ONRAMP WIRELESS

TOTAL REACH NETWORK

EMS Operator Guide

Communication System 2.1

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

EMS Operator Guide, Communication System 2.1

010-0107-00 Rev. A

September 13, 2013

Contents

Figures

Tables

Revision History

Revision	Release Date	Change Description
A	September 13, 2013	Initial release.

1 Introduction

The Element Management System (EMS) is a component of the On-Ramp Total Reach Network through which users can configure, interact and manage the other components of the network in a simple and efficient manner. As part of its functions, the EMS also provides users with Notifications and Alarms, thereby alerting a user in case a network element needs attention.

For ease of explanation, we have organized this user guide into four sections.

- Basic Network Operation to describe daily activities and management of an operational system. While the devices are in operation, operators continuously monitor and manage the deployed devices and keep track of the events and notifications.
- Network Installation and Expansion to describe the deployment of Access Points and endpoints and how to initially configure them in the EMS.
- EMS System Administration describes how to manage users and notifications in the EMS system.
- Advanced Features and Network Troubleshooting describes features that would only be used by an advanced EMS operator or specialist. This section also provides some tips and techniques for troubleshooting common issues that could be found in an operational network.

1.1 Overview of On-Ramp Total Reach Network

The On-Ramp Wireless Total Reach technology network monitors critical infrastructure devices in a wide-area territory. A network deployment contains many Access Points (APs) that are geographically distributed in a specific territory. The APs create a wireless network which monitors Connected by On-Ramp endpoints. Available endpoint devices can include:

- Federal Aviation Administration (FAA) obstruction light Remote Monitoring Units (RMUs)
- Schweitzer Engineering Lab WSO-11 Distribution line Fault Circuit Indicators (FCIs)
- Smart Meters
- GridSense Transformer IQ
- Koncar Gas Pressure Sensors: KONWPT
- GE MDS WiYZ-R Remote

The Total Reach network provides advantages for wide area sensor networking. The Total Reach network enables powered and battery operated Transmission and Distribution Smart and Remote Monitoring applications. The network is deployed in an infrastructure efficient star topology and operates at -142 dBm receive sensitivity.

The following figure illustrates the functional overview of the On-Ramp Total Reach network.

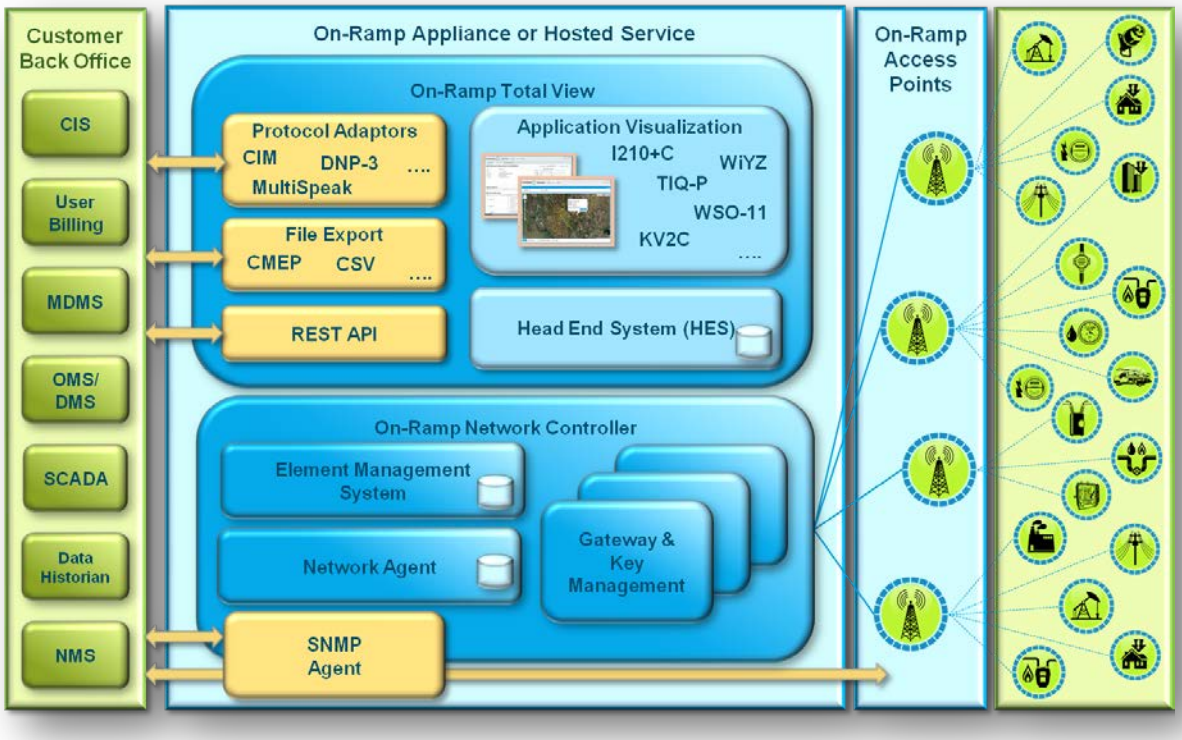


Figure 1. Functional Overview of the On-Ramp Total Reach Network

The On-Ramp Wireless EMS provides network control and alarm status for the On-Ramp Wireless Gateway (GW), Access Points (APs), and devices (Nodes) in the network.

NOTE: Application Operators and Specialists use the On-Ramp Wireless OTV application and APIs for application-level data collection and alarms.

1.2 EMS Overview

The main functions that the EMS performs are:

1. To set-up and configure the network components such as Access Points, Gateways, and devices.
2. To monitor the health of network components during operation. This involves staying informed of the device activities and taking corrective measures in case of notifications or warnings.
3. To perform network troubleshooting when issues arise using the available diagnostic screens and system logs.
4. Other tasks such as network expansion and firmware code download.

1.2.1 User Roles

In the following user guide, activities are described by the person who may be performing them. It is possible for different organizations to have different individuals in these roles, or for a single individual to perform multiple roles. For the purposes of this document, the roles are defined to be as discrete as possible to allow for organizational flexibility.

Operator roles are typically filled by operations engineers with less experience while Specialist roles are filled by highly skilled engineers capable of debugging and triaging system issues.

Table 1. User Roles

Role	Description
Network Specialist	■ Monitors Access Point commissioning progress and initial network health ■ Monitors Endpoint installation progress and health ■ Plans and executes expansion of communication systems ■ Triages network alarms as escalated by the network operator ■ Monitors the health of the On-Ramp Network and backhauls
Access Point Network Installer	■ Physically installs Base Stations in the field ■ Could be customer internal resources or outside contractors
Network Operator	■ Works with endpoint manufacturers to acquire and input endpoint keys into EMS ■ Performs daily monitoring and management of communication systems ■ Support network expansions projects ■ Subscribes to EMS notifications and escalates problems to specialist as needed
Back Office IT Administrator	■ Appliance installation ■ Daily monitoring of IT systems ■ Sets up log archival mechanisms
Applications Specialist	■ Monitors initial application data and performance ■ Engages with application manufacturer on installation procedures ■ Subscribes to OTV Alarms ■ Triages application alarms as escalated by the applications operator
Applications Operator	■ Works with installers to input meta data of newly installed endpoints ■ Performs daily monitoring and management of application data ■ Subscribes to OTV Alarms ■ Escalates problems to specialist as needed

1.2.2 EMS Screen Features and Overview

The On-Ramp Wireless Total Reach Network Element Management System (EMS) is the subsystem that handles the Operations, Administration, and Maintenance (OA&M) functions for the network. In this capacity, the EMS monitors the network components and reports data to the Network Operator for use in managing the system operation. The EMS provides a web-based view to configure network elements and monitor notifications and events.

- It has an SNMP v3/v2 interface for northbound notifications to third party managers (MOMs) like CA Spectrum.

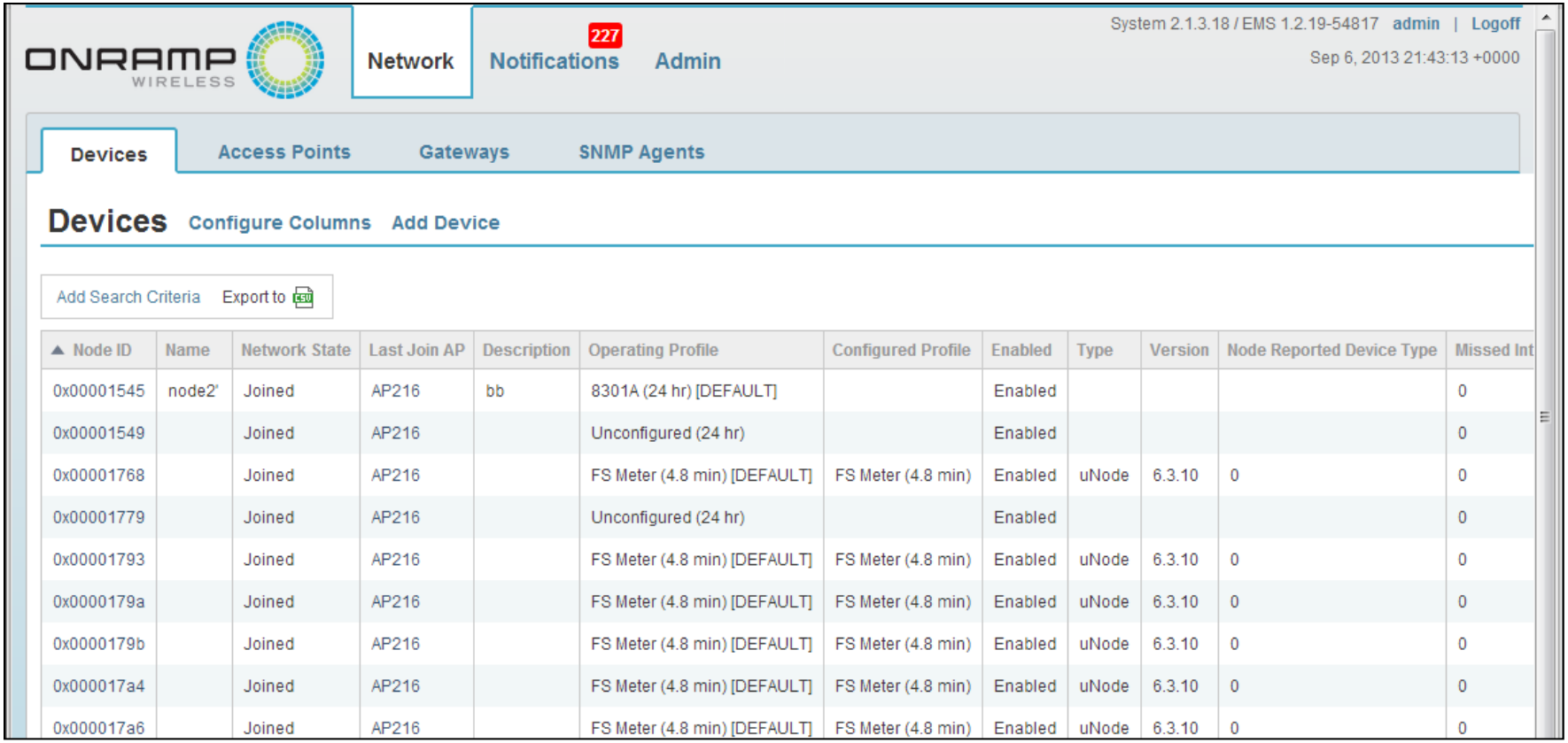
- It supports role-based user accounts for administrators and operators and also has read-only views for guests.
- It supports Active Directory for single-sign on or application user authentication.
- It can be used to perform remote software OTA upgrades of On-Ramp Total Reach Nodes and host device firmware.

Sample login screens for various roles, such as Administrator, Operator, and Guest are shown on the following pages. Note the access levels for Operator and Guest are not as extensive as for an Administrator.

The screen features are described in the following table:

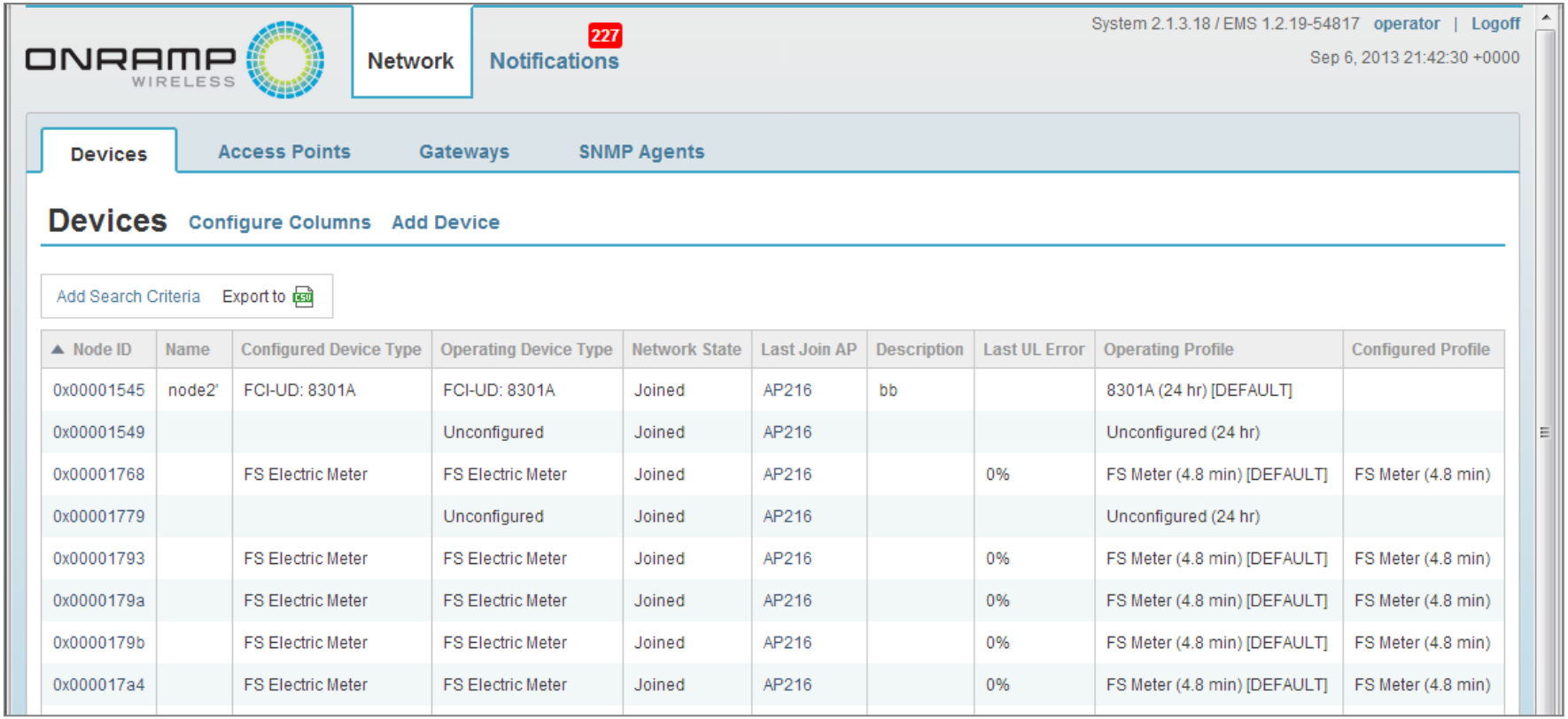
Table 2. Description of Screen Features

Feature	Description
Device Selection	The default screen for any role (administrator, operator or guest) that lists the devices in the network and related status information.
Access Point Selection	Lists the Access Points connected to the network and related status information.
Gateway Selection	Lists the Gateways in the network and related status Information.
Notifications Selection	View notifications and notification details.
Administrator Functions	Provides administrator settings like Adding/Modifying a user, Changing Network Agent Properties, and other advanced settings.
Device Listing Pane	Lists the devices and related status information.
Search Criteria	Filters devices based on certain criteria.
Add New Device	Add and configure a new device/Node.
SNMP Selection	View/modify SNMP agent details.
EMS Version and Logged-In Role	Shows username of logged in user as well as current software version.
Configure Columns	Modifies the Node properties (e.g., Node ID, Name, Configured Device Types, etc.) that are shown on the Device Listing Pane.
Export Device List	Allows you to export the list of Nodes, along with visible device information, to a CSV File on the system.



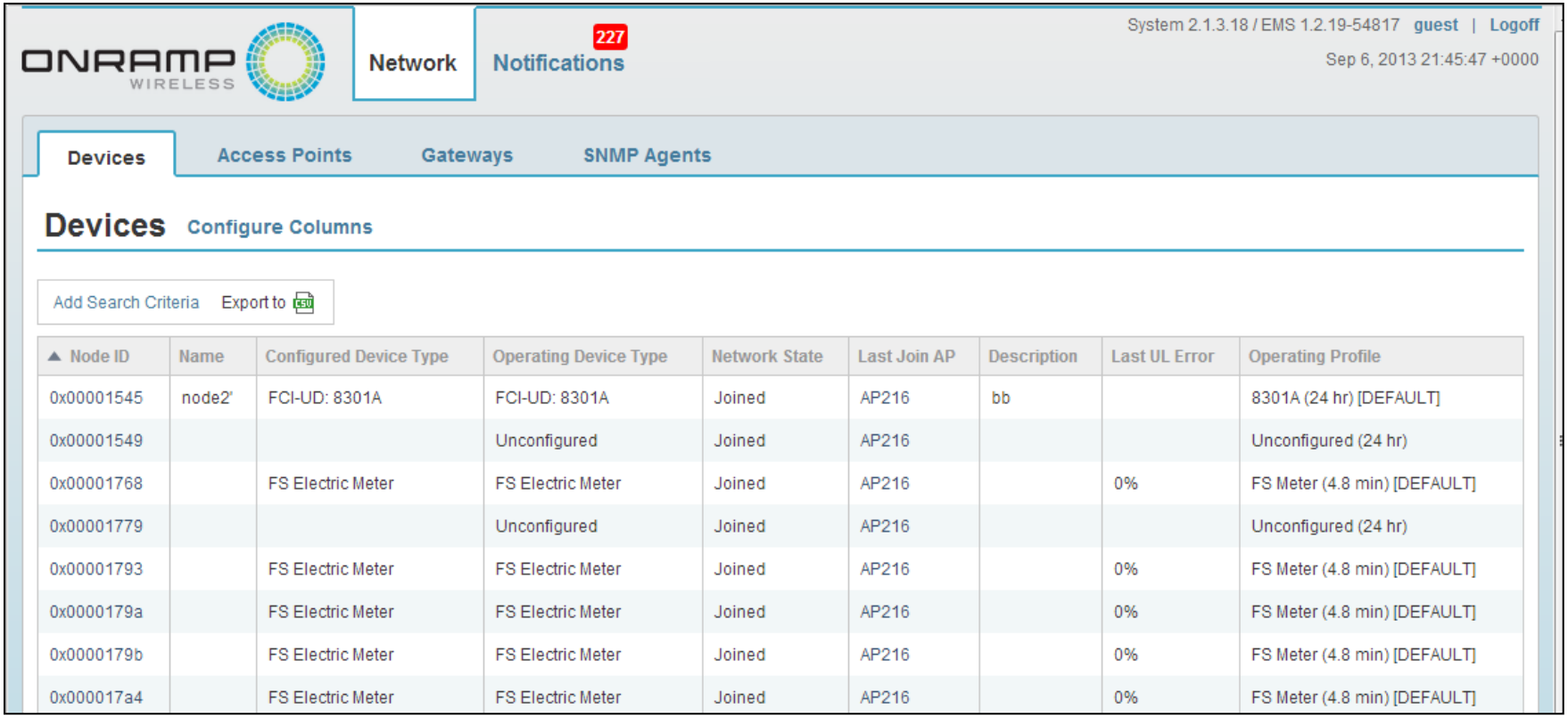
Node ID	Name	Network State	Last Join AP	Description	Operating Profile	Configured Profile	Enabled	Type	Version	Node Reported Device Type	Missed Int
0x00001545	node2'	Joined	AP216	bb	8301A (24 hr) [DEFAULT]		Enabled				0
0x00001549		Joined	AP216		Unconfigured (24 hr)		Enabled				0
0x00001768		Joined	AP216		FS Meter (4.8 min) [DEFAULT]	FS Meter (4.8 min)	Enabled	uNode	6.3.10	0	0
0x00001779		Joined	AP216		Unconfigured (24 hr)		Enabled				0
0x00001793		Joined	AP216		FS Meter (4.8 min) [DEFAULT]	FS Meter (4.8 min)	Enabled	uNode	6.3.10	0	0
0x0000179a		Joined	AP216		FS Meter (4.8 min) [DEFAULT]	FS Meter (4.8 min)	Enabled	uNode	6.3.10	0	0
0x0000179b		Joined	AP216		FS Meter (4.8 min) [DEFAULT]	FS Meter (4.8 min)	Enabled	uNode	6.3.10	0	0
0x000017a4		Joined	AP216		FS Meter (4.8 min) [DEFAULT]	FS Meter (4.8 min)	Enabled	uNode	6.3.10	0	0
0x000017a6		Joined	AP216		FS Meter (4.8 min) [DEFAULT]	FS Meter (4.8 min)	Enabled	uNode	6.3.10	0	0

Figure 2. EMS Screen Features (Administrator Login Role)



Node ID	Name	Configured Device Type	Operating Device Type	Network State	Last Join AP	Description	Last UL Error	Operating Profile	Configured Profile
0x00001545	node2'	FCI-UD: 8301A	FCI-UD: 8301A	Joined	AP216	bb		8301A (24 hr) [DEFAULT]	
0x00001549			Unconfigured	Joined	AP216			Unconfigured (24 hr)	
0x00001768		FS Electric Meter	FS Electric Meter	Joined	AP216		0%	FS Meter (4.8 min) [DEFAULT]	FS Meter (4.8 min)
0x00001779			Unconfigured	Joined	AP216			Unconfigured (24 hr)	
0x00001793		FS Electric Meter	FS Electric Meter	Joined	AP216		0%	FS Meter (4.8 min) [DEFAULT]	FS Meter (4.8 min)
0x0000179a		FS Electric Meter	FS Electric Meter	Joined	AP216		0%	FS Meter (4.8 min) [DEFAULT]	FS Meter (4.8 min)
0x0000179b		FS Electric Meter	FS Electric Meter	Joined	AP216		0%	FS Meter (4.8 min) [DEFAULT]	FS Meter (4.8 min)
0x000017a4		FS Electric Meter	FS Electric Meter	Joined	AP216		0%	FS Meter (4.8 min) [DEFAULT]	FS Meter (4.8 min)

Figure 3. EMS Screen Features (Operator Login Role)



Node ID	Name	Configured Device Type	Operating Device Type	Network State	Last Join AP	Description	Last UL Error	Operating Profile
0x00001545	node2'	FCI-UD: 8301A	FCI-UD: 8301A	Joined	AP216	bb		8301A (24 hr) [DEFAULT]
0x00001549			Unconfigured	Joined	AP216			Unconfigured (24 hr)
0x00001768		FS Electric Meter	FS Electric Meter	Joined	AP216		0%	FS Meter (4.8 min) [DEFAULT]
0x00001779			Unconfigured	Joined	AP216			Unconfigured (24 hr)
0x00001793		FS Electric Meter	FS Electric Meter	Joined	AP216		0%	FS Meter (4.8 min) [DEFAULT]
0x0000179a		FS Electric Meter	FS Electric Meter	Joined	AP216		0%	FS Meter (4.8 min) [DEFAULT]
0x0000179b		FS Electric Meter	FS Electric Meter	Joined	AP216		0%	FS Meter (4.8 min) [DEFAULT]
0x000017a4		FS Electric Meter	FS Electric Meter	Joined	AP216		0%	FS Meter (4.8 min) [DEFAULT]

Figure 4. EMS Screen Features (Guest Login Role)

2 EMS System Administration

This section describes how to perform important Administrative functions such as Adding a User, Notification/Alarm Groups, and LDAP Domains.

