



# On-Ramp Total View Operator Guide

OTV Release 1.2

**On-Ramp Wireless Confidential and Proprietary.** This document is not to be used, disclosed, or distributed to anyone without express written consent from On-Ramp Wireless, Inc. The recipient of this document shall respect the security of this document and maintain the confidentiality of the information it contains. The master copy of this document is stored in electronic format, therefore any hard or soft copy used for distribution purposes must be considered as uncontrolled. Reference should be made to On-Ramp Wireless, Inc. to obtain the latest revision.

On-Ramp Wireless Incorporated  
10920 Via Frontera, Suite 200  
San Diego, CA 92127  
U.S.A.

Copyright © 2015 On-Ramp Wireless, Inc.  
All Rights Reserved.

The information disclosed in this document is proprietary to On-Ramp Wireless, Inc. and is not to be used or disclosed to unauthorized persons without the written consent of On-Ramp Wireless, Inc. The recipient of this document shall respect the security of this document and maintain the confidentiality of the information it contains. The master copy of this document is stored in electronic format, therefore any hard or soft copy used for distribution purposes must be considered as uncontrolled. Reference should be made to On-Ramp Wireless, Inc. to obtain the latest version. By accepting this material the recipient agrees that this material and the information contained therein is to be held in confidence and in trust and will not be used, copied, reproduced in whole or in part, nor its contents revealed in any manner to others without the express written permission of On-Ramp Wireless, Inc.

On-Ramp Wireless, Inc. reserves the right to make changes to the product(s) or information contained herein without notice. No liability is assumed for any damages arising directly or indirectly by their use or application. The information provided in this document is provided on an “as is” basis.

This document contains On-Ramp Wireless, Inc. proprietary information and must be shredded when discarded.

This documentation and the software described in it are copyrighted with all rights reserved. This documentation and the software may not be copied, except as otherwise provided in your software license or as expressly permitted in writing by On-Ramp Wireless, Inc.

Any sample code herein is provided for your convenience and has not been tested or designed to work on any particular system configuration. It is provided “AS IS” and your use of this sample code, whether as provided or with any modification, is at your own risk. On-Ramp Wireless, Inc. undertakes no liability or responsibility with respect to the sample code, and disclaims all warranties, express and implied, including without limitation warranties on merchantability, fitness for a specified purpose, and infringement. On-Ramp Wireless, Inc. reserves all rights in the sample code, and permits use of this sample code only for educational and reference purposes.

This technology and technical data may be subject to U.S. and international export, re-export or transfer (“export”) laws. Diversion contrary to U.S. and international law is strictly prohibited.

RPMA<sup>®</sup> (Random Phase Multiple Access) is a registered trademark of On-Ramp Wireless, Inc.

Other product and brand names may be trademarks or registered trademarks of their respective owners.

On-Ramp Total View Operator Guide

010-0106-00 Rev. D

November 5, 2015

# Contents

---

<b>1 Introduction .....</b>	<b>1</b>
<b>2 On-Ramp Total View Overview .....</b>	<b>2</b>
<b>3 Operating OTV.....</b>	<b>3</b>
3.1 Logging in to OTV .....	3
3.2 Alarms vs. Devices List.....	4
3.3 Device Detail View .....	4
3.4 Devices List.....	5
3.5 Alarms Detail View .....	8
3.5.1 Alarms and Alarm Detail.....	10
3.5.2 Acknowledging Alarms .....	13
3.6 Using Google Maps.....	15
3.7 Exporting Device Data .....	16
3.8 Charting Data .....	17
<b>4 Managing Devices.....</b>	<b>18</b>
4.1 Maintenance/Operational/Out of Service Modes .....	18
4.2 Device Properties/Metadata Import .....	20
4.2.1 Bulk update of Operational State .....	21
4.3 Device Groups .....	22
4.3.1 Adding Devices to a Group through OTV .....	22
4.3.2 Device Group Management .....	22
4.3.3 Device Group Actions.....	23
4.3.4 Importing Devices into a Group.....	23
<b>5 Administering OTV .....</b>	<b>25</b>
5.1 Viewing Reports .....	25
5.2 OTV Notifications .....	28
5.2.1 Notification Groups .....	28
5.2.2 Creating and Editing Notification Groups .....	29
5.3 Understanding Email Alerts .....	30
5.4 Maintaining an Active Directory Account .....	31
5.5 Maintaining a Local Account .....	32
5.5.1 Administrator .....	32
5.5.2 Operator.....	33
5.5.3 Guest Account .....	33
5.5.4 Service Account.....	33
5.5.5 Adding a Local User Account .....	34

5.5.6 Editing a Local User Account .....	37
5.6 Advanced Administration Features .....	38
5.6.1 Adding New Device Types .....	38
5.6.2 Customizing OTV .....	39
<b>Appendix A Sample Config Properties File .....</b>	<b>40</b>
<b>Appendix B Abbreviations and Terms .....</b>	<b>46</b>

## Figures

Figure 1. On-Ramp Wireless RPMA Network.....	2
Figure 2. Device Detail View .....	4
Figure 3. Devices List.....	6
Figure 4. Device Detail .....	7
Figure 5. Clear Alarms Screen.....	8
Figure 6. Alarms Screen with Active Alarms.....	8
Figure 7. Alarms Section on Device Detail .....	11
Figure 8. View All Alarms Page .....	12
Figure 9. Using Date Range on View All Alarms Page.....	13
Figure 10. Alarm Acknowledgement Feature .....	14
Figure 11. Alarm Acknowledgement Confirmation .....	15
Figure 12. Viewing devices in Google Maps.....	16
Figure 13. Sample Gas Pressure Plot .....	17
Figure 14. Maintenance Mode Filter .....	18
Figure 15. Device Properties Page for Maintenance Mode.....	19
Figure 16. Device Properties Page for Operational Mode .....	19
Figure 17. Device Import Feature .....	20
Figure 18. Group Formation Import Feature .....	24
Figure 19. Reports Page .....	25
Figure 20. Status Reports Page.....	26
Figure 21. Active Users Page .....	26
Figure 22. Software Reports Page.....	27
Figure 23. Notifications Page Overview.....	28
Figure 24. Notification Page Buttons .....	29
Figure 25. New Notification Group Example.....	29
Figure 26. Email Notification Example .....	31

Figure 27. “My Profile” Page ..... 34

Figure 28. Adding a User ..... 35

Figure 29. Assigned Device Types Section ..... 36

Figure 30. Editing User Information ..... 37

Figure 31. Configuration Page ..... 38

Tables

Table 1. Device Supplement Documents..... 1

Table 2. Web Browsers That Support All OTV Features ..... 3

Table 3. Alarm and Device State Icons and Descriptions..... 9

Table 4. Operational Mode Behaviors ..... 20

# Revision History

---

Revision	Release Date	Change Description
A	August 21, 2013	Initial draft.
B	March 7, 2014	Updated various procedures for clarification.
C	September 11, 2014	Updated for OTV 1.1.
D	November 5, 2015	Updated for OTV 1.2.

# 1 Introduction

---

This document provides On-Ramp Total View (OTV) administrators and operators with the following information:

- The role of OTV in an RPMA network.
- Account configuration and maintenance for OTV.
- End-device commissioning and configuration using OTV.

Instructions specific to devices used on your network may be found in the corresponding device supplement documents shown in Table 1.

**Table 1. Device Supplement Documents**

Document Title	Document Control Number
OTV Supplement: KONWPT Sensor	010-0069-00
OTV Supplement: Obstruction Lighting (RMU)	010-0097-00
OTV Supplement: Overhead FCI	010-0098-00
OTV Supplement: TransformerIQ-P	010-0099-00
OTV Supplement: Electric AMI	010-0100-00
OTV Supplement: WiYZ Remote	010-0104-00

This document does not provide information on OTV installation. It is assumed that the reader has a basic familiarity with On-Ramp Wireless devices and network concepts.

This document may be used in conjunction with the following publications which are available for On-Ramp Wireless RPMA networks:

- *OTV REST API Guide (010-0038-00)*
- *EMS Operator Guide, System Release 1.4 (010-0045-00)*
- *EMS Operator Guide, System Release 2.1 (010-0107-00)*
- *Network Operational Procedures and Implementation Guidelines, System Release 1.4 (010-0075-00)*

## 2 On-Ramp Total View Overview

On-Ramp Total View (OTV) formats and passes application data from the Gateway to various databases. Application data can then be viewed from the OTV web graphical user interface (GUI) or formatted and delivered to another system or data warehouse for further analytics. OTV's web-based GUI enables application operators to view, list, and sort application data and alarms.

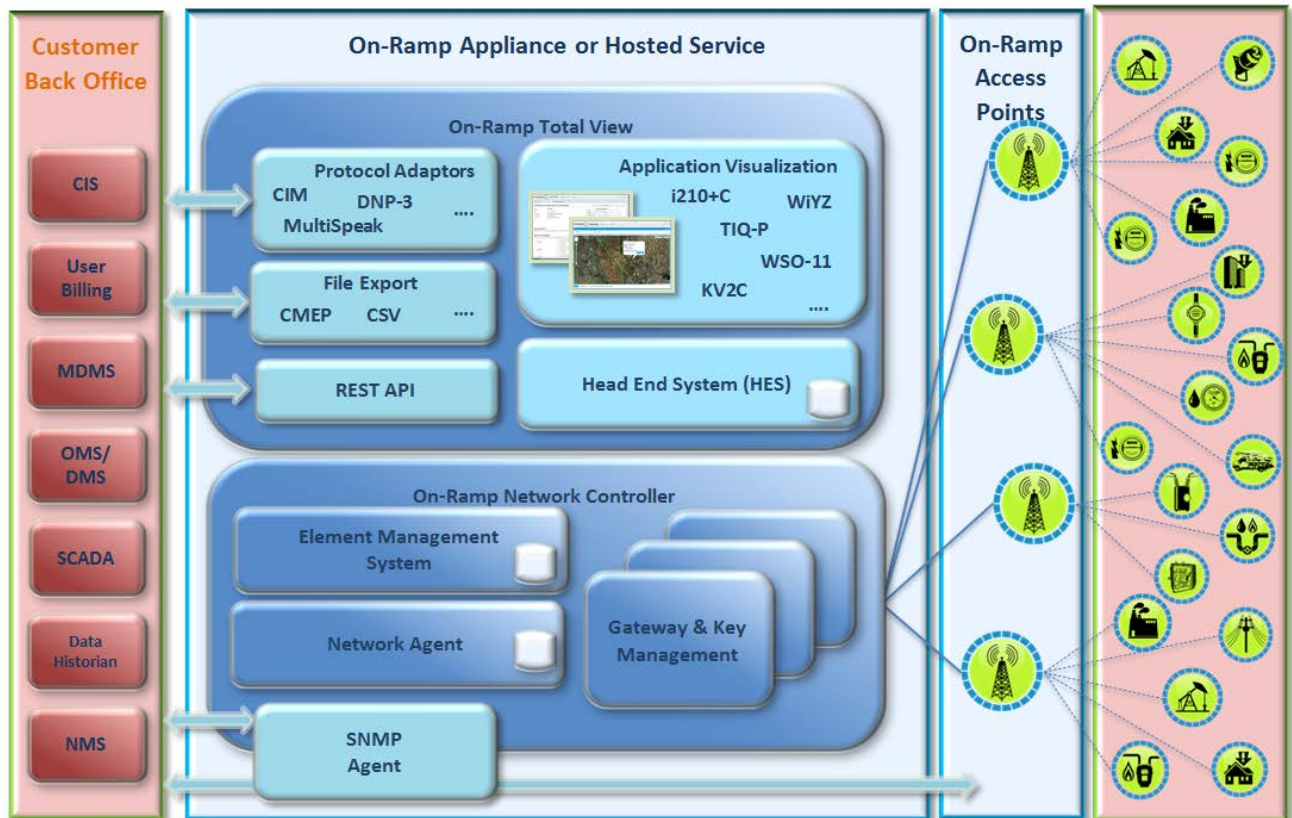


Figure 1. On-Ramp Wireless RPMA Network

On-Ramp Total View (OTV) supports four levels of users:

1. Operators
2. Guests
3. Administrators
4. Service Role

This document aims to provide general guidance for using OTV for Operators, Guests, and Administrators. The Service Role is required to support the REST API and is covered in the *OTV REST API Guide (010-0038-00)*. Refer to the corresponding supplement document for information specific to the devices used in your application. See Table 1 for a current list of supplemental documents.



## 3 Operating OTV

---

### 3.1 Logging in to OTV

Use the following steps to log in to OTV:

1. Open a web browser, and type:

```
http://<ip address of the OTV server or DNS name>:<port of otv server instance>/otv
```

The following table lists popular web browsers that support all OTV features.

**Table 2. Web Browsers That Support All OTV Features**

Browser	Version
Chrome	4.0.298.0 (Linux, Mac, Windows)
Epiphany	2.29.x (Linux)
Firefox	3.6 and higher
Internet Explorer	8 and higher
Opera	10.10 (Mac OS X 10.6.2, Linux)
Safari	4

2. From the **Source** drop-down list, select **company Domain AP**, **Domain LDAP** or **Local Account**. These options are dependent on how the OTV properties file is configured. (LDAP [Lightweight Directory Access Protocol] provides access to an organization's central directory of users.)

- ❑ Active Directory and LDAP use are enabled during OTV installation. Consult your IT administrator for more information.
- ❑ If the drop-down list is not visible, the Active Directory or LDAP configuration is not set up. Log in with local account access using an account created in section 5.4.

3. In the **UserID** field, type the user ID for this account.

**NOTE:** Use the Active Directory account **UserID** when logging in to OTV through the **company Domain**. Or use the LDAP account if this option has been configured. If the **company Domain** is not active, use an account created in section 5.4.

4. In the **Password** field, type the password for this account.
5. Click **Login**. When logged in, the screen in Figure 6 displays.

**NOTE:** When logging in to OTV, the tabs displayed are different for each account type. For example, when logging on to OTV with an administrator role, additional tabs are displayed that are not available when using a Guest role, which is read-only.

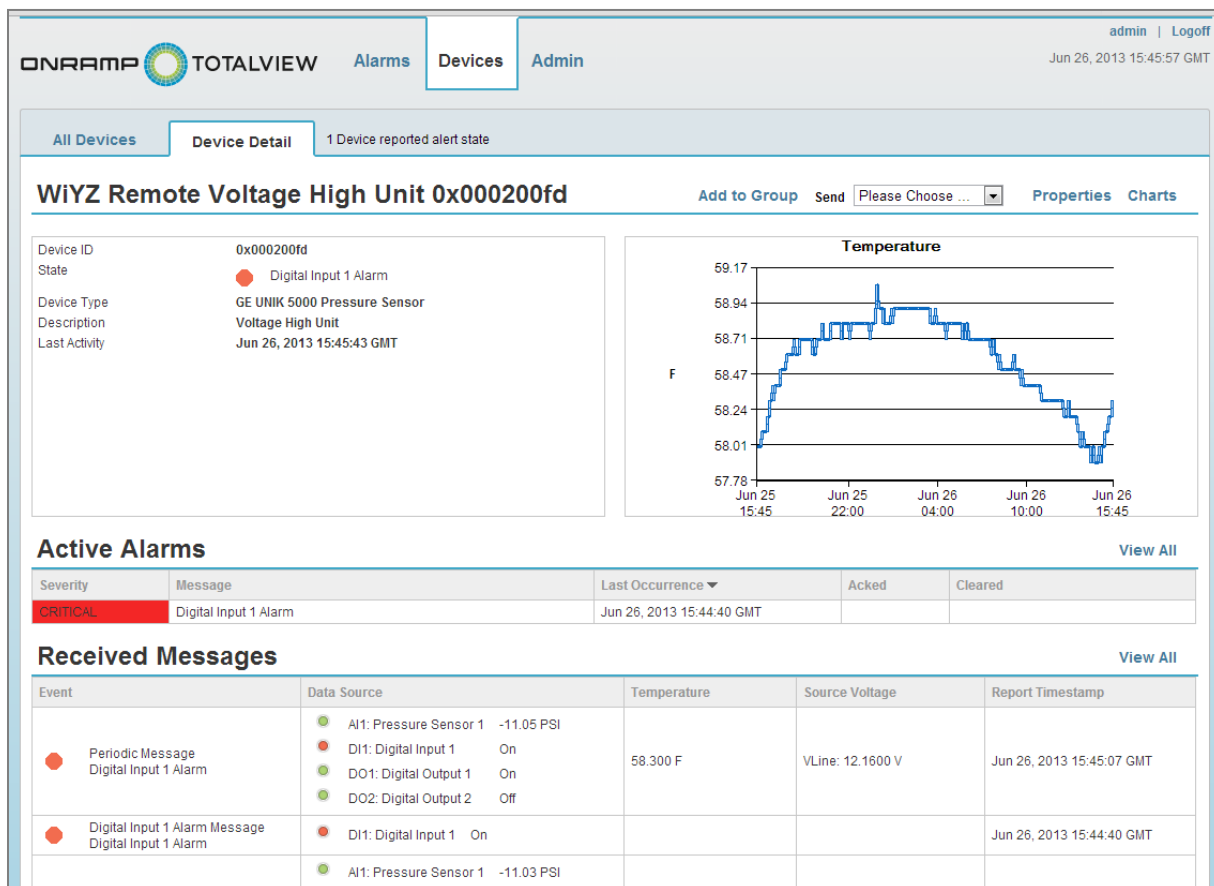
## 3.2 Alarms vs. Devices List

Operators should note the difference between OTV views for Alarms and Device List. The Alarms screen is a **summary** of the latest **alarms** sent by sensor devices on the network, while the Device screen is a listing of the **status** from all sensor devices on the network.

