Created using Integrati Pro v18.1.0 software and Inner Range Mobile Reader App v1.0.35*



**INNER RANGE recommends that all Inner Range systems  
be installed & maintained by FACTORY CERTIFIED  
TECHNICIANS.**

**For a list of Accredited Dealers in your area refer to the  
Inner Range Website.**

**<http://www.innerrange.com>**

---

# *Integriti Mobile Reader Communications Handler*

---

## **Description of the Mobile Reader Communications Handler:**

---



The Inner Range Mobile Reader is an Android smartphone application that allows security personnel to view and verify cardholder details with a simple scan of a user's access card. The app requires no additional hardware since it uses the smartphone's NFC technology to read the unique card serial numbers of MIFARE DESFire© EV1 & EV2 cards. Mobile Reader supports Inner Range SIFER cards and HID DESFire© cards.

The Mobile Reader Communications Handler provides a high level interface between the Integriti controller and the Mobile Reader App.

The MOBILE READER Communications Handler also processes incoming messages from MOBILE READER and can update the relevant Integriti entities.

The MOBILE READER Communications Handler requires the following;

- The Inner Range Mobile Reader App (Available from the Android Play Store)
- One IR-996927 interface license is required for each Mobile Device with App.
- SIFER Card Enrolment Station (IR-994751AU)

## Features:

---

### **User Identification:**

On presentation of a valid card, Mobile Reader displays the user photo, user location, card status and additional user and card information. The information displayed can be configured from the Integriti Server to include any user properties, card properties and custom fields such as Employee ID, Student ID, and Department.

Mobile Reader can be set to the specific location or area where the smartphone is located. When user information is displayed the user's location will be displayed in red if it does not match the device location. This allows security personnel to identify users that may have entered areas without authorisation.

### **Suspending Cards:**

If a user doesn't match the cardholder photo, security personnel can immediately suspend the card from the Mobile Reader application. The suspended card will no longer provide access to any doors until reactivated from the Integriti Server.

### **Emergency Muster:**

In the event of an emergency, Mobile Reader can be used as a "check-in" reader at an emergency mustering assembly point. The operator can select a muster point location and areas that are being evacuated. Multiple smartphones running Mobile Reader can be used collaboratively during an emergency evacuation.

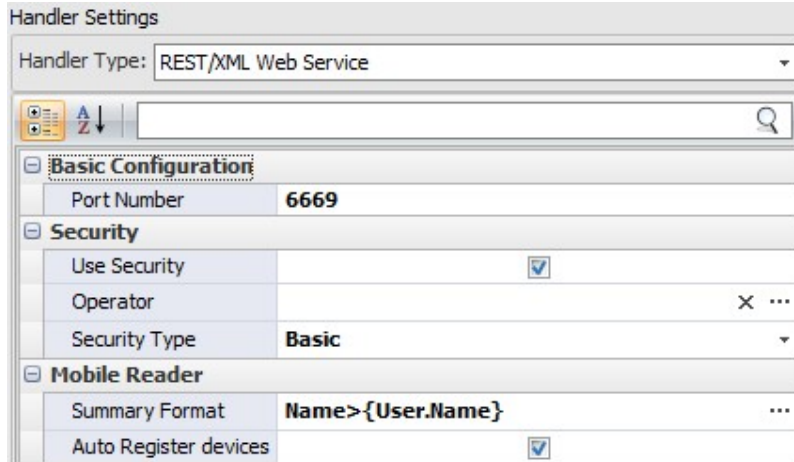
As users present their cards at the "check-in" reader, their location is updated to the muster point. In muster mode the app displays the number of users still inside the evacuation areas, the number of users at the muster point and the total number of users at all muster points.

Mobile Reader provides a scrollable list of all users still inside an area or building as well as their last known location. Additionally, an operator can search for users by name to quickly determine their last known location. Access to this critical information provides emergency services with accurate information for a focused and timely response.

## Configuring the Communications Handler


To create the Communications Handler, follow the procedure below.

1. Open the  panel from the  tab.
2. Click the  button to create a new communications handler.



Handler Settings	
Handler Type:	REST/XML Web Service
<div style="border: 1px solid gray; padding: 2px;"> <span>Basic Configuration</span> </div>	
Port Number	6669
<div style="border: 1px solid gray; padding: 2px;"> <span>Security</span> </div>	
Use Security	<input checked="" type="checkbox"/>
Operator	<input type="text"/> x ...
Security Type	Basic
<div style="border: 1px solid gray; padding: 2px;"> <span>Mobile Reader</span> </div>	
Summary Format	Name>{User.Name} ...
Auto Register devices	<input checked="" type="checkbox"/>

