User's Guide

INSIGHT Remote Monitoring

Covering Release/Revision Date: 12/28/2016

This document is provided for informational purposes only and may contain errors. Winland Electronics reserves the right, without notice, to make changes to this document or in product design or specifications. Winland Electronics disclaims any warranty of any kind, expressed or implied, and does not guarantee that any results or performance described in the document will be achieved by you. All statements regarding Winland Electronics future direction and intent are subject to change or withdrawal without notice and represent goals and objectives only.

Document Revision History	
Revision A, February 10, 2016	
Changes	**Sections Affected**
Initial release	

Table of Contents

List of Figures

List of Tables

Preface

The INSIGHT remote monitoring platform provides access to the EA800-ip console to monitor sensors, log sensor data, notify users of alert conditions, track user responses to alerts, and schedule reports.

Intended Audience

This guide is intended for INSIGHT resellers, customers, and users who are responsible for administrating and monitoring EA800-ip systems.

What Is in This Guide

This guide is organized into the following chapters:

- Chapter 1, Overview summarizes the remote monitoring, remote management, and reporting features of INSIGHT.

- Chapter 2, Getting Started describes how to obtain an INSIGHT account, establish an Internet connection through the EA800-ip console, and log in to the INSIGHT host server.

- Chapter 3, Monitoring Devices describes how to use the dashboard to monitor your devices and sensors, including how to acknowledge sensor readings and respond to alert conditions.

- Chapter 4, Account Administration describes how to use the account tree to manage customer accounts, User IDs, devices, sensors, locations, and groupings.

- Chapter 5, Managing Reports describes how to create and schedule sensor log reports and alert reports.

- Chapter 6, Managing Profiles describes the use of profiles to notify users of alert conditions and guide users in responding to alert conditions.

A glossary and an index are also provided.

Related Materials

The following documents are referenced in this guide:

■   *EnviroAlert EA800-ip Quick Start Guide*

■   *EnviroAlert EA800-ip Installation/Owner's Manual*

EnviroAlert documents can be found at <u>www.winland/resources.com</u>.

For information about industry and government environmental monitoring requirements, see the following links:

■   *Vaccine Storage & Handling Toolkit*, Centers for Disease Control and Prevention, <u>https://www.cdc.gov/vaccines/hcp/admin/storage/toolkit/storage-handling-toolkit.pdf</u>

■   *CFR Title 21, Chapter 1, Part 11, Electronic Records; Electronic Signature*s; <u>http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11</u>

■   *Part 11, Electronic Records; Electronic Signatures — Scope and Application*; <u>http://www.fda.gov/RegulatoryInformation/Guidances/ucm125067.htm</u>

Documentation Conventions

This guide uses the following documentation conventions:

■   **NOTE** provides additional information.

■   **CAUTION** without an alert symbol indicates the presence of a hazard that could cause damage to equipment or loss of data.

■   **⚠ CAUTION** with an alert symbol indicates the presence of a hazard that could cause minor or moderate injury.

■   **⚠ WARNING** indicates the presence of a hazard that could cause serious injury or death.

■   **⚠ DANGER** indicates the presence of a hazard that will cause serious injury or death.

■   Text in blue font indicates a hyperlink (jump) to a figure, table, or section in this guide, and links to websites are shown in <u>underlined blue</u>. For example:

  ❑   Table 1-2 lists problems related to the user interface and remote agent.

  ❑   See "Installation Checklist" on page 6.

  ❑   For more information, visit <u>www.winland.com</u>.

- Text in **bold** font indicates user interface elements such as a menu items, buttons, check boxes, or column headings. For example:

  ❑ Click **Start**, point to **Programs**, point to **Accessories**, and then click **Command Prompt**.

  ❑ Under **Notification Options**, select the **Warning Alarms** check box.

- Text in `Courier` font indicates a file name, directory path, or command line text. For example:

  ❑ To return to the root directory from anywhere in the file structure: Type `cd /root` and press ENTER.

  ❑ Enter the following command: `sh ./install.bin`

- Key names and key strokes are indicated with UPPERCASE:

  ❑ Press CTRL+P.

  ❑ Press the UP ARROW key.

- Text in *italics* indicates terms, emphasis, variables, or document titles. For example:

  ❑ For a complete listing of license agreements, refer to the *Software End User License Agreement*.

  ❑ What are *shortcut keys*?

  ❑ To enter the date type *mm/dd/yyyy* (where *mm* is the month, *dd* is the day, and *yyyy* is the year).

- Topic titles between quotation marks identify related topics either within this manual or in the online help, which is also referred to as *the help system* throughout this document.

Technical Support

Technical Support is available during local standard working hours excluding observed Holidays.

Support Headquarters	Winland Electronics, Inc 1950 Excel Drive Mankato, MN 56001 USA
Telephone	Toll Free: 800.635.4269
Website	www.winland.com
INSIGHT Support E-mail	insightsupport@winland.com
Technical Support E-mail	techsupport@winland.com

1   **Overview**

The INSIGHT platform provides remote environmental monitoring, data logging, and system auditing. Anywhere you have access to the Internet through a computer or a smart device, you can receive E-mail and text alerts, securely monitor your environment, manage your sensors, and generate reports. The Winland Electronics remote monitoring solution protects data security, integrity, and privacy with a proprietary, encrypted data protocol and secure socket layer (SSL) data traffic.

Remote Monitoring

With INSIGHT, environmental monitoring is not a passive exercise. The INSIGHT dashboard (Figure 1-1)shows the status of each EA800-ip device. From the device level, you can drill down to see the status and details for each sensor. For each sensor, you have the ability to acknowledge sensor readings to comply with industry or regulatory requirements. When a sensor reading exceeds its thresholds, the INSIGHT platform issues an alert. To ensure that an alert is noticed, the INSIGHT platform provides a way to send alert notifications automatically by E-mail or text message to a list of users called a *notification profile*. When it comes time for action in response to an alert, the INSIGHT platform enables you to create a plan of action, called a *response profile*, for each device and sensor. The response profile is a sequence of actions that ensures a consistent response to each alert, according to your standard operating procedures (SOP). The INSIGHT platform records acknowledgments and responses that you perform to provide evidence of compliance. For more information about monitoring devices, see Chapter 3, "Monitoring Devices".
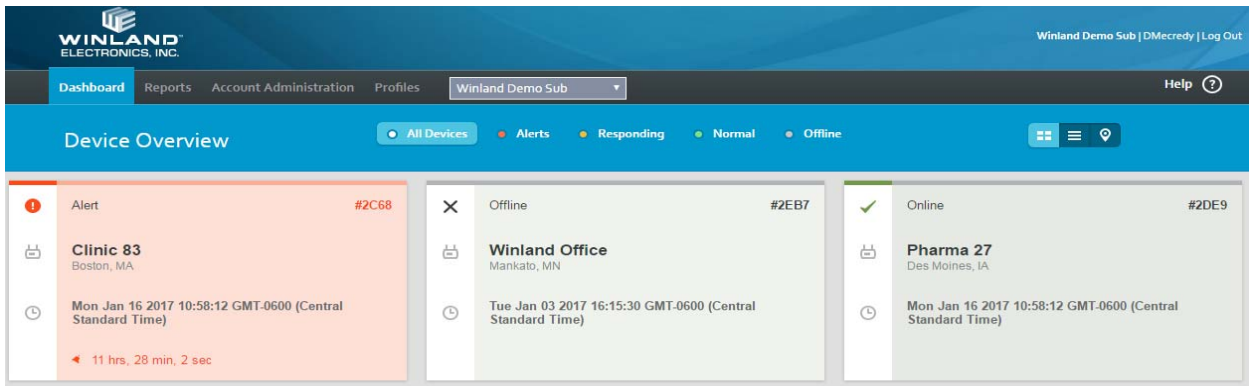