2.1 User Management

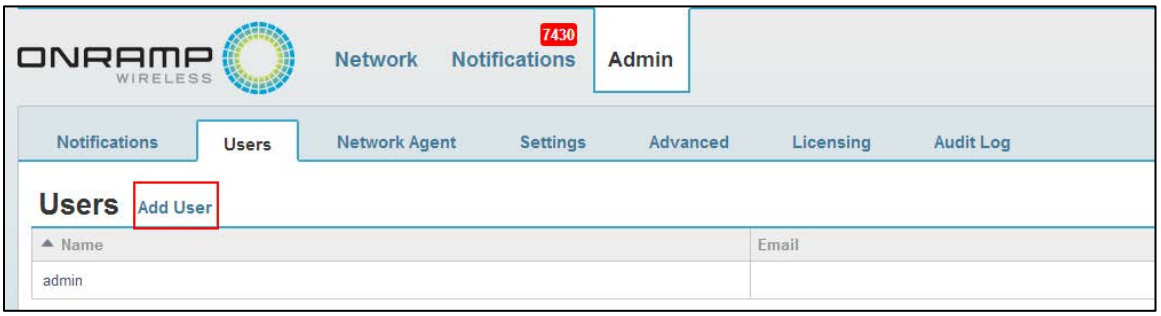
Users can be set up as local user accounts or via LDAP/Active Directory authentication. Additionally, multiple domains can be used in combination with local user accounts.

NOTE: Adding an LDAP/Active Directory domain requires the IT Administrator to provide the required configuration information.

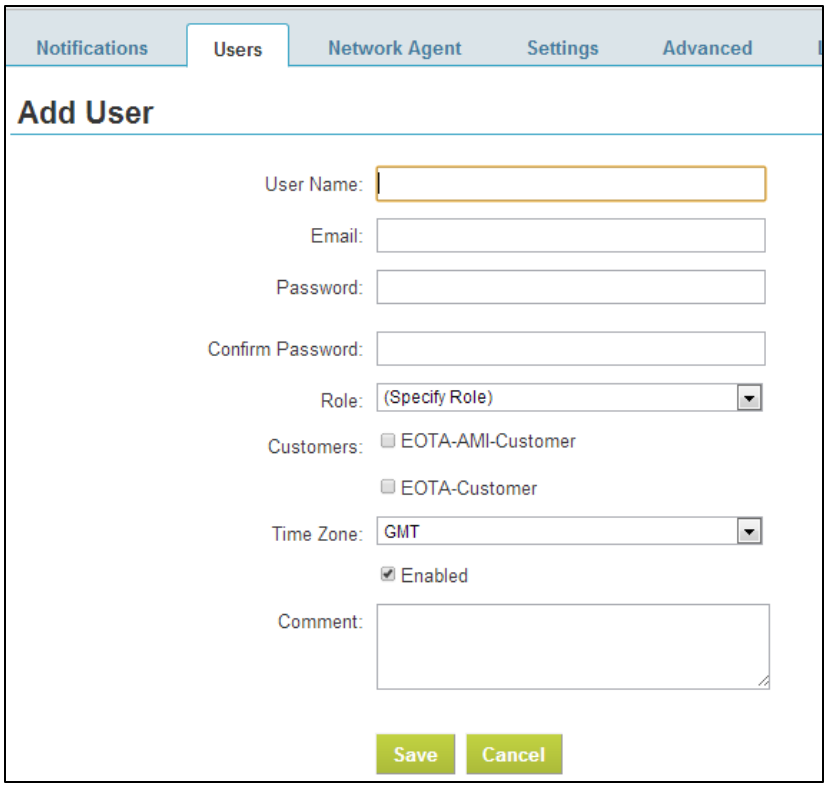
2.1.1 Adding a Local User

This section describes how to add Users to an existing customer's account.

1. Log in to the EMS with an Account that has Administrator privileges.
2. Under the **Admin → Users** tab, click on **Add User.**



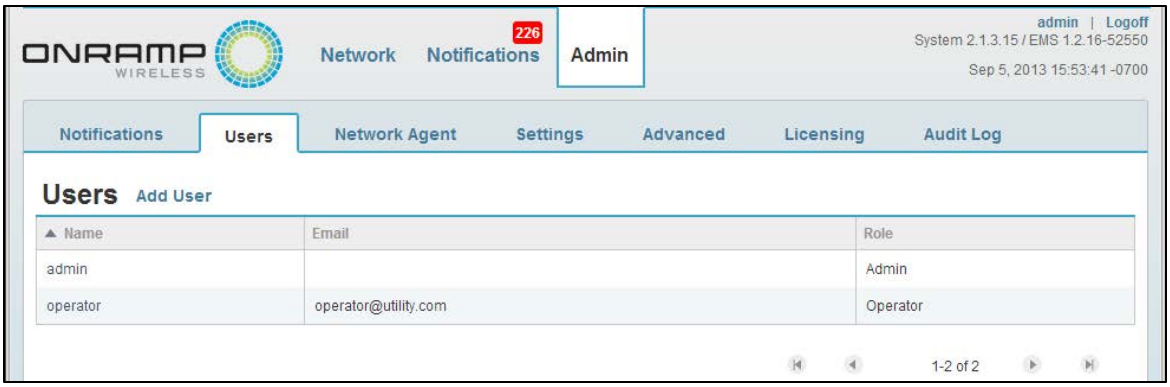
3. Fill in the details for the following **Add User** screen.



Add User Field	Description
User Name*	Enter a relevant user name.
Email	Enter the user's email ID.
Password*	Enter a password. Password must be more than 6 characters.
Confirm Password	Re-enter the password to confirm it.
Role*	Select a role. Account roles and associated privileges are described in section 1.2.1 User Roles.
Customers	Select the customer for which this user account will be operated.
Time Zone	Select an appropriate time zone and select the **Enabled** button below.
Comment	Add any operational comments.

* Indicates required field.

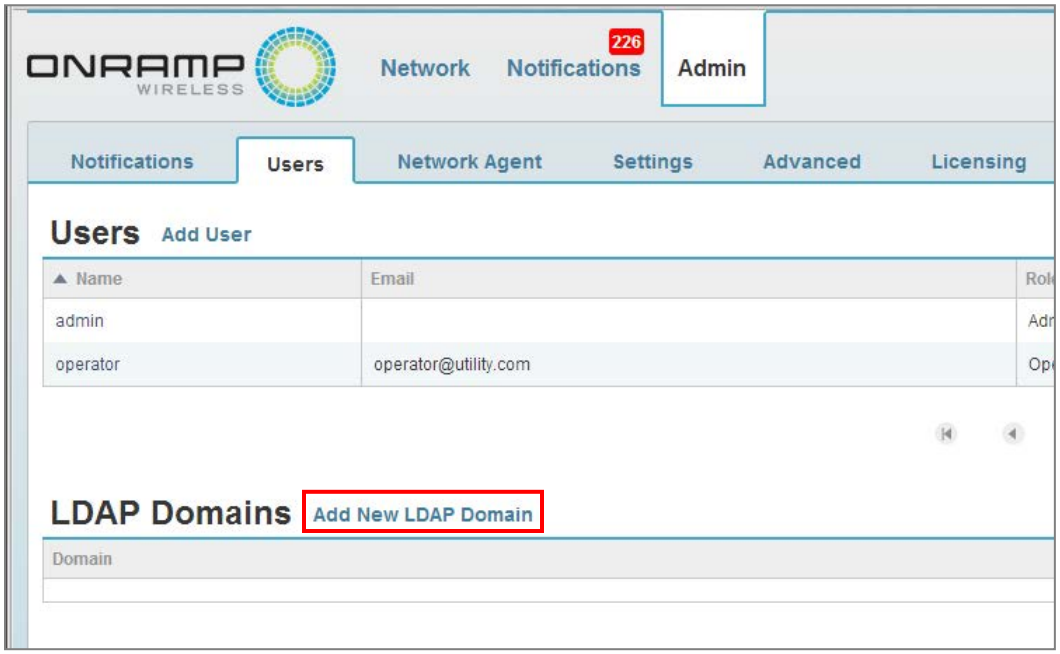
4. When finished filling in the fields for adding a user, click on **Save**.
5. As shown in the following figure, verify that the user has been added with the correct role in the **Admin → Users** page.



2.1.2 Adding an LDAP Domain

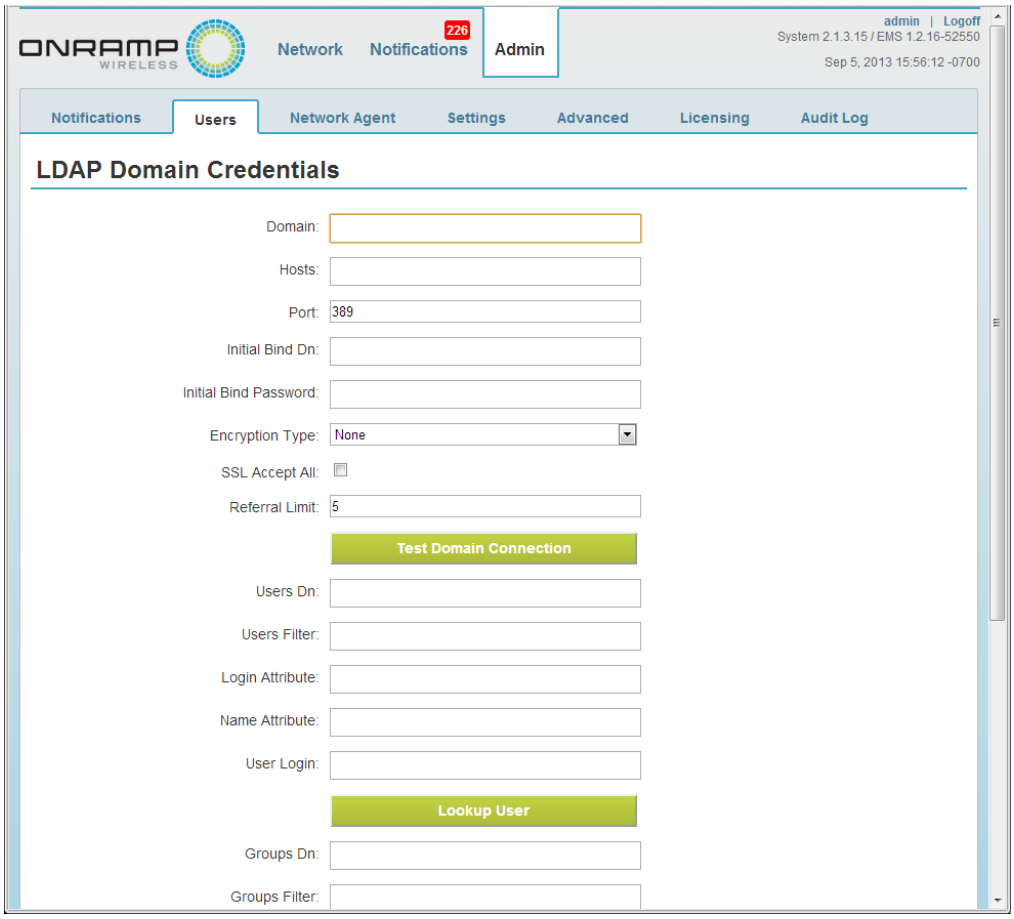
Adding an LDAP domain requires the IT Administrator to provide the required configuration information.

1. Log in to the EMS with an Account that has Administrator privileges.
2. Click on **Admin** → **Users** tab → **Add New LDAP Domain.**



3. The following screen is displayed. Fill in the required fields and configure accordingly. The table following the screen provides LDAP examples for field entries.

   NOTE: The same screen is used for both LDAP and Active Directory authentication.



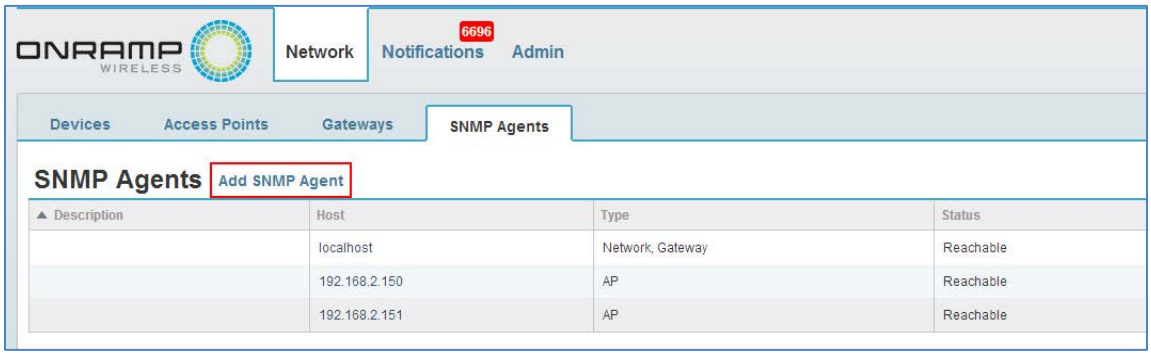
LDAP Domain Credentials Field	Example Field Entry
Domain*	onramp.local
Hosts*	ldap.onramp.local
Port	636
Initial Bind Dn	
Initial Bind Password	
Encryption Type	SSL
SSL Accepts All	Enabled
Referral Limit	5
Users Dn	ou=People
Users Filter	
Login Attribute*	uid
Name Attribute	cn
User Login	
Groups Dn	ou=Groups
Groups Filter	
Members Attribute*	uniqueMember

* Indicates required field.

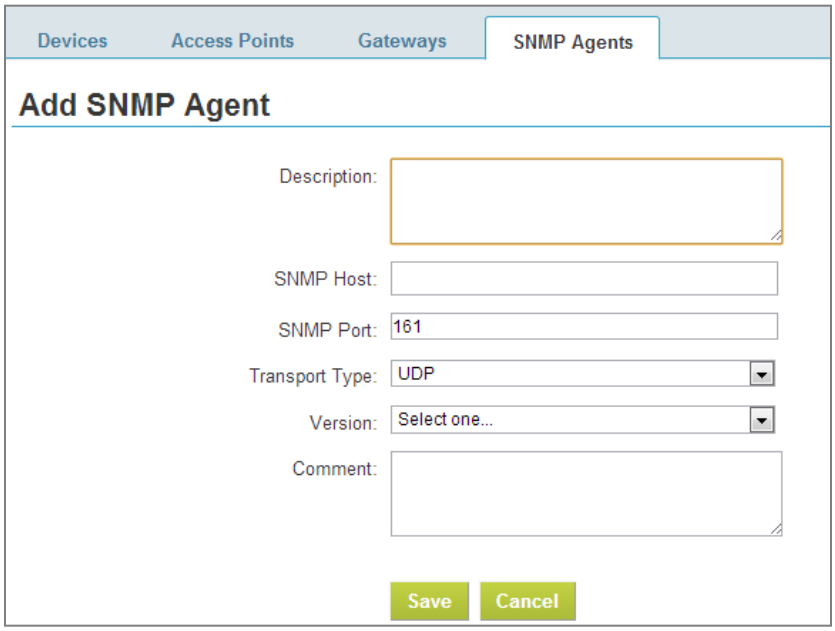
4. For the **User Login** field, add a username and click on **Lookup User**. This populates the "Groups User Dn" field.
5. Click on **Lookup Group**. This lists the user individually along with LDAP groups in which the user belongs. Selecting LDAP groups allows a wider range of users to access EMS.
6. Select a role in the pull-down menu for the user or group. If this is a multiple-customer system, you need to select which customers the user or group is allowed to view or operate. To select multiple customers, use Ctrl + click.
7. Click **Save**.

2.2 Adding an SNMP Agent

1. Under **Network → SNMP Agents** tab, click on **Add SNMP Agent**



2. Complete the information in the next screen for SNMP Agents.



3. Fill in the following information on the **Add SNMP Agent** screen.

Add SNMP Agent Field	Description
Description*	Enter the description for the new agent.
SNMP Host*	Enter the desired SNMP host IP address.
SNMP Port*	Do not change the default of 161 for this field.
Transport Type*	From the dropdown menu, select the proper value for the network setup – either UDP or TCP. Contact the Network Specialist or IT Administrator for assistance.
Version*	For production systems, always select version 3. Contact Network Specialist for assistance.
Comments	Add comments about this operation for the audit log.

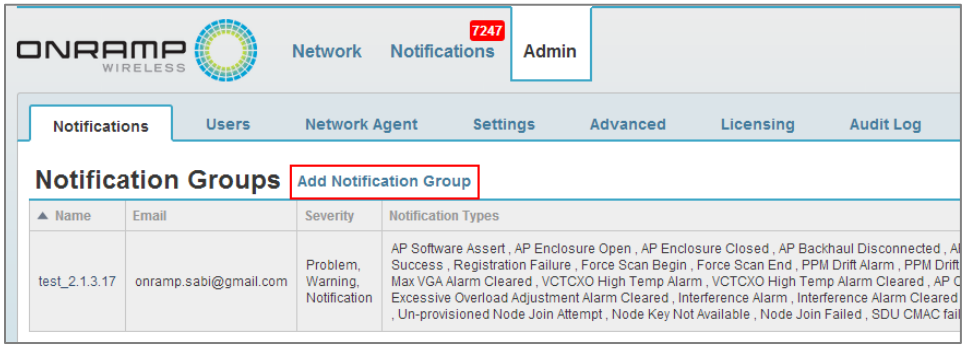
* Indicates required field.

4. Click on **Save.** The SNMP Agent should now be added.
5. Verify from the **Network → SNMP Agents** page.

2.3 Adding a Notification Group for Email Alerts

This section describes how to create a Notification group that manages email alerts for certain Device Events like Gateway Down, AP online, etc. Refer to the *Appliance Deployment Guide (010-0109-00)* for SMTP configuration.