Figure 1



3. Give the review sender a Name and add any necessary details in the Notes field.
4. Choose a “Handler Type” of Rest/XML Web Service.
5. Set up parameters as follows:
  - Choose a port to connect to (or leave this at the default port).
  - Select your level of security ‘Use Security’.
    - If ‘Use Security’ is not checked, every client can access the XML API (you can of course limit access on a network level). In that case, if you set an operator, every API action is tunnelled through that operator, so in case that operator has no permissions on certain entities and/or certain operations, the API command will not execute (or will execute but return none or partial results, depends on the case).
    - If ‘Use Security’ is checked, a client using the API must authenticate by one of the available methods (see below). In that case, if you set an operator, Integriti validates that the operator matches the authenticated given and if not, rejects the API call. If it does match (or if you didn’t set an operator), it performs the requested task under that operator’s credentials, as described.
  - Security Type:
    - Basic - Passwords are sent in clear text.
    - HTTPS - Same as basic but over a secure channel, recommended.
  - If the Security Type is not Basic then you should select an Operator. Click the  to open the list of operators.

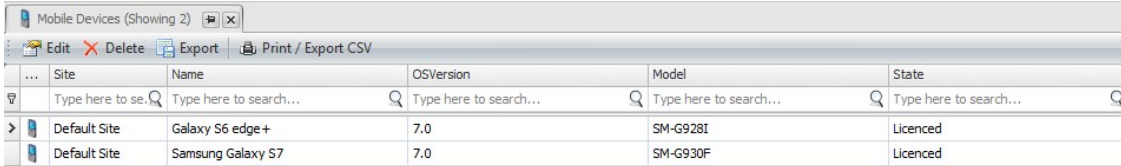
**6.** Mobile Reader specific settings:

- Summary Format – This refers to the information displayed on the Mobile reader app when a card credential is successfully checked. See the **Modifying Summary Format** section for more details.
- Auto Register – With Auto Register enabled, each new mobile device will be registered and have their state set to “Licensed” on first connection until the maximum number of Mobile Reader Licenses is reached.

## Mobile Devices and their state

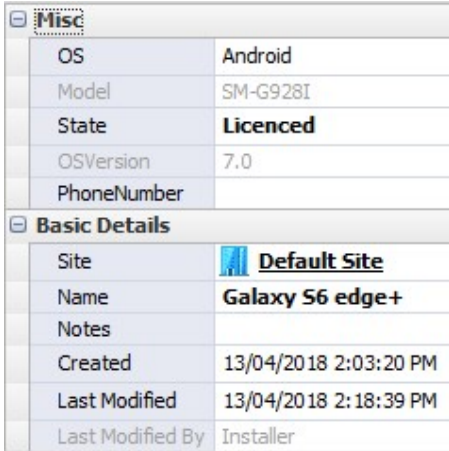
To view Mobile Devices and check their state, follow the procedure below.

1. Open the  **Mobile Device** panel from the  **Administration** tab.
2. Editing a Mobile Device allows the ability to change a given devices state.



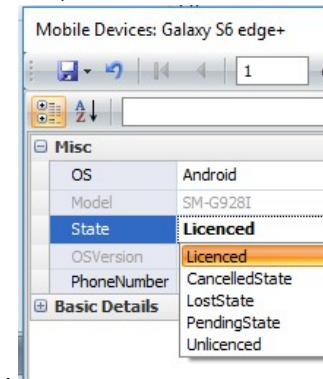
Site	Name	OSVersion	Model	State
Default Site	Galaxy S6 edge+	7.0	SM-G928I	Licenced
Default Site	Samsung Galaxy S7	7.0	SM-G930F	Licenced

3. Selecting a device and clicking on Edit displays the chosen devices settings.



OS	Android
Model	SM-G928I
State	<b>Licenced</b>
OSVersion	7.0
PhoneNumber	
<b>Basic Details</b>	
Site	<b>Default Site</b>
Name	<b>Galaxy S6 edge+</b>
Notes	
Created	13/04/2018 2:03:20 PM
Last Modified	13/04/2018 2:18:39 PM
Last Modified By	Installer

4. Selecting the drop down arrow next to State allows any device to quickly be placed in any other state, as shown.




OS	Android
Model	SM-G928I
State	<b>Licenced</b>
OSVersion	Licenced
PhoneNumber	CancelledState
<b>Basic Details</b>	
	LostState
	PendingState
	Unlicenced



## Card Enrolment

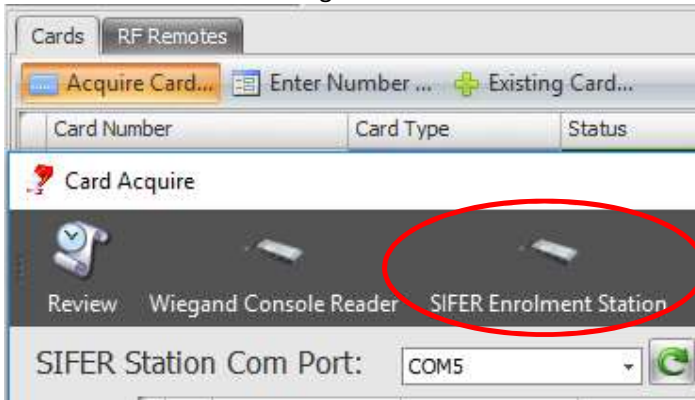
The SIFER Card Enrolment Station is designed to conveniently allow SIFER cards to be enrolled into an Inner Range Integrity system at a computer workstation using the Integrity software. This allows system administrators to enroll new SIFER cards into the Integrity system without the need to physically enter the card data into the system.