Figure 1-1. INSIGHT *Dashboard*

Remote Management

As your environment and requirements change, you can use the INSIGHT platform to change your EA800-ip system. Using the INSIGHT account tree (Figure 1-2), you have remote control of the following:

■ EA800-ip devices—You can update and delete devices. You can change device parameters such as password, keypad lock, and data collection frequency (see "Managing Devices" on page 27).

■ Sensors—You can add and delete wired sensors. You can update wired and wireless sensor parameters, such as high and low thresholds, and alert delay time (see "Managing Sensors" on page 30).

With INSIGHT, you add *User IDs* and *locations* to control who can monitor and manage users and devices in the account tree. A User ID includes a user name with which to log in to INSIGHT, the person's name, address, phone number, primary and secondary E-mail addresses, and a user permission level. A location is a named set of users and devices associated with a street address.

■ For information about User IDs, see "Managing Users IDs" on page 24.

■ For information about Locations, see "Managing Locations" on page 33.
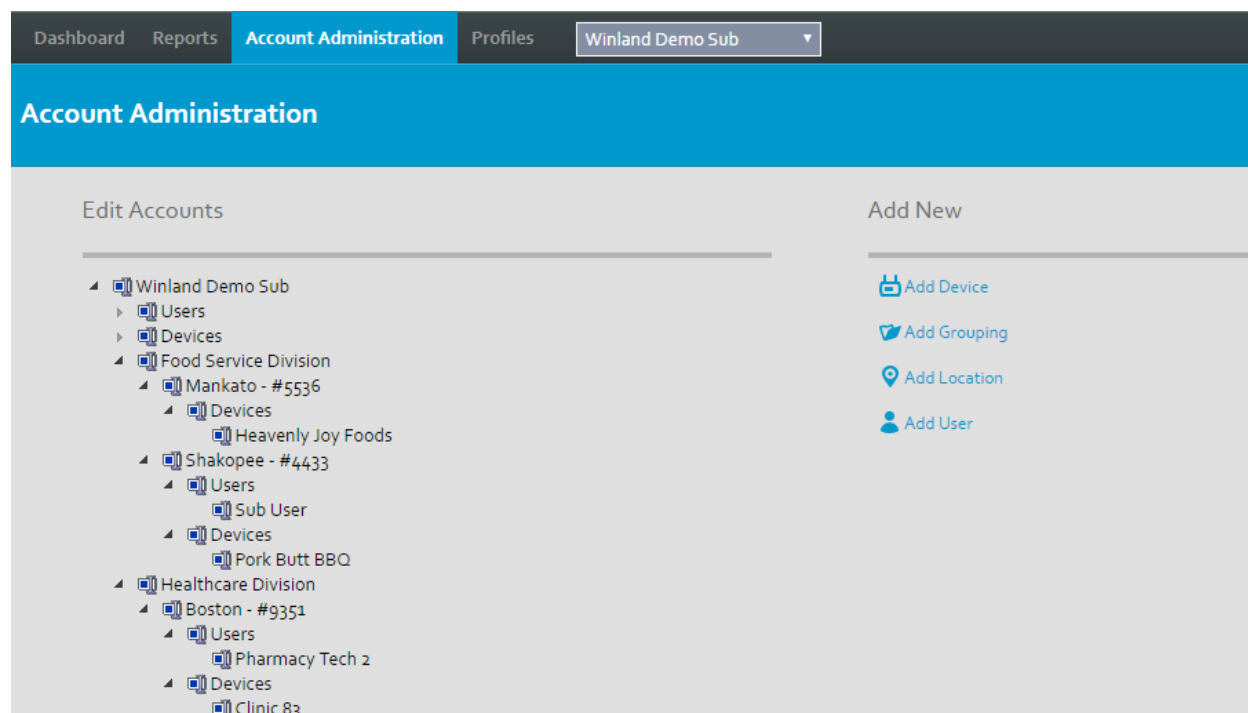

Figure 1-2. INSIGHT Account Tree

Reporting

The INSIGHT platform receives sensor data from an EA800-ip device every 30 seconds, as seen on the dashboard. The INSIGHT platform also receives sensor log and alert log data from the EA800-ip device and stores it in the INSIGHT database. It is from this database that INSIGHT creates sensor log reports and alert reports in the forms of listings and graphs. INSIGHT maintains device and sensor log data online for 18 months. Beyond 18 months up to 36 months, log data is available from INSIGHT support by request.

The EA800-ip console stores sensor log data in memory at the interval specified by the Collection Frequency parameter, up to 10,000 data points. This interval can be 5, 15, 30, 60, or 120 minutes. The EA800-ip regularly transmits log data to the INSIGHT database. For information about the Collection Frequency parameter, see "Adding a Device" on page 28.

You can generate a report for one or more sensors covering a time period of up to 31 days. Several types of reports are available on-demand in HTML, PDF, and CSV formats, depending on the report. You can also schedule reports to be created and distributed to selected users by E-mail. For more information about reports, see Chapter 5, "Managing Reports".

Figure 1-3. INSIGHT *Reports*

2   Getting Started

The process starts with a request for an INSIGHT account. You may be a reseller, or you may be a customer who wants to implement remote monitoring on a new or existing EA800-ip system. The EA800-ip console connects to the Internet through its Ethernet port, and your user name and password provide secure access to the INSIGHT host server. Add your EA800-ip devices, sensors, and user IDs to INSIGHT, and you are ready to monitor your environments anywhere you have access to the Internet.

Requesting an INSIGHT Account

The INSIGHT remote monitoring platform is available through a reseller network or directly from Winland Electronics. To request an INSIGHT account as reseller or a customer, send an email to insightsupport@winland.com or call 800.635.4269.

After receiving your request, Winland Electronics will send you an E-mail with an attached PDF form. If you are a reseller, the PDF form asks for company billing information, the name of the responsible party, and an E-mail address to serve as a user name.

If you are a customer, the PDF form asks for the company billing information plus the following:

- Name of the security company that installed your EA800-ip console (if applicable)
- EA800-ip system account information (if applicable)
- An E-mail address to serve as a user name

After receiving your completed PDF form, Winland Electronics or your reseller will send you an E-mail containing your user name, a temporary password, and the URL with which to access the INSIGHT host server.