1. Under the **Admin → Notifications** tab, click on **Add Notification Group.**

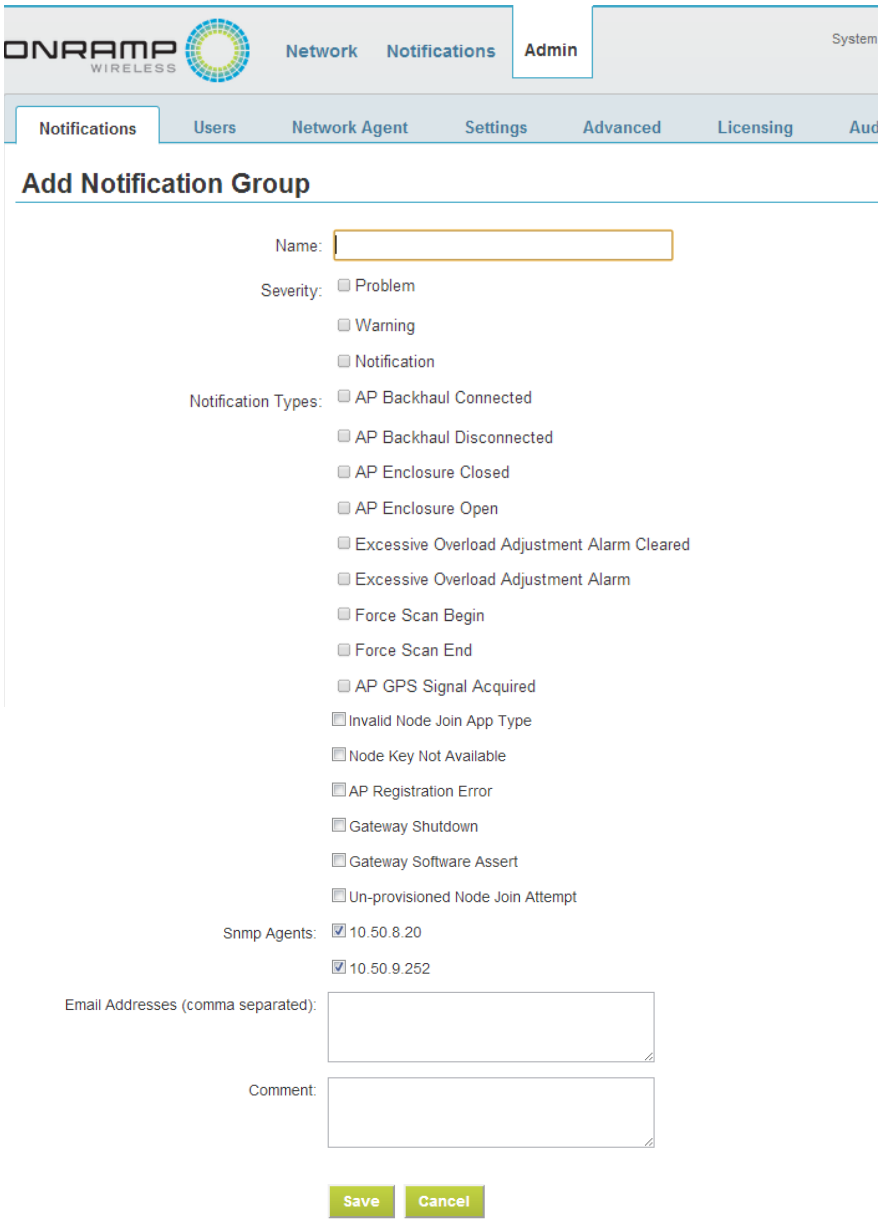


2. The **Add Notification Group** screen allows configuration of the notification group and is shown on the following page. Fill in the details for the **Add Notification Group** screen.

Add Notification Group Field	Description
Name*	Enter a notification group name.
Severity	In this field you can select more than one checkbox. Depending on the severity group selected (i.e., Problem, Warning, Notification), default options are displayed and relevant Notification Types are automatically selected. You can select/de-select any of the Notification Types. Select the severity group for which you want to receive email notifications. Choosing all three Severity groups automatically selects all of the Notification Types listed for all three severity groups. The Notification Types that are automatically selected for each Severity are defined in Appendix A.

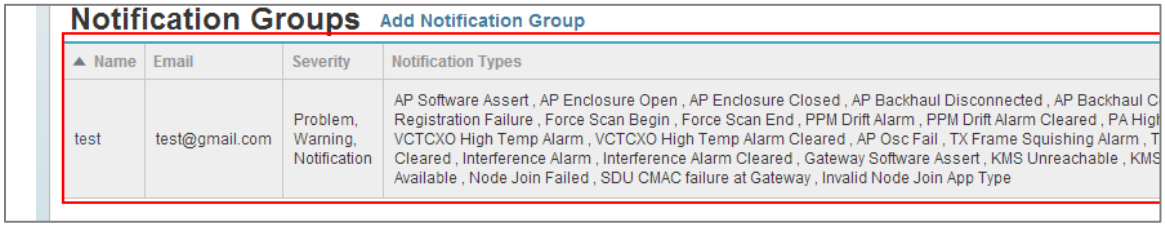
Add Notification Group Field	Description
Notification Types	Select/deselect the appropriate Notification Types in the list of checkboxes.
SNMP Agents	Select the SNMP Agents for which you want to receive notifications.
Email Addresses* (comma separated)	Enter the email address(es) that will receive the Notifications. For multiple email addresses, use a comma to separate.
Comment	Add any appropriate operation comments.

* Indicates required field.

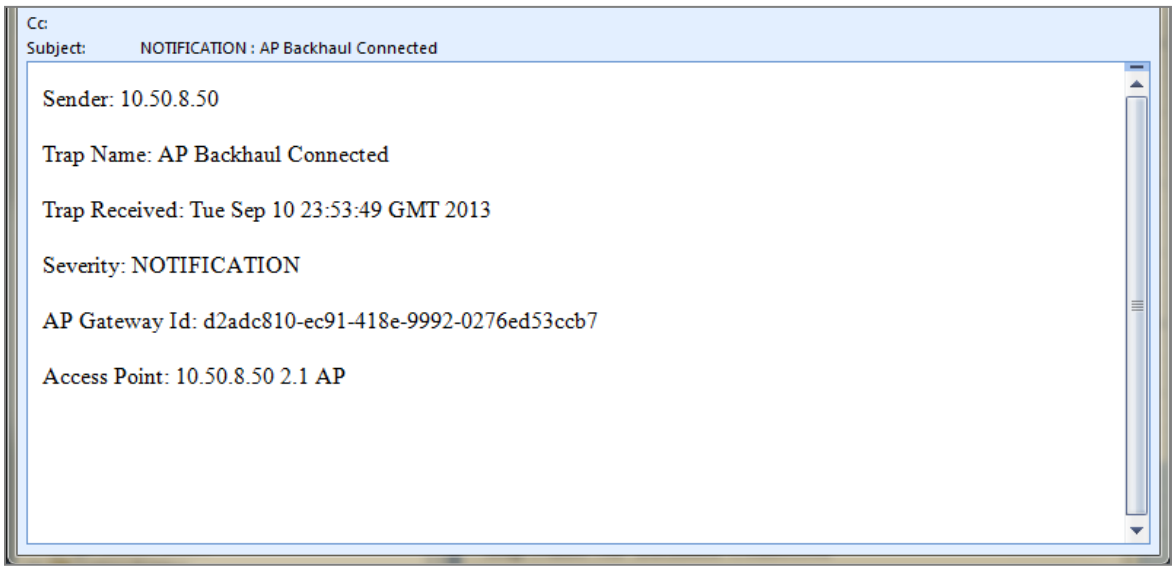


3. Click on **Save.**

4. Verify that the notification group has been added in the **Admin → Notifications** page.

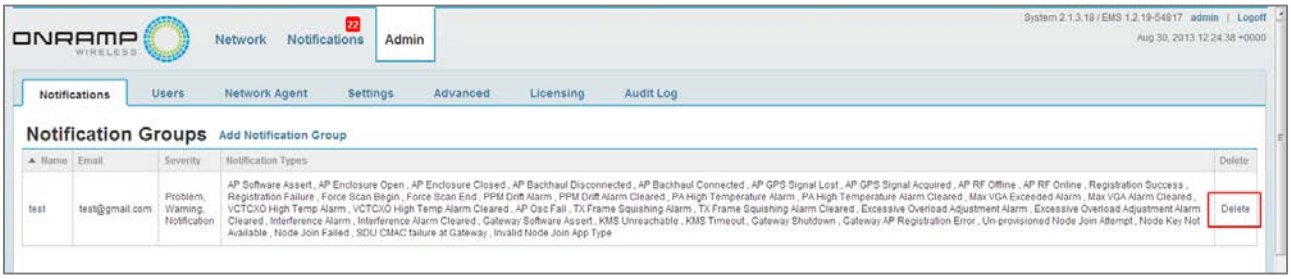


After a notification group has been setup and SMTP emails have been configured, subscribed users receive emails with information about the notification.

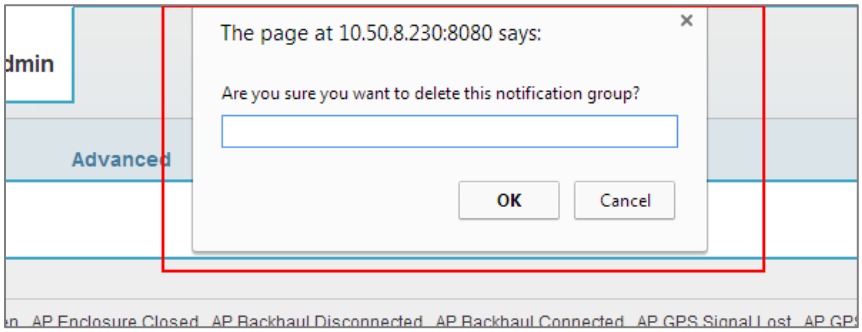


2.4 Deleting a Notification Group

1. Navigate to the **Admin → Notifications** tab. On the rightmost column, as shown below, is the **Delete** button for each notification group.



2. Clicking on the **Delete** button displays a popup dialog box asking for verification that you want to delete the notification group. A comment box is provided so that you can provide a reason for the deletion. The comment is stored in the Audit Logs. Press **OK** to delete the notification.



3. Verify that the group has been deleted by going to the **Admin → Notifications** page.

3 Network Installation and Expansion

On-Ramp Total Reach networks are purchased as a hosted network or network appliance. The setup and configuration of this network appliance is out of the scope for this EMS operator guide. The reader may reference the *On-Ramp Wireless Appliance Data Sheet (010-0039-00)* and On-Ramp Wireless Appliance Deployment Guide (010-0109-00) for CommSysm2.1 for more information.

This section covers the operational scenarios for network installation and expansion that require an interface with the EMS.

3.1 Adding an Access Point

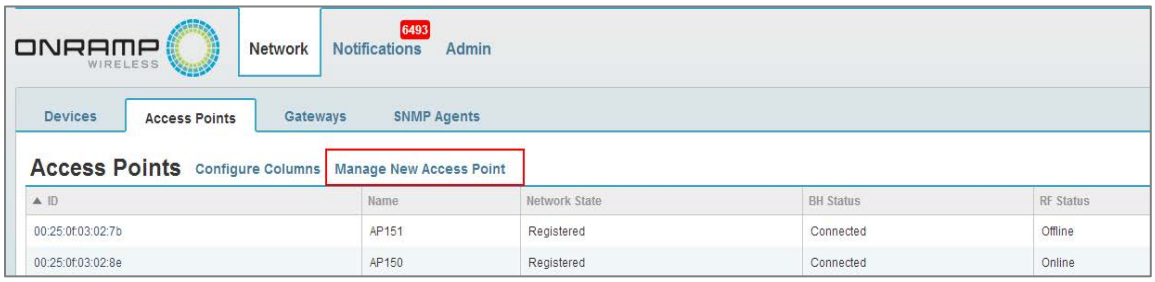
Access Points (APs) are geographically dispersed throughout a wide territory and communicate upstream with the On-Ramp Gateway and downstream with the On-Ramp radio enabled endpoints:

- Upstream: APs communicate upstream with the Gateway through Transmission Control Protocol/Internet Protocol (TCP/IP) over various types of physical backhauls. The physical backhauls are based on the specifics of the network deployment. A typical backhaul might consist of a leased line and/or microwave.
- Downstream: APs provide an RPMA wireless coverage footprint for thousands of wireless end-point devices or nodes.

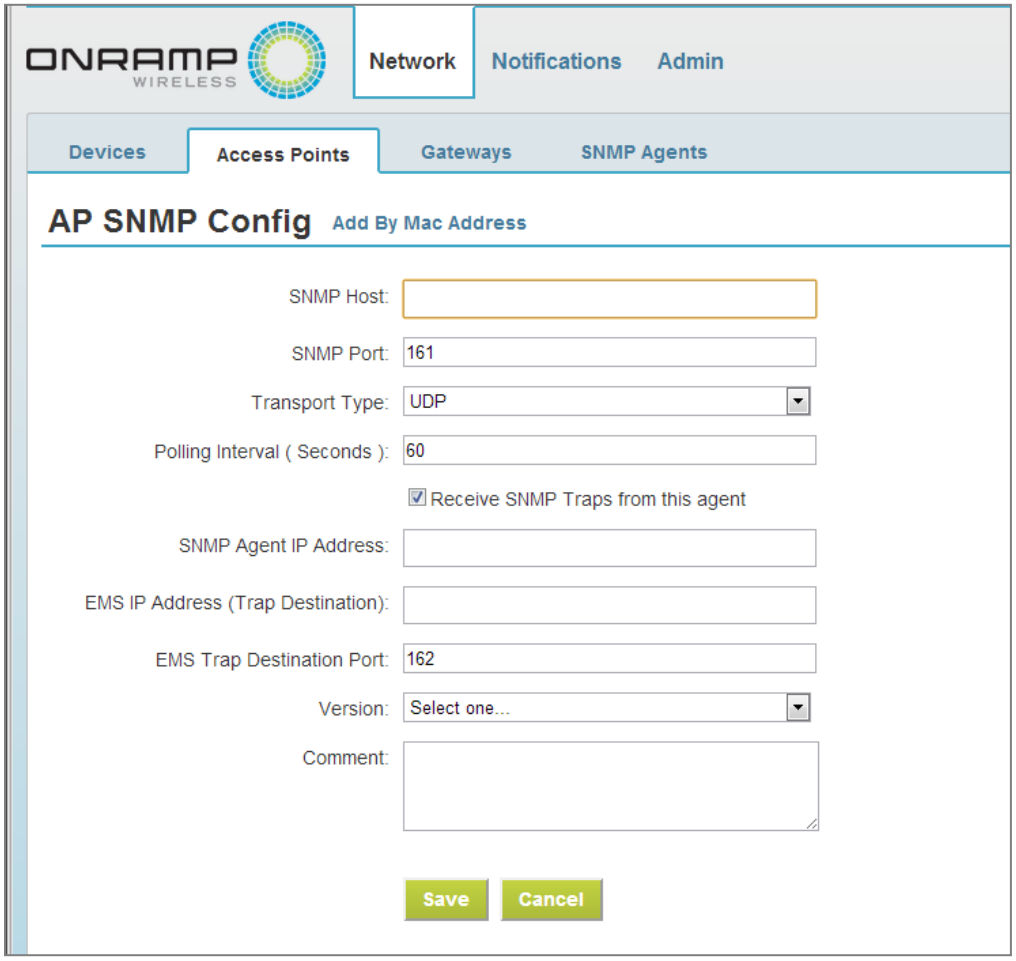
The AP Deployment Guide (010-0021-00) for CommSys 2.1, covers the physical AP installation and initial configuration of the AP. This is typically done by a field installation crew. After communication between the AP and Gateway has been established, the field crew waits while a Network Operator or Network Specialist completes the addition of the AP to the EMS.

To add an AP at the EMS, complete the following steps:

1. Under **Network → Access Points**, click on **Manage New Access Point**.



2. In the next screen, fill the following details

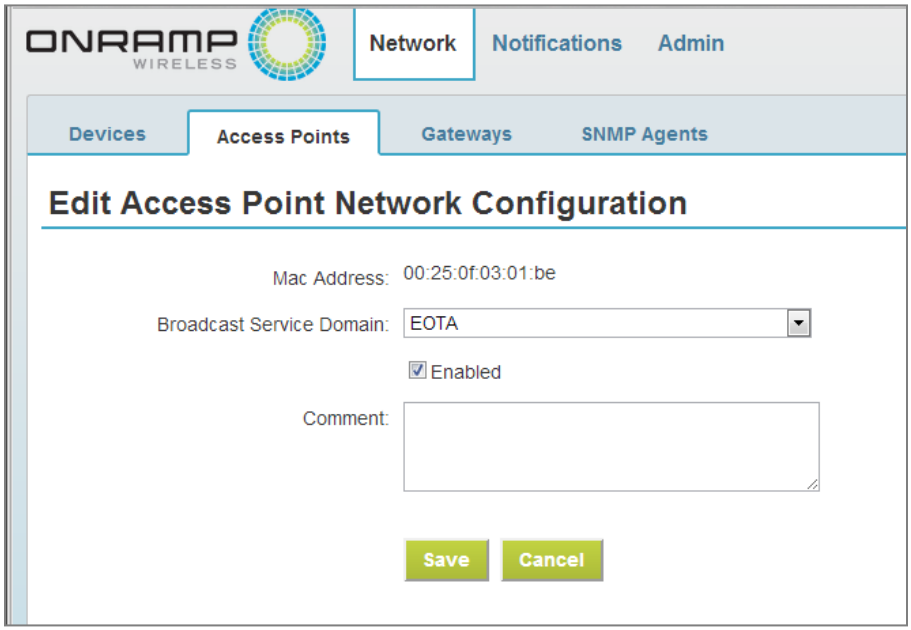


AP SNMP Config Field	Description
SNMP Host*	Enter the AP IP address which is available from the Network Specialist or IT Administrator.
SNMP Port*	Do not change the default of 161 for this field.
Transport Type*	From the dropdown menu, select the proper value for the network setup – either UDP or TCP. Contact the Network Specialist or IT Administrator for assistance.
Polling Interval *(Seconds)	Do not change the default value of 60 seconds for this field.
Receive SNMP Traps from this Agent	Leave the checkbox checked.
SNMP Agent IP Address*	This field is auto-populated by the EMS and should not be changed.
EMS IP Address* (Trap Destination)	This field is auto-populated by the EMS and should not be changed.
EMS Trap Destination Port*	Do not change the default of 162 for this field.

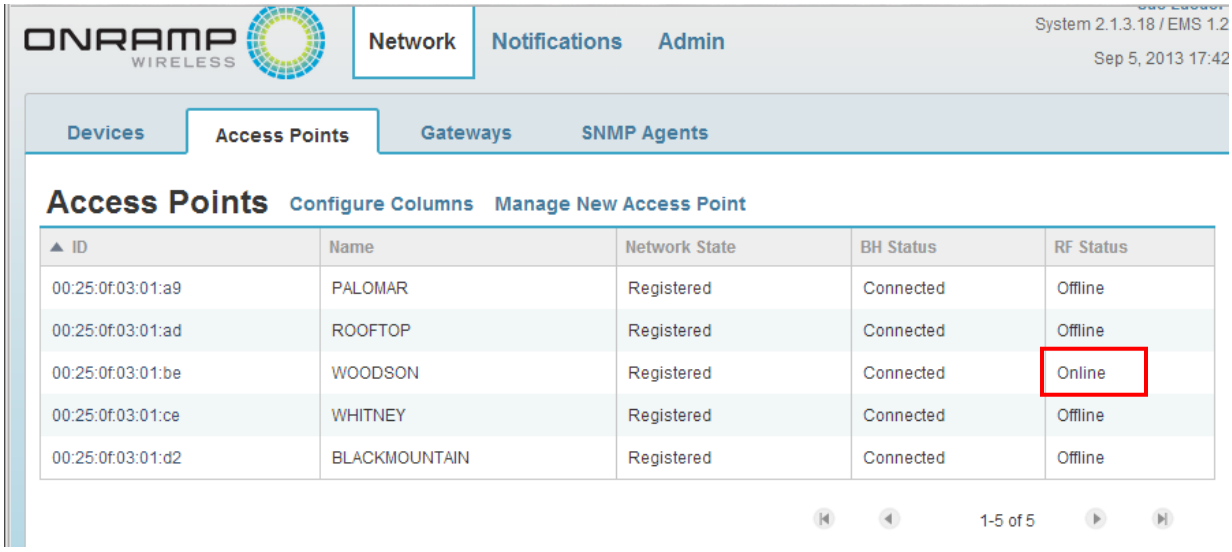
AP SNMP Config Field	Description
Version	For production systems, always select version 3. Contact Network Specialist for assistance.
Comment	Add a comment about the configuration activity for the audit log.

* Indicates required field.

3. When you have filled in all of the fields, click **Save.**
4. Set up the Broadcast Service Domain by clicking on **Edit Network Configuration**.
5. Select the required **Broadcast Service Domain** from the dropdown menu and select **Enabled**. At this point, the AP begins the process of going online and on the air.