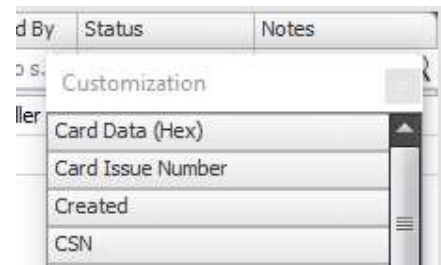
 For existing sites wishing to use the Mobile Reader functionality all cards used on site must have been enrolled using the SIFER Card Enrolment Station either initially or via re-enrolment.

1. Connect the SIFER Card Enrolment Station to the workstation running System Designer or Gatekeeper

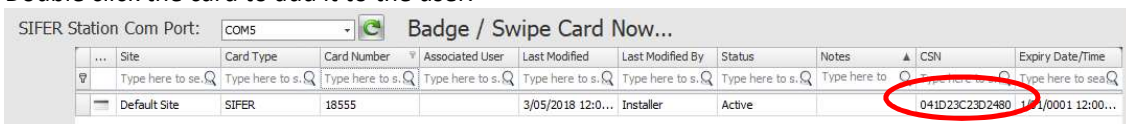
2. Navigate to  under the  tab and select the user that you wish to add a card to.
3. Using the Acquire Card option, cards can then be presented at the Enrolment station and selected in the list to be assigned to the chosen user.



4. Once SIFER Enrolment Station is selected both the large and small LED's on the SIFER Reader should turn blue to indicate that connection is active and ready for card presentation.
5. Ensure that the CSN column is visible, if not enable it from the column chooser menu by right clicking.



6. Badge the card at the enrolment station and observe the card data being displayed in the list.
7. Double click the card to add it to the user.

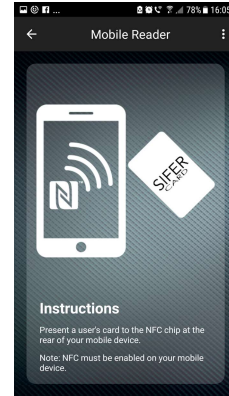


8. When presenting the same card to Mobile Reader the associated user's information can now be correctly returned from the Integrity Server.

## Connecting Mobile Reader to the Integriti Server

Start the Mobile reader app on the Android device.

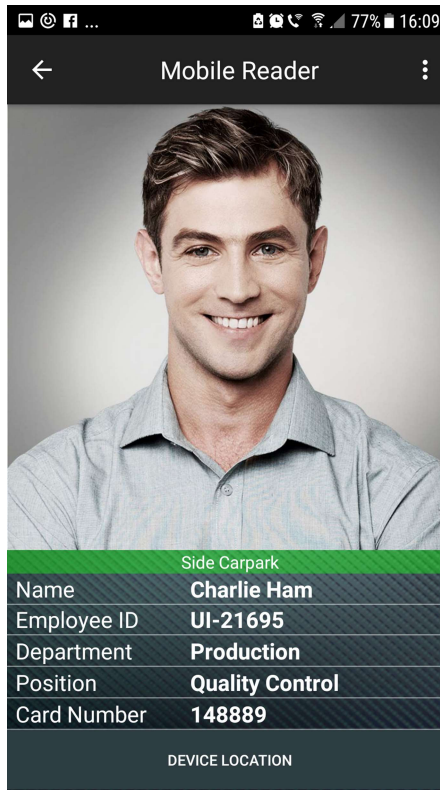
1. Enter the login credentials of the Operator specified in the Comms Handler settings.
2. Enter the IP address and Port number of the Integriti Server to connect to.
3. Login



## Checking a user's credential

Start the Mobile Reader app on the Android device.

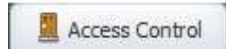
1. Once logged in badge a user's card at the Mobile Reader.
2. The user's credential will then be checked and displayed on the Mobile reader app.





## Mobile Muster

Mobile Reader muster requires Locations to be created that are enabled as muster point's. In order to move current onsite users into muster locations a Location List must be created.

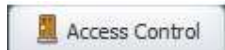


1. Open the **Locations** panel from the **Access Control** tab.
2. Click **+ Add New** and enter a Name for the muster Location .
3. Under General enable Muster point .

