



ULP CIMA Operator Guide

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. 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 to obtain the latest revision.

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

Copyright © 2011 On-Ramp Wireless Incorporated.
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. 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 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 Incorporated.

On-Ramp Wireless Incorporated 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 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, Incorporated.

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 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 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.

Ultra-Link Processing™ is a trademark of On-Ramp Wireless.

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

ULP CIMA Operator Guide

010-0046-00 Rev. E

November 29, 2011

Contents

1 Introduction.....	1
2 ULP Network and CIMA Overview	2
2.1 ULP Network Overview	2
2.2 CIMA Overview	3
3 Operating CIMA.....	4
3.1 Logging in to CIMA.....	4
3.2 Maintaining an Active Directory Account	4
3.2.1 Editing an Active Directory Account	5
3.3 Maintaining a Local Account and Roles.....	5
3.3.1 Administrator Role	5
3.3.2 Operator Role	6
3.3.3 Guest Role.....	6
3.3.4 Adding a Local User Role.....	6
3.3.5 Editing a Local User Account	8
3.4 Configuring CIMA.....	9
3.4.1 Adding a Gateway	9
3.4.2 Configuring CIMA Administrator Email.....	10
3.4.3 Using Maintenance Mode.....	12
Appendix A Email Alert Examples.....	14
Appendix B New Devices	15
Appendix C Abbreviations and Terms	16

Figures

Figure 1. Functional Overview of the ULP Network	2
--	---

Tables

Table 1. Abbreviations and Terms	16
--	----

Revision History

Revision	Release Date	Change Description
A	December 10, 2010	Initial release to system release 1.2.4.7.
B	December 14, 2010	Updated to system release 1.2.5.2.
C	May 17, 2011	Updated to system release 1.2.5.16.
D	June 9, 2011	Updated to system release 1.2.5.17.
E	November 18, 2011	Applied the following changes: <ul style="list-style-type: none">■ Updated to CIMA 1.01■ Added Maintenance Mode■ Reorganized to include only basic CIMA features

1 Introduction

This document provides Critical Infrastructure Monitoring Application (CIMA) administrators and operators with the following information:

- CIMA account configuration and maintenance.
- Ultra-Link Processing™ (ULP) end device commissioning and configuration with CIMA.

Application-specific information is provided in supplemental documentation. The following supplements are available for CIMA 1.01:

- CIMA Software Installation Guide
- EMS Operator Guide
- ULP CIMA Supplement: Obstruction Lighting Guide
- ULP CIMA Supplement: Overhead Fault Circuit Indicator
- ULP CIMA Supplement: RMU Light Wiring Guide

This document does not provide the following information:

- Gateway hardware or software installation.
- CIMA hardware or software installation.
- Element Management System (EMS) hardware or software installation.

Node physical installation of software and hardware. It is assumed that network components are installed and ready to use.

2 ULP Network and CIMA Overview

2.1 ULP Network Overview

- The On-Ramp Wireless Ultra-Link Processing™ (ULP) technology network monitors critical infrastructure devices for territories with wide areas of coverage. A network deployment contains many Access Points (APs) that are geographically distributed in specified territories. The APs create a wireless network to monitor end devices

The ULP network provides several advantages for wide-area sensor networking, such as:

- Enabling both 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. This level provides a 40dB link budget advantage over competitive technologies.
- When combined with a unique, multiple access scheme, the network can service hundreds of thousands of sensors on a single network.
- The network is deployed in above-ground, pad-mount, and below-ground applications.
- The link budget advantage allows a ULP system to reliably operate in the unlicensed 2.4 GHz ISM band, which eliminates spectrum and recurring data service charges.
- The link budget advantage also provides utility companies with a network that meets the performance and security requirements of their critical infrastructure.

The following figure illustrates the functional overview of the ULP network and provides example applications.