**NOTE:** When logging into OTV, the Alarms screen is shown first but for the purposes of this document, the Device Detail view is described first.

## 3.3 Device Detail View

The Device Detail view (shown in Figure 2) displays detailed information about a selected device. Because the information in these tables varies depending on the devices connected to your network, refer to the corresponding device supplement document for descriptions of the table headings and other device-specific information. See Table 1 for a current list of supplemental documents. The sections for the Device Detail view are described below the figure.



**Figure 2. Device Detail View**

**Device Detail view:** Clicking an alarm (Alarms view) or device row (Devices view) displays a detailed screen for the selected device, as shown in Figure 2. Clicking a row in the Active Alarms

section may bring up a second screen that provides further information about the device and any faults detected.

**NOTE:** The column headings for a detailed device screen such as shown in Figure 2 differs depending on the device.

This screens' sections are described as follows:

**Summary** – This section shows a summary of information about the device and its current state. To the right of the summary is a chart that is customizable per application.

**Add To Group** – This link enables the operator to add this specific device to an existing Device Group or a new one.

**Properties** – On the Properties view, the operator selects the device's mode (operational or maintenance or out of service) and specifies device attributes such as location details and GPS coordinates. This data may also be referred to as device metadata. For details about this feature, refer to the corresponding supplemental document for the device.

**Charts** – On the Charts view, the operator selects from predefined charts available for the device application. For available charts, consult the corresponding OTV supplemental document for the device.

**Active Alarms** – This section shows the active alarms for the selected device. Clicking a row brings up another detail screen where the operator may acknowledge alarm.

**Received Messages** – This represents the communications path flow from the device to the network.

**Sent Messages** – This represents the communications path flow from the network to the devices. The availability of this feature depends on your device and application. For further information, consult the corresponding OTV supplemental document for the device.

## 3.4 Devices List

To see the Devices List, click on the **All Devices** tab. The Devices List view displays status from devices on the network so that you can view their performance. State icons for device data are shown in Table 3. To filter the list by device type, click on the **Device Type** drop-down menu and select the desired device type.

The **Search** field allows a text search of all devices.

The **Advanced Search** link allows for users to search for devices based off of specific metadata fields.

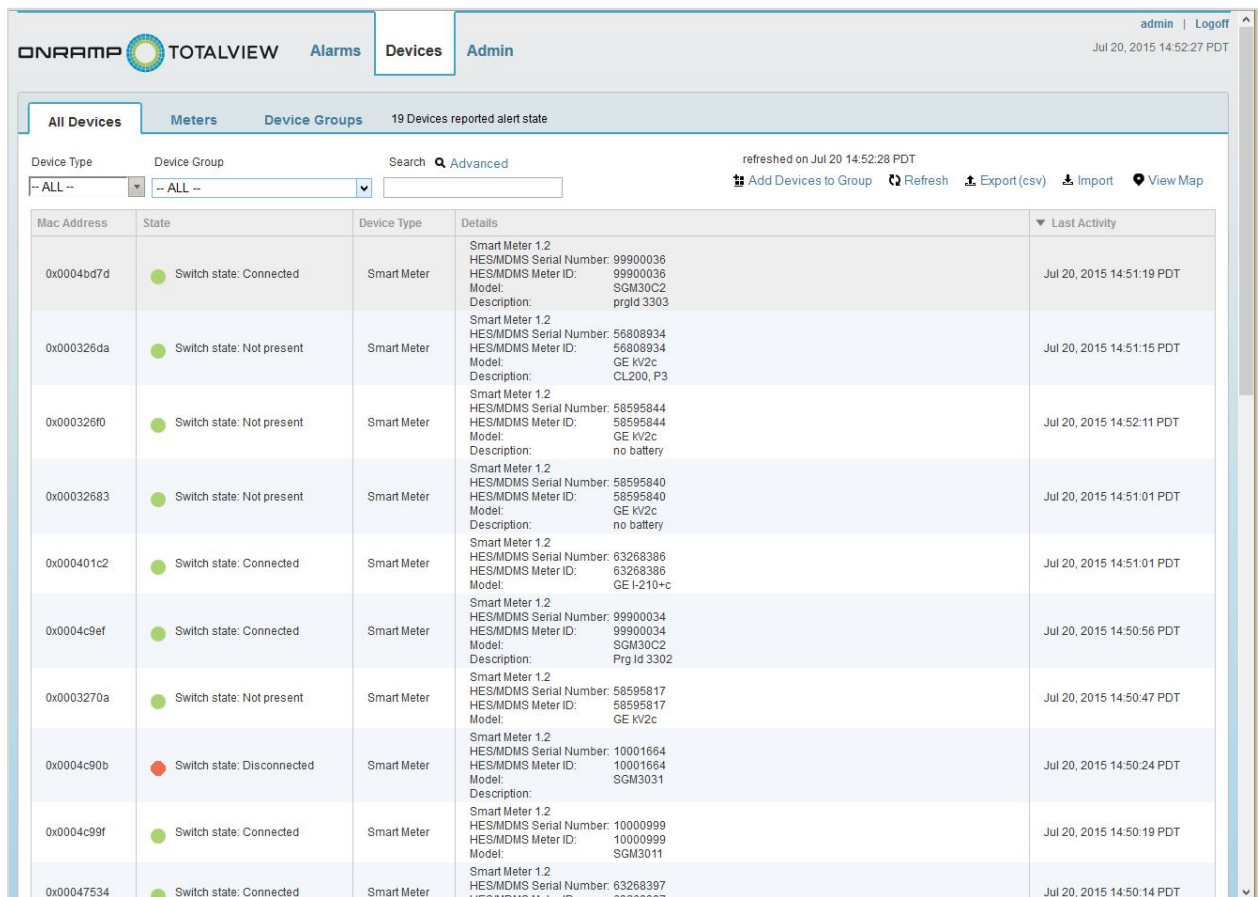
The **Add Devices to Group** link adds all devices in the table listing to a new or existing group. For detailed group functionality, refer to section 4.3 Device Groups.

The **Refresh** link performs a one-time refresh of the Alarms table.

The **Export** link exports the entire table listing to a .csv file. Specific device types may have additional export options. For specific export options, consult the corresponding OTV supplemental document for that device.

The **Import** link shows a history of previously uploaded device files. This screen contains an **Import File** link, which allows files of select types to be uploaded to OTV. One such file may contain device metadata. Device metadata may be added, removed, or updated. For additional device metadata import specifications, see section 4.2 Device Properties/Metadata Import. Additionally, devices can be added to a group using the Group Formation option on the Import File dialog box. See section 4.3.3 for information about group import. Specific device types may have additional import options. For specific import options, consult the corresponding OTV supplemental document for that device.

The **View Map** link changes the table listing into a Google Maps view. For additional information on enabling Google Maps, refer to section 3.6 Using Google Maps.



The screenshot shows the ONRAMP TOTALVIEW interface with the 'Devices' tab selected. The page displays a list of 19 devices, all of which are 'Smart Meter' type. The table includes columns for Mac Address, State, Device Type, Details, and Last Activity. The 'State' column uses colored circles to indicate the device's status: green for 'Connected', red for 'Disconnected', and grey for 'Not present'. The 'Details' column provides specific information for each device, including HES/MDMS Serial Number, HES/MDMS Meter ID, Model, and Description. The 'Last Activity' column shows the timestamp of the last update for each device.

Mac Address	State	Device Type	Details	Last Activity
0x0004bd7d	Switch state: Connected	Smart Meter	Smart Meter 1.2 HES/MDMS Serial Number: 99900036 HES/MDMS Meter ID: 99900036 Model: SGM30C2 Description: prgld 3303	Jul 20, 2015 14:51:19 PDT
0x000326da	Switch state: Not present	Smart Meter	Smart Meter 1.2 HES/MDMS Serial Number: 56808934 HES/MDMS Meter ID: 56808934 Model: GE KV2c Description: CL200, P3	Jul 20, 2015 14:51:15 PDT
0x000326f0	Switch state: Not present	Smart Meter	Smart Meter 1.2 HES/MDMS Serial Number: 58595844 HES/MDMS Meter ID: 58595844 Model: GE KV2c Description: no battery	Jul 20, 2015 14:52:11 PDT
0x00032683	Switch state: Not present	Smart Meter	Smart Meter 1.2 HES/MDMS Serial Number: 58595840 HES/MDMS Meter ID: 58595840 Model: GE KV2c Description: no battery	Jul 20, 2015 14:51:01 PDT
0x000401c2	Switch state: Connected	Smart Meter	Smart Meter 1.2 HES/MDMS Serial Number: 63268386 HES/MDMS Meter ID: 63268386 Model: GE I-210-c	Jul 20, 2015 14:51:01 PDT
0x0004c9ef	Switch state: Connected	Smart Meter	Smart Meter 1.2 HES/MDMS Serial Number: 99900034 HES/MDMS Meter ID: 99900034 Model: SGM30C2 Description: Prg Id 3302	Jul 20, 2015 14:50:56 PDT
0x0003270a	Switch state: Not present	Smart Meter	Smart Meter 1.2 HES/MDMS Serial Number: 58595817 HES/MDMS Meter ID: 58595817 Model: GE KV2c	Jul 20, 2015 14:50:47 PDT
0x0004c90b	Switch state: Disconnected	Smart Meter	Smart Meter 1.2 HES/MDMS Serial Number: 10001664 HES/MDMS Meter ID: 10001664 Model: SGM3031 Description:	Jul 20, 2015 14:50:24 PDT
0x0004c99f	Switch state: Connected	Smart Meter	Smart Meter 1.2 HES/MDMS Serial Number: 10000999 HES/MDMS Meter ID: 10000999 Model: SGM3011	Jul 20, 2015 14:50:19 PDT
0x00047534	Switch state: Connected	Smart Meter	Smart Meter 1.2 HES/MDMS Serial Number: 63268397 HES/MDMS Meter ID: 63268397	Jul 20, 2015 14:50:14 PDT

Figure 3. Devices List

Clicking on a device row brings up the device detail screen, shown in Figure 4. Device Detail on the following page.

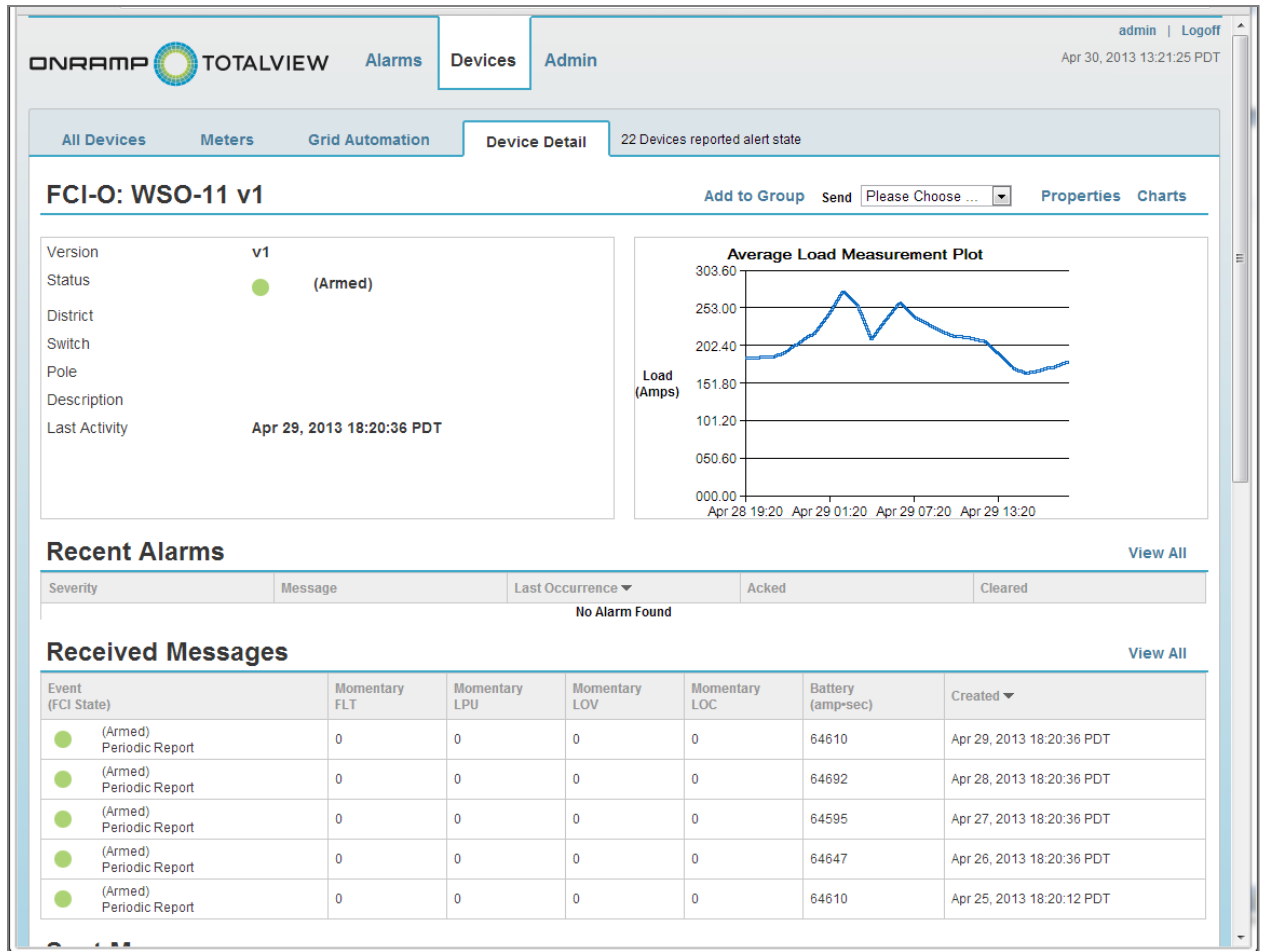


Figure 4. Device Detail

## 3.5 Alarms Detail View

After logging in, a screen is displayed showing active alarms on the system. If there are no alarms the screen shows no alarms.