6. After the AP completes GPS time sync and aligns RF Metrics, the AP RF Status displays *Online* as shown below. This indicates that the AP is on the On-Ramp Network and endpoints may begin to join the AP.

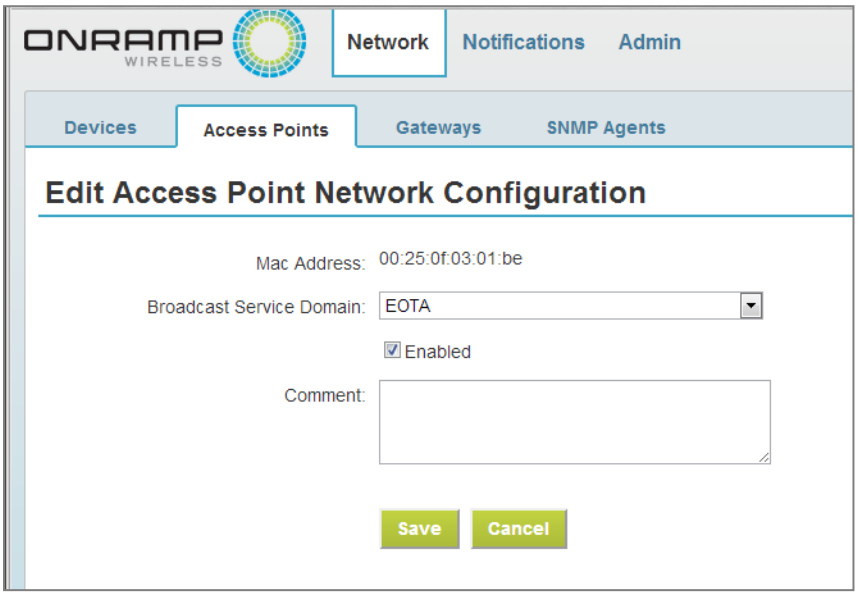


3.2 Configuring an Access Point

Once an AP has been added and is online the network, any changes to its settings should be reviewed, approved, and carefully planned by a Network Specialist.

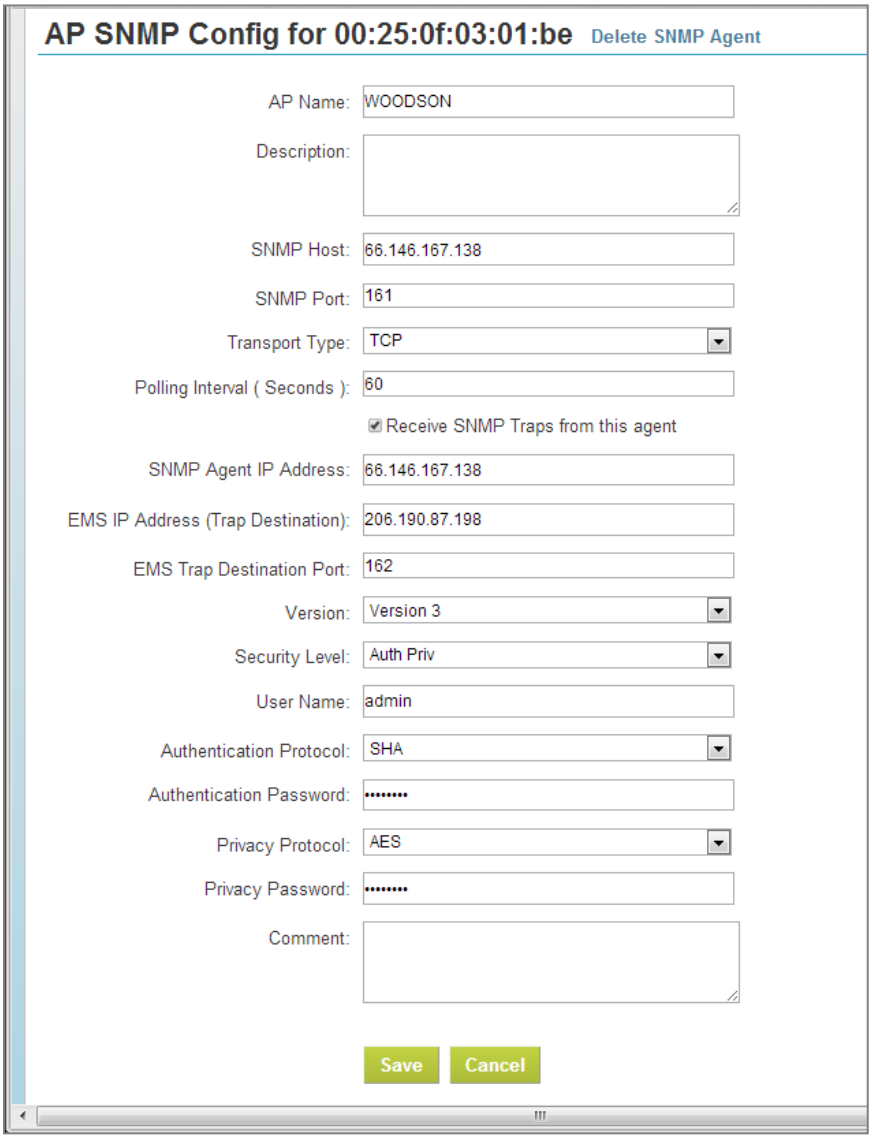
3.2.1 AP Network Configuration

The Broadcast Service Domain (BSD) can be thought of as a “network” or “sub-network”. In small networks only one BSD is needed. Multiple BSD’s would primarily be used when one network is used by many customers` or when a customer finds it easier to manage a large network by dividing into multiple BSDs.



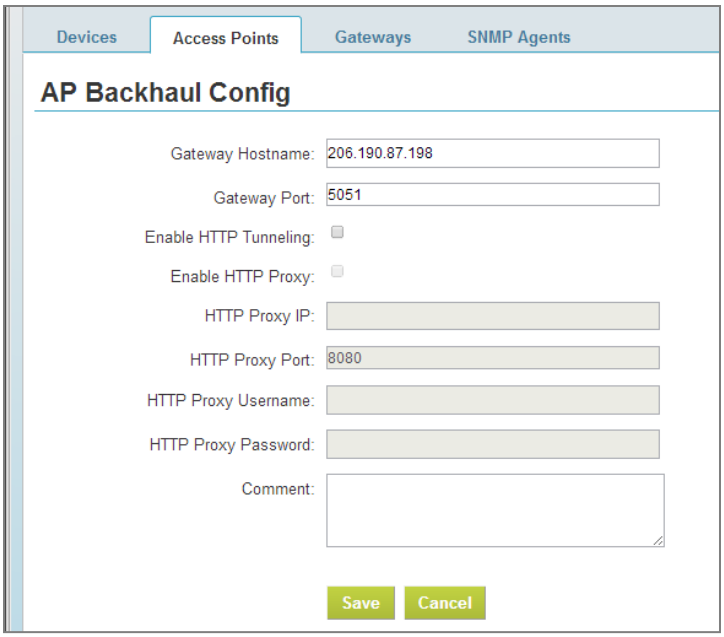
3.2.2 AP SNMP Configuration

The communication protocol for APs is SNMP so the SNMP configuration is the data used to communicate to the AP over TCP/IP. The Network Specialist must work with IT Network Administrator to make changes to this data.



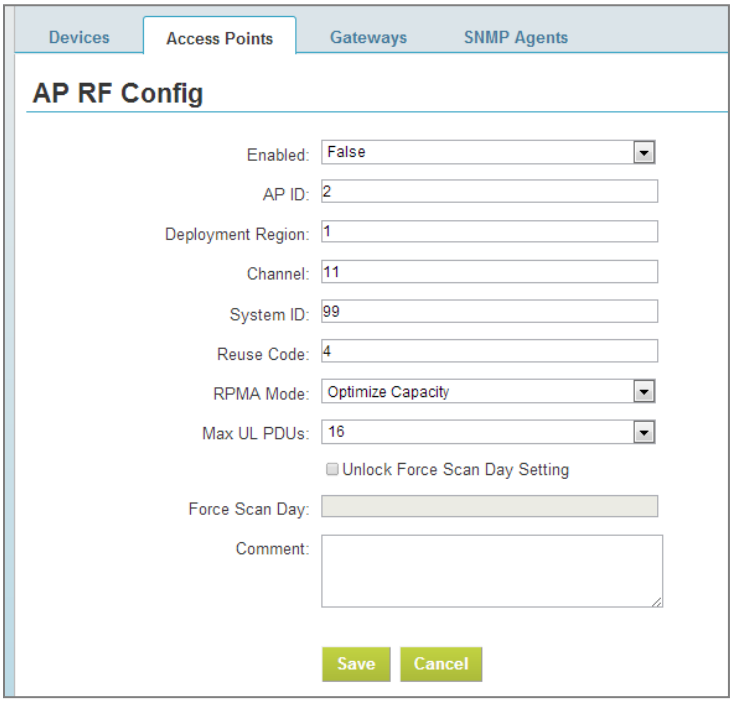
3.2.3 AP Backhaul Configuration

The following screen displays AP backhaul configuration information which is needed by the AP to communicate with the Gateway. This data is set up when the AP is initially deployed and should rarely, if ever, be changed for an AP.



3.2.4 AP RF Configuration

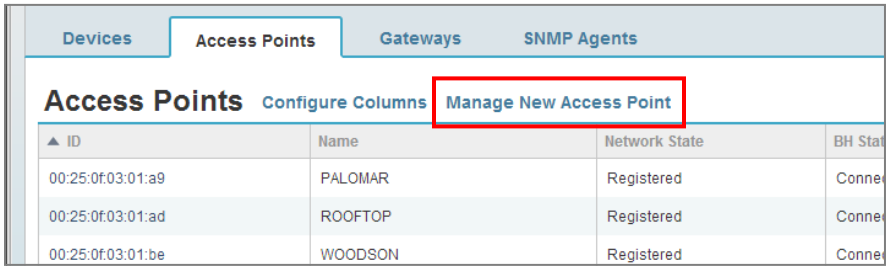
The AP RF configuration page is where the operator can view RPMA network parameters. RPMA parameters are read only unless the AP is disabled (i.e., Enabled = False). Any changes to these parameters have significant impacts on the system and should only be done in close coordination with the Network Specialist and possibly On-Ramp Wireless support, if needed.



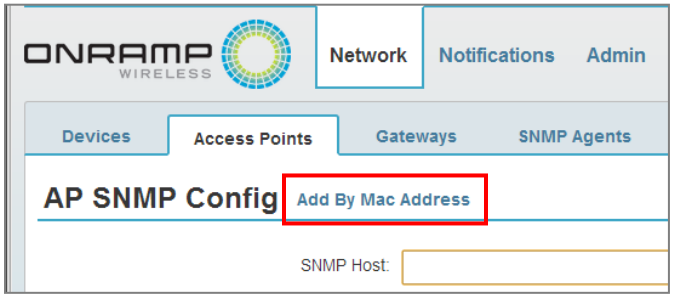
3.3 Adding an Access Point based on MAC ID

To add an AP based on MAC ID, complete the following steps:

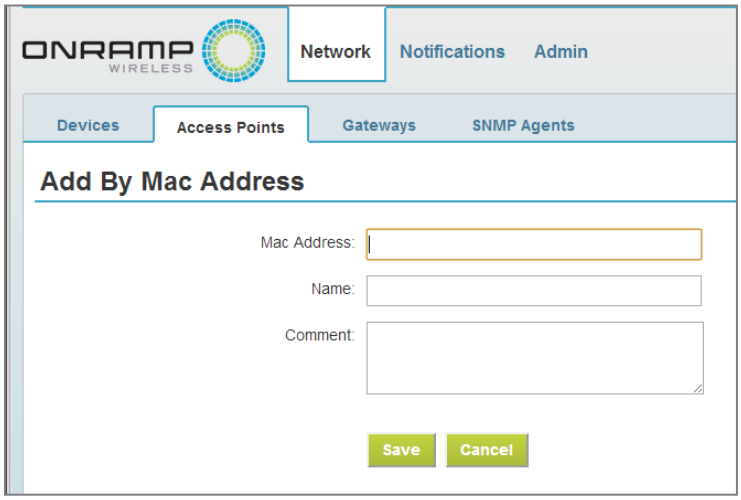
1. Under **Network → Access Points**, Click **Manage New Access Point** button.



2. In the next screen, click on **Add by Mac Address**



3. In the following screen, fill the fields as shown below



Add By Mac Address Field	Description
Mac Address*	Enter the MAC Address.
Name*	Enter the AP host name or IP address.
Comment	Add comments to be stored in the audit log.

* Indicates required field.

4. Click **Save.** The AP should now be added if the MAC Address is valid.

3.4 Adding a Device or Node

Nodes may be added to EMS using an ingested comma separated value (.CSV) file or manually, as explained in the following subsections. It is most common for devices to be added to the EMS system in advance of physical installation. It is up to the Application Specialist and customer representative to design a proper endpoint deployment methodology for the coordination of deployed devices and actual physical location configuration in EMS and OTV. However, it is imperative that a system and process exist so that devices that join a network are not "lost" and that location information is archived in EMS so that endpoints are tracked by Node ID and physical location after deployment. The design of this process is outside the scope of this EMS guide.

NOTE: Only devices on CommSystem version 1.4 require manual creation at EMS. Nodes on CommSystem version 2.1 automatically publish their profile and configuration information. The following table provides lists of application types that are available for CommSystem 1.4 versus CommSystem 2.1.

1.4 Applications	2.1 Applications
■ WSO-11 ■ GE MDS WiYZ ■ Gridsense TIQ-P ■ RMU Obstruction Light Monitor ■ KONWPT ■ CSE Demand Response ■ uConnect	■ Smart Meter

3.4.1 Adding Devices Using Ingest File

To add the devices using an ingest file, the operator must first have a valid ingest device file. Typically, a device manufacturer delivers a block of device security keys and manifest file that contains the list of Node IDs to be added to the network. This manifest file can be used to generate an ingest file.

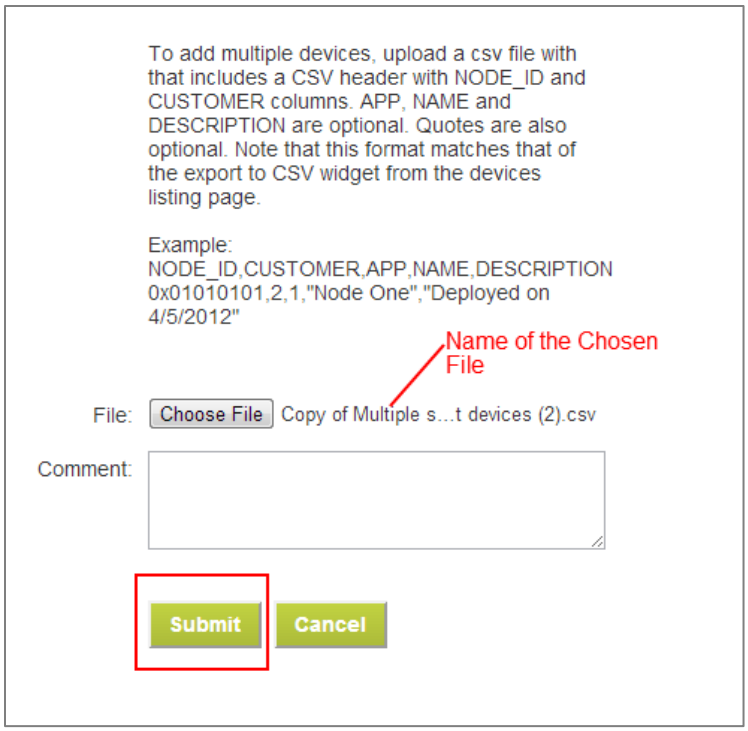
An example ingest node file is shown in Appendix B and is for reference purposes only.

1. Log in to the EMS with an account with Administrator privileges.
2. Under the **Network → Devices** tab, click on **Add Device.**

3. When the following screen appears, click on **Add Multiple Devices.**

4. After the following screen appears, click on **Choose File** to select the .CSV ingest file containing the nodes.

5. After you select the file, add a comment about the operation and then click **Upload**. The device data is uploaded to EMS but the nodes are NOT added until you click **Submit**, as shown in the following screen. You will see confirmation of the added devices, but any devices that were already configured in EMS are not added or modified from the ingest file.



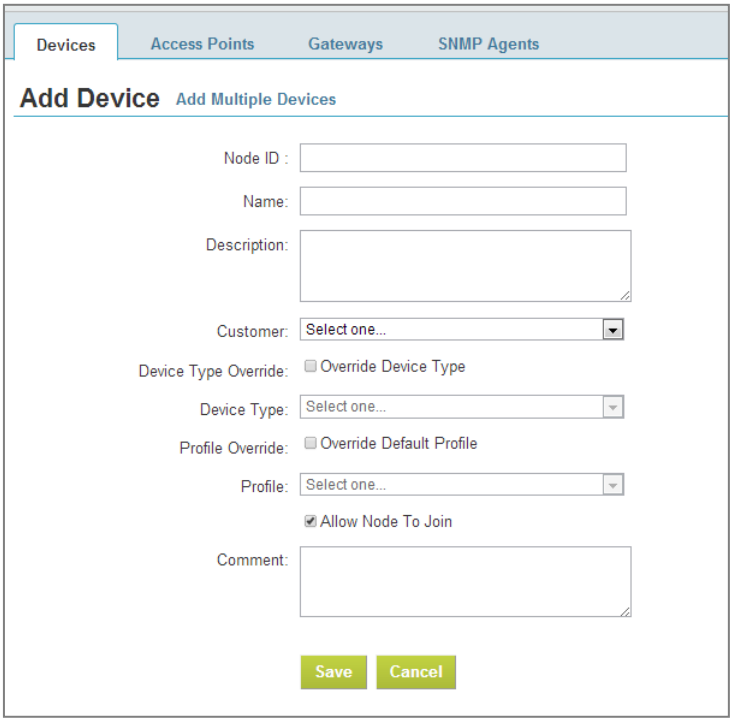
6. Verify that the complete list of devices was imported by navigating to the **Network → Devices** page.

3.4.2 Entering Devices Individually

You may add devices one at a time by following these steps:

1. Under Network → Devices, click on **Add Device.**

2. Wait for the following screen to appear.



3. Complete the information for the following fields.

Add Device Field	Description
Node ID*	Enter the Node ID, in hexadecimal format. **NOTE:** The leading "0x" is not required.
Name	Enter a descriptive Node Name, if known. Often this field is left blank until the device is deployed on the network and the field is eventually used to store the device location.
Description	Enter a Node description, if available.
Customer*	For multi-customer systems, select the relevant customer from the dropdown menu.
Device Type Override	Check the box for this field. **NOTE:** This is relevant for CommSystems version 1.4 Nodes only.
Device Type	From the dropdown menu, select the type of application associated with this Node ID.
Override Default Profile	Check the box for this field. **NOTE:** This is relevant for CommSystems version 1.4 Nodes only.
Profile	Select the operating device profile of the Node.
Allow Node to Join	Check .the box for this field
Comment	Add a comment for the audit log.

* Indicates required field.

4. Click **Save**. After the node is added, a green tab on top of the page reports '*Nodes are added Successfully'* and the Node is now listed under **Devices**.

5. Repeat steps 3 and 4 for as many Nodes that need to be added.

6. Verify the complete list of Nodes by navigating to the **Network→ Devices** page.

4 Basic Network Operation

This section describes the daily operational activities such as logging into the EMS, monitoring the system for notifications and status, and managing device details and configuration.