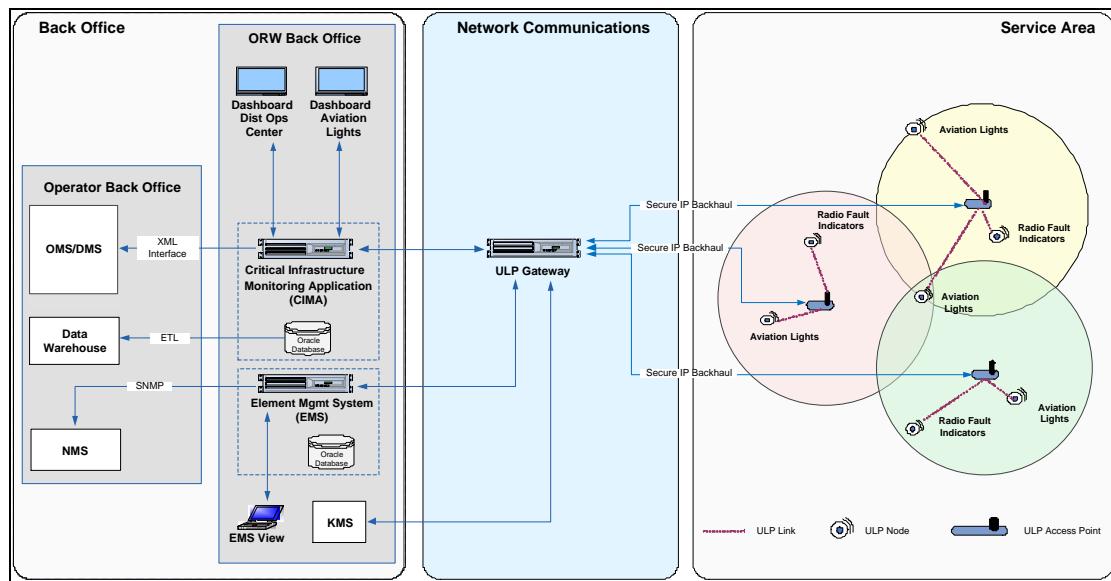


Figure 1. Functional Overview of the ULP Network

2.2 CIMA Overview

CIMA formats and passes application data from the Gateway to various databases. Application data can then be formatted and passed to an operating and maintenance system or data warehouse to enable a collection of data analytics.

A web-based User Interface (UI) enables application operators to view, list, and sort application data. The operator can also view application-level alarms using CIMA.

NOTE: Operators can use the On-Ramp Wireless EMS for network-level controls and alarms.

3 Operating CIMA

The following sections describe how to use the CIMA application.

3.1 Logging in to CIMA

Use the following steps to log in to CIMA:

1. Open a web browser, and type:

`http://<ip address of the CIMA server or DNS name>:8080/cima`

2. From the **Source** drop-down list, select **company Domain or Local Account**.
Installations typically use the Active Directory.

- Active Directory use is enabled during CIMA installation.
For additional information on information on Active Directory setup, see the *CIMA Software Installation Guide*.
- If the drop-down list is not visible, the Active Directory configuration is not set up. Log in with local account access using an account created in [Maintaining an Active Directory Account](#).

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

NOTE: Use the Active Directory account **UserID** when logging in to CIMA through the **company Domain**. If the **company Domain** is not active, use an account created in [Maintaining an Active Directory Account](#).

4. In the **Password** field, type the password for this account.

NOTE: Use the Active Directory account **UserID** when logging in to CIMA through the **company Domain**. If the **company Domain** is not active, use an account created in [Maintaining an Active Directory Account](#).

If you have forgotten your password or require assistance, contact On-Ramp Wireless Customer Support.

5. Click **Login**.

3.2 Maintaining an Active Directory Account

For systems that use Active Directory for CIMA account maintenance, account creation and editing functions are usually controlled by the Information Technology (IT) group responsible for Active Directory account maintenance. The only exceptions are defined in Section 3.2.1 Editing an Active Directory Account.