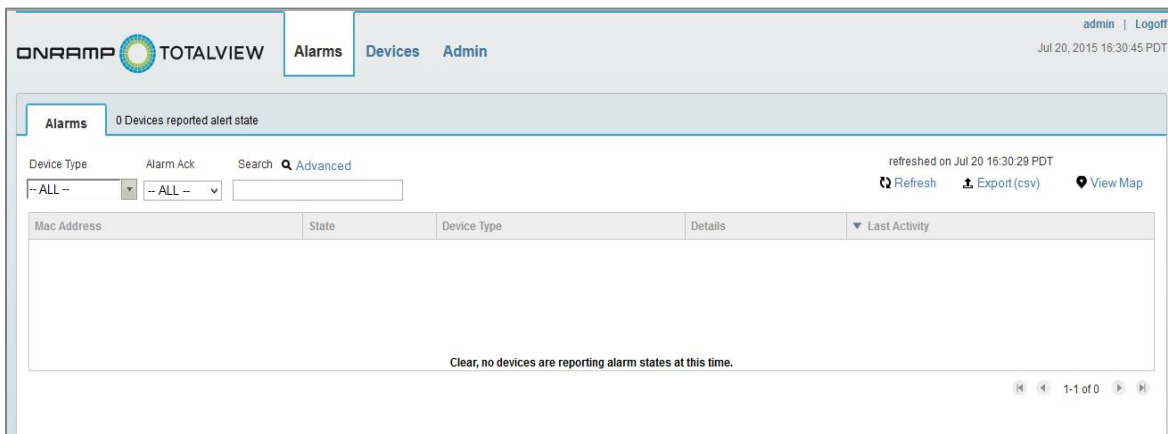


Figure 5. Clear Alarms Screen

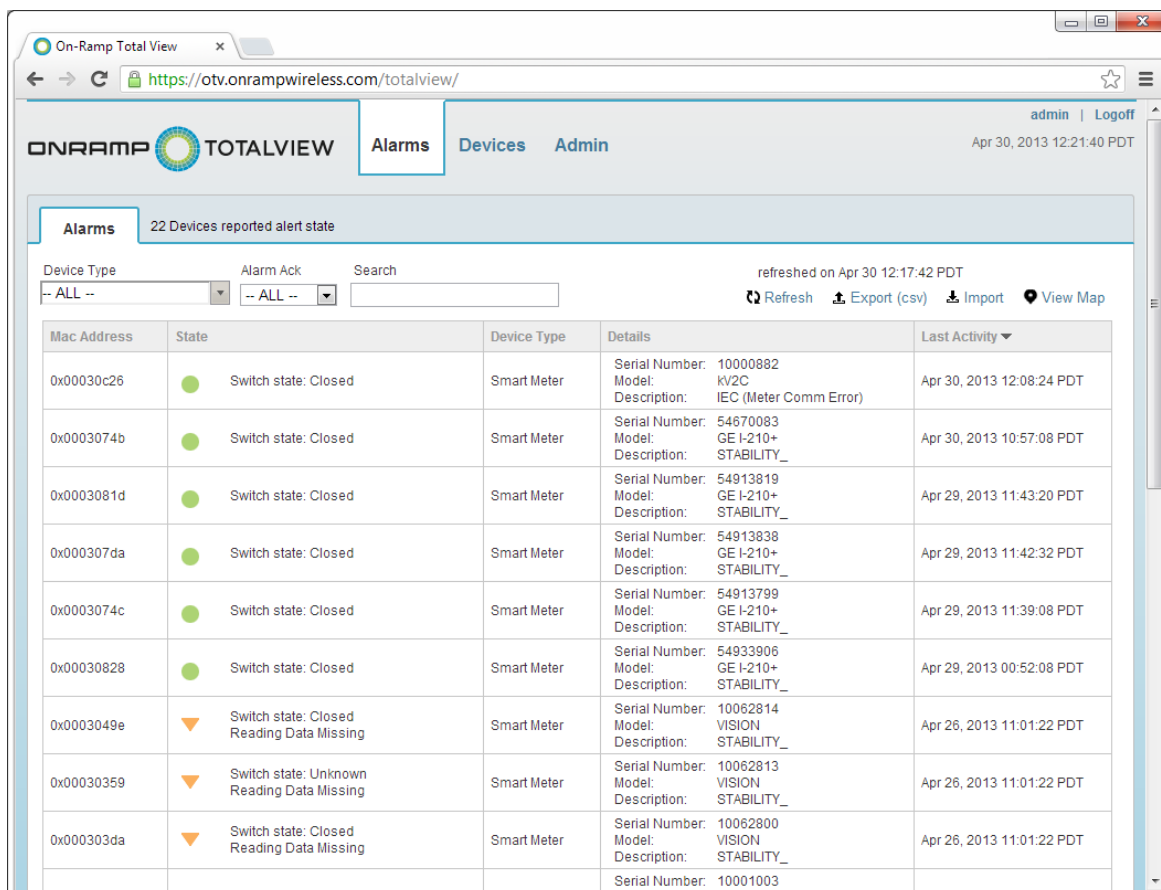


Figure 6. Alarms Screen with Active Alarms

**Device Type Selector:** Allows filtering on specific device types. Select –All– to see all device types available on your network.

**Alarm Acknowledge (Ack) Selector:** Allows filtering on alarm acknowledgement status for a given Device Type.

**Search:** Allows text search for alarms and devices.











**Advanced Search:** Allows for search for alarms and devices by device metadata.

**Alarms:** Each row lists alarm (under Alarms view) and device (under Devices view) status information. Clicking a row highlights it and displays a detailed device status screen, as shown in Figure 2.

The table columns for the alarm or device lists are defined as follows:

- **Mac Address:** A unique hexadecimal ID number assigned to a particular device.  
**NOTE:** Mac Address has to be enabled under Admin -> My Profile for this column to be present.
- **State:** State icons are graphical representations of alarm or device data status. These are defined in the following table.

**Table 3. Alarm and Device State Icons and Descriptions**

Icon	Description
	Clear; no problem detected
	Critical incident
	Minor incident
	Major incident
	Informational Event
	Device is marked as “Out of Service”
	Clear, in Maintenance mode
	Critical incident, in Maintenance mode; no email alerts
	Minor incident, in Maintenance mode
	Major incident, in Maintenance mode

- **Device Type:** This is a brief description assigned to a particular sensor device. The devices listed differ depending on what devices are used on your network.
- **Description:** Gives a brief description of the device characteristics such as its location, type or model.  
**NOTE:** Device information displayed differs depending on what kind of sensor device is connected to the network. For device-specific information, refer to the corresponding OTV supplemental document for that device. See Table 1 for a list of supplemental documents available.

- **Last Activity:** This column shows the date and time of the last alarm (Alarms view) or device data (Devices view) update.

**NOTE:** Clicking on a column heading under either Alarms or Devices views performs an ascending or descending alphabetic, numeric or date sort.

**Refresh:** Clicking this button updates the contents of the Alarm or Device table with the latest received data.

**Data Status:** Displays date and time of last refresh.

**List/Map Select:** Specifies how to display device information, either as a table (default) or on Google Maps.

### 3.5.1 Alarms and Alarm Detail

An Alarms screen displays when a user logs into OTV. This screen provides status information about alarms triggered by a device. Alarms may range from minor events that are informational, to critical events that require further action. For a given application, for example, the Alarms view may not show any results (no alarms), while the Devices view shows status from active devices on your application's network.

**NOTE:** Device information displayed is different depending on what kind of sensor device is connected to the network. For device-specific information, refer to the corresponding OTV supplemental document for the device. See Table 1 for a list of supplemental documents.

The alarm status information can be filtered using the **Device Type** drop-down menu. Selecting a particular device type refreshes the display to show only alarms of that device type.

The **Alarm Ack** (alarm acknowledge) drop-down allows the operator to filter by alarms which have been acknowledged (Aked) or not acknowledged (Not Aked). For instructions on acknowledging alarms, see section 3.5.2 Acknowledging Alarms.

The **Search** field allows a text search of all devices, searching in the description fields and other attributes.

The **Advanced Search** link allows for users to search for devices and alarms by specific device metadata.

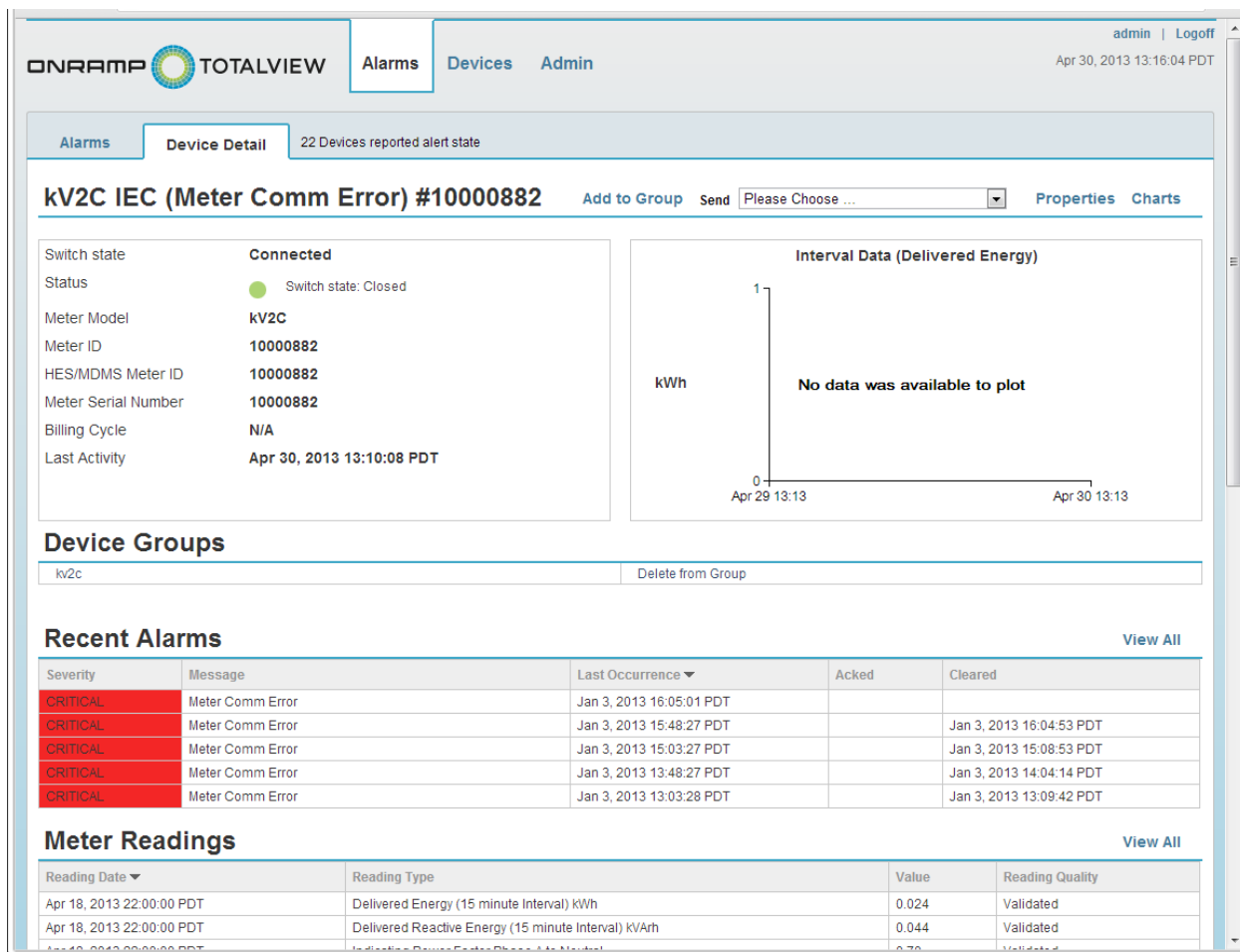
The **Refresh** link performs a one-time refresh of the Alarms table.

The **Export** link exports the entire table listing to a .csv file. Specific device types may have additional export options. For specific export options, consult the corresponding OTV supplemental document for the device.

The **View Map** link changes the table listing into a Google Maps view. For additional information on enabling Google Maps, refer to section 3.6 Using Google Maps.

Alarms and Device State icons are defined in Table 3. Detailed alarm information may be viewed in the **Active Alarms** section on the Device Detail screen.





**Figure 7. Alarms Section on Device Detail**

Because this list only displays alarms which have not received a clear message from the device, clicking on **View All** will display the list of all alarms that the device has received. Figure 8 displays an example of this list whereby the user can use the **Date Range**, **Severity**, **Acknowledgement**, and **State** filters to quickly display specific alarms. The date and time may be changed by clicking the Date Range button and then entering the desired range of dates and times. Additionally, clicking on **Export (csv)** on this page will create a .csv file of the alarms displayed on this page.

**NOTE:** Time is calculated from the time zone setting in your profile. You may filter alarms by their severity, acknowledged status, or state (cleared or active). To do so, select the desired filter criteria as shown below.

admin | Logout

Jul 20, 2015 17:25:41 PDT

ONRRAMP TOTALVIEW

Alarms

Devices

Admin

Alarms

Device Detail

Meter Alarms

19 Devices reported alert state

Alarms for GE kV2c Wired for "Reverse Energy Flow" #58595803

Severity

Acknowledgement

State

-- ALL --

-- ALL --

-- ALL --

refreshed on Jul 20 17:24:47 PDT

Export(csv)

Refresh

Date Range

Severity	Message	Last Occurrence	Acked	Cleared
MAJOR	Power Fail	Jul 4, 2015 15:04:45 PDT		Jul 4, 2015 15:08:54 PDT
MAJOR	Power Fail	Jul 4, 2015 14:58:28 PDT		Jul 4, 2015 15:02:33 PDT
MAJOR	Power Fail	Jul 4, 2015 14:52:11 PDT		Jul 4, 2015 14:56:01 PDT
MAJOR	Power Fail	Jul 4, 2015 14:45:54 PDT		Jul 4, 2015 14:50:50 PDT
MAJOR	Power Fail	Jul 4, 2015 13:57:44 PDT		Jul 4, 2015 14:01:45 PDT
MAJOR	Power Fail	Jul 4, 2015 13:32:51 PDT		Jul 4, 2015 13:36:31 PDT
MAJOR	Power Fail	Jul 4, 2015 13:07:57 PDT		Jul 4, 2015 13:11:37 PDT
MAJOR	Power Fail	Jul 4, 2015 12:43:04 PDT		Jul 4, 2015 12:46:54 PDT
MAJOR	Power Fail	Jul 4, 2015 12:18:06 PDT		Jul 4, 2015 12:21:51 PDT
MAJOR	Power Fail	Jul 4, 2015 11:53:14 PDT		Jul 4, 2015 11:56:57 PDT
MAJOR	Power Fail	Jul 4, 2015 11:28:20 PDT		Jul 4, 2015 11:32:04 PDT
MAJOR	Power Fail	Jul 4, 2015 11:03:27 PDT		Jul 4, 2015 11:07:11 PDT
MAJOR	Power Fail	Jul 4, 2015 10:38:34 PDT		Jul 4, 2015 10:42:27 PDT
MAJOR	Power Fail	Jul 4, 2015 10:13:41 PDT		Jul 4, 2015 10:17:34 PDT
MAJOR	Power Fail	Jul 4, 2015 09:48:48 PDT		Jul 4, 2015 09:53:31 PDT
MAJOR	Power Fail	Jul 4, 2015 09:23:55 PDT		Jul 4, 2015 09:27:37 PDT
MAJOR	Power Fail	Jul 4, 2015 08:59:02 PDT		Jul 4, 2015 09:02:43 PDT
MAJOR	Power Fail	Jul 4, 2015 08:34:08 PDT		Jul 4, 2015 08:37:40 PDT
MAJOR	Power Fail	Jul 4, 2015 08:09:15 PDT		Jul 4, 2015 08:12:57 PDT
MAJOR	Power Fail	Jul 4, 2015 07:44:22 PDT		Jul 4, 2015 07:47:44 PDT
MAJOR	Power Fail	Jul 4, 2015 07:19:29 PDT		Jul 4, 2015 07:24:51 PDT
MAJOR	Power Fail	Jul 4, 2015 06:54:36 PDT		Jul 4, 2015 06:58:17 PDT
MAJOR	Power Fail	Jul 4, 2015 06:29:43 PDT		Jul 4, 2015 06:33:14 PDT
MAJOR	Power Fail	Jul 4, 2015 06:04:50 PDT		Jul 4, 2015 06:08:30 PDT
MAJOR	Power Fail	Jul 4, 2015 05:39:57 PDT		Jul 4, 2015 05:43:37 PDT

Figure 8. View All Alarms Page

For example, if you want to see all Major alarms:

1. Select Major from the Severity drop-down menu.
2. Select Active or Cleared from the State drop-down to see alarms that are still active or those that have been cleared.