Installing the EA800-ip System

The EA800-ip system supports up to 12 environmental sensors (4 wired and 8 wireless). With an Internet connection and the purchase of an INSIGHT subscription, you can monitor your environmental sensors remotely. For information about installing the EA800-ip system, see the *EnviroAlert EA800-ip Installation/Owner's Manual* and the *EnviroAlert EA800-ip Quick Start Guide*.

Establishing an Internet Connection

After installing the EA800-ip console and sensors, establish an Internet connection to the INSIGHT host server. If this is an existing installation providing local monitoring, begin with Step 1 to enable the Cloud client mode and establish an Internet connection. If this is a new EA800-ip installation, the Cloud client mode is enabled by default, and you can proceed to Step 3.

1. To enable the Cloud client mode, do the following at the EA800-ip console Main menu:

   a. Select **System↵**, **Configuration↵**, **Network↵**, **Client Mode↵**.

   b. In the Client Mode menu, select **CLOUD↵**.

2. If your network uses dynamic host configuration protocol (DHCP) to assign the IP address, select **ENABLED↵** in the DHCP menu. Otherwise, to specify a static IP address, select **DISABLED↵**, and then do the following:

   a. Enter the IP address in the Local Address screen, and then press ↵.

   b. Enter the subnet mask in the Subnet screen, and then press ↵.

   c. Enter the gateway address in the Gateway Address screen, and then press ↵.

   d. Enter the domain name server (DNS) address in the DNS Address screen, and then press ↵.

3. Connect a 10/100BASE-TX Ethernet cable from the EA800-ip Ethernet port to an Internet switch, router, or bridge.

4. Confirm a successful connection to the host server. On the EA800-ip console Main Menu, select **System↵**, **Configuration↵**, **Network↵**, **Diagnostics↵**. The Diagnostics screen should show a valid IP address in the IP-^ field, as shown:

```
          DIAGNOSTICS
 Time:  08/20 08:38:37

 IP-v: 192.168.001.024

 IP-^: 023.096.008.019

 Sync-^:  08/20 08:38:00

 Xfer-^:  08/20 08:37:00

 Xfer: 0X upd:pts
```

If you are unable to establish an Internet connection, contact INSIGHT support at insightsupport@winland.com or call 800.635.4269.

Logging in to the INSIGHT Platform

To log in to the INSIGHT platform:

1. Open a Web browser using the URL you received in your account confirmation E-mail or; go to www.winlandinsight.com. The INSIGHT platform supports the following Web browsers:

    ■   Microsoft® Internet Explorer® 11 or later

    ■   Google Chrome®

    ■   Firefox®

2. In the INSIGHT login window, type your user name, temporary password, and then click **Log In**.

    > **NOTE**
    >
    > The INSIGHT platform operates over the Internet from a host server. You can check the status of the INSIGHT platform before logging in by clicking **Insight Status** in the login window.

3. After the first login with your temporary password, the system prompts you to change your password, and to provide a secret question. In the Change Password window, copy and paste the temporary password, and then click **CHANGE PASSWORD**:

    ■   Current password

    ■   New password (minimum of eight alphanumeric characters, uppercase or lowercase, and at least one special character). Validate the new password by typing it a second time.

    ■   Security question and the answer

4. Read the End User License Agreement, check the **I accept the terms of this license** check box, and then click **ACCEPT**.

The INSIGHT platform opens with the dashboard, as shown in Figure 2-1. Common to every application page are the ① menu tabs, the ② customer account selector, the ③ current customer account, User ID, and **Log Out** button, and the ④ **Help** button. The

■   The menu tabs provide access to the application tasks.

■   The customer account selector is available only to users with Customer Admin permission (typically, a reseller) to select from multiple customer accounts.

■   The **Log Out** button closes the platform.

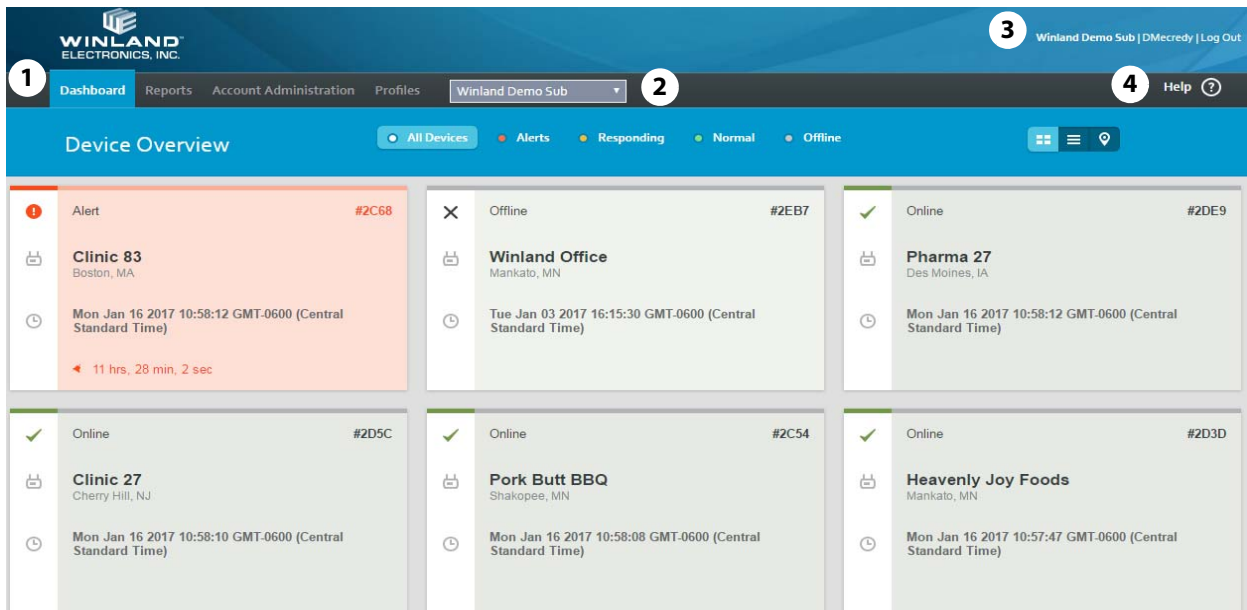■   The **Help** button opens online help for each tab page.

Figure 2-1. INSIGHT *User Interface*

Configuring INSIGHT

 If you requested INSIGHT as a *reseller*, the user name you received has *Customer Admin* permission. Customer Admin permission means that you have authority to add customer accounts (see "Managing Customer Accounts" on page 22).

If you requested INSIGHT as a *customer*, the user name you received has *Admin* permission. Admin permission means you have authority to add users and configure your monitoring environment.

With your environment monitoring plan in hand, do the following to configure a basic monitoring environment:

1. Add your devices and sensors, selecting the corresponding response profile for each. See "Adding a Device" on page 28 and "Adding a Wired Sensor" on page 30.

2. Add one or more notification profiles to cover your users, selecting from the devices and sensors you added previously. ("Adding a Notification Profile" on page 42).

3. Add a User ID for each of your users, selecting the corresponding notification profiles for each. See "Adding a User ID" on page 25.