3.2.1 Editing an Active Directory Account

Use the following steps to edit a user account:

1. Log in to CIMA as an administrator or the account holder.
2. Click the **Config → 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**.

3.3 Maintaining a Local Account and Roles

CIMA contains the following types of roles for user accounts:

- Administrator
- Operator
- Guest

When a user account role is created in the CIMA system, it is created with an admin, operator, or a guest role. These role types apply to both Local Accounts and Active Directory-enabled systems.

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

For additional information, see the *CIMA Software Installation Guide*.

3.3.1 Administrator Role

For first-time CIMA installations that do not use Active Directory controlled logins, the Administrator (admin) account is the only account available. This admin account only manages users created in Local Accounts. If using Active Directory, user maintenance is handled by the IT group. For Local Account login, the default UserID is *admin*, and the default password is *onramp*.

The administrator role has complete control over the CIMA 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 users. If this is the first time that a local system administrator logs in to the CIMA

system, the system administrator should change the default account password for the local default admin user.

The following steps are recommended for proper password maintenance:

1. Change the default password for the default local admin user account.
2. Create user accounts for all other CIMA 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.
3. For day-to-day operations in the CIMA system, it is recommended that the administrator create users with the operator role.

3.3.2 Operator Role

The operator role allows operators to use CIMA for day-to-day operations. This is the default security type role for an operator. Users with the operator role can only view information and data for device types they have access to. When the administrator creates an Operator account, they must choose the expected application types that the operator will need to view. For example, a user with the operator role can edit application details and change a device to maintenance mode, as described in Section 3.4.3, Using Maintenance Mode.

The operator role does not allow the following CIMA functions:

- Adding and deleting a Gateway
- Adding and deleting users

3.3.3 Guest Role

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

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

3.3.4 Adding a Local User

Use the following steps to add a CIMA local user:

1. From the login page, log in with an administrator account.

2. Click the **Config** tab.

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

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

Default View Data Type

CIMA supports multiple end device applications. Users are typically only concerned with a particular application. This field defines the default view that CIMA displays for the user when they log in to use CIMA.

- Time Zone**
Choose the time zone to use for the display from the **Default Time Zone (GMT offset)** drop-down list.
- Display Node ID**
Used for CIMA to display the Node ID for the operator. Select the **DisplayNode ID** check box for the On-Ramp Wireless ULP Node ID.
- 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. Click the **Security** tab.

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

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

Assigned Data Types	Available Data Types
	FAA Light FCI Smart Meter SysMon

Cancel **Save**

6. Select one role from the list of **Available Roles** and drag and drop it to the **Assigned Roles** section.
7. Select **Available Data Types** and drag and drop them to **Assigned Data Types**.
NOTE: If the user has access to multiple data types, such as rights for an administrator or other privileged user, drag multiple **Available Data Types** to **Assigned Data Types**.
8. Click **Save**.

3.3.5 Editing a Local User Account

Use the following steps to edit a user account:

1. Click the **Config** → **Users** tabs.
2. Highlight to an account name to select it for editing.
3. Modify the profile and security information as needed.
4. Click **Save**.

3.4 Configuring CIMA

To configure CIMA, ensure that the ULP network is running and under control of the EMS, as described in the *EMS Operator Guide*.

Use the following steps to configure CIMA:

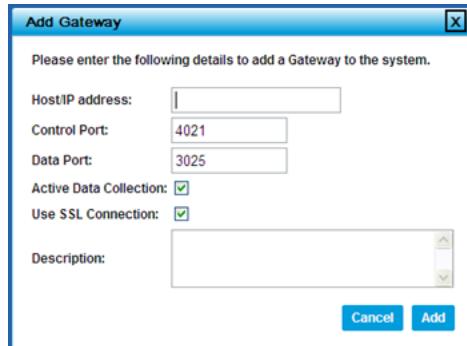
1. Log in as **admin**.
2. Add a Gateway, as shown in Section 3.4.1, Adding a Gateway.
3. Configure the default missed interval alert timeouts.