You can also perform more detailed searches by combining search criteria. For example, if you want to find all Major alarms since 8:00:00 am on July 3, 2015 which have not been acknowledged:

1. Enter the date and time as shown on the next page.
2. Then select Not Acknowledged under Acknowledgement.

The screenshot displays the ONRAMP TOTALVIEW interface. The top navigation bar includes 'Alarms', 'Devices', and 'Admin'. The 'Alarms' section is active, showing 'Meter Alarms' for 19 devices. The main heading is 'Alarms for GE kV2c Wired for "Reverse Energy Flow" #58595803'. Below this, there are filters for Severity (ALL), Acknowledgement (ALL), and State (ALL). A table lists alarms with columns for Severity, Message, Last Occurrence, Acked, and Cleared. A 'Select Dates' dialog box is overlaid on the table, showing a calendar for July 2015. The date 4 is selected, and the time range is set from 08:00 to 00:00. The 'To' checkbox is checked for 'Current time'. The dialog has 'Cancel' and 'Ok' buttons.

Severity	Message	Last Occurrence	Acked	Cleared
MAJOR	Power Fail	Jul 4, 2015 15:04:45 PDT		Jul 4, 2015 15:08:54 PDT
MAJOR	Power Fail			Jul 4, 2015 15:02:33 PDT
MAJOR	Power Fail			Jul 4, 2015 14:56:01 PDT
MAJOR	Power Fail			Jul 4, 2015 14:50:50 PDT
MAJOR	Power Fail			Jul 4, 2015 14:01:45 PDT
MAJOR	Power Fail			Jul 4, 2015 13:36:31 PDT
MAJOR	Power Fail			Jul 4, 2015 13:11:37 PDT
MAJOR	Power Fail			Jul 4, 2015 12:46:54 PDT
MAJOR	Power Fail			Jul 4, 2015 12:21:51 PDT
MAJOR	Power Fail			Jul 4, 2015 11:56:57 PDT
MAJOR	Power Fail			Jul 4, 2015 11:32:04 PDT
MAJOR	Power Fail			Jul 4, 2015 11:07:11 PDT
MAJOR	Power Fail			Jul 4, 2015 10:42:27 PDT
MAJOR	Power Fail	Jul 4, 2015 10:13:41 PDT		Jul 4, 2015 10:17:34 PDT
MAJOR	Power Fail	Jul 4, 2015 09:48:48 PDT		Jul 4, 2015 09:53:31 PDT
MAJOR	Power Fail	Jul 4, 2015 09:23:55 PDT		Jul 4, 2015 09:27:37 PDT
MAJOR	Power Fail	Jul 4, 2015 08:59:02 PDT		Jul 4, 2015 09:02:43 PDT
MAJOR	Power Fail	Jul 4, 2015 08:34:08 PDT		Jul 4, 2015 08:37:40 PDT
MAJOR	Power Fail	Jul 4, 2015 08:09:15 PDT		Jul 4, 2015 08:12:57 PDT
MAJOR	Power Fail	Jul 4, 2015 07:44:22 PDT		Jul 4, 2015 07:47:44 PDT
MAJOR	Power Fail	Jul 4, 2015 07:19:29 PDT		Jul 4, 2015 07:24:51 PDT
MAJOR	Power Fail	Jul 4, 2015 06:54:36 PDT		Jul 4, 2015 06:58:17 PDT
MAJOR	Power Fail	Jul 4, 2015 06:29:43 PDT		Jul 4, 2015 06:33:14 PDT
MAJOR	Power Fail	Jul 4, 2015 06:04:50 PDT		Jul 4, 2015 06:08:30 PDT
MAJOR	Power Fail	Jul 4, 2015 05:39:57 PDT		Jul 4, 2015 05:43:37 PDT

Figure 9. Using Date Range on View All Alarms Page

### 3.5.2 Acknowledging Alarms

Alarms sent by devices to OTV may be acknowledged (Acked) or not (Not Acked). Proceed as follows to acknowledge an alarm:

1. Click the Alarms or Devices List view.
2. Click the row for the specific alarm to acknowledge. The alarm or device detail screen displays.
3. Click the View All link in the Alarms section. This displays the table of alarms that have been sent.
4. Click the row of the desired alarm to acknowledge. This displays the Alarm Details screen, shown below:

The screenshot shows the On-Ramp Total View Operator Guide interface. The top navigation bar includes 'Alarms', 'Devices', and 'Admin'. The main content area is titled 'Alarms for GE KV2c Wired for "Reverse Energy Flow" #58595803'. A modal window titled 'Alarm Details: Power Fail: Mac Address 0x000326e7' is open, displaying the following information:

- Alarm:** Power Fail
- Additional Information:** Smart Meter 58595803 has the following MAJOR condition: Meter has measured grid side power failure. This message was received from this device at 07/04/2015 21:00:14 Coordinated Universal Time (server time) Smart Meter 1.2 Details: Emcm Reported Meter ID: 58595803 Bill Cycle: Description: Wired for "Reverse Energy Flow" Sent conn req state @17:33 7/1 HES/MDMS Serial Number: 58595803 Model: GE KV2c State: Emcm Reported Serial Number: 58595803 HES/MDMS Meter ID: 58595803 Zip: Street Address: City: Data Reporting Config Name: KV2C\_ProgramId\_7202 Mac Address: 0x000326e7
- Severity:** MAJOR
- First Occurrence:** Jul 4, 2015 13:57:44 PDT
- Last Occurrence:** Jul 4, 2015 13:57:44 PDT
- Cleared At:** Jul 4, 2015 14:01:45 PDT
- Acknowledge:** No (dropdown menu)

The modal window has 'Cancel' and 'Save' buttons at the bottom right. The background shows a table of alarms with columns for Severity, Message, and State.

**Figure 10. Alarm Acknowledgement Feature**

- Click the Acknowledge drop-down menu and select Yes. A confirmation window displays as shown below:

The screenshot shows the 'Alarms for GE kV2c Wired for "Reverse Energy Flow" #58595803' page. The page has a table of alarms with columns for Severity, Message, and State. A modal window titled 'Alarm Details: Power Fail: Mac Address 0x000326e7' is open, showing details about the power fail alarm. The details include the alarm type (Power Fail), the smart meter ID (58595803), and the message (Smart Meter 58595803 has the following MAJOR condition: Meter has measured grid side power failure). A confirmation dialog box is also present, asking 'You are going to acknowledge the alarm. Are you sure you want to continue?' with 'Cancel' and 'Yes' buttons.

**Figure 11. Alarm Acknowledgement Confirmation**

6. Click Yes to confirm you want to acknowledge the alarm.
7. Click Save. The alarm on the screen now displays as an acknowledged alarm.

## 3.6 Using Google Maps

When latitude and longitude coordinates of any devices are entered, an operator may view the devices on Google Maps.

### Enabling Google Map viewing for a user

1. Click the Admin tab, then click Users and click the User on which to enable Maps views (must have Administrator rights).
2. Click the checkbox beside **Enable Google Maps** and Save

### Entering Latitude and Longitude values

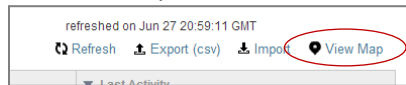
1. From the Alarms or Devices List view select the device you want to see on Google Maps by clicking in the row.
2. Click the Properties link, enter the latitude and longitude values and Save.



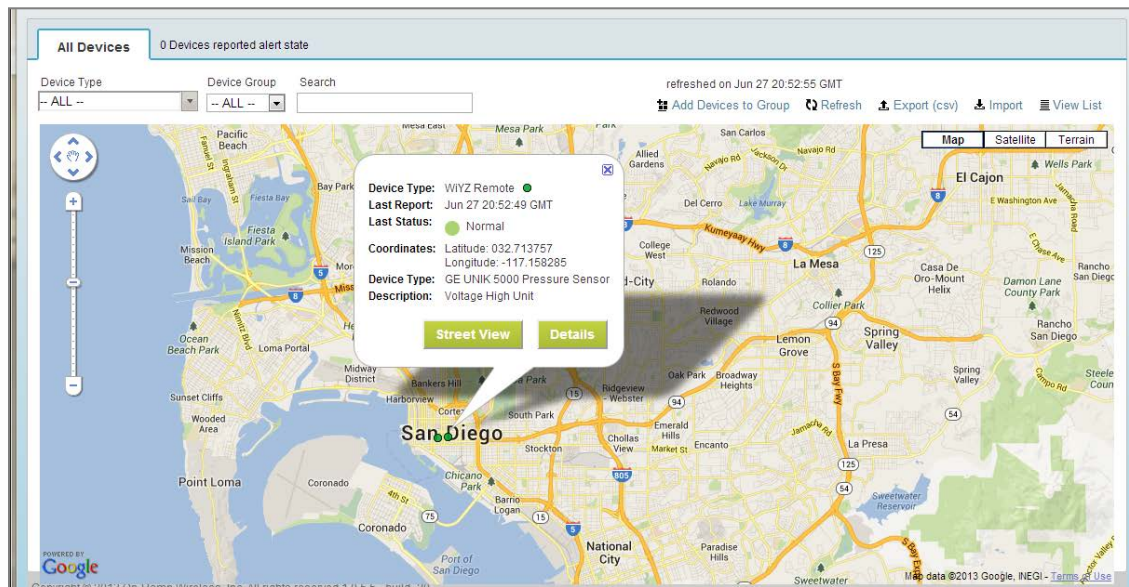
**NOTE:** Coordinates must be entered as numeric values such as -84.1553, or 38.1.

## Viewing Devices on Google Maps

1. Click the Alarms or Devices List view. On the right side of the screen above the listing, click the View Map link.



2. OTV maps the coordinates of the devices specified and displays a small colored icon for each device on Google Maps. The color of the icon indicates the alarm state of the device. Clicking on the icon brings up location information about the device. Note that Street View will not always be an option depending on its availability by Google.



**Figure 12. Viewing devices in Google Maps**

3. Click the View List link to return to table view.

## 3.7 Exporting Device Data

OTV allows a user to export data from nodes in .csv (comma-separated values) format. This data may be used for further manipulation depending on your application. Different device types may have additional export options. For available export options, consult the corresponding OTV supplemental document for the device.

### To export Received Messages data:

1. Click on one of the following:
  - ❑ A row in Alarms, **or**
  - ❑ A row in Devices List view, **or**
  - ❑ The Details button on Maps view
2. Click the View All link in the Received Messages section.

3. Click the Export link on the right side of the screen above the table.
4. The .csv file downloads to your computer.

### To export Hex data:

**NOTE:** This feature is not available for Smart Meters.

1. Click a row in either Alarms or Devices List view.
2. Click the View All link in the Received Messages section.
3. Click the Hex link on the right side of the screen above the table.
5. Click the Export link on the right side of the screen above the table.
6. The .csv file downloads to your computer.

## 3.8 Charting Data

Data sent from devices may be plotted on a graph to show trends and response activity over a period of time. This can be useful to fine tune the network for optimal performance. Charts may be viewed by clicking on the **Charts** link on the Device Detail screen or from the Received Messages view for all devices except Smart Meters as follows:

1. Select the row of the desired device in the Alarms or Devices List view.
2. The device detail screen displays. Click the View All link in the Received Messages section.
3. Click the Plot link. A graph is displayed similar to what is shown in the following figure. The actual data displayed varies depending on the device and data type selected.
4. Use your cursor to mouse across the graph to display key data points.

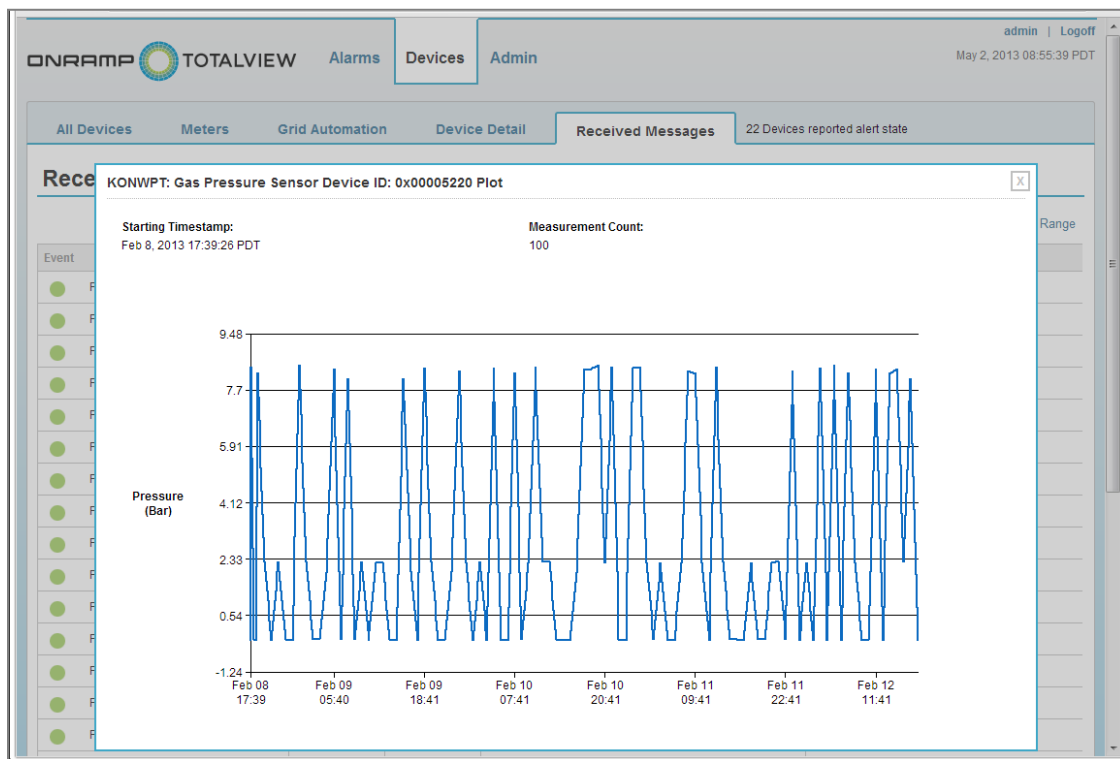


Figure 13. Sample Gas Pressure Plot

## 4 Managing Devices

### 4.1 Maintenance/Operational/Out of Service Modes

When devices are initially listed in OTV, they are in maintenance mode by default. When the device is in maintenance mode, fault notifications for the devices are not sent to the specified email recipients. The purpose of maintenance mode is not to burden users with fault notifications when the device is not yet deployed in the RPMA Network for operation. When a device is in maintenance mode, the state of the device in the Devices list or Alarms list shows a wrench symbol inside the state icon, as shown here:

The screenshot shows the ONRAMP TOTALVIEW interface with the 'Devices' tab selected. The top navigation bar includes 'Alarms', 'Devices', and 'Admin'. The 'Devices' tab has sub-tabs for 'All Devices', 'Meters', and 'Grid Automation'. A search bar is present with the text 'maintenance' entered. The table below lists devices in maintenance mode, with a wrench icon in the state column for each row.

Mac Address	State	Device Type	Details	Last Activity
0x00005213	In Maintenance	KONWPT: Gas Pressure Sensor	Device ID: 0x00005213	Apr 30, 2013 12:21:24 PD
0x00005212	In Maintenance	KONWPT: Gas Pressure Sensor	Device ID: 0x00005212	Apr 30, 2013 12:21:22 PD
0x00005209	In Maintenance	KONWPT: Gas Pressure Sensor	Device ID: 0x00005209	Apr 30, 2013 12:21:03 PD
0x000003fc	In Maintenance (Armed)	FCI-O: WSO-11	Version: v1	Apr 29, 2013 18:20:33 PD
0x000003f8	In Maintenance (Armed)	FCI-O: WSO-11	Version: v1	Apr 29, 2013 18:20:29 PD
0x000003f7	In Maintenance (Armed)	FCI-O: WSO-11	Version: v1	Apr 29, 2013 18:20:28 PD
0x000003f6	In Maintenance (Armed)	FCI-O: WSO-11	Version: v1	Apr 29, 2013 18:20:27 PD
0x000003f3	In Maintenance (Armed)	FCI-O: WSO-11	Version: v1	Apr 29, 2013 18:20:24 PD
0x000003f1	In Maintenance (Armed)	FCI-O: WSO-11	Version: v1	Apr 29, 2013 18:20:22 PD
0x00000400	In Maintenance (Armed)	FCI-O: WSO-11	Version: v1	Apr 29, 2013 18:20:12 PD

Figure 14. Maintenance Mode Filter

The Device Properties panel shows the current mode as shown below.