4.1 Logging into the EMS

To log in to the EMS, complete the following steps:

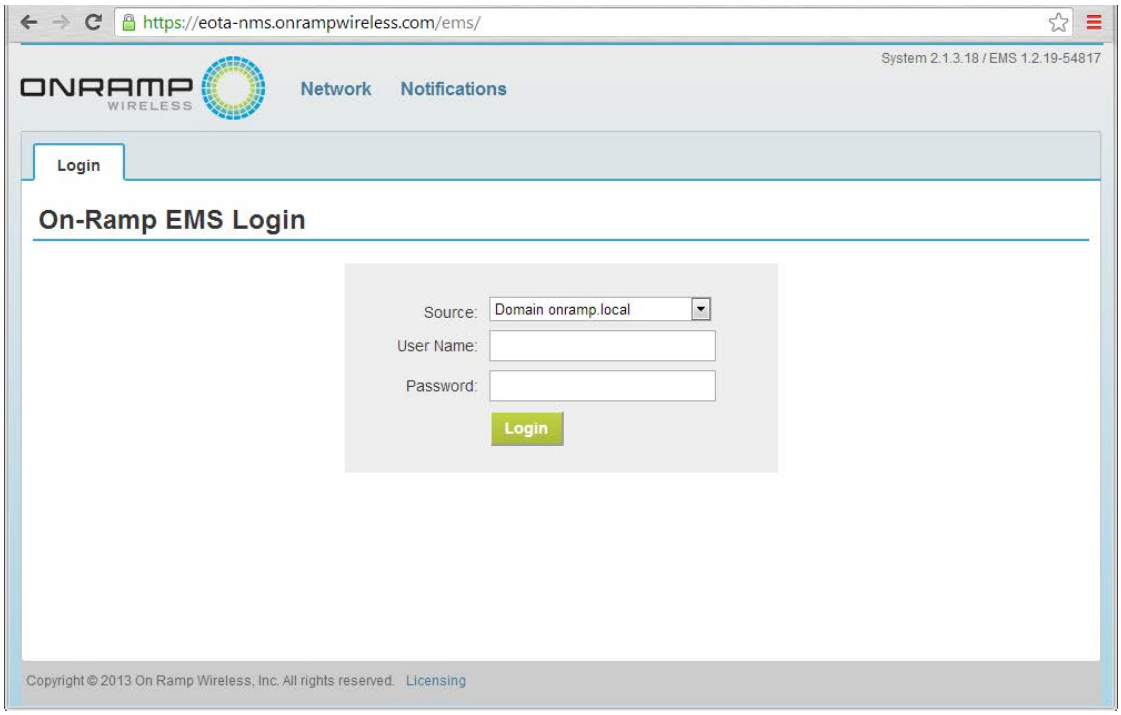
1. Open a web browser, and type:

   `http://<ip address of the EMS server or DNS name>:8080/ems`

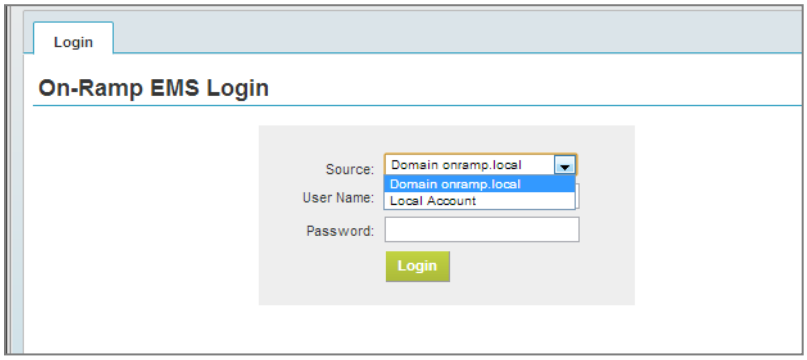
   NOTE: The following popular web browsers support all On-Ramp Total View (OTV) features:

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

2. The following login screen is displayed.



3. From the **Source** dropdown list, select **company Domain** or **Local Account**. Typically, most production installations use the Active Directory. Adding an LDAP domain requires the IT Administrator to provide the required configuration information. See section 2.1.2 Adding an LDAP Domain.



   - If LDAP login is available, there should be a dropdown menu option listing the available domains. This option allows EMS access to the organization's Active Directory.
   - If the dropdown list is not visible, the Active Directory configuration is not set up. Log in with local account access with an account that was previously created. Contact your administrator for account information.

4. In the **User Name** field, type the user name for this account.
5. In the **Password** field, type the password for this account.
6. Click **Login**.

4.2 Types of User Accounts

The EMS supports the following types of accounts:

- Admin
- Operator
- Guest

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

- When configuring Local Accounts, the IT administrator creates and maintains the accounts.
- When using Active Directory, the company's Information Technology (IT) group is responsible for setting up the EMS accounts. In this case, accounts are created according to account type (admin, operator, or guest) and are mapped to the Active Directory. For more information, see the EMS Software Installation Guide.

The following sections describe each type of account in the EMS.

4.2.1 Administrator Account

In new EMS installations that are not using Active Directory controlled logins, the administrator (admin) account is the only default account available. The admin account only manages accounts created in Local Accounts. If using Active Directory, the internal company's IT group maintains the account. For **Local Account** login, the default User ID is *admin*, and the default password is *onramp*.

NOTE: It is strongly recommended that during system setup that the admin password be changed and individual user accounts are created for every possible user on the system. The "admin account is to be used for initial system setup only. No operational system should have an admin account in use.

The administrator account has complete control over the network configuration, network operation, and Local Account administration. 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 system administrator logs in to the EMS system, the system administrator should change the default account password for the local default admin account.

It is recommended that the administrator:

- Change the default password for the local default admin account.
- Create an account for all other EMS operators that have access to the system and never use the default admin account for any operations, when using Local Accounts.

For most operations in EMS system, it is recommended that the administrator create operator type accounts.

4.2.2 Operator Account

The operator type of account allows operators to configure the network end device network parameters. If operators log in to the system as a user with this type of account, EMS account administration cannot be performed.

4.2.3 Guest Account

The guest type of account allows guest account users to view and monitor the network operation. Guests are not allowed to modify any system parameters or device configuration.

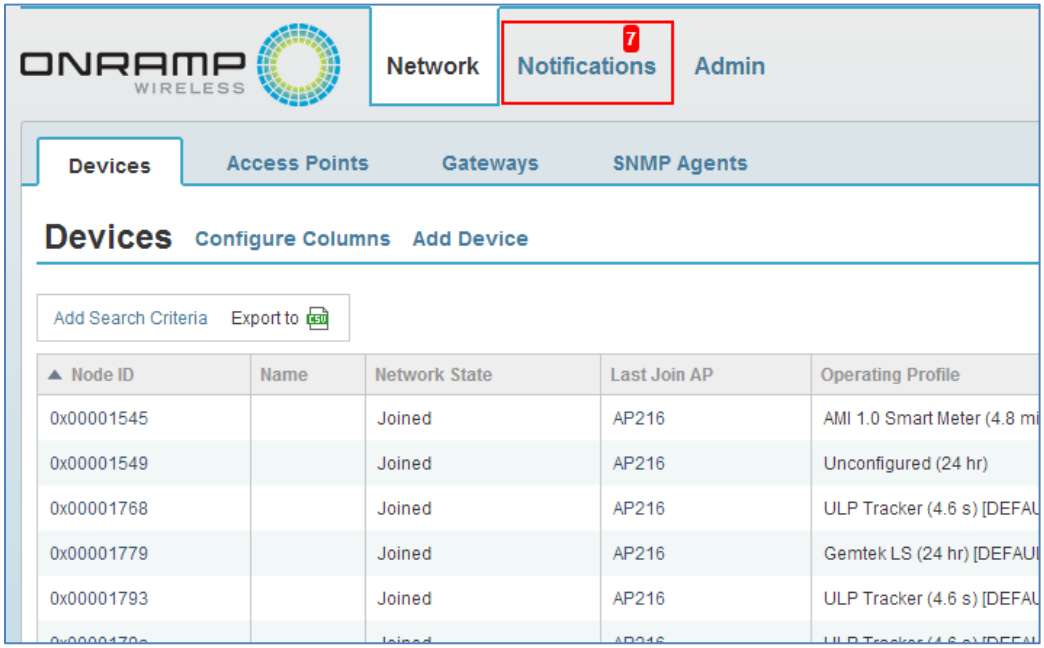
When logging in to the EMS, different tabs display for different types of accounts. For example, when logging in to the EMS with an administrator account, the tabs that display are different than those of a read-only account.

4.3 Monitoring and Managing the Overall System

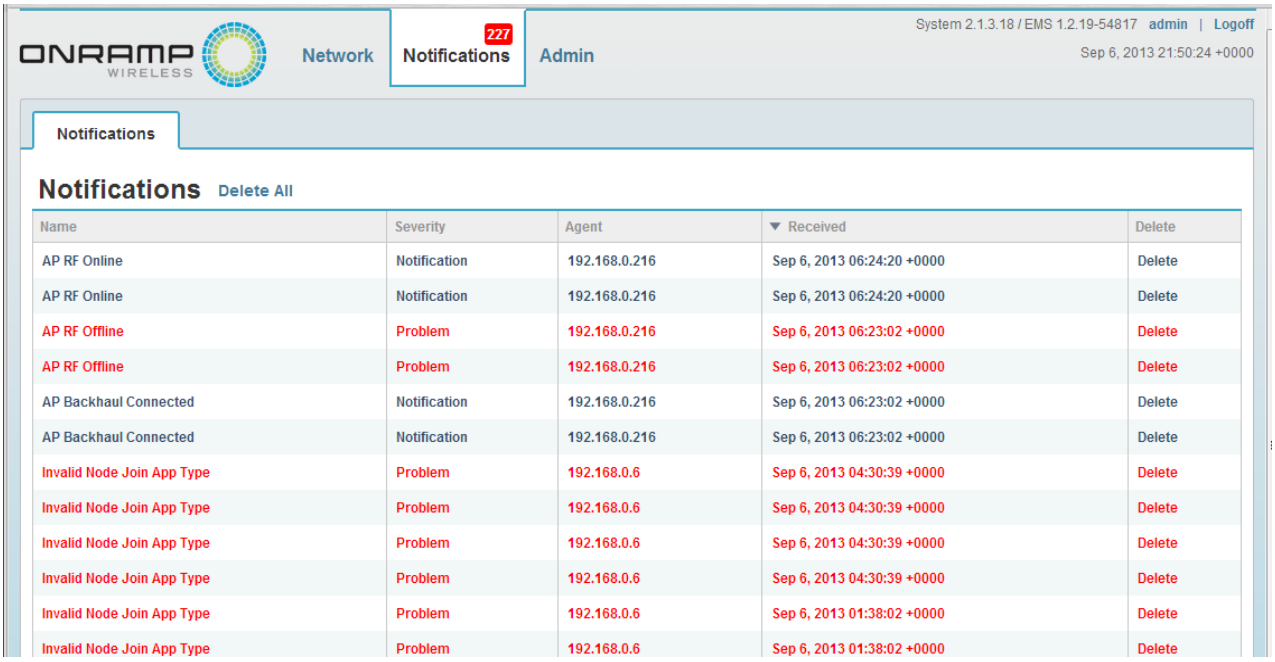
4.3.1 Monitoring System Notifications

The Notifications tab on the home screen of the EMS provides details of all the system warnings and alerts.

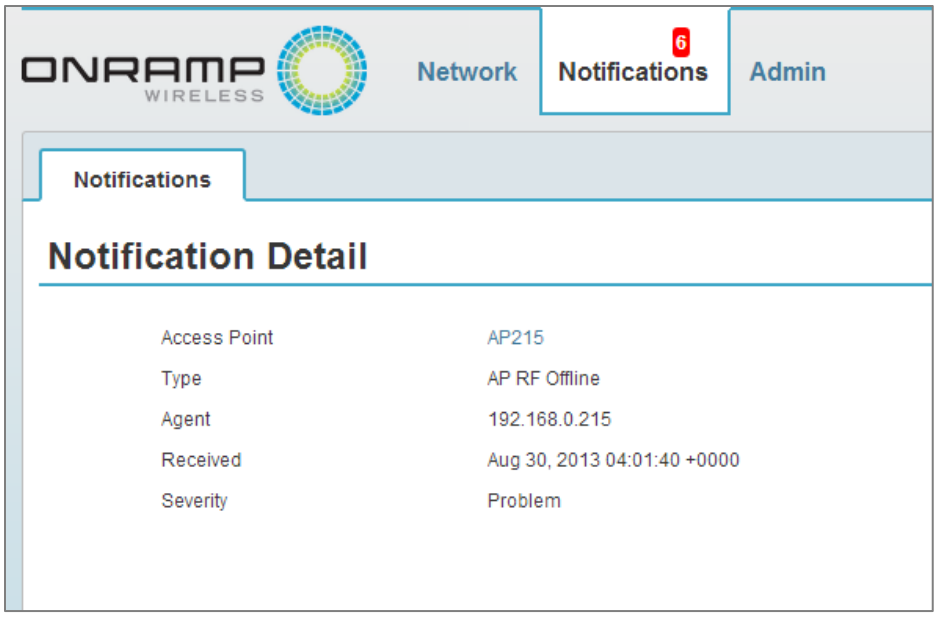
1. Click on the **Notifications** Tab in the upper left corner. The number in red indicates the current number of active notifications.



2. The following Screen Contains the list of all System Notifications along with their summary listed in columns



3. Clicking on any particular Notification provides more details about the event, as shown below. The following figure gives the details for the first Notification 'AP RF Offline' in the previous figure.

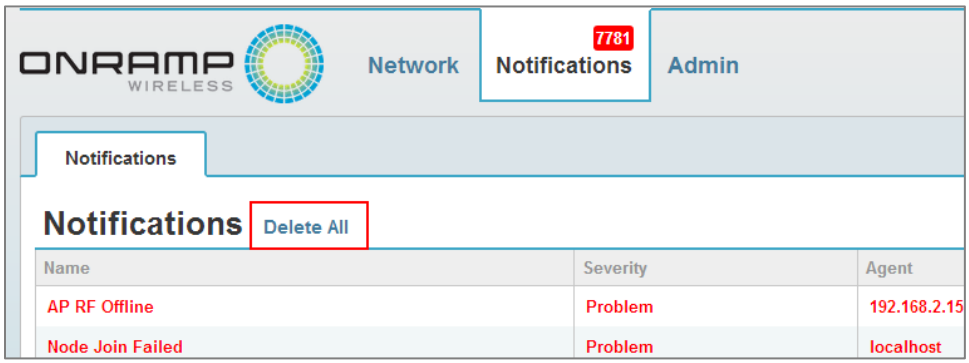


4.3.2 Deleting All System Notifications

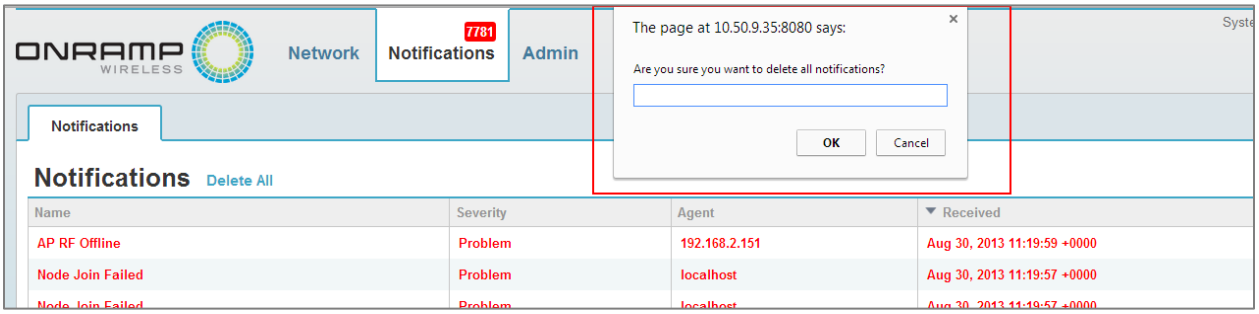
This section describes how to delete all of the system notifications.

1. Click on the **Notifications** Tab in the upper left corner.

2. Click on **Delete All** as shown below



3. Clicking on the **Delete** button displays a popup dialog box asking for a Comment that will be stored in the Audit Logs. A reason should always be entered. Press **OK** to delete the notification.



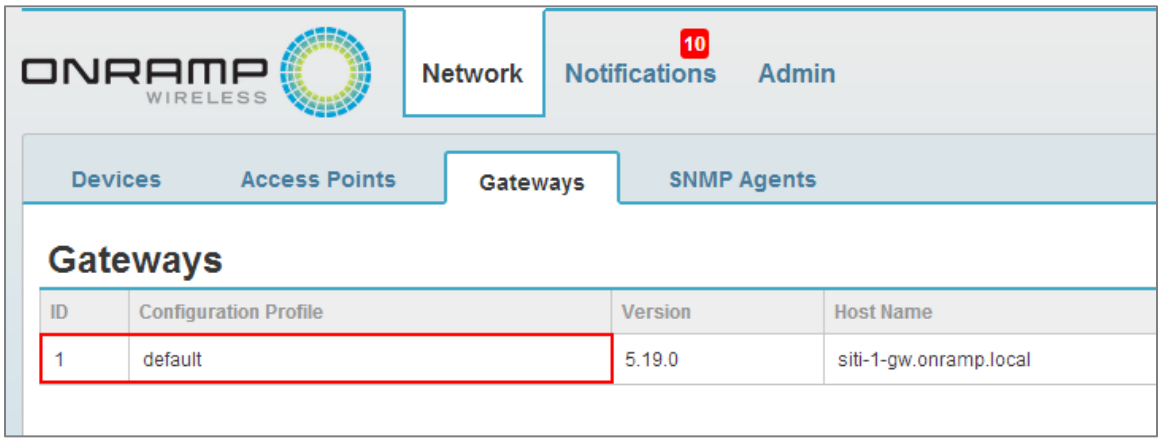
4. Verify that the Notifications have been deleted

4.4 Monitoring and Managing Gateways

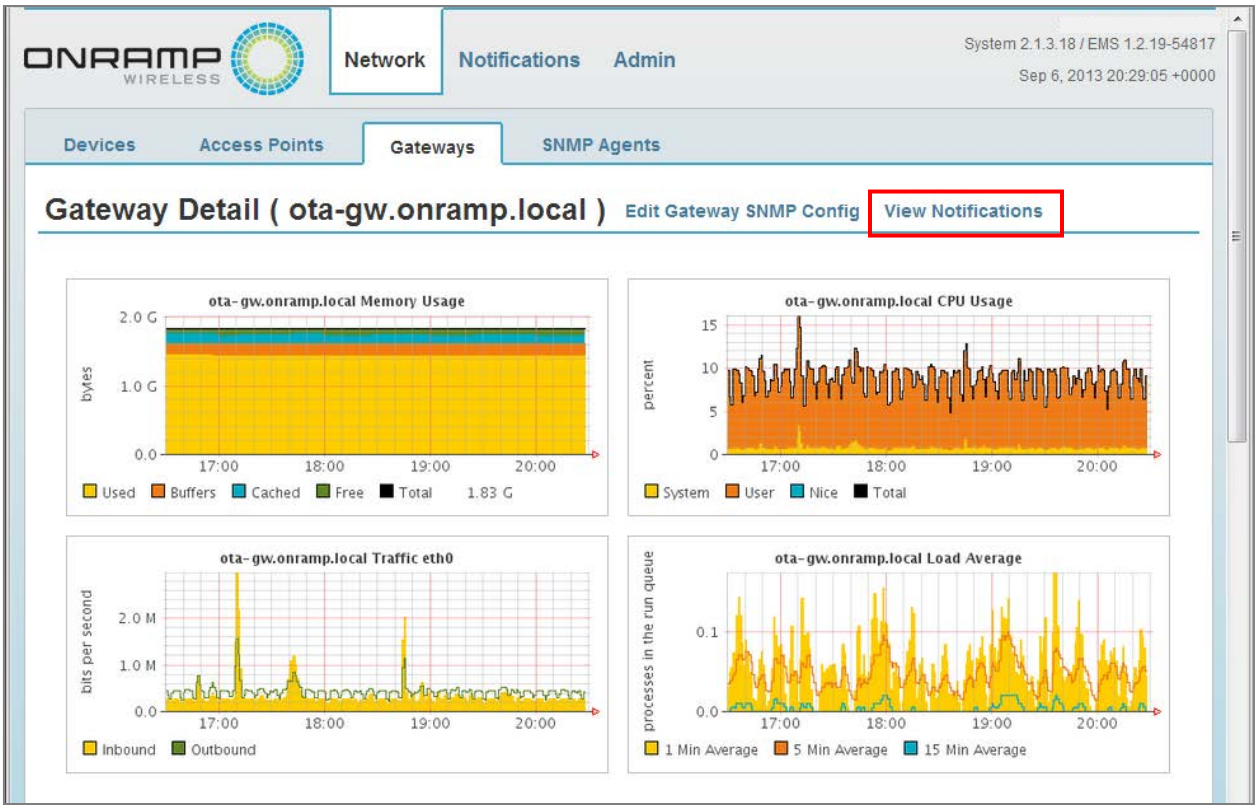
4.4.1 Monitoring Gateway Notifications

The Gateway (GW) is at the center of the On-Ramp Total Reach network and is monitoring the network constantly. Monitoring events from the Gateway is important to ensuring network health.