3.4.1 Adding a Gateway

Use the following steps to add a Gateway to CIMA:

1. From the login page, click the **Gateway** tab.
2. Click **Add Gateway**.

NOTE: If this is the first time adding a Gateway to CIMA, the dialog is blank.



3. In the **Host IP address** field, type the IP address or DNS name of the Gateway for the system.
4. In the **Control Port** field, the default value is **4021**.
Do not change this value.
5. In the **Data Port** field, the default value is **3025**.
Do not change this value.
6. Select the **Active Data Collection** check box.
7. Select the **Use SSL Connection** check box.

8. Optional: In the **Description** field, type a description for the Gateway. The description can be any user-specific information, such as the physical location or internal name for the Gateway.
9. Click **Add**.
10. Confirm the new Gateway information.

3.4.2 Configuring CIMA Administrator Email

CIMA runs on a workstation server that uses facilities to assist CIMA system administrators in monitoring the health of the CIMA server hardware and the software outside of end-user applications.

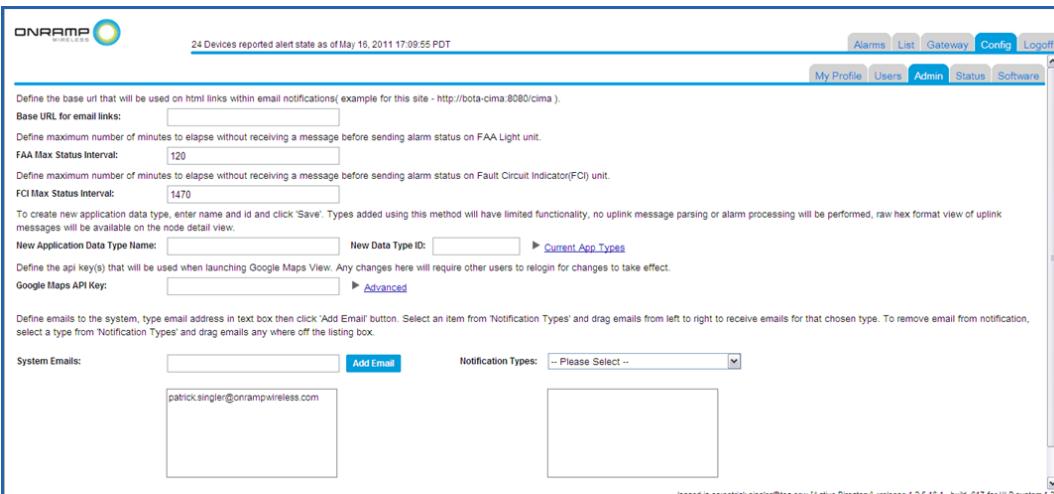
Email monitors the general health of the CIMA server hardware and software.

Use the following steps to configure the CIMA email alarm:

1. Log in to CIMA as **Admin**.

NOTE: The Admin page enables all data applications to be configured. In this section, only CIMA administration settings are described. Do not change settings not related to this configuration.

2. From the login page, click the **Config** → **Admin** tabs.



The screenshot shows the CIMA Admin configuration page. At the top, there are tabs for Alarms, List, Gateway, Config (which is selected), and Logoff. Below the tabs, there are several configuration fields:

- Base URL for email links:
- FAA Max Status Interval:
- FCI Max Status Interval:
- New Application Data Type Name: New Data Type ID: [Current App Types](#)
- Google Maps API Key: [Advanced](#)
- System Emails: [Add Email](#) Notification Types:

 A list of emails is shown in a box: patrick.singler@onrampwireless.com. A note at the bottom right of the page reads: 'logged in as patrick.singler@onrampwireless.com (active) Firewall release 1.2.5.16.1 build 817 for U3 system 1.2s'.

3.