The screenshot shows the ONRAMP TOTALVIEW web interface. The top navigation bar includes 'Alarms', 'Devices' (selected), and 'Admin'. The user is logged in as 'admin' on 'Apr 30, 2013 12:56:12 PDT'. Below the navigation bar, there are tabs for 'All Devices', 'Meters', 'Grid Automation', 'Device Detail' (selected), and 'Properties'. A status message indicates '22 Devices reported alert state'. The main heading is 'Properties for KONWPT: Gas Pressure Sensor: 0x00005213'. The 'Operation State' is set to 'Maintenance' in a dropdown menu, with a note: 'Fault notification will not be sent.' Below this are input fields for 'Description', 'Latitude', and 'Longitude'. At the bottom, there is a message: 'Update device Attributes and click 'Save'. Use 'Delete' to remove the device from display.' and two buttons: 'Delete' and 'Save'. A link for 'Diagnostic Details' is also present.

Figure 15. Device Properties Page for Maintenance Mode

When a device is ready for network operation, the operator should change the mode from **Maintenance** to **Operational** in the drop-down menu from the Device Properties view.

The screenshot shows the ONRAMP TOTALVIEW web interface, similar to Figure 15 but with the 'Operation State' set to 'Operational'. The note now reads: 'Fault notification will be sent if it is configured.' The 'Delete' and 'Save' buttons remain at the bottom.

Figure 16. Device Properties Page for Operational Mode

After clicking **Save**, the device sends a fault notification when a fault occurs in the future.

If a device has been decommissioned, then the operator may choose to set the Operation State to **Out of Service**. At this point, an operator may choose to drop data from this device for performance reasons and alarms are also ignored. This is a convenient way to differentiate decommissioned devices in a large network. Device operational states may be changed in bulk using the Device Properties/Metadata Import specified in section 4.2.

**Table 4. Operational Mode Behaviors**

Device Operational State	Device alarm State (List and Device views)	Generates OTV Alarm Notifications	Generates email Notifications of Alarms	Parses Application Payloads
Maintenance	Yes (with wrench)	No	No	Yes
Operational	Yes	Yes	If configured	Yes
Out of Service	No (shown grey)	No	No	Yes with option to disable

## 4.2 Device Properties/Metadata Import

The **Import File** link on **Devices** → **Import File Listing View** allows modification of properties or metadata for multiple devices when the Device Info option is selected. For example, you can populate the latitude and longitude values for multiple devices at one time. Please note that the device must have joined the network and be present in the OTV user interface before the properties can be modified.

**Figure 17. Device Import Feature**

`tns:ulp_node_id` is the On-Ramp Wireless unique device identifier  
`tns:attribute_name` is the key for the metadata field to update  
`tns:attribute_value` is the actual metadata field value

**NOTE:** XML schemas are located on the On-Ramp Wireless website, [onrampwireless.com](http://onrampwireless.com), so access to the internet is required to run this import tool.

To update device properties metadata, the import file must be in the following xml format:

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:node_meta_info xmlns:tns="http://www.onrampwireless.com/node_meta_info/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.onrampwireless.com/node_meta_info/
../../../../main/xsd/node_meta_info_import.xsd ">
  <tns:node_attribute>
    <tns:ulp_node_id>199715</tns:ulp_node_id>
    <tns:attribute>
      <tns:attribute_name>Latitude</tns:attribute_name>
      <tns:attribute_value>33.01372</tns:attribute_value>
    </tns:attribute>
    <tns:attribute>
      <tns:attribute_name>Longitude</tns:attribute_name>
      <tns:attribute_value>-117.096932</tns:attribute_value>
    </tns:attribute>
  </tns:node_attribute>
</tns:node_meta_info>
```

To add or remove properties from the OTV devices, contact On-Ramp Wireless support personnel at [support@onrampwireless.com](mailto:support@onrampwireless.com) to assist in database modifications. On-Ramp Wireless provides a tool to assist customers in managing device properties and metadata and automatically creating this XML file. For access to this tool, contact On-Ramp Wireless support personnel at [support@onrampwireless.com](mailto:support@onrampwireless.com).

## 4.2.1 Bulk update of Operational State

To update the operational state of multiple devices, a file import can be uploaded using the following format:

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:node_meta_info xmlns:tns="http://www.onrampwireless.com/node_meta_info/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.onrampwireless.com/node_meta_info/
../../../../main/xsd/node_meta_info_import.xsd ">

  <tns:node_attribute>
    <tns:ulp_node_id>199715</tns:ulp_node_id>
    <tns:operation_state>Operational</tns:operation_state>
    <tns:attribute>
      <tns:attribute_name>Latitude</tns:attribute_name>
      <tns:attribute_value>33.01372</tns:attribute_value>
    </tns:attribute>
    <tns:attribute>
      <tns:attribute_name>Longitude</tns:attribute_name>
      <tns:attribute_value>-117.096932</tns:attribute_value>
    </tns:attribute>
  </tns:node_attribute>
```

```
</tns:node_attribute>
</tns:node_meta_info>
```

Where valid operational states are:

- Operational
- Maintenance
- Out of Service

## 4.3 Device Groups

Device Groups must first be created in OTV by navigating to **Devices → Device Groups** and clicking on **Create New Group**. A new window appears asking the user for the group name as well as if the group will be Multicast or not. Additionally, device groups can be created by importing a file with all the information needed to form a group.

### 4.3.1 Adding Devices to a Group through OTV

Through the **All Devices**, **Meters**, or **Grid Automation** pages, the following steps can be performed to add multiple devices to a pre-existing group:

1. Search for devices based on device type, state, description, and possibly other metadata specific to a particular device type.
2. When your search has appropriately narrowed the list of devices in your Devices table to the devices you are interested in, click on the **Add Devices to Group** link.
3. Select an existing group from the dropdown menu.
4. Click **Submit** to add the devices in the table listing to the group.

Additionally, devices can be added to a group on a per-device basis through the following steps:

1. Find the device in question by searching for or filtering it out on the **All Devices** page.
2. Click on the row of the device in question to be brought to the **Device Details** page.
3. Click on the **Add to Group** link.
4. Using the dropdown menu, select the group that the device should be placed in and then click on **Submit** to add the device to that group.

### 4.3.2 Device Group Management

Users can manage device groups by navigating to **Devices → Device Groups**. From this screen, a table of all device groups on the network is displayed with the individual name of each group, multicast state, pending devices, and total devices. The following options can be applied to one or more device groups when the checkbox next to a group is checked:

- **Delete:** Allows the operator to remove the selected group from the user interface (UI). If messages have already been sent for the group, then the group is made inactive. If no

messages have been sent for the group, then the group is simply deleted. In either case, the group is no longer displayed in the UI. Deletion can be applied to multiple groups at the same time. Note that a multicast group must be empty in order for it to be deleted from this page.

- **Edit Name:** Allows the operator to update the name of a group. Note that name editing can only be performed to one group at a time.
- **Create New Group:** Allows the user to create a new group by entering a unique name. The user can also specify whether this new group is multicast or not by using the checkbox next to the multicast option.

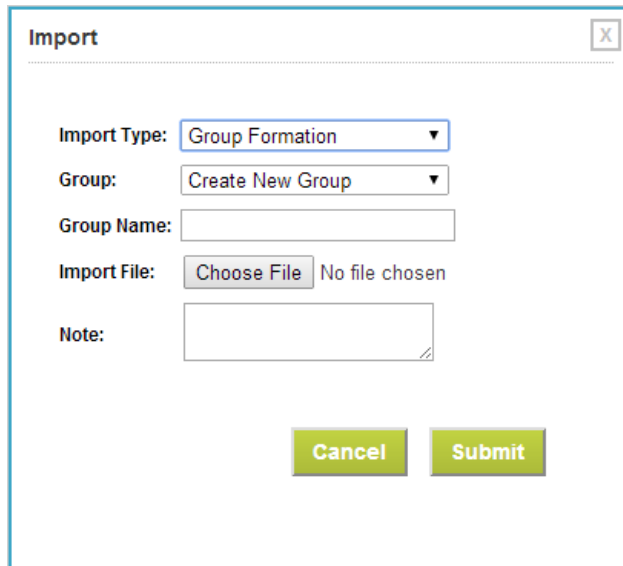
### 4.3.3 Device Group Actions

From the Device Groups page, selecting an individual group takes the user to the **Device Group Detail** page where the following actions can be applied to devices which have been added to the group. Multiple devices can be selected at a time using the checkbox on the left side of the table.

- **Import Devices:** This is defined in section 4.3.4. Note that the format listed in section 4.3.4 applies here but only the devices listed in the file are imported to the group that is currently being viewed by the user.
- **Manage Tasks:** Displays a dialog box that allows the operator to specify scheduled tasks for the group. The tasks available for scheduling vary depending on the device type of the group. For available scheduled tasks for a device type, consult the corresponding OTV supplemental document for that device.
- **Messages:** Allows the operator to send a message to all devices in the group and to view all previously sent messages for the selected device group. The types of messages available for sending to devices depend on the device types in the group and may also depend on specific profiles for the device. If there is more than one device type in the group, then only generic message options are available. Some device types may have specific messages. For more information, consult the corresponding OTV supplemental document for that device.
- **Delete:** Deletes all devices that have been selected by the checkboxes on the page. Note that for multicast groups, this deletion will not happen immediately and may take a few seconds for the page to update.

### 4.3.4 Importing Devices into a Group

The **Import File** link on the **Devices → Import File Listing View** allows devices to be added to a group via file import when the Group Formation option is selected. The file format supported is the hex Mac Address of the device, separated by new lines. The leading 0x is not required to be present. The leading 0's are also not required to be present. Different device types may have additional file formats supported. For available formats, consult the corresponding OTV supplemental document for that device.



The image shows a software dialog box titled "Import" with a close button (X) in the top right corner. Inside the dialog, there are several input fields and buttons. The "Import Type:" field is a dropdown menu currently showing "Group Formation". The "Group:" field is another dropdown menu showing "Create New Group". Below these is a text input field for "Group Name:". The "Import File:" section includes a "Choose File" button and the text "No file chosen". At the bottom left is a "Note:" label followed by a text area. At the bottom center are two green buttons: "Cancel" and "Submit".

**Figure 18. Group Formation Import Feature**

In the Import dialog box, you may select to import all devices in the file into a new group or an existing group.

# 5 Administering OTV

## 5.1 Viewing Reports

Clicking the Admin → Reports tab brings up the Reports screen, shown below.

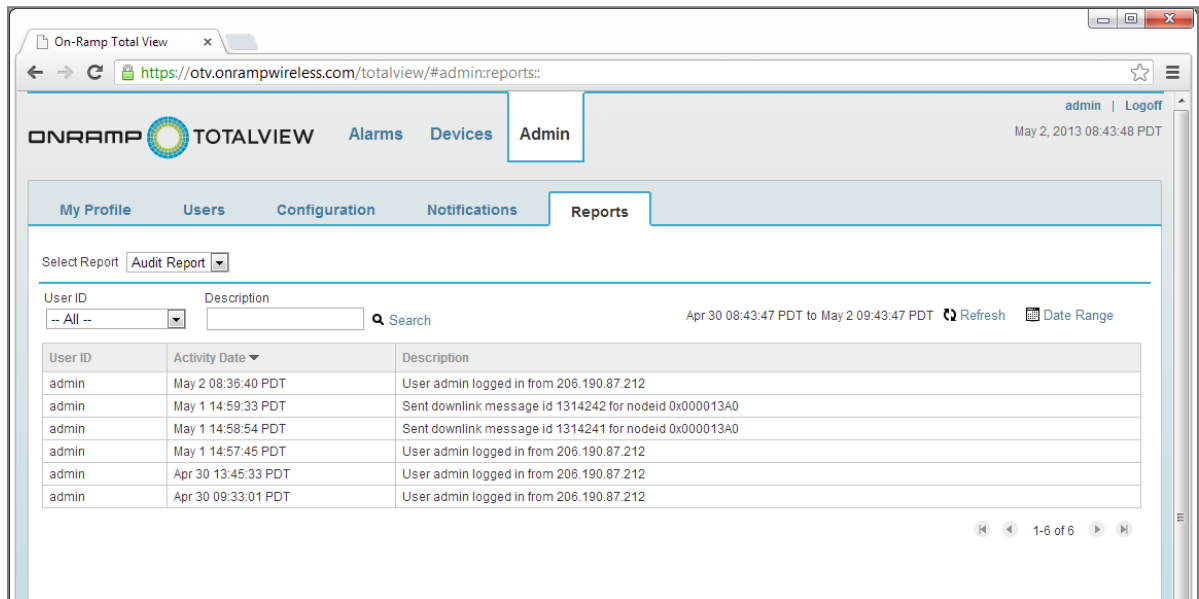


Figure 19. Reports Page

A drop-down menu in the upper left corner allows you to display the following reports: Audit Report, Status, Active Users, and Software. These reports are defined on the following pages along with example screens. To access these reports:

1. Use the User ID drop-down menu to select a user. The report only returns information for that user.
2. Use the Date Range link to specify the range of dates for information displayed in the report.
3. Use the Search field to search on a specific keyword.
4. Clicking on the column headings of the table sorts the information alphabetically or by date.

**Audit Report:** Displays a detailed history of configuration changes, attempted logins, successful or unsuccessful, and downlink messages (i.e., messages sent to APs and devices) in OTV, by user. Select "--All--" in the User ID field to see all users' activities. An Audit Report example is shown in the figure above.

**Status:** Shows the last status update of system processes: Alarm Notification, Alarm Processing, HES Receiver and Alarm Detection.