At some point, you may also want to do the following to assign alert response procedures, control user/device access, and organize the account tree:

■ Add one or more response profiles to cover your EA800-ip devices and sensors. See "Adding a Response Profile" on page 44. Remember to update your device and sensor configurations to include a response profile.

■ Add locations, and then populate them with users and devices. See "Adding a Location" on page 33 and "Working with Locations" on page 20.

■ Add groupings, and then populate them with locations. See "Adding a Grouping" on page 36 and "Working with Groupings" on page 21.

3 Monitoring Devices

The dashboard is your window to your monitored environments. You can customize the dashboard to show devices based on device status, sensor status, or specific keywords. Using the dashboard, you can acknowledge a sensor reading, and document your response to an alert with a plan of action.

Using the Dashboard

To view the dashboard, click the **Dashboard** tab, as shown in Figure 3-1. In this example, there are six tiles ①, each representing a different EA800-ip device. Opposite the Device Overview banner, there are several filter radio buttons ② and three dashboard view buttons ③ from which to choose.
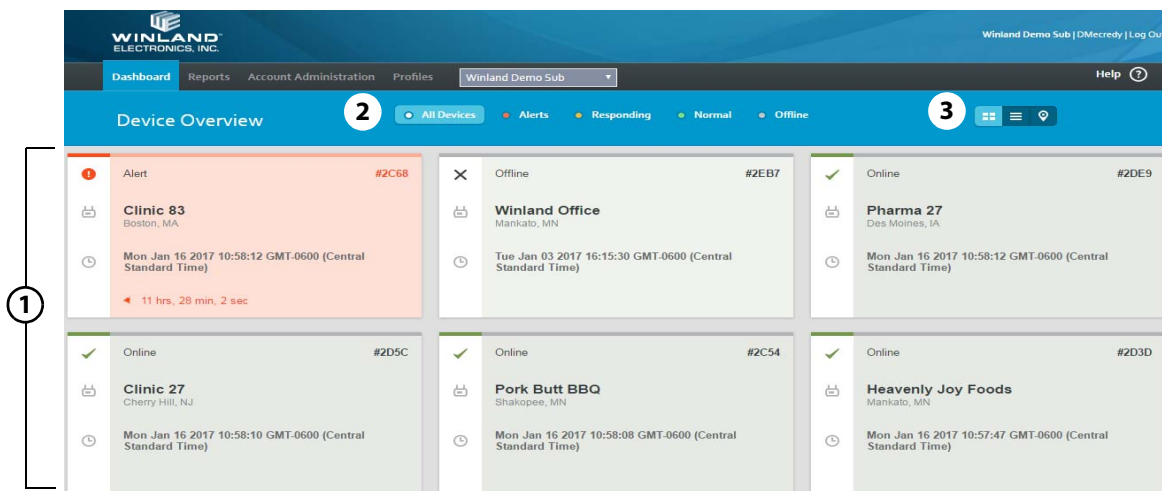
Figure 3-1. Dashboard—Device Overview
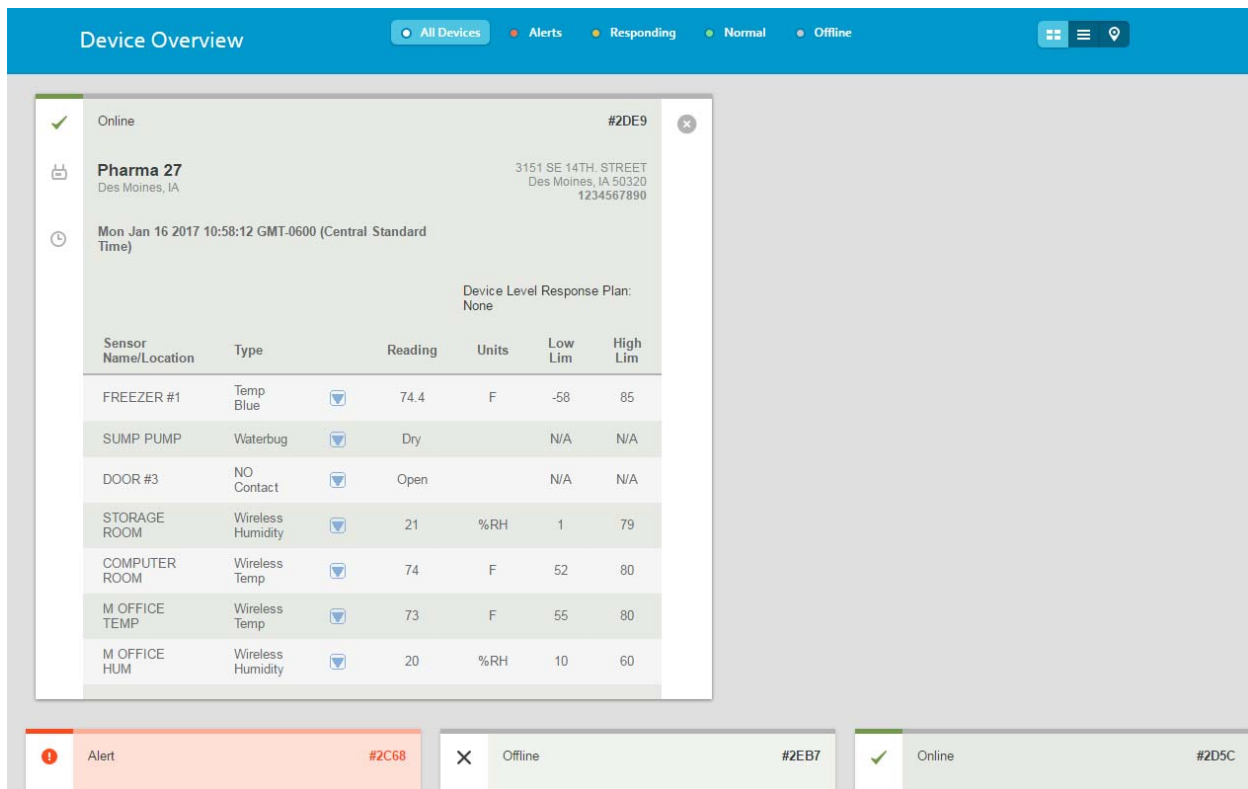
Regardless of the filter or dashboard view, each view includes the following:

■ Device/sensor status:

❑ Green indicates Online; the device is operating normally.

❑ Red indicates Alert; one or more sensors have exceeded a threshold.

❑ Yellow indicates Responding; a response to an alert is in progress.

❑ Gray indicates Offline; the device is not communicating with the host.

■ User-defined name for the device

■ EA800-ip equipment serial number (ESN)

■ City and state/province where the device is located, based on address information from the customer account or from the location in which the device is a member.

■ Date/time that sensor data was last received from the device

■ Elapsed time while in an alert condition[1]

Dashboard Views

There are three dashboard views: Device Overview, Device List View, and Map View.

Choose the dashboard view using the view buttons ⊞ ☰ ◉ . Click ⊞ (Device Overview) to display each device as a tile. Click on a tile to display the sensor information for that device, as shown in Figure 3-2.