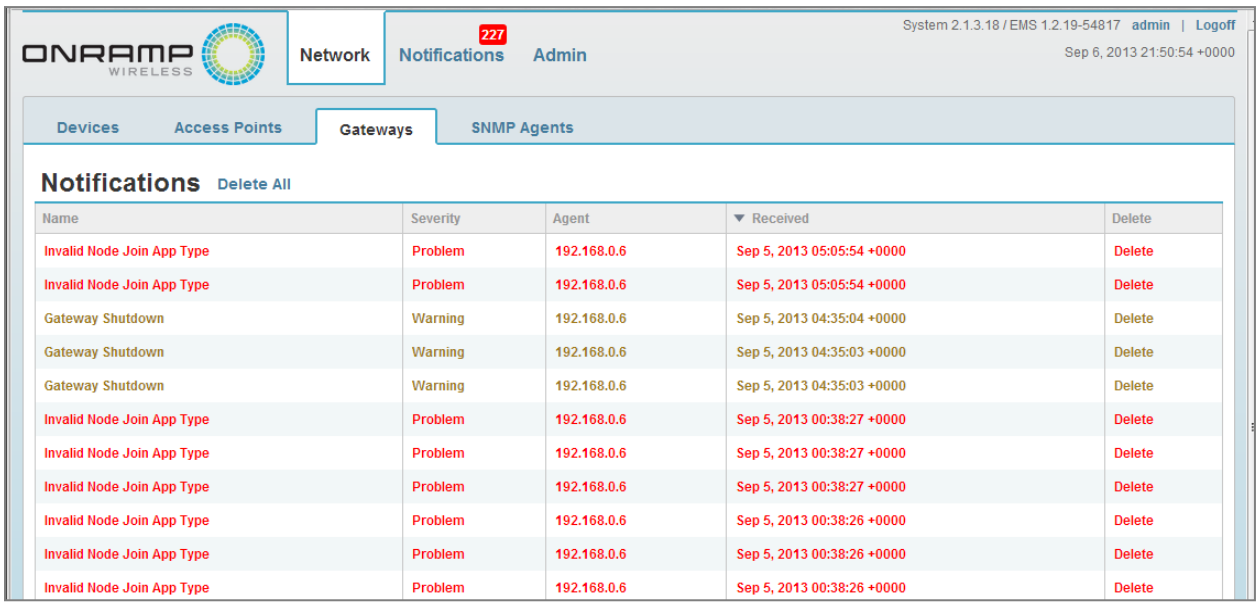
1. Navigating to the **Network → Gateways** tab shows a list of Gateways in the System. Click on any of the GW IDs/Configuration Profiles to view more details about it.



2. The following figure shows the Gateway Details page which contains important Gateway information like Latest Notifications and Gateway Information, in addition to charting dynamic Memory Usage, CPU Usage, Load Average, and graphs for Traffic over the Ethernet Port on the Gateway. Click on **View Notifications** to view Gateway Notifications.

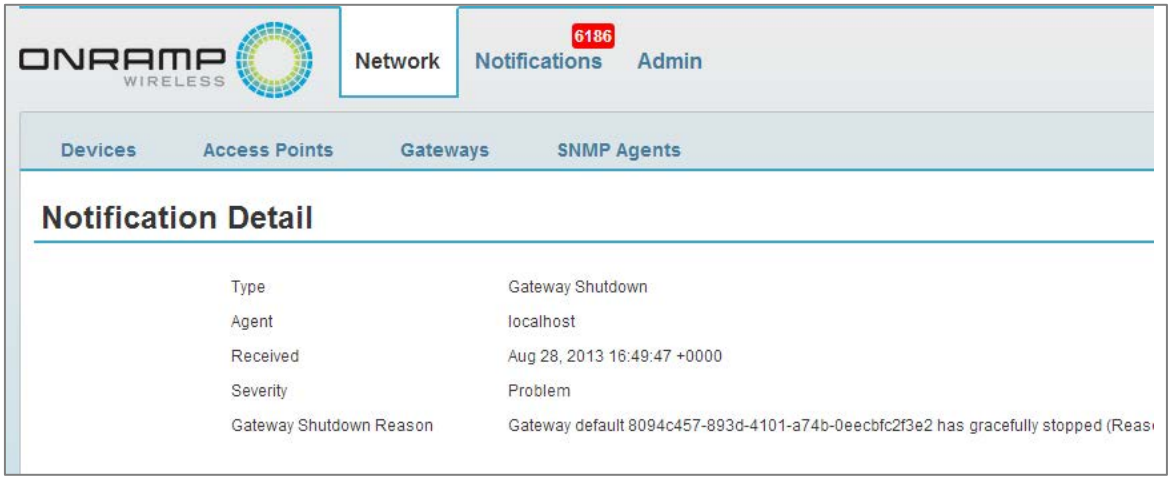


3. The following screen shows a list of notifications for the Gateway. Click on the Notification name in the leftmost column to view more details.



Name	Severity	Agent	Received	Delete
Invalid Node Join App Type	Problem	192.168.0.6	Sep 5, 2013 05:05:54 +0000	Delete
Invalid Node Join App Type	Problem	192.168.0.6	Sep 5, 2013 05:05:54 +0000	Delete
Gateway Shutdown	Warning	192.168.0.6	Sep 5, 2013 04:35:04 +0000	Delete
Gateway Shutdown	Warning	192.168.0.6	Sep 5, 2013 04:35:03 +0000	Delete
Gateway Shutdown	Warning	192.168.0.6	Sep 5, 2013 04:35:03 +0000	Delete
Invalid Node Join App Type	Problem	192.168.0.6	Sep 5, 2013 00:38:27 +0000	Delete
Invalid Node Join App Type	Problem	192.168.0.6	Sep 5, 2013 00:38:27 +0000	Delete
Invalid Node Join App Type	Problem	192.168.0.6	Sep 5, 2013 00:38:27 +0000	Delete
Invalid Node Join App Type	Problem	192.168.0.6	Sep 5, 2013 00:38:26 +0000	Delete
Invalid Node Join App Type	Problem	192.168.0.6	Sep 5, 2013 00:38:26 +0000	Delete
Invalid Node Join App Type	Problem	192.168.0.6	Sep 5, 2013 00:38:26 +0000	Delete

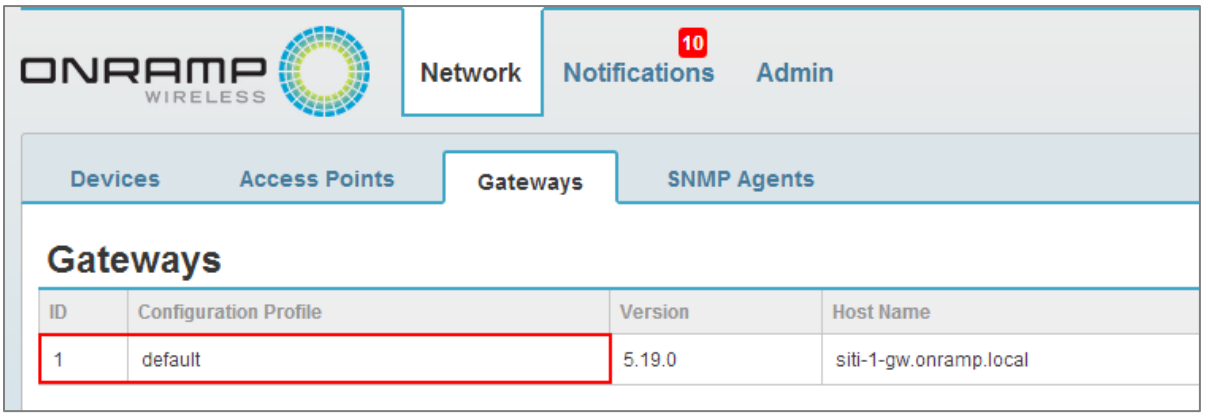
4. The following figure shows a sample Notification Details screen.



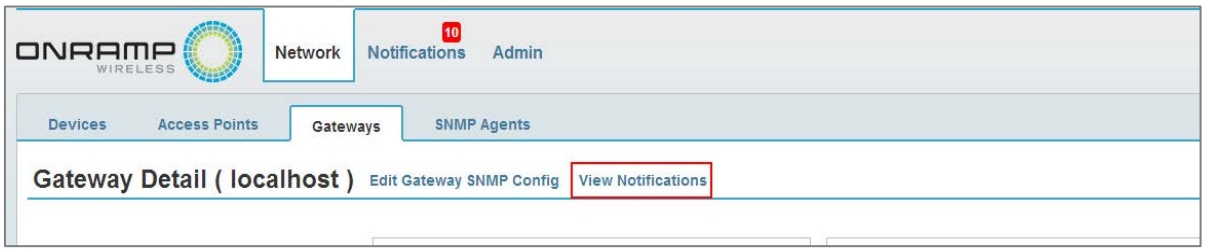
4.4.2 Deleting Gateway Notifications

This describes how to delete Gateway notifications. Deleting notifications should only be done if the notification has been handled and is no longer needed to display network status or health.

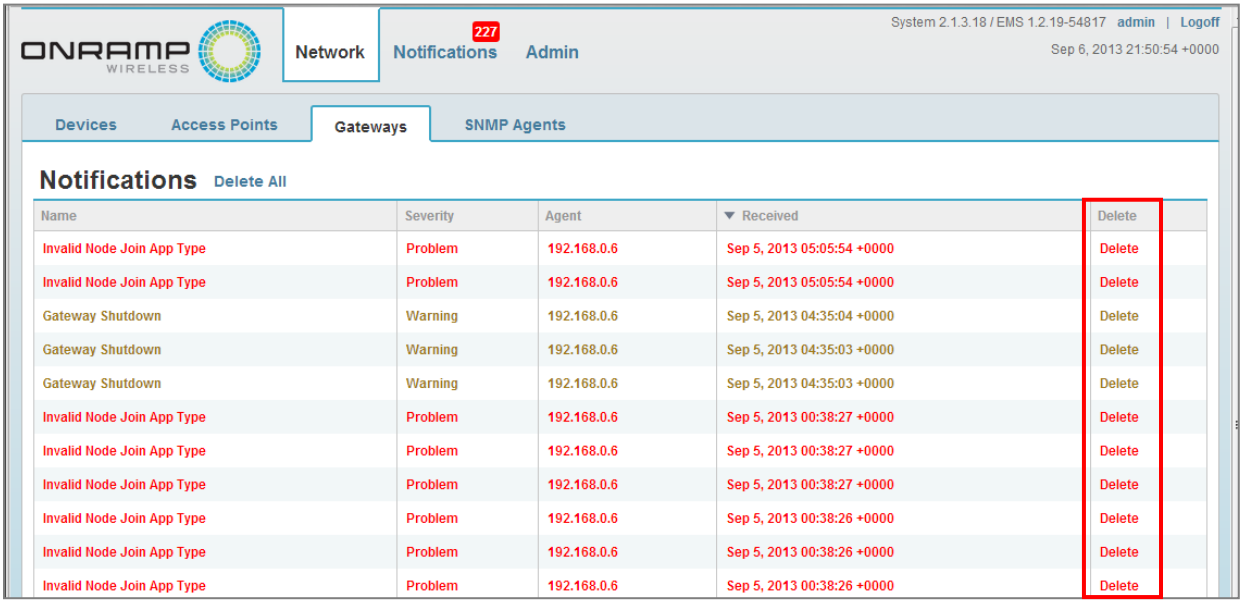
1. Navigating to the **Network → Gateways** tab shows a list of Gateways in the System. Click on any of the Gateway IDs/Configuration Profiles to view more details about that Gateway.



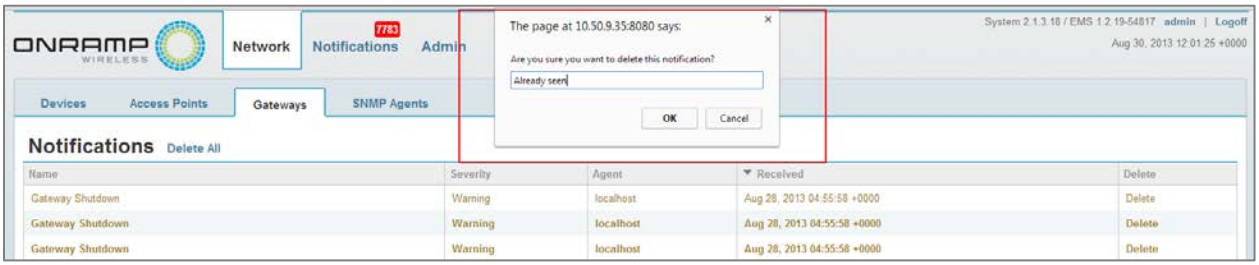
2. Click on **View Notifications** to view Gateway notifications.



3. The following Screen shows a list of all notifications for the Gateway. The rightmost column allows you to **Delete** notifications.



4. Clicking on the **Delete** button displays a popup dialog box asking for a comment that will be stored in the Audit Logs. A reason should always be entered. Press **OK** to delete the notification.



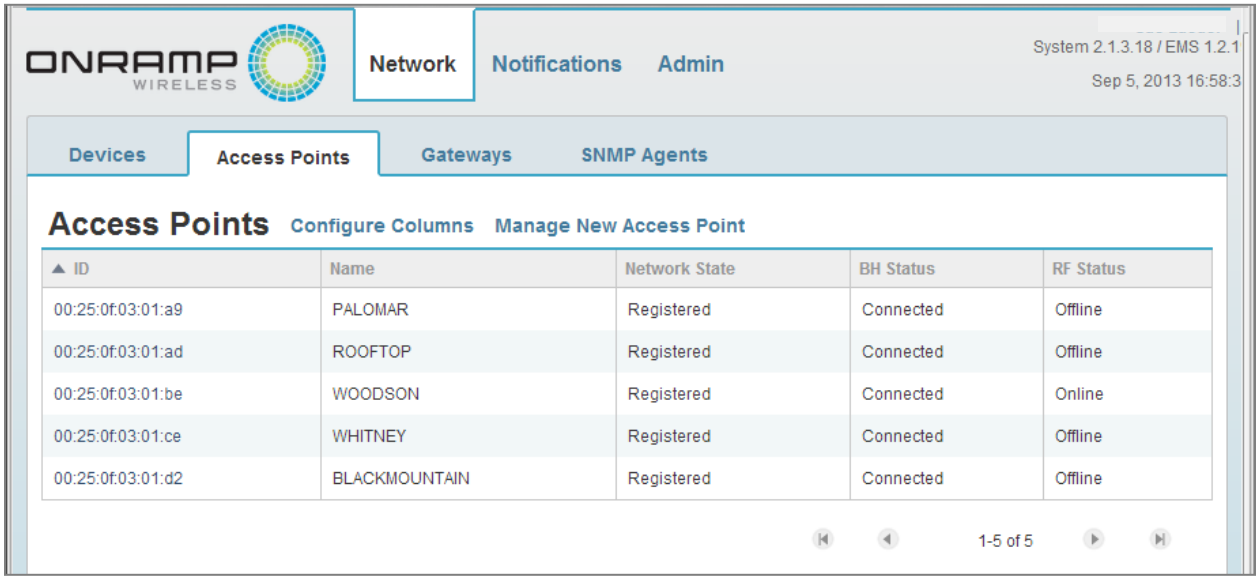
5. Verify that the notification has been deleted from the GW Notifications Page

4.5 Monitoring and Managing Access Points

4.5.1 Monitoring Access Point Events

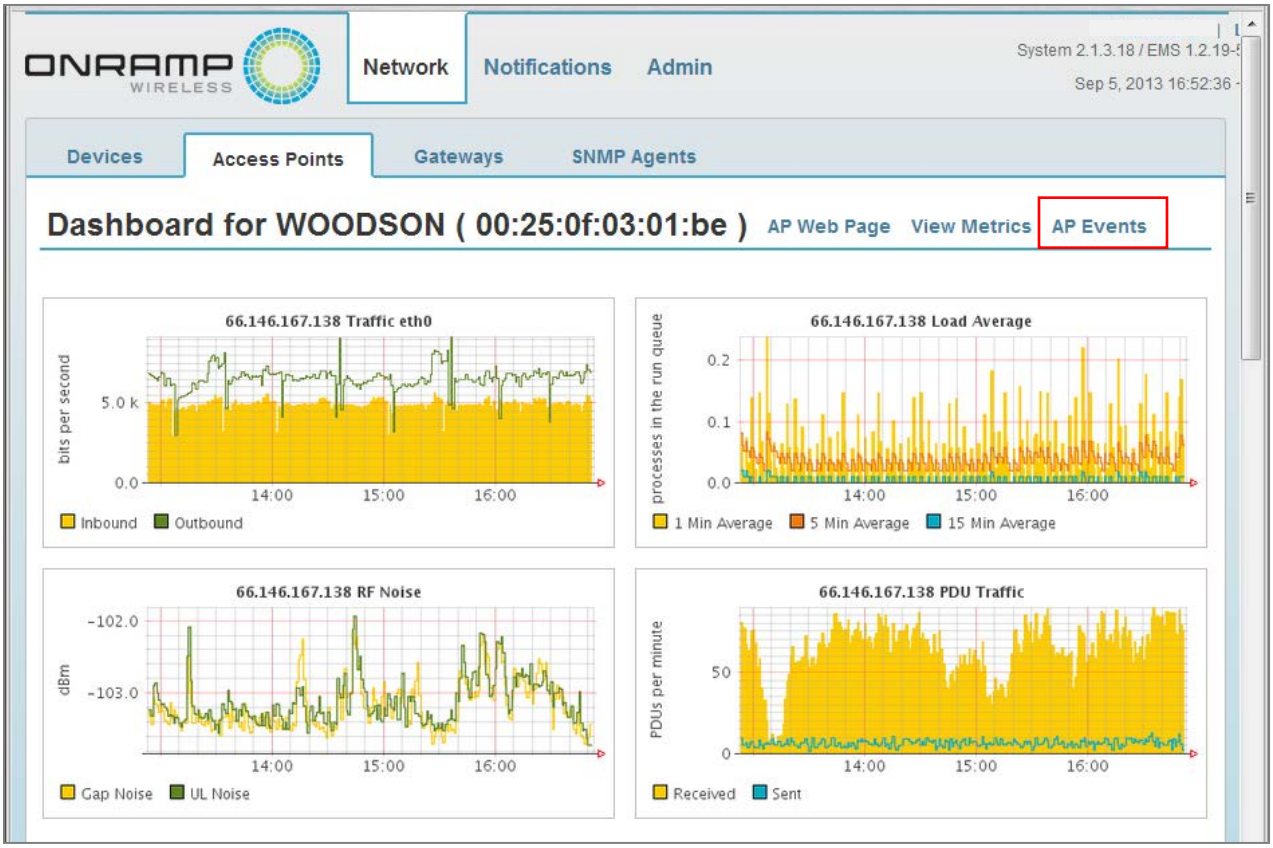
This is used to monitor Events like Access Point State Change or Gateway Connection Status associated with an Access Point. The Network Operator may monitor State Change Status events or Gateway connection status, but Network Specialists have the required knowledge to view the AP Phy Stats events.

1. Under the **Network → Access Points** tab, Click on any of the AP IDs to view AP details page.

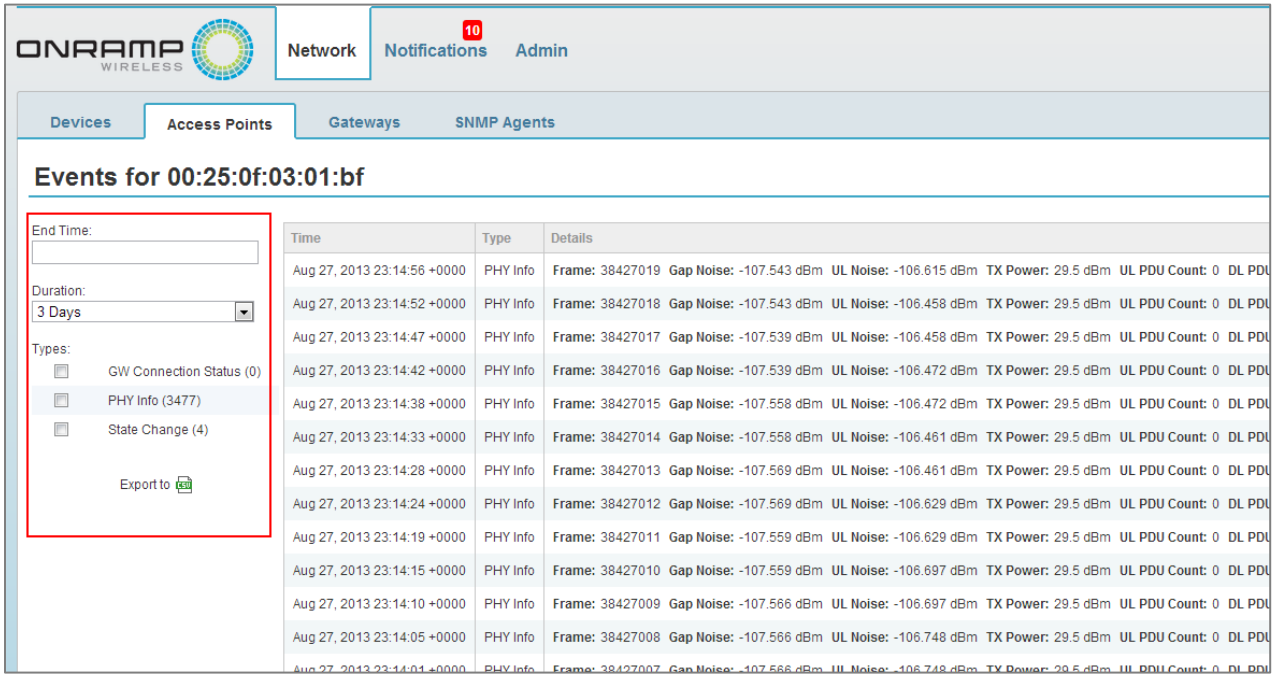


▲ ID	Name	Network State	BH Status	RF Status
00:25:0f:03:01:a9	PALOMAR	Registered	Connected	Offline
00:25:0f:03:01:ad	ROOFTOP	Registered	Connected	Offline
00:25:0f:03:01:be	WOODSON	Registered	Connected	Online
00:25:0f:03:01:ce	WHITNEY	Registered	Connected	Offline
00:25:0f:03:01:d2	BLACKMOUNTAIN	Registered	Connected	Offline

2. The AP Details Page shows important AP information like Latest Notifications, Network Status Details, AP Status Details, RF Configuration Details, Backhaul Configuration Details and AP Statistics. Click on **AP Events** to view events associated with the AP.