General	
Muster point	<input checked="" type="checkbox"/>
Maximum User Count	0
High User Count	0



Muster locations are specific points set out for emergency situations throughout a site. i.e The fire assembly area.



4. Open the **Location List** panel from the **Access Control** tab.
5. Click **+ Add New** and enter a Name for the Location List.
6. Next Add the areas of a specific building/site to the Location List that are required to be included in the Mobile Reader muster count.

Controller Name	Address	Name
New Controller 'SC00939Z'	A1	Area 1
New Controller 'SC00939Z'	A2	Lower Level Area
New Controller 'SC00939Z'	A4	Reception
.....		
New Controller 'SC00939Z'	A3	Casuarina Area
	L1	Muster Location 1
	L2	Muster Location 2
	L3	Muster Location 3

7 of 7 Areas shown (3 in list / 4 not in list)

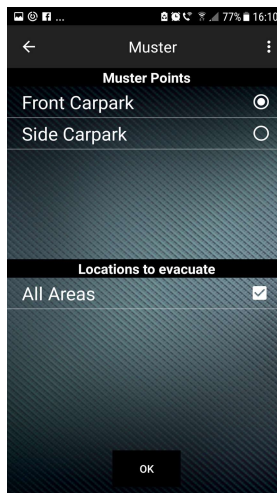
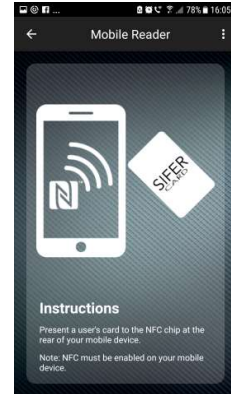


A Location List contains areas of a building or site that you wish to perform a muster on, The Location List cannot contain the muster locations as the count of the muster is to include onsite users only.

## Performing a Mobile Reader Muster.

Start the Mobile Reader app on the Android device

1. Enter the login credentials of the Operator specified in the Comms Handler settings.
2. Enter the IP address and Port number of the Integriti Server to connect to.
3. Click login then Navigate to Menu>Actions>Muster.
4. When performing a Mobile reader Muster, Select the Muster Point (Location) i.e Fire assembly Area.
5. Followed by the Locations to Evacuate (Location List).



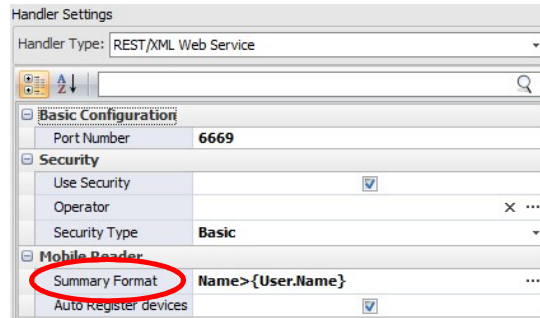
6. Badge each user's cards at the Mobile Reader/s and observe the Number Inside, as each user's card is badged the user's location is then updated to be the chosen Muster Location.
7. The user's location is then also updated in the Integriti Server and Controller/s.



*The User list is capped and displays only the first 200 users.*

## Modifying Summary Format – Information displayed on the Mobile Reader App.

The Summary Format determines which user, card or custom fields are displayed on the app.



### Summary Format Explained:

The user information is displayed in the Mobile Reader app as a 2 column grid. The columns are separated with a “>” character.

**Name>{User.Name}** will be displayed as:

Name	Charlie Ham
------	-------------

Headings can be created by entering a format string that does not contain the > character.

*For example:*

**User Information** will be displayed as:

User Information
------------------

The text of any user, card or custom field that exceeds the length of the column will be wrapped onto the next row.

However, if a field length exceeds two rows the text will be truncated.

*For example:*

A user that has a very long name will be displayed as:

Name	Sean Benjamin Rodgers
------	--------------------------

A user, card or custom field can have a prefix or suffix by adding text before or after the field name in the summary format.

*For example:*

The Employee Id custom field bellow can be prefixed with “UI-” .

**Employee ID>{User.cf\_EmployeeID}**                      Employee ID>**UI-**{User.cf\_EmployeeID}

Lastly fields that use date and time such as USER EXPIRY require specific formatting.

*For Example:*

**Start>{User.StartDateTime:dd / MM / yy H - mm}**

Refer to the following MICROSOFT website for date time format strings.

<https://docs.microsoft.com/en-us/dotnet/standard/base-types/custom-date-and-time-format-strings>

A simpler option to use **f**.

For example:

**Start>{User.StartDateTime:f}** will automatically output the date/time format as.

“Tuesday, April 10, 2018 3:51 PM”

***Below is an example of a configured summary format and how it is displayed in the app:***