Figure 3-2. Dashboard—Device Overview, Sensor Detail

---

[1] Applies only when an alert condition exists

Click ☰ (Device List View) to present the devices in a table. Click on a row in the table to reveal the sensor information for that device, as shown in Figure 3-3. For accounts with many devices, the Device List View makes reading easier with:

■ First, Previous, Next, and Last paging (lower right)

■ Devices per page (Show entries, upper left)

■ Search function to filter device entries by keyword (upper right)

■ Sorting by sensor name, sensor type, sensor reading, units of measure, and limits by clicking the corresponding column labels.

Device List View

All Devices · Alerts · Responding · Normal · Offline

Show entries 10 ▼   Search:

STATUS	DEVICE NAME	ESN	LOCATION	LAST READING	
Online	Pharma 27	2DE9	Des Moines - #26101	Mon Jan 16 2017 10:58:12 GMT-0600 (Central Standard Time)	⊖

✓ Online   3151 SE 14TH. STREET Des Moines, IA 50320 | 1234567890

Sensor Name/Location	Type		Reading	Units	Low Lim	High Lim
FREEZER #1	Temp Blue	▼	74.5	F	-58	85
SUMP PUMP	Waterbug	▼	Dry		N/A	N/A
DOOR #3	NO Contact	▼	Open		N/A	N/A
STORAGE ROOM	Wireless Humidity	▼	21	%RH	1	79
COMPUTER ROOM	Wireless Temp	▼	74	F	52	80
M OFFICE TEMP	Wireless Temp	▼	74	F	55	80
M OFFICE HUM	Wireless Humidity	▼	20	%RH	10	60

No response plan is associated with any sensors on this device.

Alert	Clinic 83	2C68	Boston - #9351	Mon Jan 16 2017 10:58:12 GMT-0600 (Central Standard Time)	⊕
Online	Clinic 27	2D5C	New Jersey - #79811	Mon Jan 16 2017 10:58:10 GMT-0600 (Central Standard Time)	⊕
Offline	Winland Office	2EB7	Winland Demo Sub	Tue Jan 03 2017 16:15:30 GMT-0600 (Central Standard Time)	⊕
Online	Pork Butt BBQ	2C54	Shakopee - #4433	Mon Jan 16 2017 10:58:08 GMT-0600 (Central Standard Time)	⊕

Figure 3-3. Dashboard—Device List View

Click ▣ (Map View) to display a map with a marker indicating the geographic position and status of each device (Figure 3-4). Initially, the marker position on the map is determined by the billing information that you provided when you requested an INSIGHT account. However, marker positions can change as you create and modify locations. For more information about locations, see "Managing Locations" on page 33.

Click-and-drag to move the map up, down, left, and right. Use the other navigation tools to change your view of the map:

■ ▦ Road ▾—Mouse over the pull-down menu to view a standard road map, aerial view, or street-side view.

■ ◉—Locate Me centers the map and zooms in the approximate location based on the gateway IP address.

■ ⊕—Zoom In

■ ⊖—Zoom Out
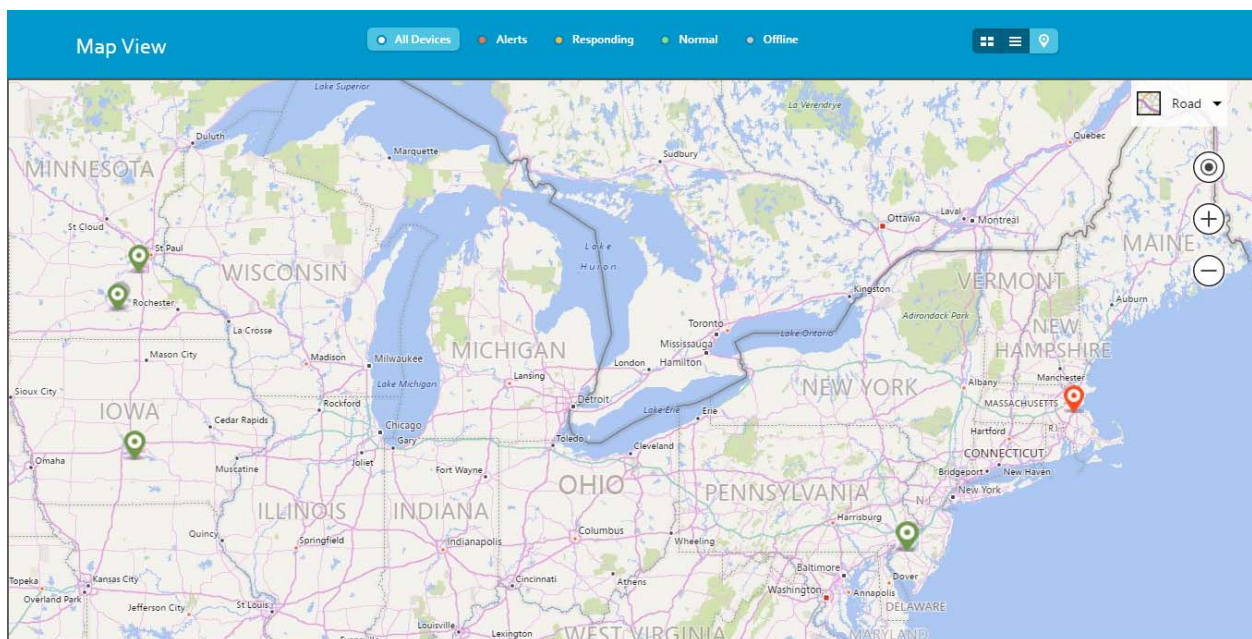
Figure 3-4. Dashboard—Map View

To show sensor information for a device, click on the corresponding marker. For example, click on the marker in Iowa to show sensors for Pharma 27 (Figure 3-4). If there is more than one device at a location, click the **<** and **>** tabs to page through the devices.
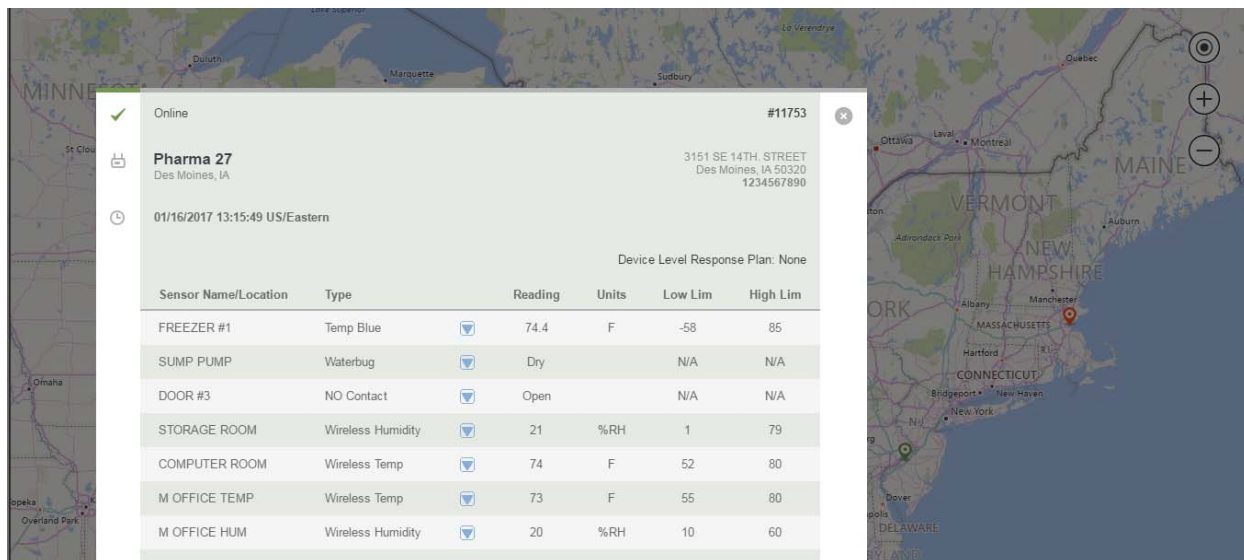
Figure 3-5. Device Detail from Map View