3. The following screen shows an example of a list of Device Events. On the left side are Event Filters to screen unwanted events.

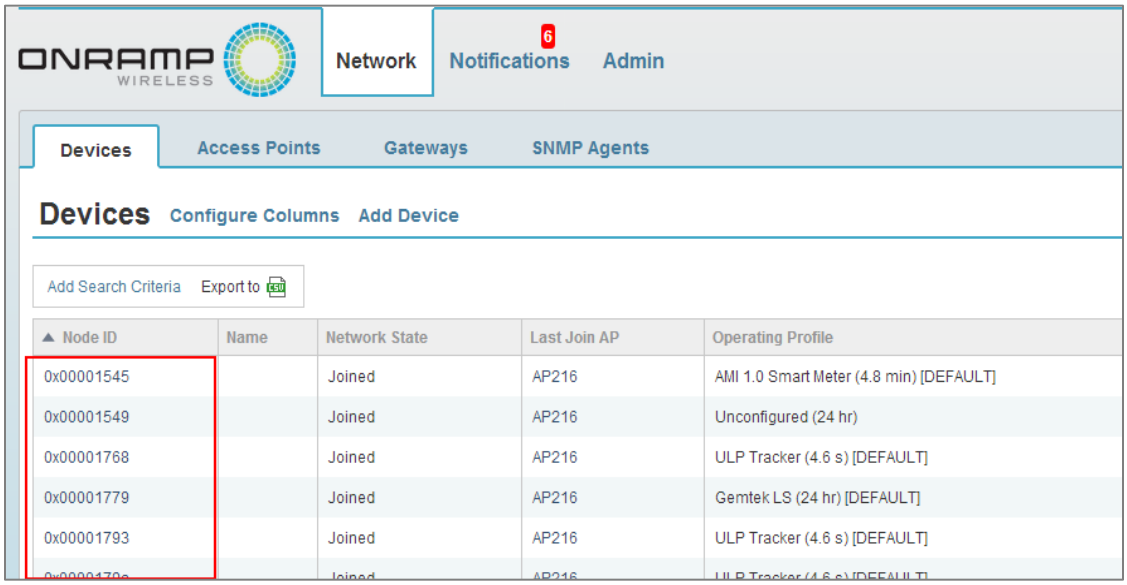


4.6 Monitoring and Managing Endpoints

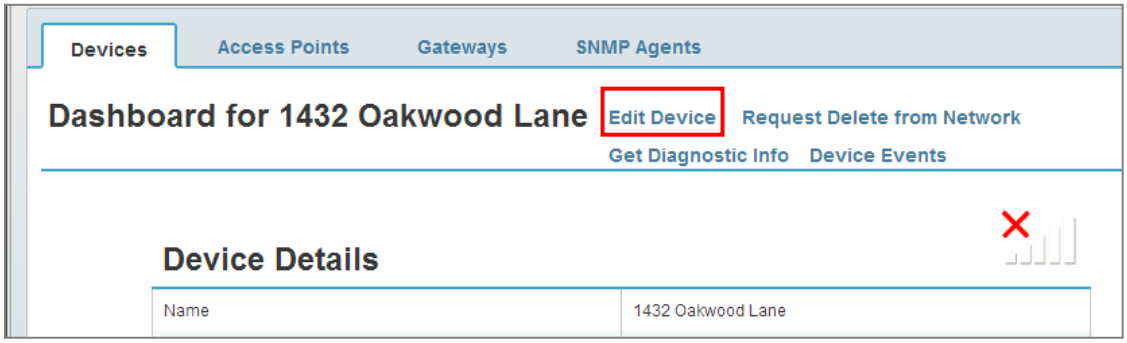
4.6.1 Editing Endpoint Details

This allows an operator to edit the device configuration while the device is in operation

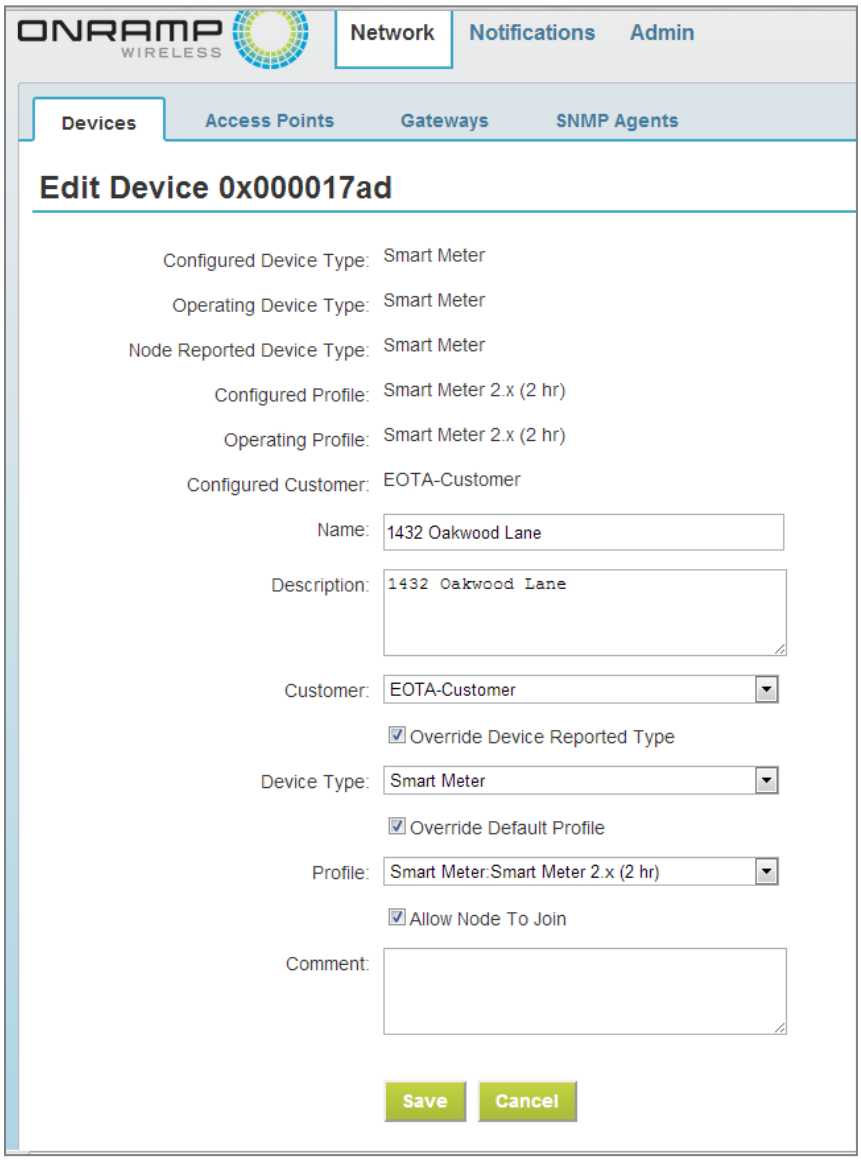
1. Under the **Network → Devices** tab, which is also the default login screen , click on any of the Device IDs listed in the leftmost column to view more details about the device



2. As shown in the figure below, click on **Edit Device** to edit a device.



3. In the following screen, change the parameters as required and click on **Save.**

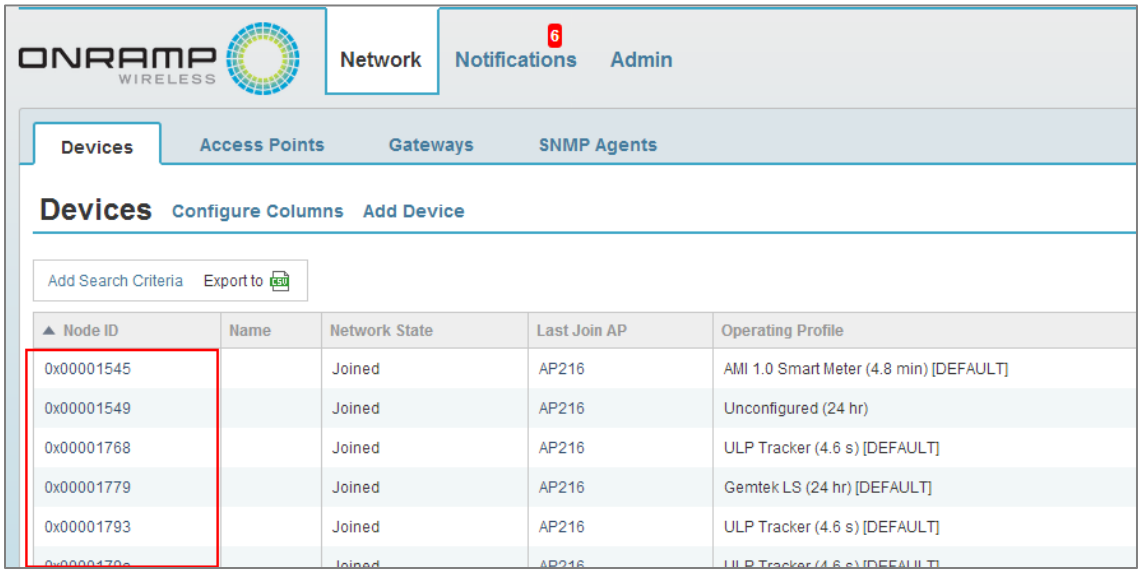


4. Any name or description changes take effect immediately. Changes to the Profile take place after an Update Interval for the device has occurred. Verify from the **Network → Devices** page after the UI Interval.

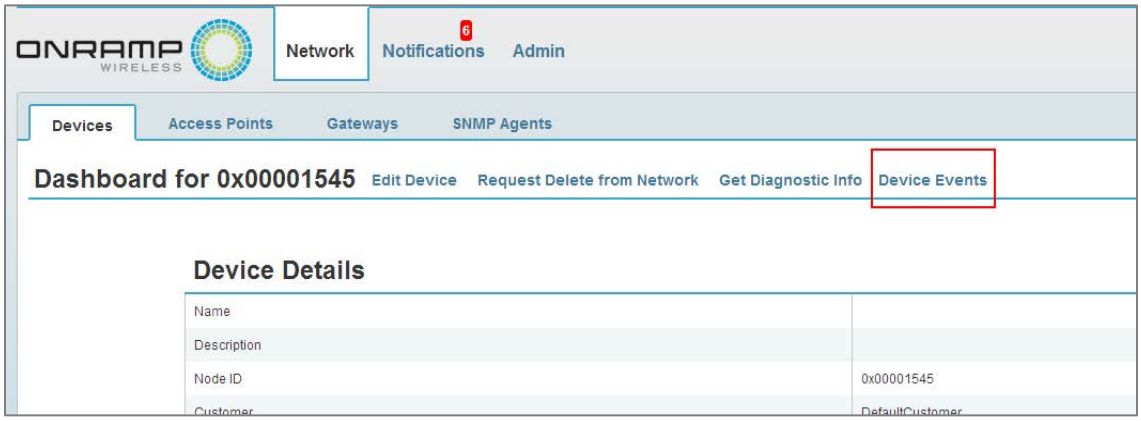
4.6.2 Monitoring Device Events

Important device information such as Join status, Physical Statistics, and UL/DL SDU Statistics is available here. The Network Operator may monitor Join Status events, but Network Specialists have the required knowledge to view the other event types such as Phy Stats and SDU stats.

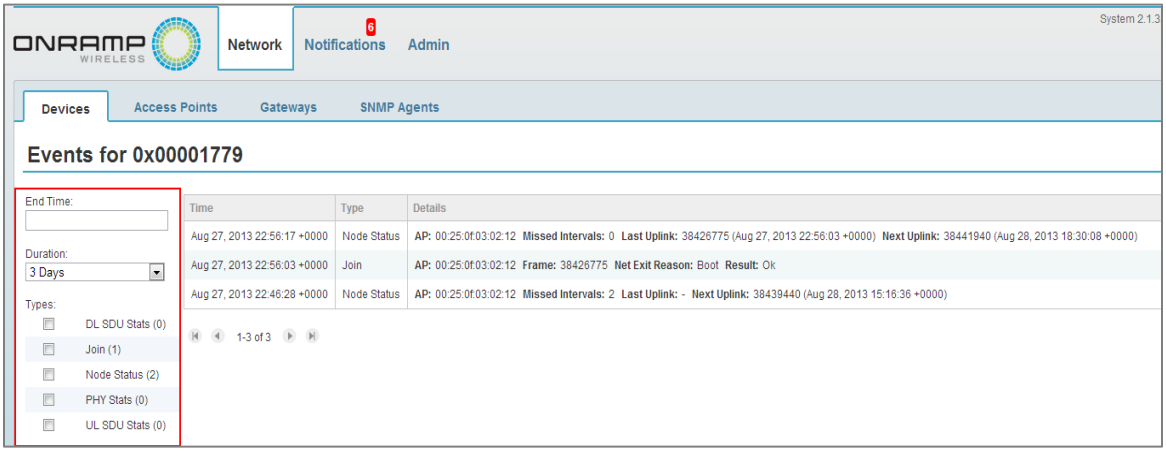
1. Under the **Network → Devices** tab, which is also the screen shown upon initial login, click on any of the Device IDs listed in the leftmost column to view more details about the device



2. As shown in the figure below, click on **Device Events** to view the events associated with the device



3. The following screen shows a sample example of a list of Device Events. On the left side are Event Filters to filter out unwanted events.



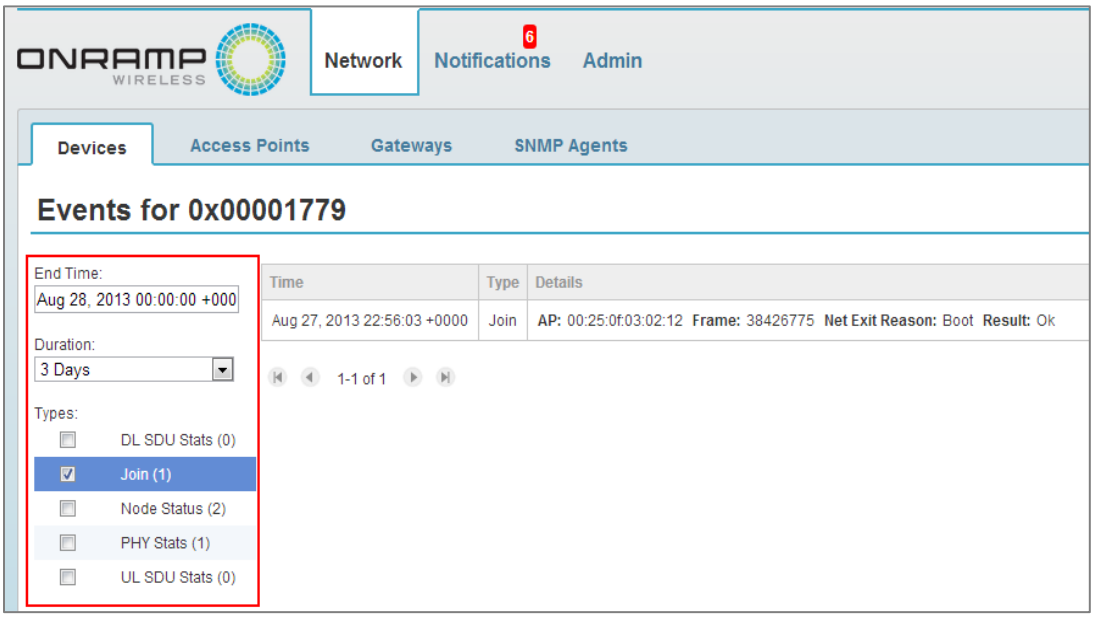
4. The filters that can be set are:

   a. **End Time:** This only shows the Device Events up to the selected Date and Time.

   b. **Duration:** This shows the events in the selected duration. For example, selecting 1 Hour only shows Events within the last 1 hour.

   c. **Type:** This is a multi-select list which can filter the events based on the event type Join/DL SDUs/UL SDUs/Physical Stats/Node Stats.

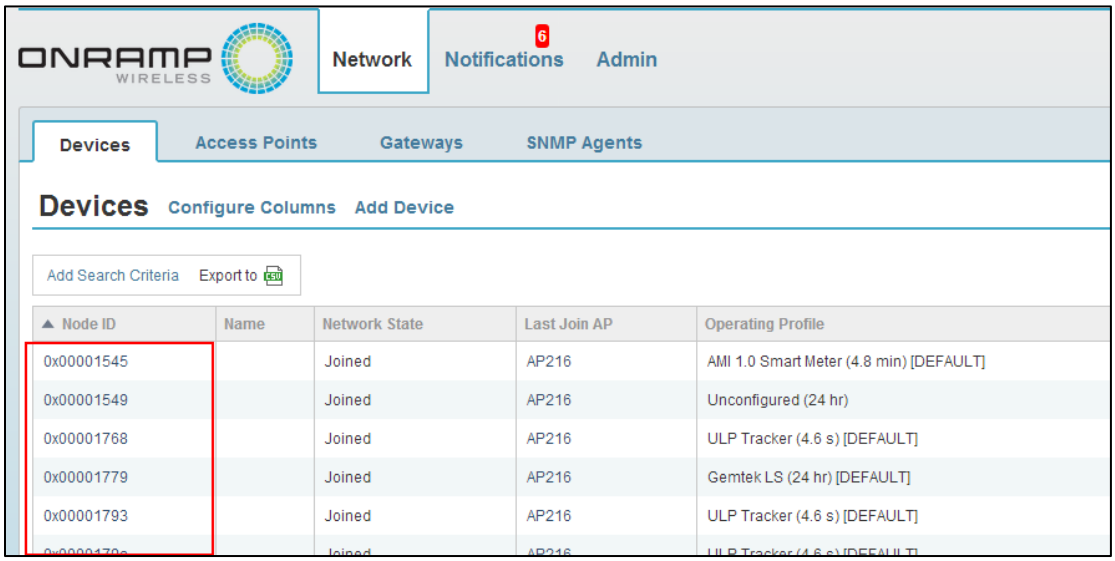
   The following figure shows an example of the Device Event Messages with **End Time** as 00:00:00 Hours, 28th of August, 2013, **Duration** as 3 Days and **Join Type** selected. So, all 'Join' events for device 0x00001779 generated in the last three days, before 00:00:00 of 28th August, 2013, are shown, as indicated below.



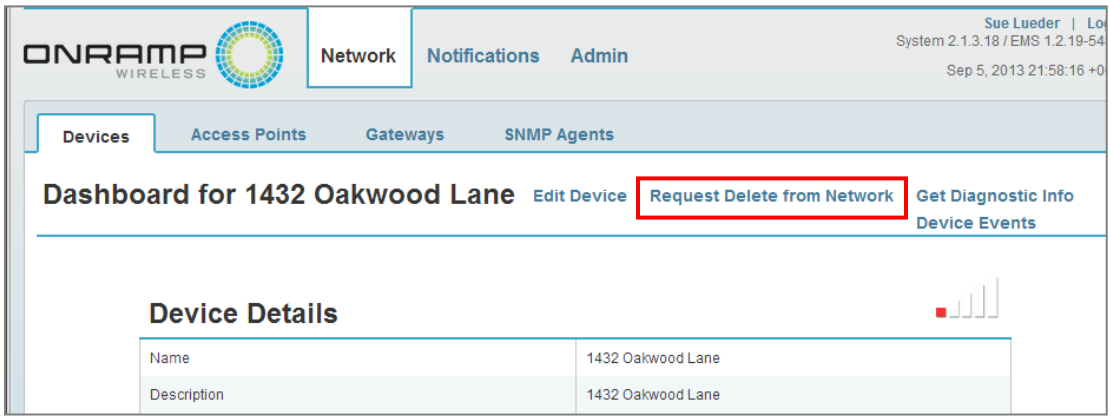
4.6.3 Deleting a Device from the Network

This describes how to delete a device from the network

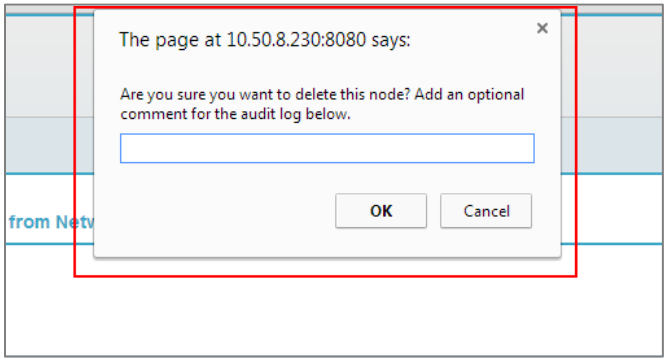
1. Under the **Network → Devices** tab, which is also the default login screen, click on any of the Device IDs listed in the leftmost column to view more details about the device.