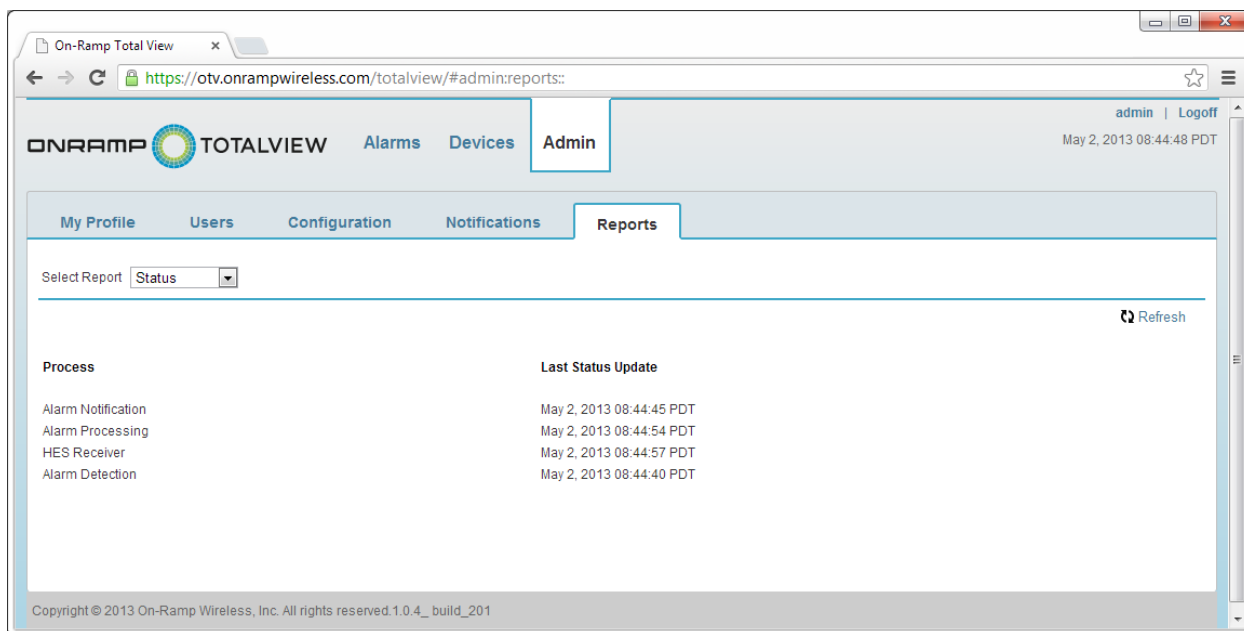


Figure 20. Status Reports Page

**Active Users:** Displays the log-in time and IP address of current system users.

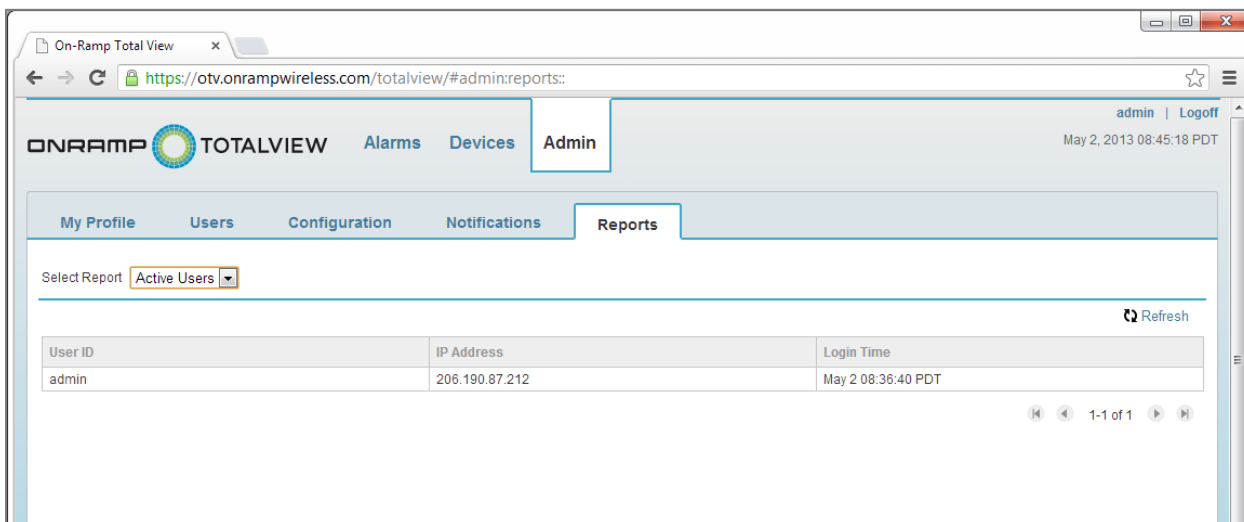
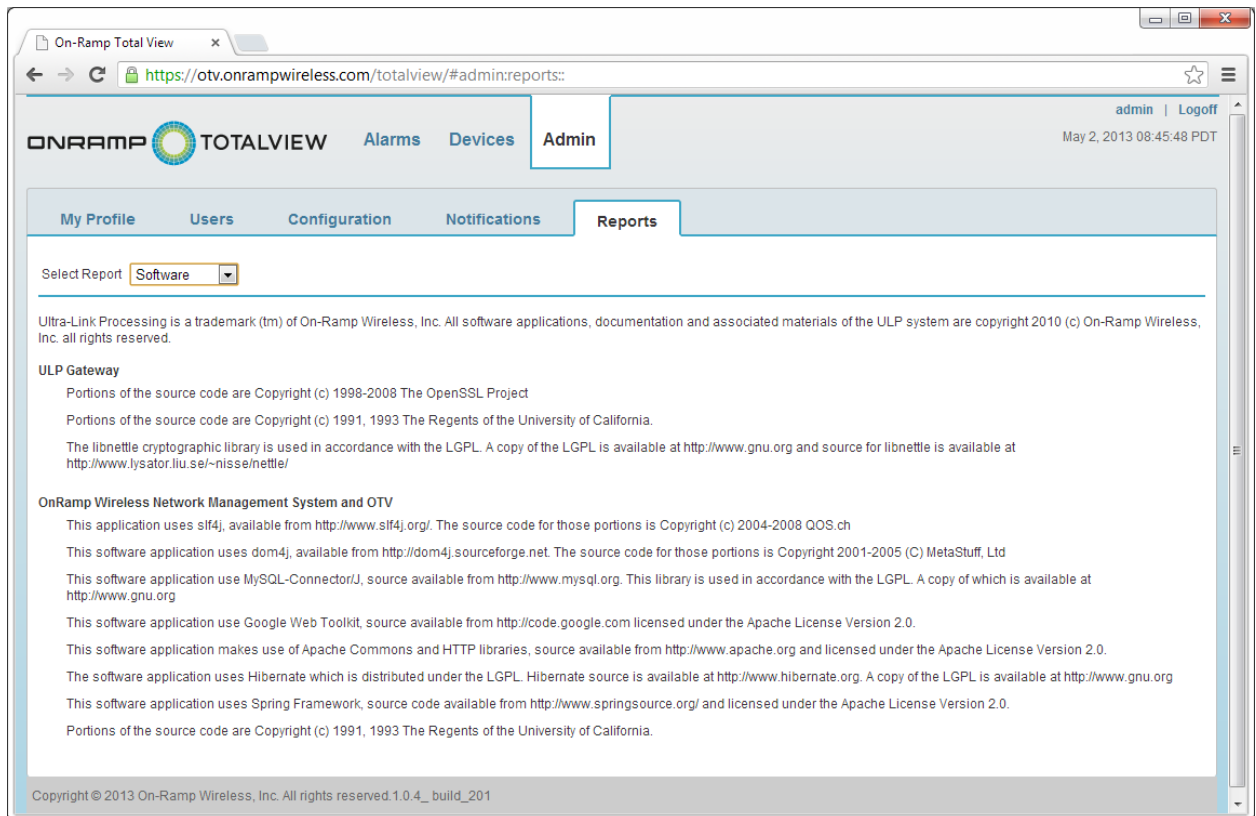


Figure 21. Active Users Page



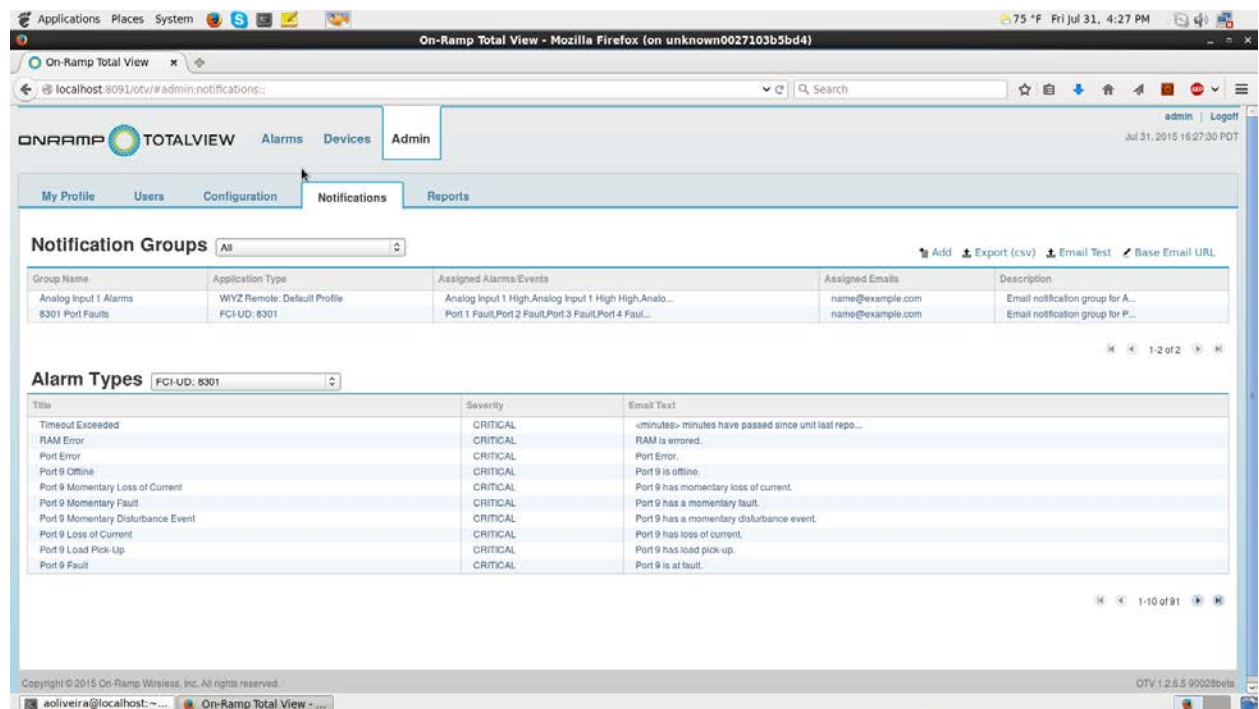
**Software:** Displays detailed information about software used in OTV.



**Figure 22. Software Reports Page**

## 5.2 OTV Notifications

One of the key functions of OTV is to display and manage email alerts triggered by an alarm condition in one or more devices connected to the RPMA network. Responding to these alerts allows health management of the network and devices. To begin configuring these notifications, navigate to **Admin → Notifications**.



**Figure 23. Notifications Page Overview**

This page is split into two camps: **Notification Groups** and **Alarm Types**. Notification groups display a list of all notification groups that have been created on the network. Alarm types list the supported alarms for a given device type. Next to Notification Groups at the top of the page, the drop-down menu allows users to filter out groups by their specific device types. A similar drop down menu can be found next to Alarm Types, allowing users to see all alarms for a specific device type.

### 5.2.1 Notification Groups

The Notification Groups section is broken into several subpages of up to 10 notification groups per page. At a glance, a user can see the name of the group under **Group Name**, the type of device that the notification group belongs to under **Application Type**, a list of the alarms that will send out an email when triggered under **Assigned Alarms/Events**, a list of the email addresses that these notifications will be sent to under **Assigned Emails**, and a brief description of the group found under **Description**. Clicking on an individual Alarm Group will open up the **Notification Group Editor** where a user can make changes to the existing notification group. At the bottom right of this page are the navigation buttons where a user can cycle between the different pages of notification groups that are on the network.

Taking a closer look at Figure 23, we can see the following buttons listed above the table itself:

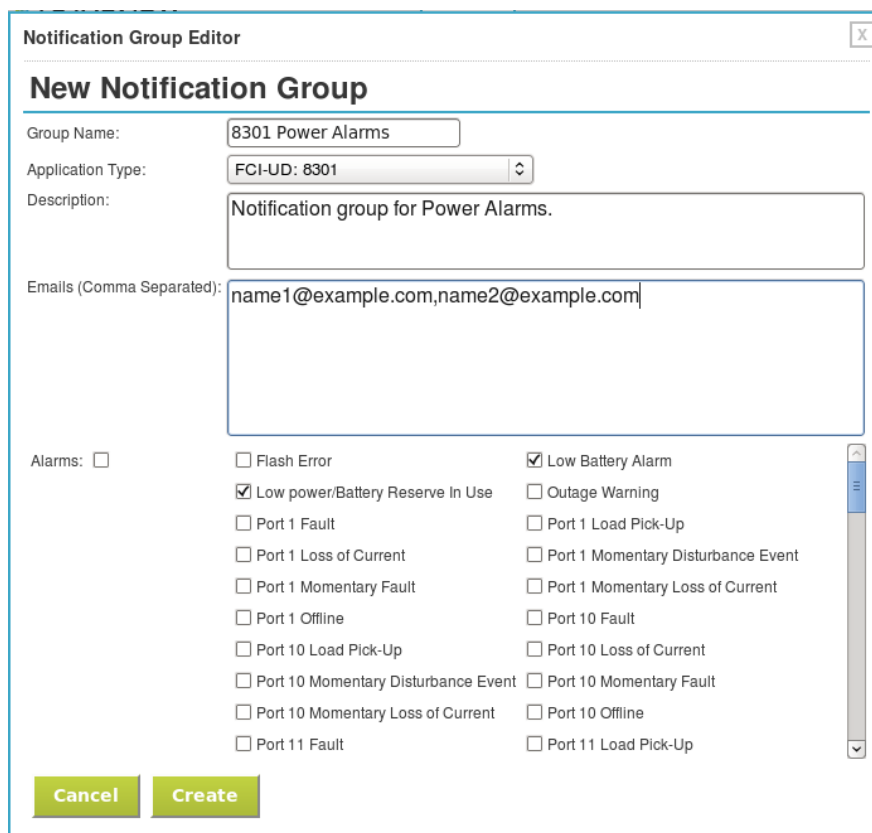
 **Add**  **Export (csv)**  **Email Test**  **Base Email URL**

**Figure 24. Notification Page Buttons**

- **Add:** Opens the **Notification Group Editor** window
- **Export (csv):** Creates a .csv file of all notification groups that a user can download
- **Email Test:** Allows users to send out a test email to confirm that their email options have been configured correctly
- **Base Email URL:** Allows users to edit the email address that OTV uses to send out these Notification Emails

## 5.2.2 Creating and Editing Notification Groups

To create a new Notification Group, click on the **Add** button detailed in the previous section. From here, the **Notification Group Editor** window should appear. The following figure shows an example of how this window looks.



The screenshot shows the "Notification Group Editor" window with the title "New Notification Group". It contains the following fields and options:

- Group Name:** 8301 Power Alarms
- Application Type:** FCI-UD: 8301
- Description:** Notification group for Power Alarms.
- Emails (Comma Separated):** name1@example.com,name2@example.com
- Alarms:**
  - ☐ Flash Error
  - ☒ Low power/Battery Reserve In Use
  - ☐ Port 1 Fault
  - ☐ Port 1 Loss of Current
  - ☐ Port 1 Momentary Fault
  - ☐ Port 1 Offline
  - ☐ Port 10 Load Pick-Up
  - ☐ Port 10 Momentary Disturbance Event
  - ☐ Port 10 Momentary Loss of Current
  - ☐ Port 10 Offline
  - ☐ Port 10 Load Pick-Up
  - ☒ Low Battery Alarm
  - ☐ Outage Warning
  - ☐ Port 1 Load Pick-Up
  - ☐ Port 1 Momentary Disturbance Event
  - ☐ Port 1 Momentary Loss of Current
  - ☐ Port 10 Fault
  - ☐ Port 10 Loss of Current
  - ☐ Port 10 Momentary Fault
  - ☐ Port 10 Offline
  - ☐ Port 11 Fault
  - ☐ Port 11 Load Pick-Up

At the bottom, there are two buttons: **Cancel** and **Create**.

**Figure 25. New Notification Group Example**

The Notification Group Editor is broken into the following sections:

- **Group Name:** An empty text field where the user can enter in a name for the new Notification Group.
- **Application Type:** A drop-down menu that allows the user to select the device type for this group. This selection determines what types of alarms show up in this window.
- **Description:** An empty text field where the user can enter in a simple description for the new Notification Group. This description will show up in OTV and in any exports of Notification Groups.
- **Emails:** An empty text field where users can enter in email addresses that are separated by commas. Any alarm that is triggered that belongs to this new notification group will send out an email to the addresses listed in this section.
- **Alarms:** This section varies depending on what device is chosen from the Application Type menu. However, there will always be check boxes from which a user can select which alarms for which they want to be notified.
- **Events:** Not pictured in Figure 25. However, this section is functionally identical to the Alarms section. The alarms listed in this section only pertain to AMI devices and, as such, they do not appear unless **Smart Meter** is selected from the Application Type menu.

After all fields have been filled in with the necessary information, clicking on **Create** saves the Notification Group to OTV. After this, any alarms that are triggered (from those specified in the notification group) will begin sending out email notifications.

**NOTE:** Any alarms that are triggered while a device is in **Maintenance Mode** will not send out email notifications.

To edit a Notification Group, simply click on the group that needs to be edited from the Notifications Page. The editor window reappears and looks just like the one displayed in Figure 25 with a few minor exceptions:

- After the Application Type is selected (when the Notification Group is created), it cannot be edited from this screen.
- **Create** has been replaced with **Delete** and **Save**, allowing users to delete the Notification Group or save changes made from this screen.

Aside from the two exceptions listed above, any field can be edited and will update throughout OTV after clicking on **Save** at the bottom of the window.