Dashboard Filters
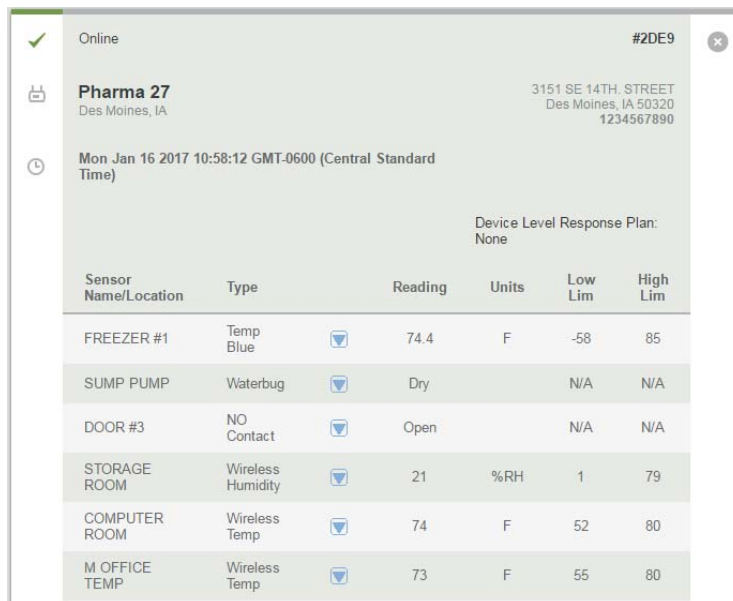
For all dashboard views, the dashboard filter buttons determine which devices to show based on the device operational state or sensor state. Table 3-1 describes the dashboard filters.

Table 3-1. Dashboard Filters

Dashboard Filter	Description
All Devices	Displays all EA800-ip devices regardless of operational or sensor state.
Alerts (Red)	Displays EA800-ip devices that have one or more sensors that have an alert condition.
Responding (Yellow)	Displays EA800-ip devices that have one or more alerts for which a response is in progress.
Normal (Green)	Displays EA800-ip devices that are communicating with the INSIGHT host server.
Offline (Gray)	Displays EA800-ip devices that are not communicating with the INSIGHT host server.

Displaying Sensor Information

Depending on your dashboard view, click on a tile or table entry to show sensor information. Figure 3-6 is a tile showing the sensor list for the Pharma 27 device. To minimize the tile, click ⊗.

Sensor Name/Location	Type		Reading	Units	Low Lim	High Lim
FREEZER #1	Temp Blue	▼	74.4	F	-58	85
SUMP PUMP	Waterbug	▼	Dry		N/A	N/A
DOOR #3	NO Contact	▼	Open		N/A	N/A
STORAGE ROOM	Wireless Humidity	▼	21	%RH	1	79
COMPUTER ROOM	Wireless Temp	▼	74	F	52	80
M OFFICE TEMP	Wireless Temp	▼	73	F	55	80

Figure 3-6. Device Sensor List

The sensor list shows the following information for each sensor:

■ Sensor Name/Location—Name that was assigned when the sensor was added to the EA800-ip device.

■ Type—Wired or wireless sensor type including temperature, humidity, water, and contact (normally closed and normally open)

■ ▼ button that acknowledges a sensor value or responds to an alert. The EA800-ip device issues an alert when a sensor reaches its low/high limit, or when a contact sensor reads other than its normal state. For more information about alerts, see "Responding to an Alert" on page 16.

■ Reading—Numerical or boolean value reported by the sensor

■ Units—Unit of measure that applies to the Reading, Low Lim, and High Lim values, such as Celsius (C), Fahrenheit (F), and relative humidity percentage (RH%)

■ Low Lim—Sensor reading at or below which the EA800-ip device issues an alert

■ High Lim—Sensor reading at or above which the EA800-ip device issues an alert

In addition to the standard device information, the device tile also shows the Device Level Response Plan (also known as the *device response profile*). The device response profile is a sequence of actions that have been prescribed for an alert condition that occurs on any sensor connected to the device. If there is a response plan link present, you can click it to review or edit the device response profile. You can specify a response profile by modifying an existing device.
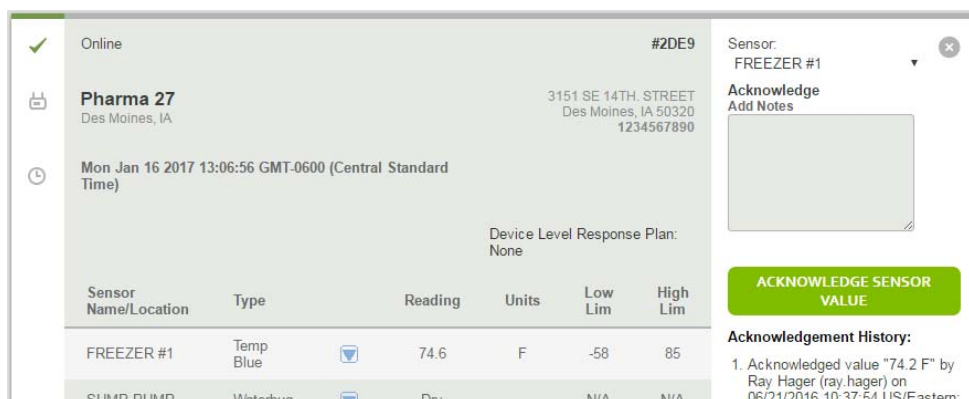
■ For more information about adding and modifying response profiles, see "Response Profiles" on page 44.

■ For information about specifying a response profile on an existing device, see "Modifying a Device" on page 29.

Acknowledging Sensor Readings

Some industry and government regulations require that a human being periodically validate normal sensor readings. This validation is called an *acknowledgment*. The INSIGHT platform records and maintains acknowledgment data for compliance purposes.

To acknowledge a sensor reading:

1. In the dashboard device sensor list, click ⬇ on the sensor, and then select **Acknowledge**.

2. In the Acknowledgment window (Figure 3-7), review the Acknowledgment History for any helpful information.

3. In the Add Notes field, type some appropriate notes, and then click **ACKNOWLEDGE SENSOR VALUE**. In addition to your notes, your entry in the Acknowledgment History will include the acknowledged value, your name and user name, and a date/time stamp.