2. As shown in the figure below, click on **Request Delete from Network** to delete the Device.



3. Clicking on the **Delete** button displays a popup asking for a Comment that'll be stored in the Audit Logs. A reason may be entered. Press **OK** to delete the notification.



4. The Device is not necessarily immediately deleted. If this node has already joined the network, it is deleted upon completion of the next Update Interval/Keep Alive Interval Time. Verify that the node has been deleted after this period by navigating to the **Network → Devices** page.

5 Advanced Features and Network Troubleshooting

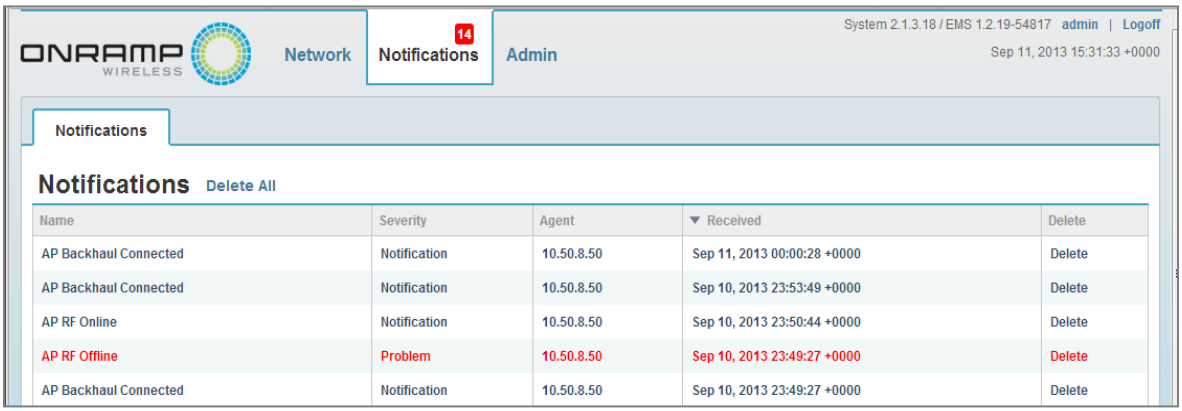
This section addresses the most typical troubleshooting procedures needed for a deployed On-Ramp Total Reach Network running Communication Systems version 2.1. Any issues that do not fall into the following categories should be escalated to On-Ramp Wireless technical support. See Appendix A for the list of all possible errors and notifications from the EMS system.

5.1 Access Point Backhaul Issues

The first indication of connection problems to an AP is if the AP text becomes red and italicized in the AP list display.

If the AP backhaul is completely down, there will not be any notifications sent to an operator, so it is important for an operator to actively monitor APs with known intermittent backhauls and triage them before they cause the AP to go offline. APs will automatically go offline after a configurable amount of time. This value is defaulted to one hour.

When the AP backhaul comes back, the operator will see notifications from the AP indicating the history of the event and current state of the AP. Any Network Operator or Specialist should register to receive these notifications in order to monitor and review issues with the backhaul. Viewing notifications will show the history of a backhaul outage event. In the example below, the AP backhaul was lost, the AP went offline as a result, and once the backhaul was connected again, the AP came back line:



Triaging an AP backhaul requires knowledge of the IT network and backhaul types in use on the network. Some steps to attempt during triage of a backhaul problem are:

- Can you ping or log into the Access Point via SSH?
- Can the Access Point ping or log into the Gateway via SSH?
- If a modem is being used and is reachable, verify the modem is functioning properly.

5.2 Node Initial Join Problems

There is a short list of reasons why an endpoint with an On-Ramp Wireless radio will not join the network. Because endpoints are generally provisioned with security keys and radio configuration during the manufacturing process, this is one area in which an error could occur and a device will not join. Here are some of the alarms an operator may see related to node join failures:

Alarm/Notification Name	Description	Operator Intervention to Triage/Clear Alarm
Invalid Node Join App Type	A node has attempted to join with an invalid app type. Contact Network Specialist and On-Ramp Support for assistance in discovering the problem.	Contact Network Specialist and On-Ramp Support.
Node Join Failed	A Node has attempted to join with invalid security keys. Contact Network Specialist and On-Ramp Support for assistance.	Resolve the key mismatch on the node.
Node Key Not Available	A Node has attempted to join and the keys have not been loaded into the KMS. Contact Network Specialist and On-Ramp Support for assistance in discovering the problem.	Load the keys into the KMS.
Un-provisioned Node Join Attempt	A node without keys has attempted to join a secure network. Disable the node and return to the manufacturer.	Disable the node and return to the manufacturer.

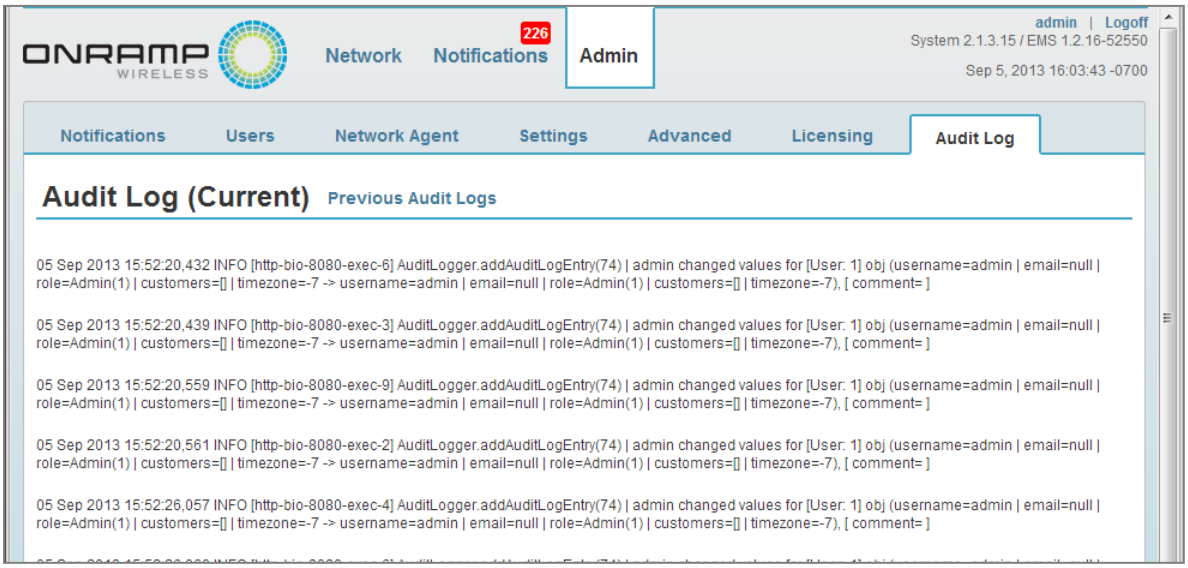
Typically these alarms occur if an end device is trying to join the network but it was not correctly provisioned and added to the EMS. To fix the problem, ensure the node and keys were properly added to the EMS and KMS. If this does not resolve the issue, the operator will need assistance from the Network Specialist, the device manufacturer, and possibly On-Ramp Wireless technical support.

5.3 Node Network Connectivity Problems

When a device has joined the network, the operator must actively monitor its join state to the network. The operator may also use OTV and MAS system to monitor reliability of the node connection to the network.

5.4 Audit Log

The EMS provides an Audit Log of all operator actions on the system so that the Network Operators and Specialists can investigate and keep records of changes on the system.



Appendix A System Notifications

This section summarizes On-Ramp Total Reach network notifications. The following table contains a short summary for each alarm, including:

1. Network element affected by the alarm
2. Severity of the alarm
3. Short description of the alarm and possible root causes
4. Alarm clearing condition
5. Available operator intervention approaches

The following table provides details for each alarm, such as descriptions for each alarm and how to proceed when receiving each type of alarm. Note that the severity of notifications may be modified by the operator.

Table 3. Alarm Type, Severity, Description, and Clearing Condition

Frequency of Occurrence	Total Reach Network Element	Alarm/Notification Name	Default Severity	Description
Occasionally	AP	AP Backhaul Disconnected	warning	Network connectivity between the AP and Gateway is broken. An operator should use standard networking debugging tools to verify the availability of the backhaul connectivity between the AP and Gateway. For example, the operator can ping the AP to validate that it is available through the backhaul network. When re-establishing the backhaul connectivity, the operator may need to contact the backhaul provider to help diagnose the issue. **Possible Root Cause:** An AP backhaul error has occurred and the AP is not reachable to the Gateway. **Operator Intervention:** This alarm could occur if the backhaul to the AP goes down for longer than one hour. **Clearing Condition:** AP Backhaul Connected again
Often	AP	AP Enclosure Open	warning	This warning is generated by an AP lid being opened, which is always an unplanned activity. APs are not designed to be opened in an operational system. If the environment is a lab environment then this is possible. The alarm will be cleared when the AP lid is closed. If the operator receives an AP open lid alarm for an operational AP, an unauthorized person may be opening the AP's lid. Appropriate action, per internal policies, should be taken such as alerting security. **Possible Root Cause:** An AP lid has been opened. **Operator Intervention:** None. If unexpected then a site visit should be arranged because this could indicate a security breach on the Base Station and AP. **Clearing Condition:** AP Enclosure Closed
Rarely	AP	AP GPS Signal Lost	warning	This alarm is the result of an AP that loses its ability to get a valid GPS tracking signal. This is most likely due to a physical problem with either the AP and/or GPS antenna connected to the AP. This type of alarm would likely be seen in conjunction with other alarms (e.g., AP offline) as an AP cannot operate without a GPS fix. The operator may need to roll a service truck to establish whether there is any issue with the antenna connectivity of the GPS antenna to the AP. **Possible Root Cause:** An AP has lost its GPS fix due to antenna problems or other GPS system failure. **Operator Intervention:** AP and base station may require repairs. **Clearing Condition:** AP GPS Signal Acquired
Rarely	AP	AP Osc Fail	problem	This notification will notify the operator that a minor GPS glitch has occurred and should be reported to On-Ramp Wireless. **Possible Root Cause:** Minor GPS synchronization glitch. **Operator Intervention:** None. **Clearing Condition:** Automatically resolved by the AP.

Frequency of Occurrence	Total Reach Network Element	Alarm/Notification Name	Default Severity	Description
Occasionally	AP	AP RF Offline	problem	The operator has taken an AP offline and it is no longer on the air or there has been an interruption in GPS timing resulting in the AP going offline. A notification will be sent when the AP is back online. **Possible Root Cause:** The operator has taken an AP offline and it is no longer on the air or there has been an interruption in GPS timing resulting in the AP going offline. **Operator Intervention:** Bring the AP back online via the EMS or AP web page or investigate a GPS connection problem. **Clearing Condition:** AP RF Online
Never	AP	AP Software Assert	problem	The AP has experienced an unexpected software assert. Please report this to On-Ramp Wireless. **Possible Root Cause:** The AP has experienced an unexpected software assert. **Operator Intervention:** None. **Clearing Condition:** Automatically resolved by the AP.
Rarely	AP	Excessive Overload Adjustment Alarm	warning	This alarm could occur if a critical mass of endpoints are joined to a non-optimal AP. This could develop over time in an operational system. The solution would be to attempt a system rescan to force endpoints to join their optimal AP. **Possible Root Cause:** The AP has determined that the node capacity is reaching its limit. **Operator Intervention:** A forced rescan may resolve the issue by causing endpoints to re-allocate across optimal Aps. **Clearing Condition:** Automatically cleared when the AP over load condition has been resolved.
Occasionally	AP	Interference Alarm	warning	This alarm may occur if a jammer appears in the same channel as the AP. The operator should contact a Network Specialist for assistance in resolving the issue. **Possible Root Cause:** A jammer is interfering with the AP operation. **Operator Intervention:** Use RF site survey tools to identify a more optimal channel for the AP. **Clearing Condition:** Automatically cleared when the interference is resolved.
Rarely	AP	Max VGA Exceeded Alarm	warning	AP Factory Calibration failure. RMA the AP to On-Ramp Wireless **Possible Root Cause:** AP Factory Calibration failure. **Operator Intervention:** RMA the AP to On-Ramp Wireless **Clearing Condition:** Max VGA Alarm Cleared
Never	AP	PA High Temperature Alarm	warning	This notification indicates a serious hardware issue with the AP. The AP should be decommissioned, replaced, and sent to On-Ramp Wireless. **Possible Root Cause:** The hardware is faulty. **Operator Intervention:** Replace the AP and return it to On-Ramp Wireless. **Clearing Condition:** PA High Temperature Alarm Cleared

Frequency of Occurrence	Total Reach Network Element	Alarm/Notification Name	Default Severity	Description
Never	AP	PPM Drift Alarm	warning	A PPM Drift alarm is indicative of an AP calibration issue. If this occurs on an operational or new AP, the AP should be immediately sent back to On-Ramp Wireless as an RMA. **Possible Root Cause:** Possible AP calibration issue. An AP crystal drifted out of tolerance. **Operator Intervention:** Immediately return the AP to On-Ramp wireless via the proper RMA process. **Clearing Condition:** PPM Drift Alarm Cleared
Rarely	AP	Registration Failure	notification	This event indicates a serious communication issue between the Gateway and AP. Please contact an On-Ramp Network Specialist for assistance. **Possible Root Cause:** An unexpected error has occurred during AP registration. **Operator Intervention:** Contact On-Ramp Network Specialist for assistance. **Clearing Condition:** AP successfully registers.
Often	AP	Registration Success	notification	A notification to the system that AP registration with the gateway has been successful. **Possible Root Cause:** A notification to the system that AP registration with the gateway has been successful. **Operator Intervention:** None. **Clearing Condition:**
Never	AP	TX Frame Squishing Alarm	warning	Contact On-Ramp Wireless Network Specialist for assistance. **Possible Root Cause:** Improper network configuration. **Operator Intervention:** Contact On-Ramp Network Specialist for assistance. **Clearing Condition:** TX Frame Squishing Alarm Cleared
Never	AP	VCTCXO High Temp Alarm	warning	This notification indicates a serious hardware issue with the AP. The AP should be decommissioned, replaced, and sent to On-Ramp Wireless. **Possible Root Cause:** The hardware is faulty. **Operator Intervention:** Replace the AP and return it to On-Ramp Wireless. **Clearing Condition:** VCTCXO High Temp Alarm Cleared
Rarely	Gateway	Force Scan Begin	notification	The AP has entered a Force Scan operation. A notification will be sent when the Force Scan operation has completed. **Possible Root Cause:** A force scan operation has been initiated by an operator. **Operator Intervention:** None. **Clearing Condition:** Force Scan End

Frequency of Occurrence	Total Reach Network Element	Alarm/Notification Name	Default Severity	Description
Never	Gateway	Gateway AP Registration Error	problem	An unexpected error has occurred during AP registration. Contact On-Ramp Network Specialist for assistance. **Possible Root Cause:** An unexpected error has occurred during AP registration. **Operator Intervention:** Contact On-Ramp Network Specialist for assistance. **Clearing Condition:** AP registration is successful.
Never	Gateway	Gateway Shutdown	warning	If the Gateway stops unexpectedly please contact On-Ramp Wireless for assistance. **Possible Root Cause:** An error in the Gateway subsystem has caused the process to stop. **Operator Intervention:** Contact IT Administrator and network specialist for assistance. **Clearing Condition:** The Gateway has restarted.
Never	Gateway	Gateway Software Assert	notification	If the Gateway stops unexpectedly please contact On-Ramp Wireless for assistance. **Possible Root Cause:** An error in the Gateway subsystem has caused the process to stop. **Operator Intervention:** Contact IT Administrator and network specialist for assistance. **Clearing Condition:** The Gateway has restarted.
Never	Gateway	SDU CMAC Failure at Gateway	problem	An error has occurred with a node security key. Contact On-Ramp Network Specialist for assistance. **Possible Root Cause:** 1. The node or KMS has an invalid key for a node. 2. Invalid deployment configuration. 3. A bad actor is injecting bad data into the uplink. 4. Someone has failed to circumvent SDU authentication, there is an intentional corruption of an otherwise valid SDU, or someone is trying to replay SDUs. **Operator Intervention:** Contact On-Ramp Network Specialist for assistance. **Clearing Condition:**

Frequency of Occurrence	Total Reach Network Element	Alarm/Notification Name	Default Severity	Description
Never	KMS	KMS Timeout	problem	The Gateway was unable to reach the KMS. Contact IT Administrator and network specialist for assistance. **Possible Root Cause:** This could occur due to some misconfigurations of the Appliance. **Operator Intervention:** Contact IT Administrator and network specialist for assistance. **Clearing Condition:** KMS is available.
Never	KMS	KMS Unreachable	problem	The Gateway was unable to reach the KMS. Contact IT Administrator and network specialist for assistance. **Possible Root Cause:** This could occur due to some misconfigurations of the Appliance. **Operator Intervention:** Contact IT Administrator and network specialist for assistance. **Clearing Condition:** KMS is available.
Never	Node	Invalid Node Join App Type	problem	A node has attempted to join with an invalid app type. Contact Network Specialist and On-Ramp Support for assistance in discovering the problem. **Possible Root Cause:** A node has attempted to join with an invalid app type. **Operator Intervention:** Contact Network Specialist and On-Ramp Support. **Clearing Condition:** None.
Rarely	Node	Node Join Failed	problem	A Node has attempted to join with invalid security keys. Contact Network Specialist and On-Ramp Support for assistance. **Possible Root Cause:** The Node attempted to join the network with invalid security keys. **Operator Intervention:** Resolve the key mismatch on the node. **Clearing Condition:** Node successfully joins network.
Rarely	Node	Node Key Not Available	problem	A Node has attempted to join and the keys have not been loaded into the KMS. Contact Network Specialist and On-Ramp Support for assistance in discovering the problem. **Possible Root Cause:** The Node attempted to join the network and keys were not found in the KMS. **Operator Intervention:** Load the keys into the KMS. **Clearing Condition:** Node successfully joins network.
Rarely	Node	Un-provisioned Node Join Attempt	problem	A node without keys has attempted to join a secure network. Disable the node and return to the manufacturer. **Possible Root Cause:** A node without keys has attempted to join a secure network. **Operator Intervention:** Disable the node and return to the manufacturer. **Clearing Condition:** Node successfully joins network.

Appendix B Sample Ingest Node File

The following content shows the structure of an example ingest node file which is an excel .csv file.

NODE_ID	NAME	APP	CUSTOMER
0x00001d19	‘node1’	1	4
0x00001a1c	‘node2’	1	4
0x00001aba	‘node3’	2	4
0x00001d19	‘node4’	2	4
0x0000aa1c	‘samplenode’	2	4
0x0000bab8	‘testnode’	2	4
0x0000cd13	‘node8’	1	4
0x0000da1c	‘node9’	3	5
0x00000ab7	‘node10’	1	5
0x00003d19	‘node11’	1	5

Appendix C Abbreviations and Terms

Abbreviation/Term	Definition
AP	Access Point. The On-Ramp Total Reach network component geographically deployed over a territory.
CSV	Comma Separated Value
Dashboard	Web page view of the aggregated end-device monitoring data.
EMS	Element Management System. The network component that provides a concise view of the On-Ramp Total Reach network for controls and alarms.
FAA	Federal Aviation Administration
FCI	Fault Circuit Indicator. The Schweitzer Engineering Laboratories (SEL®) designed end device that remotely monitors distribution lines for voltage and/or current faults.
GPS	Global Positioning System
GW	Gateway. The network appliance that provides a single entry point into the back office for the On-Ramp Total Reach network. A gateway talks upstream to the EMS and CIMA. It talks downstream to multiple APs.
IP	Internet Protocol
KMC	Key Management Client
KMS	Key Management System
MAC	Media Access Control
Node	The generic term used interchangeably with end point device.
On-Ramp Total Reach	The On-Ramp Wireless proprietary wireless communication technology.
On-Ramp Total View	The network component that passes data from the Gateway to the associated upstream databases.
ORW	On-Ramp Wireless™
OTA	Over-the-Air
OTV	On-Ramp Total View
PA	Power Amplifier
PHY	Physical Layer
PPM	Parts per million
RF	Radio Frequency
RMU	Remote Monitoring Unit. The end device that monitors Federal Aviation Administration (FAA) obstruction lights.
RPMA	Random Phase Multiple Access
SDU	Service Data Unit
SMTP	Send Mail Transport Protocol
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TX	Transmit
UDP	User Datagram Protocol
UI	Update Interval
VGA	Variable Gain Amplifier