## 5.3 Understanding Email Alerts

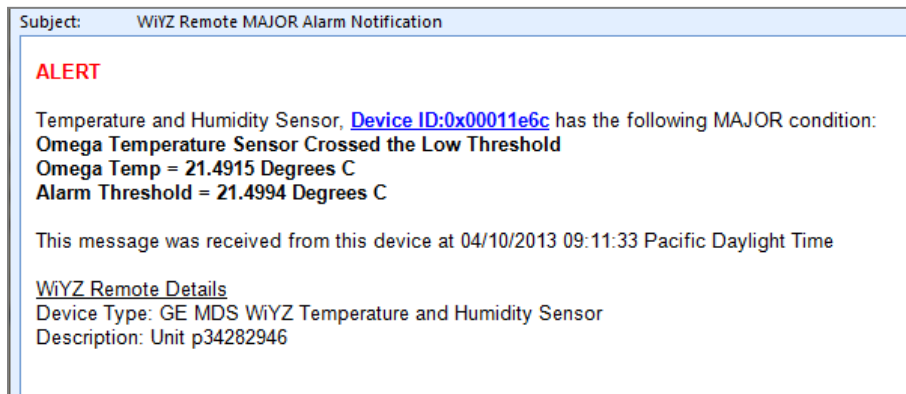
After properly configuring a Notification Group, triggered alarms on the network will begin sending email notifications. Responding to these alerts allows users to manage the health of the network and devices. The following example shows an email alert generated by an alarm. Each email identifies the following information:

- Description as entered into OTV for the device
- Short description of the alarm

- Time stamp for the message
- Manufacturing details regarding the device being monitored.

**NOTE:** The information differs depending on the actual device. For more details, consult the corresponding OTV supplemental document for that device.

The following example email highlights an analog threshold-crossing alarm on a WiYZ temperature sensor.



**Figure 26. Email Notification Example**

After an email alert is sent, the operator may ignore the alert or acknowledge it, as described in section 3.5.2 Acknowledging Alarms.

Each device supports a configurable timeout value configured in the OTV config.properties file called **<device\_type>.status.interval.max.minutes**. The setting of this parameter defines the maximum amount of time in minutes between two successive messages from the device before OTV generates an Unreachable alarm condition. This is an application-level alarm that informs operators that a device may have stopped communicating to the network and some investigation may be required.

Refer to the corresponding device supplement document for specific instructions related to the particular device. Table 1 provides a list of available supplements.

## 5.4 Maintaining an Active Directory Account

For systems that use Active Directory for OTV account maintenance, account creation and editing functions are usually controlled by the Information Technology (IT) group responsible for Active Directory account maintenance.

Use the following steps to edit a user account:

1. Log in to OTV as an administrator or the account holder.
2. Click the **Admin → Users** tabs.
3. Highlight to select the account to edit.

4. Edit the profile information.

**NOTE:** For Active Directory accounts, only the local administrator or user can modify the profile section of an account. The corporate IT group responsible for Active Directory account maintenance must change all of the account information in the security section.

5. Click **Save**.

## 5.5 Maintaining a Local Account

OTV contains the following types of user roles:

- Administrator
- Operator
- Guest
- Service

When a user role is created, each additional role that is created in the OTV system is created as an admin, an operator, or a guest. These role types exist for both Local Accounts and Active Directory-enabled systems.

- When configuring **Local Accounts**, the Local Account administrator creates and maintains the roles.
- When using Active Directory, the IT group is responsible for setting up OTV roles. Roles are created according to role type (admin, operator, or guest) and are mapped to the Active Directory.

For additional information, contact On-Ramp Wireless customer support at [support@onrampwireless.com](mailto:support@onrampwireless.com).

### 5.5.1 Administrator

Initially in OTV installations that do not use Active Directory controlled logins, the administrator (admin) role is the only default account available. This admin account can only manage accounts created in Local Accounts. If using Active Directory, account maintenance is handled by the IT group. For Local Account login, contact On-Ramp Wireless for the default User ID and password.

The administrator role has complete control over the OTV configuration, operation, and local account administration. For security, this is the equivalent to a root account for the application. When using Active Directory, the IT group that controls the Active Directory also controls the creation of accounts. If this is the first time that a local system administrator logs in to the OTV system, the system administrator should change the default account password for the local default admin account.

It is recommended that the administrator do the following:

- Change the default password for the default local admin account.

- Create an account for all other OTV operators that have access to the system and do not regularly use the default admin account for day-to-day operations when using Local Accounts.
- Create operator type roles for day-to-day operations in the OTV system.

## 5.5.2 Operator

The operator role allows operators to use OTV for day-to-day operations. This is the default account security type for an operator. Users with the “operator” role may only view information and data for the device types to which they have been given access. When the administrator creates the “operator” accounts, she must choose the expected application types that an operator must see. A user with the “operator” role can edit application details and put a device into “maintenance” mode, which is explained in section 4.1.

The operator account does not allow the following OTV functions:

- Adding users
- Deleting users
- Editing users

## 5.5.3 Guest Account

The guest account is a read-only account. It displays a read-only view for specific types of data to facilitate demonstrations. Guest account users cannot configure system parameters or change user account information.

**NOTE:** When logging in to OTV, the tabs displayed are different for each account type. For example, logging in with an administrator role displays additional tabs that are not available when using a Guest role, which is read-only.

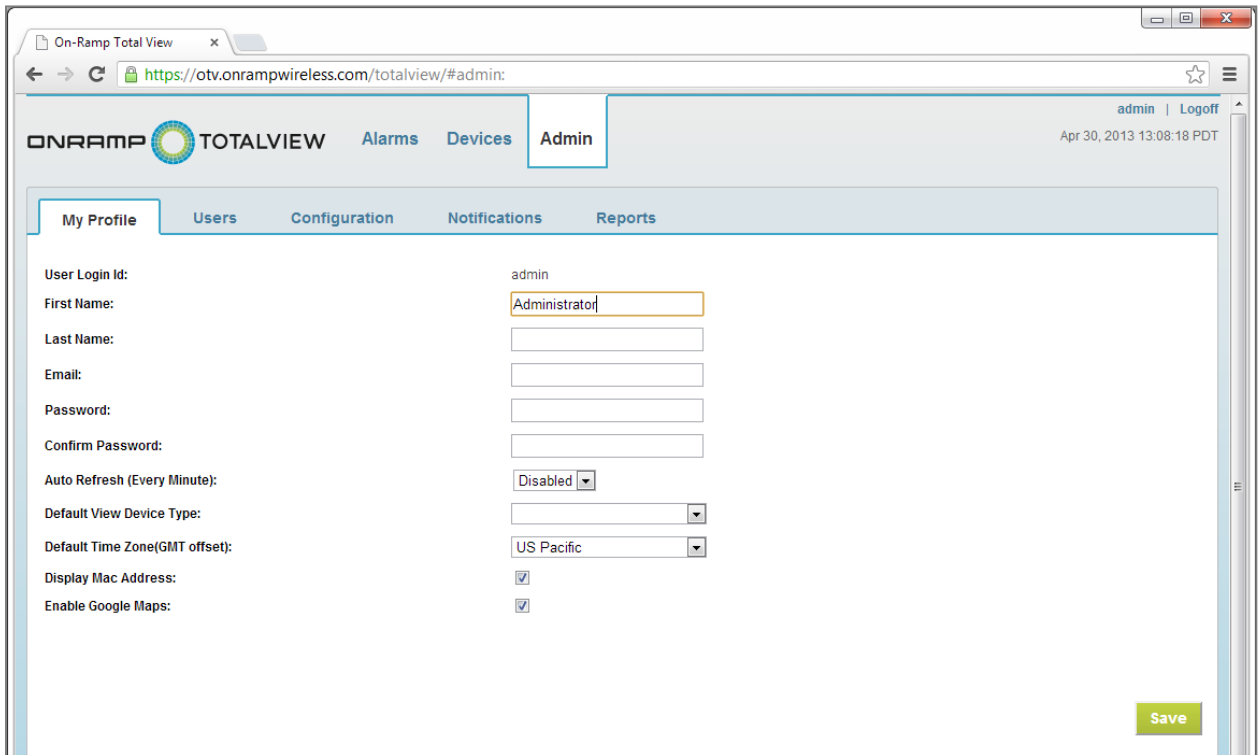
## 5.5.4 Service Account

The Service Role is required to support the REST API and is covered in the *On-Ramp Total View REST API Guide (010-0038-00)*.

## 5.5.5 Adding a Local User Account

Use the following steps to add an OTV local user account:

1. From the login page, log in with an administrator account.
2. Click the **Admin** tab.



The screenshot shows the 'My Profile' page in the On-Ramp Total View interface. The page has a header with the On-Ramp Total View logo and navigation tabs: Alarms, Devices, and Admin. The Admin tab is selected. Below the header, there are sub-tabs: My Profile, Users, Configuration, Notifications, and Reports. The My Profile sub-tab is active. The form contains the following fields:

- User Login Id: admin
- First Name: Administrator
- Last Name: (empty)
- Email: (empty)
- Password: (empty)
- Confirm Password: (empty)
- Auto Refresh (Every Minute): Disabled
- Default View Device Type: (empty)
- Default Time Zone(GMT offset): US Pacific
- Display Mac Address: ☒
- Enable Google Maps: ☒

A green 'Save' button is located at the bottom right of the form.

**Figure 27. “My Profile” Page**

3. Click **Users** → **Add User**.
4. Complete the user information.



On-Ramp Total View

https://otv.onrampwireless.com/totalview/#admin:user

admin | Logoff

Apr 30, 2013 13:08:47 PDT

ONRAMP TOTALVIEW Alarms Devices Admin

My Profile Users Configuration Notifications Reports

User Login Id:

First Name:

Last Name:

Email:

Password:

Confirm Password:

Enabled:

Auto Refresh (Every Minute):

Default View Device Type:

Default Time Zone(GMT offset):

Display Mac Address: ☐

Enable Google Maps: ☐

To assign a role to the user, drag the role name from 'Available Roles' onto 'Assigned Role' list box. A user with no role is disabled from logging in.

Assigned Role

Available Roles

- Admin
- Guest
- Operator
- Service

To assign device types to a person, drag type names from 'Available Device Types' to 'Assigned Device Types'.

Assigned Device Types

Available Device Types

- Generic Node
- FCI-UD: 8301A
- FCI-O: WSO-11
- WYZ Remote
- RML: Obstruction Light

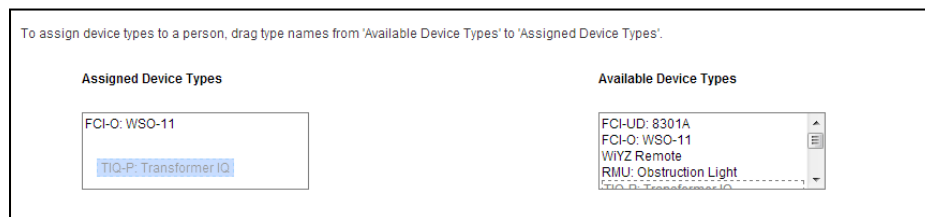
Cancel Save

Copyright © 2013 On-Ramp Wireless, Inc. All rights reserved. 1.0.4\_build\_201

**Figure 28. Adding a User**

**NOTE:** In addition to the login information, email address, and password configuration, admin users can set up account attributes for each user, as follows:

- ❑ **Enabled**  
Select Enabled or Disabled to make this user account active or inactive.
  - ❑ **Default View Device Type**  
OTV supports multiple end device applications. Users are typically only concerned with a particular application. This field defines the default view that OTV displays for the user when they log in to use OTV.
  - ❑ **Time Zone**  
Choose the time zone to use for the display from the **Default Time Zone (GMT offset)** drop-down list.
  - ❑ **Display Mac Address**  
Used for OTV to display the On-Ramp Device Mac Address for the operator.
  - ❑ **Enable Google™ Maps**  
Do not select the **Enable Google™ Maps** check box. For information about using Google Maps for geospatial display, consult your On-Ramp Wireless representative.
5. Select one role from the list of **Available Roles**, then drag and drop it into the **Assigned Role** section.
  6. Select **Available Device Types**, then drag and drop them into the **Assigned Device Types** section.



**Figure 29. Assigned Device Types Section**

**NOTE:** If the user has access to multiple data types, such as rights for an administrator or other privileged user, drag multiple **Available Device Types** to **Assigned Device Types**.

7. Click **Save**.

## 5.5.6 Editing a Local User Account

Use the following steps to edit a user account:

1. Click the **Admin** → **Users** tabs.
2. Click an account name to select it for editing. The Edit User panel displays, as shown below.

The screenshot shows the On-Ramp Total View web interface. The browser address bar displays `https://otv.onrampwireless.com/totalview/#admin:user:id=ff8081812726883a01272688698b0001`. The interface has a top navigation bar with tabs for **Alarms**, **Devices**, and **Admin**. The **Admin** tab is active, and the **Users** sub-tab is selected. The main content area is titled 'Edit User' and contains the following fields and sections:

- User Login Id:**
- First Name:**
- Last Name:**
- Email:**
- Password:**
- Confirm Password:**
- Auto Refresh (Every Minute):**
- Default View Device Type:**
- Default Time Zone(GMT offset):**
- Display Mac Address:** ☒
- Enable Google Maps:** ☒

To assign a role to the user, drag the role name from 'Available Roles' onto 'Assigned Role' list box. A user with no role is disabled from logging in.

Assigned Role	Available Roles
<input type="text" value="Admin"/>	<div>Admin Guest Operator Service</div>

To assign device types to a person, drag type names from 'Available Device Types' to 'Assigned Device Types'.

Assigned Device Types	Available Device Types
<input type="text"/>	<div>Generic Node FCI-UD: 8301A FCI-O: WSO-11 WiYZ Remote PML Obstruction Light</div>

At the bottom right, there are **Cancel** and **Save** buttons. The footer text reads: Copyright © 2013 On-Ramp Wireless, Inc. All rights reserved. 1.0.4\_build\_201

Figure 30. Editing User Information

3. Modify the profile and security information as needed.
4. Click **Save**.

## 5.6 Advanced Administration Features

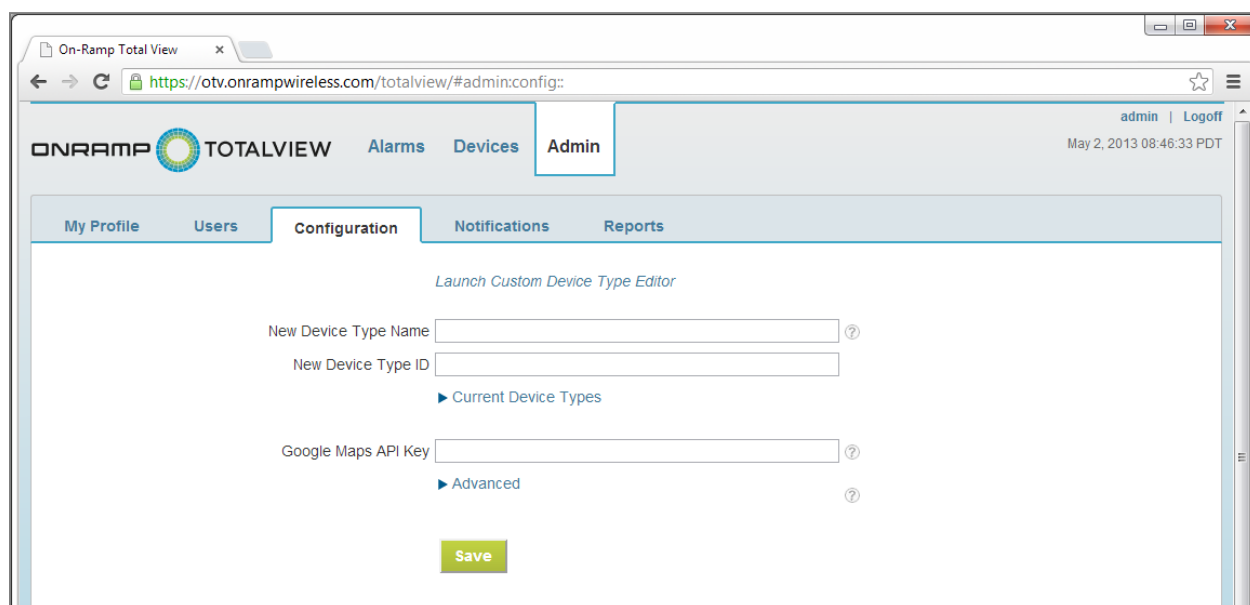
### 5.6.1 Adding New Device Types

**NOTE:** This information is geared toward device developers only.

OTV supports and recognizes many types of applications and devices. Over time, a system may add new device types. OTV facilitates the early prototyping of new device types while application alarming and packet parsing are in development. For corresponding configurations that must be made in the EMS for newly-added device types, see the *EMS Operator Guide*.