4. To select another sensor, click the Sensor pull-down menu. To minimize the Acknowledgment window, click ⊗.

Figure 3-7. Sensor Reading Acknowledgment

Responding to an Alert

When a sensor reads a value that exceeds its assigned thresholds, the EA800-ip system issues an alert. Depending on the dashboard view, the device tile, table entry, or map marker will be red. Figure 3-8 shows a device tile with an alert condition.
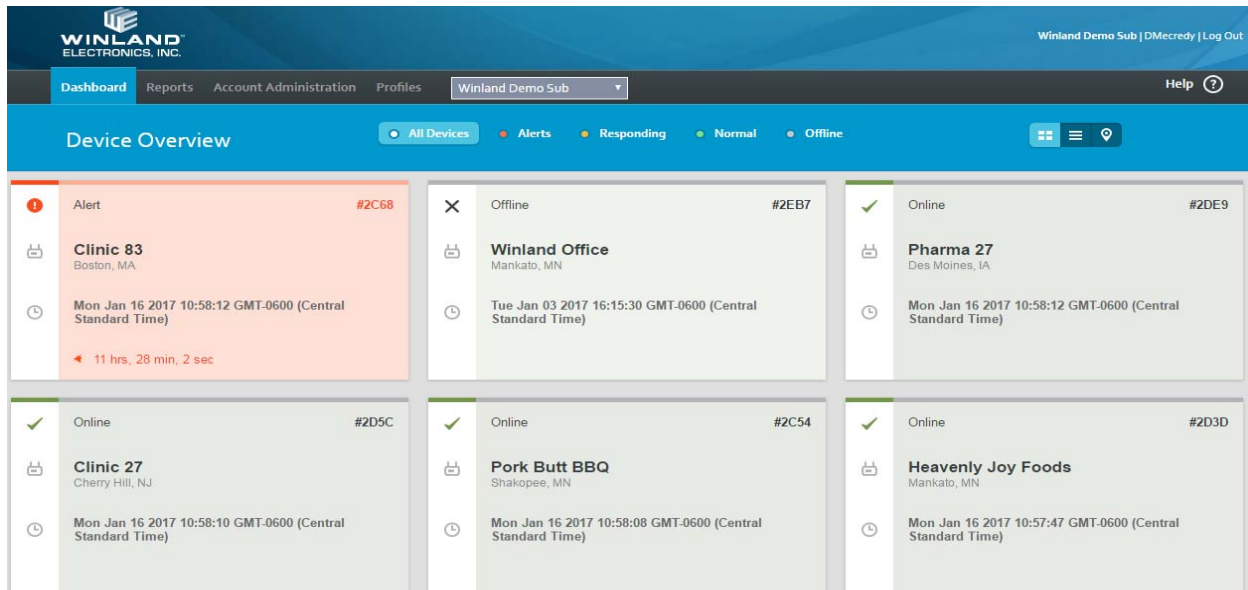
Figure 3-8. Dashboard with an Alert

Responding to an alert means performing a sequence of actions according to the response profile that is defined for the sensor. A response profile is a named series of actions that you create based on your SOP. For information about creating a response profile, see "Adding a Response Profile" on page 44.
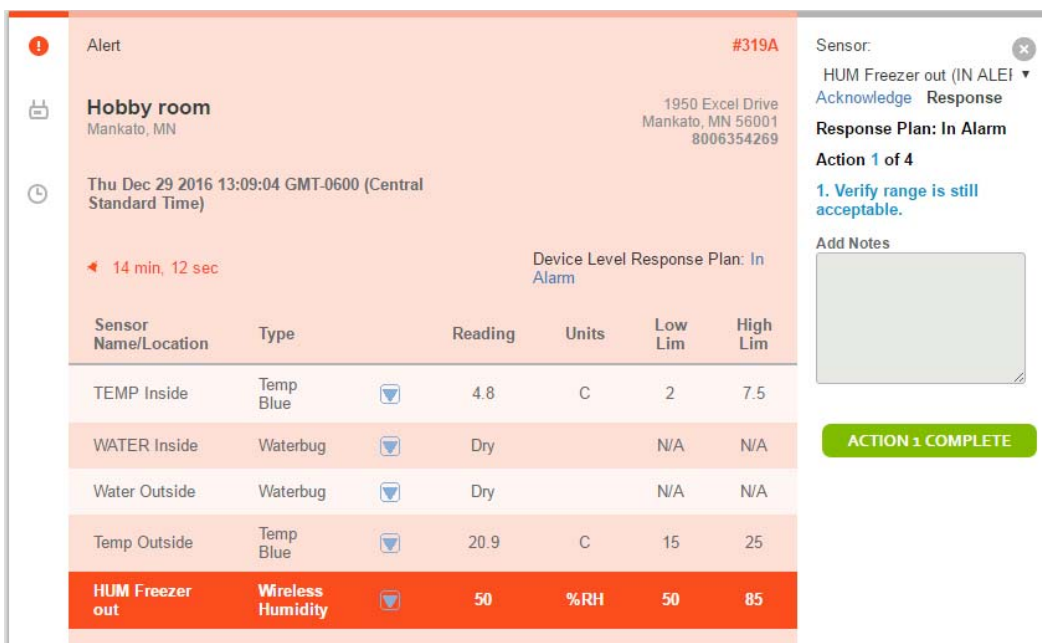
To be implemented, a response profile must assigned to a device or a sensor:

■   A response profile assigned to a device applies to all sensors connected to that device. For information about specifying a response profile for a device, see "Modifying a Device" on page 29.

■   A response profile assigned to a sensor applies only to that sensor and takes precedence over the response profile specified for the device. For information about specifying a response profile for a sensor, see "Adding a Wired Sensor" on page 30 and "Modifying Wired and Wireless Sensors" on page 32.

To respond to an alert:

1. Depending on your dashboard view, click the device tile, table entry, or map marker.

2. In the Response window (Figure 3-9), review the Action History for any helpful information.

3. If this sensor or its device has a response profile, you will be prompted to perform the first action. After performing the action and typing some appropriate notes, click **ACTION 1 COMPLETE**. Repeat this process for each action in the response profile.

4. To select another sensor, click the Sensor pull-down menu. To close the Response window, click ⊗.

While a response is in progress, the device/sensor will be yellow on the dashboard.

Figure 3-9. Alert Response

4 **Account Administration**

Account administration begins with the account tree, from which you can manage customer accounts (resellers only), user IDs, devices and their connected sensors. This chapter also describes the use of locations and groupings to control user access to devices and to organize the account tree.

Using the Account Tree

The account tree shows the users, devices, locations, and groupings in a customer account. INSIGHT uses the concept of a location to limit user access to specific users and devices. A location is a named set of users and devices associated with a street address. You can think of the customer account as a type of location with extended access over all users and devices in the account tree. For more information about moving users and devices into locations, see "Working with Locations" on page 20. For information about groupings, see "Working with Groupings" on page 21.