NOTE: Ensure that the SMTP/SMS configuration settings for the CIMA installer are preconfigured in the CIMA properties configuration file. The properties file is located in the following directory:

`<cimaserver>:/opt/onramp_apps/cima_config.properties`

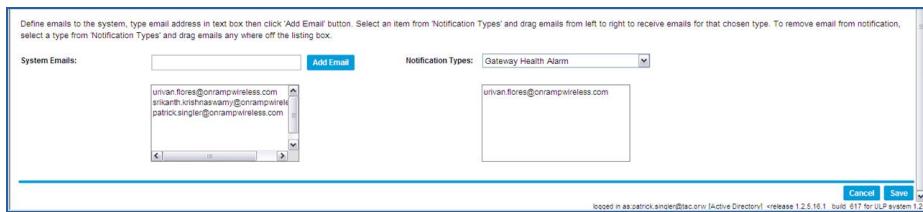
For additional information, see the *CIMA Software Installation Guide*.

3. Add email addresses to receive automated alerts from CIMA when general CIMA health alarms occur.

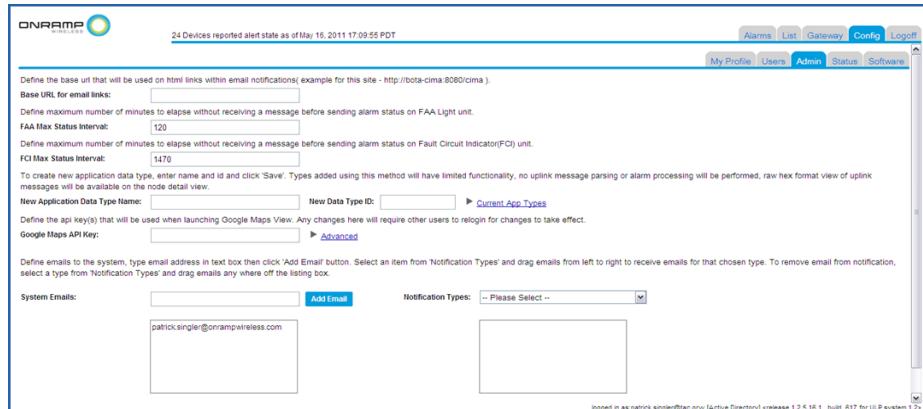
3.4.2.1 Adding Email Addresses to CIMA for the First Time

If this is the first time adding email addresses to CIMA, complete the following steps:

1. In the **System Emails** field, enter the email address.
2. Click **Add Email**.
The email address is added to the list of available emails.
3. There are two CIMA health alarm classes shown below. Select each alarm from the **Notification Types** drop-down list. Each CIMA health alarm can be configured to notify a different list of email recipients.
 - **Gateway Health Alarm**
This alarm group generates an email from CIMA when CIMA detects an issue communicating with the Gateway.
 - **Message Processing Health Alarm**
This alarm group generates an email only when there is a performance issue when processing database entries.
4. Drag the email address that was added to the **Notification Types** box.



5. Click **Save**.
6. Repeat the above steps for each general health alarm type.



7. Ensure that the CIMA installer has already configured the SMTP/SMS settings in the CIMA properties configuration file. The properties file is located in the following directory:
`<cimaserver>:/opt/onramp_apps/cima_config.properties`

For additional information about the configuration file, see the CIMA Software Installation Guide.