Use the following steps to add a new device type to OTV:

1. Log in to OTV with an administrator account.
2. Click the **Admin** → **Configuration** tab.

The screenshot shows a web browser window with the URL https://otv.onrampwireless.com/totalview/#admin.config:. The page has a header with the On-Ramp Total View logo and navigation tabs: Alarms, Devices, and Admin. The Admin tab is selected. Below the header, there are sub-tabs: My Profile, Users, Configuration, Notifications, and Reports. The Configuration tab is active. The main content area is titled "Launch Custom Device Type Editor" and contains three input fields: "New Device Type Name", "New Device Type ID", and "Google Maps API Key". Each field has a help icon (question mark). Below the "New Device Type ID" field is a link "Current Device Types". Below the "Google Maps API Key" field is a link "Advanced". At the bottom of the form is a green "Save" button.

**Figure 31. Configuration Page**

3. In the **New Device Type Name** field, enter a description.

**NOTE:** Contact your On-Ramp Wireless representative to obtain a permanent application type to be assigned a new device type ID.

4. Enter the **New Device Type ID**.

**NOTE:** This must be the same device type created in EMS for this application.

5. Click **Save**. After completing this step and the corresponding EMS configuration, OTV displays data from the new device type.

## 5.6.2 Customizing OTV

Customizing OTV involves editing external text files, `config.properties` and `<device name>.properties`, found on the OTV server. Among the settings `config.properties` affects are:

- Database connection information
- Application module configuration
- Maximum missed interval alert timeout
- Device-specific configuration
- Alarm trigger settings
- Email notification settings
- SMTP server settings
- Active directory authentication
- Users and Groups options
- Login Failure Lock Out

The file, `<device name>.properties`, affects settings specific to the particular device.

To configure OTV for a particular application, ensure that the RPMA Network is running and under control of the EMS, as described in the *EMS Operator Guide*. For more information, contact On-Ramp Wireless customer support at [support@onrampwireless.com](mailto:support@onrampwireless.com).

### Opening `config.properties` file

This properties file is located in the following directory:

```
<otvserver>:/opt/onramp_apps/otv/instance_1/config.properties
```

Use a text editor to edit and save the file. See Appendix A for a sample `config.properties` file.

### Opening `<device name>.properties` file

This properties file is located in the following directory:

```
<otvserver>:/opt/onramp_apps/otv/instance_1/<device name>.properties
```

Use a text editor to edit and save the file.

# Appendix A Sample Config Properties File

---

The following content is a sample config.properties file for reference.

```
####
# Database connection information
# User must specify the db connection info here
####

# sample oracle
#db.jdbcdriver=oracle.jdbc.driver.OracleDriver
#db.jdbcurl=jdbc:oracle:thin:@<DBHOST>:1521:<ORACLESID>
#db.userid=<DBUSER>
#db.userpwd=<DBPASS>
#db.validatequery=select 1 from dual
#hibernate.dialect=org.hibernate.dialect.Oracle10gDialect
#hibernate.show_sql=false
#hibernate.default_schema=xxxxxx

# Sample Oracle RAC URL
#db.jdbcurl=jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=on)(ADDRESS=(PROTOCOL=
TCP)(HOST=host1)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=host2)(PORT=1521))(CON
NECT_DATA=(SERVICE_NAME=service)))

# sample mysql
#db.jdbcdriver=com.mysql.jdbc.Driver
#db.jdbcurl=jdbc:mysql://<DBHOST>/<DBNAME>?zeroDateTimeBehavior=convertToNull&u
seLegacyDatetimeCode=false&useTimezone=true&serverTimezone=UTC&useGMTMillisForD
atetimes=true
#db.userid=<DBUSER>
#db.userpwd=<DBPASS>
#db.validatequery=select 1
#hibernate.dialect=org.hibernate.dialect.MySQL5Dialect
#hibernate.show_sql=false
#hibernate.default_schema=

db.jdbcdriver=${installer:db.jdbcdriver}
db.jdbcurl=${installer:db.jdbcurl}
db.userid=${installer:db.user}
db.userpwd=${installer:db.password}
db.validatequery=${installer:db.validate}
db.type=${installer:db.type}
hibernate.dialect=${installer:db.dialect}
hibernate.show_sql=false
hibernate.default_schema=${installer:db.schema}
hibernate.search.indexBase=${installer:installDir}/lucene/indexes

####
# Application Modules
# specify each application dynamic module for OTV to load
# OTV will scan the class_path property and look for a class implementing
CimaApplicationAdapterInterface and load that as adapter
#
# format is app_adapter.<app_type_id>.<property_name>
# class_path - required, specify where app jar files are located, use ';' for
path separator, '<CIMA_HOME>' in path entry will be sub'd with runtime instance
directory e.g. /opt/onramp_apps/otv/instance_1
```

```

#           in most cases adapter will be packaged in single jar file, which
has server side java classes at their normal package paths and static web
files(css,images,etc) bundled under/webapp/<GwtModuleName> path, could
optionally specify a directory on file system
           that holds same directory structure as would have been in jar
format, i.e. java class directories and 'webapp/<GwtModuleName>' directory
structure.
# spring_app_ctx_file_names - required, specify classpath locations of spring
ctx file names separated by a comma, these need to be embedded in one of the
adapter jars in class_path, and stated as /orw/application/myappctx.xml or if
file is at root of classpath just the file name
#
# path separators should always be '/'
#
# IMPORTANT - if running more than 4 adapters, may need to increase -
XX:MaxPermSize, it's defaulted to 128m on cima.java.opts setting at bottom of
this config file. could try system run w/o change, but if 'out of memory, perm
gen' errors show up in logs, then need to add at least 25m per additional
adapter over 4.
#
####
#app_adapter.7.classpath=<CIMA_HOME>/dm/faalight/faalight-adapter.jar
#app_adapter.7.spring_app_ctx_file_names=faalightAdapterContext.xml
#app_adapter.2.classpath=<CIMA_HOME>/dm/fci/fci-adapter.jar
#app_adapter.2.spring_app_ctx_file_names=fciAdapterContext.xml

####
# Application Display
# Specify the loaded application to be displayed as the single list. The
default application
# for the display is the AMI.
#
#app_adapter.10.tab_display=Meters

####
# Alarm trigger settings
####

# if OTV adapter in hes container is enabled for process checking, then OTV
can monitor keep alive timing checks with gw or amqp
# if value is blank OTV container will not perform gw keepalive stateful
trigger check
alarm.gw_keepalive_max_inactivity_secs=120
# comma separated list of process check names that will be polled for keep
alive times(OTV data parsing adapter in hes container should specify the same
process check name)
alarm.gw_keepalive_process_check_names=hes1

# Maximum amount of delay between a message's birth date(1.3 = time received in
hes, 2.0 = gw timestamp header) and any application adapter that received the
uplink in hes
# if value is blank OTV container will not perform this stateful alarm check
alarm.gw_processing_delay_max_secs=300
# comma separated list of process check names that will be polled for latest
processing times(OTV data parsing adapter in hes container should specify the
same process check name)
alarm.gw_processing_delay_process_check_names=hes1

# How often alarm checks that run periodically (as opposed as in response to
messages as they are received) will run. The lower the

```

```
# value, the less delay there will be between any changes in state and when
alarms are created, updated or cleared.
alarm.stateful_iteration_interval_secs=20

# Devices and failure types to ignore. New alarms matching these devices or
failure types will not be saved, but existing alarms
# will continue to be updated until they are cleared.
alarm.ignore.device.node.ids=0xDEADBEEF
alarm.ignore.failure_type.names=

####
# Email notification settings
####

# How often the notification process will run. The lower the value, the more
precisely the delay and reminder interval settings on
# notification groups will be honored in terms of sending emails.
notification.iteration_interval_secs=15

# Maximum amount of time after an alarm clears that it will be considered for
sending cleared notifications. When the notification
# process is running normally, this would only need to be at least 2 *
iteration_interval_secs. However, setting it a bit higher allows
# for slow downs communicating with the database or smtp server. If more than
this much time passes between notification iterations,
# some cleared notification emails could be missed, but otherwise there is no
impact to anything.
notification.cleared_alarm_window_secs=300

# SMTP server settings
notification.smtp.host=${installer:smtp.host}
notification.smtp.port=${installer:smtp.port}
#notification.smtp.user=<SMTPUSER>
#notification.smtp.password=<SMTPPASS>
#notification.smtp.tls=false
notification.from.address=OTV@Notification
notification.from.name=OTV

# Set to true to stop emails from going out over smtp
notification.test_mode=false

#####
####
#REST Web Services
#service should only be enabled for secured web servers (https)
#maxresults limits the query size
#thread.interval is the second between sdu request allowed (Throttle)
#session.token.life is the number of hours the token is valid. the token will
be auto-deleted after the expiration date
#session.token.autoextend
####

rest.services.enabled=true
rest.services.thread.interval=0
rest.services.maxresults=1000
rest.services.session.token.life=24
rest.services.session.token.autoextend=true
#####
```



```
####
# Active directory authentication
####

# List of domains to allow authentication on.
#activedirectory.domains=example.com

# Optional, per-domain LDAP configuration. Default behavior is to use DNS to
locate domain
# controllers when no hosts are supplied. The port and ssl options apply only
to manually specified hosts,
# not to automatically discovered domain controllers.
#activedirectory.example.com.ldap.hosts=dc1.example.com, dc2.example.com
#activedirectory.example.com.ldap.port=636
#activedirectory.example.com.ldap.ssl=true
#activedirectory.example.com.ldap.ssl.acceptall=true

# Per-domain mappings from active directory groups to user roles. Even with
valid credentials, a user
# will not be allowed to log in unless their active directory groups map them
to an admin, operator or guest role.
# When a user maps to multiple roles, the most privileged role will be used.
Each AD group must be specified by its
# distinguished name in quotes. These are case-sensitive.
#activedirectory.example.com.role.admin.groups="CN=EMS
Admins,DC=example,DC=com", "CN=OTV Admins,DC=example,DC=com"
#activedirectory.example.com.role.operator.groups="CN=EMS
Operators,DC=example,DC=com", "CN=OTV Operators,DC=example,DC=com"
#activedirectory.example.com.role.guest.groups="CN=EMS
Guests,DC=example,DC=com", "CN=OTV Guests,DC=example,DC=com"

# Per-domain mappings from active directory groups to data types. The types
must have spaces
# escaped (per specification for keys in properties files) and must match
exactly (including case) with the
# type names in the UI. Users that do not map to any data types will be allowed
to log in, but will
# be unable to view any node data (they must still map to a user role). The
same rules that apply for mapping
# roles apply here.
#activedirectory.example.com.datatype.FCI.groups="CN=OTV FCI
Users,DC=example,DC=com", "CN=OTV Super Users,DC=example,DC=com"
#activedirectory.example.com.datatype.FAA\ Light.groups="CN=OTV FAA
Users,DC=example,DC=com", "CN=OTV Super Users,DC=example,DC=com"

###
# LDAPv3 directory authentication
###

# List of domains to allow authentication on
#ldap.domains=widgetco.local

# Connection/protocol options:
# - When no hosts are specified, DNS will be used to located LDAP servers via
_ldap._tcp.<domain>, or
# _ldaps._tcp.<domain> if encryption is set to ssl.
#ldap.widgetco.local.hosts=ldap1.widgetco.local, ldap2.widgetco.local
# - When hosts are supplied, port defaults to 389, otherwise the port in DNS
is used. This will generally
# need to be changed when using ssl encryption (typically port 636).
```

```
#ldap.widgetco.local.port=389
# - Server connect and request timeouts.
#ldap.widgetco.local.connect_timeout_millis=5000
#ldap.widgetco.local.request_timeout_millis=15000
# - Transport security to use. Possible options are 'none', 'ssl' and
'start_tls'. See the hosts
# - comment for implications when doing DNS discovery of servers. The default
is none.
#ldap.widgetco.local.encryption.type=none
# - Whether to skip certificate verification when using ssl or start_tls
encryption.
#ldap.widgetco.local.encryption.ssl.accept_all=false

# The maximum referral depth to follow. The default value is 5. A value of 0
disables referral following.
#ldap.widgetco.local.referrals.limit=5

# Users options:
# - DN relative to the domain under which users will be searched for. By
default, the entire
# - tree under the domain will be searched.
#ldap.widgetco.local.users.dn=
# - Optional filter to use when searching for users.
#ldap.widgetco.local.users.filter=(objectClass=nmsUser)
# - Required name of attribute on user entries that is used when logging in.
#ldap.widgetco.local.users.login_attribute=uid
# - Optional name of attribute with a user's display name
#ldap.widgetco.local.users.name_attribute=cn

# Groups options:
# - DN relative to the domain under which groups will be searched for. By
default, the entire
# - tree under the domain will be searched.
#ldap.widgetco.local.groups.dn=
# - Optional filter to use when searching for groups.
#ldap.widgetco.local.groups.filter=(objectClass=groupOfUniqueNames)
# - Required name of the group attribute holding user DN(s).
#ldap.widgetco.local.groups.members_attribute=uniqueMember

# The quoted DN's of groups which grant authenticated users the admin, operator
and guest roles. Group DN
# mappings are case-sensitive. When a user is mapped to multiple roles, the
most privileged role wins.
#ldap.widgetco.local.admin.groups="CN=EMS Admins,DC=widgetco,DC=local", "CN=OTV
Admins,DC=widgetco,DC=local"
#ldap.widgetco.local.operator.groups="CN=EMS Operators,DC=widgetco,DC=local",
"CN=OTV Operators,DC=widgetco,DC=local"
#ldap.widgetco.local.guest.groups="CN=EMS Guests,DC=widgetco,DC=local", "CN=OTV
Guests,DC=widgetco,DC=local"

# The quoted DN's of groups which assign authenticated users privileges to view
assets belonging to
# the respective customer(s). Group DN mappings are case-sensitive. These
mappings are only relevant when
# the customer_id property is non-zero. When customer_id is configured, only
users which map to that customer_id
# are allowed to log in.
#ldap.widgetco.local.customer.666.groups="CN=Devil Inc.,DC=widgetco,DC=local"
#ldap.widgetco.local.customer.42.groups="CN=Answer To The Ultimate Question
LLC,DC=widgetco,DC=local"
```

```
# The quoted DNs of groups which grant authenticated users privileges to view
assets belonging to
# the respective data type(s). Group DN mappings are case-sensitive.
#ldap.widgetco.local.datatype.2.groups="CN=FCI,CN=Data
Types,DC=widgetco,DC=local", "CN=All-seeing Person,DC=widgetco,DC=local"
#ldap.widgetco.local.datatype.7.groups="CN=FAA Light,CN=Data
Types,DC=widgetco,DC=local", "CN=All-seeing Person,DC=widgetco,DC=local"

###
# Login Failure Lock Out
###

# OTV will lock out the user if the lock out is enabled and the number of
failed attempts > num_attempts.
# Once the user account is disabled, only the admin user can unlock the
account.
# The lock out feature also applies to the admin user accounts. But after the
specified admin lockout period,
# the admin user can log back in with the correct passowrd. The default period
is 10 minutes.
#
enable_lockout=yes
num_attempts=5
admin_lockout_period=10

####
# JVM settings
####
cima.java.opts=-Xmx512m -XX:MaxPermSize=128M

####
#Web Browser Title
####
cima.web.browser.title=On-Ramp Total View

####
# Web session time out
####
cima.web.session_timeout_minutes=300
```

## Appendix B Abbreviations and Terms

---

Abbreviation/Term	Definition
AP	Access Point. The RPMA Network component geographically deployed over a territory
OTV	On-Ramp Total View. The network component that passes data from the Gateway to the associated upstream databases.
EMS	Element Management System. The network component that provides a concise view of the RPMA Network for controls and alarms.
Node	The generic term used interchangeably with end point device.
ORW	On-Ramp Wireless
RMU	Remote Monitoring Unit. The end device that monitors Federal Aviation Administration (FAA) obstruction lights.
SMS	Short Message Server
SMTP	Simple Mail Transfer Protocol
UI	User Interface