3.4.3 Using Maintenance Mode

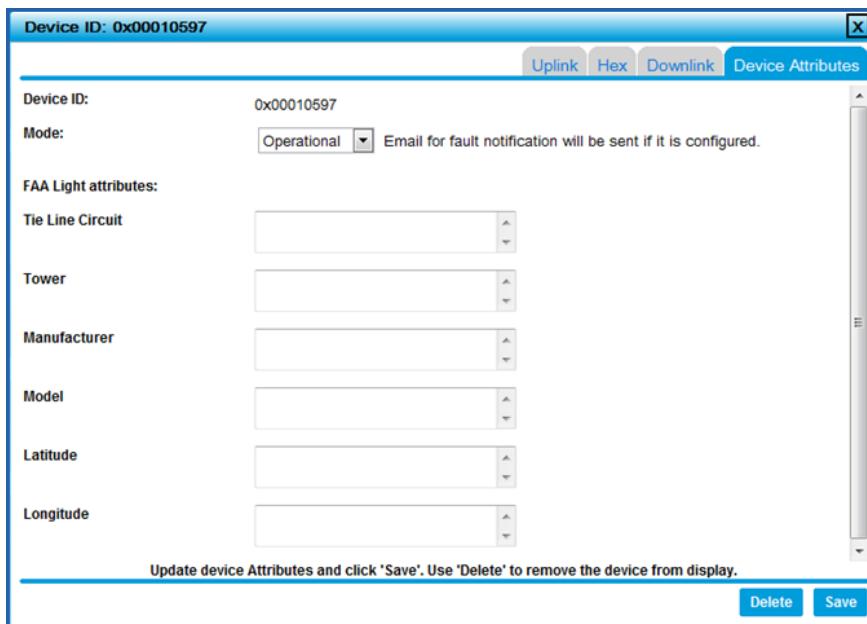
When devices are initially listed in CIMA, they are in maintenance mode by default. When the device is in maintenance mode, fault notifications for the devices are not sent to the specified email recipients. The purpose of maintenance mode is not to burden users with fault notifications when the device is not yet in deployed the ULP network for operation. When a device is in maintenance mode, the state of the device in the device list or alarm list shows a wrench symbol inside the state icon:

The device attributes panel displays the Device ID and the current mode, as shown below.

3.4.3.1 Switching to Operational Mode

Use the following steps to switch a device from **Maintenance Mode** to **Operational Mode**:

1. 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 Attributes pane.



The screenshot shows the 'Device Attributes' pane for a device with ID 0x00010597. The 'Mode' dropdown is set to 'Operational'. The pane also displays other device attributes: Tie Line Circuit, Tower, Manufacturer, Model, Latitude, and Longitude, each with a dropdown menu. A note at the bottom states: 'Email for fault notification will be sent if it is configured.' A message at the bottom of the pane says: 'Update device Attributes and click 'Save'. Use 'Delete' to remove the device from display.' There are 'Delete' and 'Save' buttons at the bottom right.

2. Click **Save**.

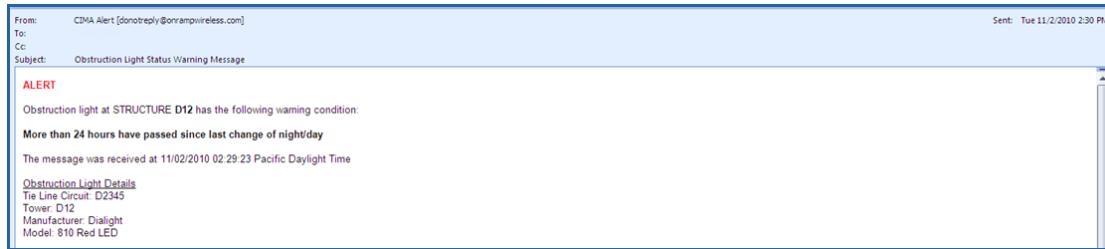
A fault notification is sent to the specified email address for the device fault condition. The device state icon is changed to the normal state when the message is sent.

Appendix A Email Alert Examples

The following example shows an email alert generated by the CIMA system. Each email identifies the following information:

- Device information, as entered into CIMA for the device
- Short description of the alarm
- Time stamp for the message
- Manufacturing details regarding the item being monitored

The following example email highlights a failure on a Dialight 810 RED LED light at structure D12 that is exhibiting a 24 hour charging system alert.

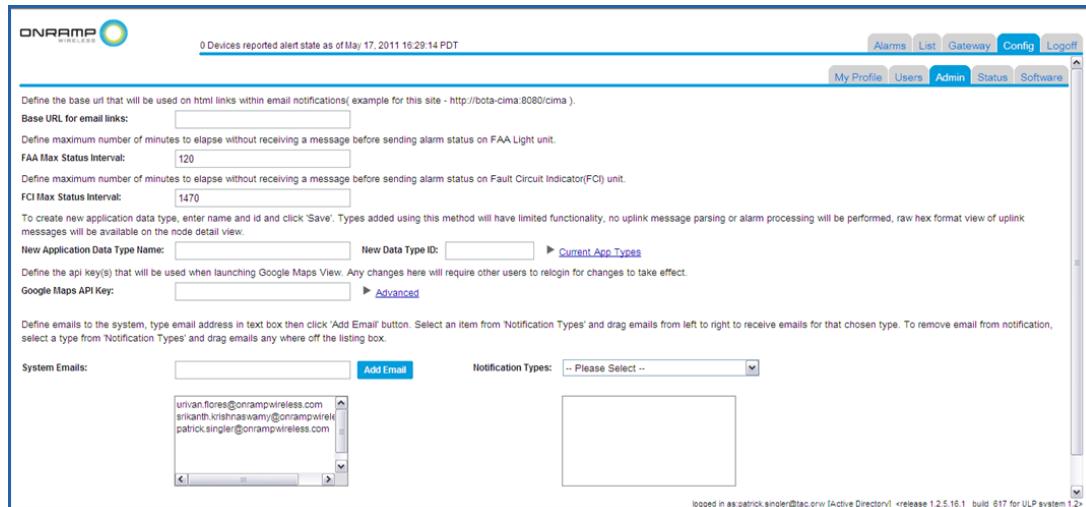


Appendix B New Devices

CIMA release 1.0.1 supports SysMon, ULP Tracker applications, and FCI and RMU FAA obstruction light applications. Over time, the system may add new device types. CIMA 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 CIMA:

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



The screenshot shows the CIMA Admin interface with the 'Config' → 'Admin' tab selected. The 'New Application Data Type' section is active. It includes fields for 'Base URL for email links', 'FAA Max Status Interval' (set to 120), 'FCI Max Status Interval' (set to 1470), 'New Application Data Type Name' (empty), 'New Data Type ID' (empty), and a 'Current App Types' button. A note states: 'To create new application data type, enter name and id and click 'Save'. Types added using this method will have limited functionality, no uplink message parsing or alarm processing will be performed, raw hex format view of uplink messages will be available on the node detail view.' Below this is a 'Google Maps API Key' field and an 'Advanced' button. On the left, a list of 'System Emails' shows 'unran.florres@onrampwireless.com', 'srikanth.krishnaswamy@onrampwireless.com', and 'patrick.singler@onrampwireless.com'. On the right, a 'Notification Types' dropdown is set to 'Please Select ..'. The status bar at the bottom indicates 'logged in as patrick.singler@onrampwireless.com (Active Directory) -> release 1.2.5.16.1, build 817 for ULP system 12'.

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

NOTE: Contact On-Ramp Wireless for additional information about how to obtain a permanent application type or to be assigned a new data type ID.

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

NOTE: This is the same data type created in CIMA for this application.

5. Click **Save**.

6. After completing this step and the corresponding EMS configuration, CIMA displays data from the new data type. The payload is displayed in hexadecimal format until a new release supports the new application.

Appendix C Abbreviations and Terms

Table 1. Abbreviations and Terms

Abbreviation/Term	Definition
AP	Access Point. The ULP network component geographically deployed over a territory.
CIMA	Critical Infrastructure Monitoring Application. The network component that passes data from the Gateway to the associated upstream databases.
FAA	Federal Aviation Administration
Gateway	The network appliance that provides a single entry point into the back office for the ULP network. A Gateway talks upstream to the EMS and CIMA. It talks downstream to multiple APs.
EMS	Element Management System. The network component that provides a concise view of the ULP 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	SMS Short Message Server
SMTP	Simple Mail Transfer Protocol
UI	User Interface
ULP	Ultra-Link Processing. On-Ramp Wireless proprietary wireless communication technology.