A user's customer account/location membership, combined with the User Permission Level, determines what the user can see and do in the account tree. Membership in the customer account gives a user access to all users, devices, locations, and groupings in the account tree. Membership in a location gives a user access to all users and devices in the same location. The User Permission Levels, listed in Table 4-1, determine what a user can do in the customer account or location of which it is a member.

Table 4-1. User Permission Levels

Permission Level	Description
Customer Admin [a]	■ View and add customer accounts ■ View, add, modify, and delete users, devices, locations, and groupings ■ Move users and devices between locations ■ Move locations between groupings
Admin	■ View, add, modify, and delete users, devices, locations, and groupings ■ Move users and devices between locations ■ Move locations between groupings
User	■ View users, devices, locations, groupings

[a] Applies across customer accounts

18

In Figure 4-1, User_1 and User_2 are members of the customer account (Customer_Acme) and have access to all users, devices, and locations. User_3 and User_4 are members of Location_1 and have access to each other and Device_4. To understand the effect of user permissions on the account tree, assume the following:

■ User_1 has Admin permission. Therefore, User_2 can view all elements in the account tree, and make changes throughout.

■ User_2 has User permission. Therefore, User_2 can view all elements in the account tree, but cannot make changes.

■ User_3 has Admin permission. Therefore, User_3 can view elements only in Location_1, and make changes only in Location_1.

■ User_4 has User permission. Therefore, User_4 can view elements only within Location_1.

```
◢  🖥 Customer_Acme
    ◢  🖥 Users
          🖥 User_1
          🖥 User_2
    ◢  🖥 Devices
          🖥 Device_1
          🖥 Device_2
          🖥 Device_3
    ◢  🖥 Location_1
        ◢  🖥 Users
              🖥 User_3
              🖥 User_4
        ◢  🖥 Devices
              🖥 Device_4
```
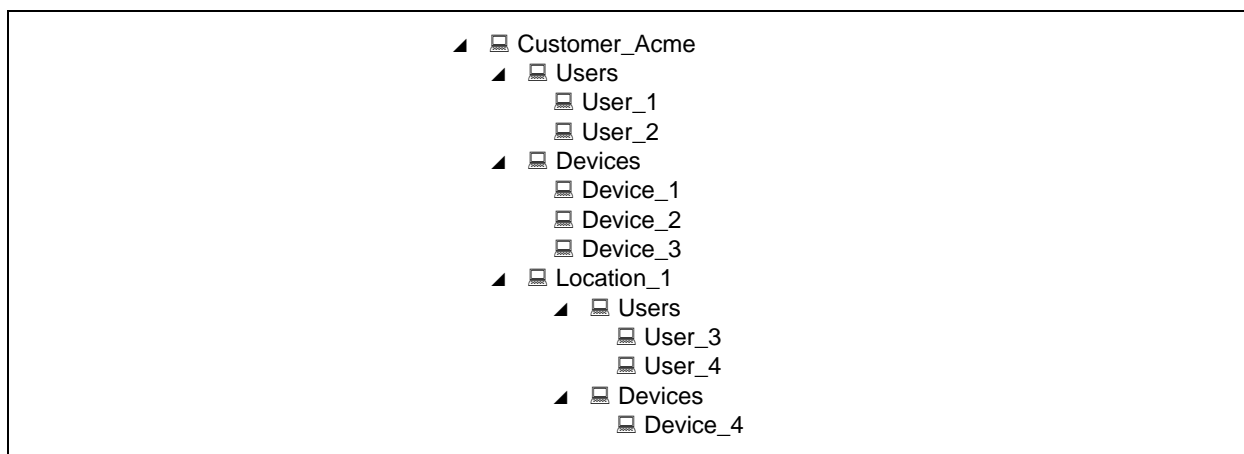
Figure 4-1. User Access, User Permission, and the Account Tree

For information about assigning a User Permission Level to a User ID, see "Adding a User ID" on page 25.

Working with Locations

To move a user or a device to a location:

1. In the account tree, drag-and-drop the user or device from one location to another. Users and devices can be moved between locations or between the customer account and a location in either direction.

2. When prompted to confirm your intention to alter the hierarchy, click **YES, I'M SURE**; otherwise, click **CANCEL**.

3. In the Edit User or Edit Device section, make any necessary changes to the user ID or device parameters, and then click **SAVE**. Otherwise, if there are no changes, click **CANCEL**.

4. Inspect the account tree to confirm the placement of the user or device in the location.

In Figure 4-2, User_3 and Device_3 move from Customer_Acme to Location_1. After the move, User_3 has access only to Device_3; User_1 and User_2 have access to all users and devices.
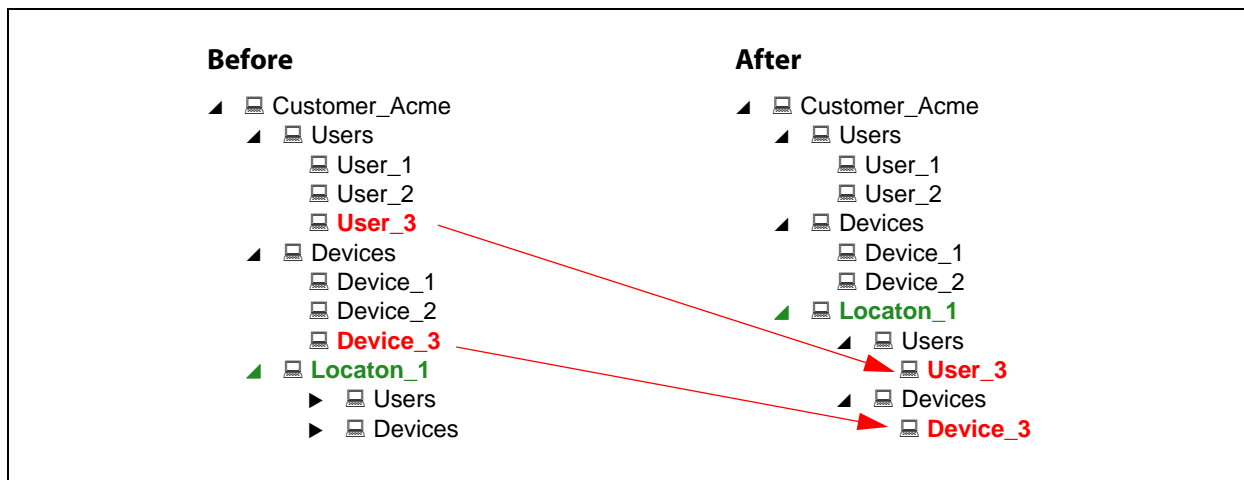
Figure 4-2. Moving Devices and Users to a Location

For information about adding, modifying, and deleting a location, see "Managing Locations" on page 33.

Working with Groupings

A grouping is a named set of one or more locations that is used to organize the account tree. Groupings do not affect user access to devices; users have access only to devices in the same location whether the location is inside a grouping or not. For information about adding, modifying, and deleting groupings, see "Managing Groupings" on page 35.

The following example adds two groupings, and then moves Location_1 and Location_2 from Customer_Acme into Division_I_Grouping; Location_3 and Location_4 into Division_II_Grouping.
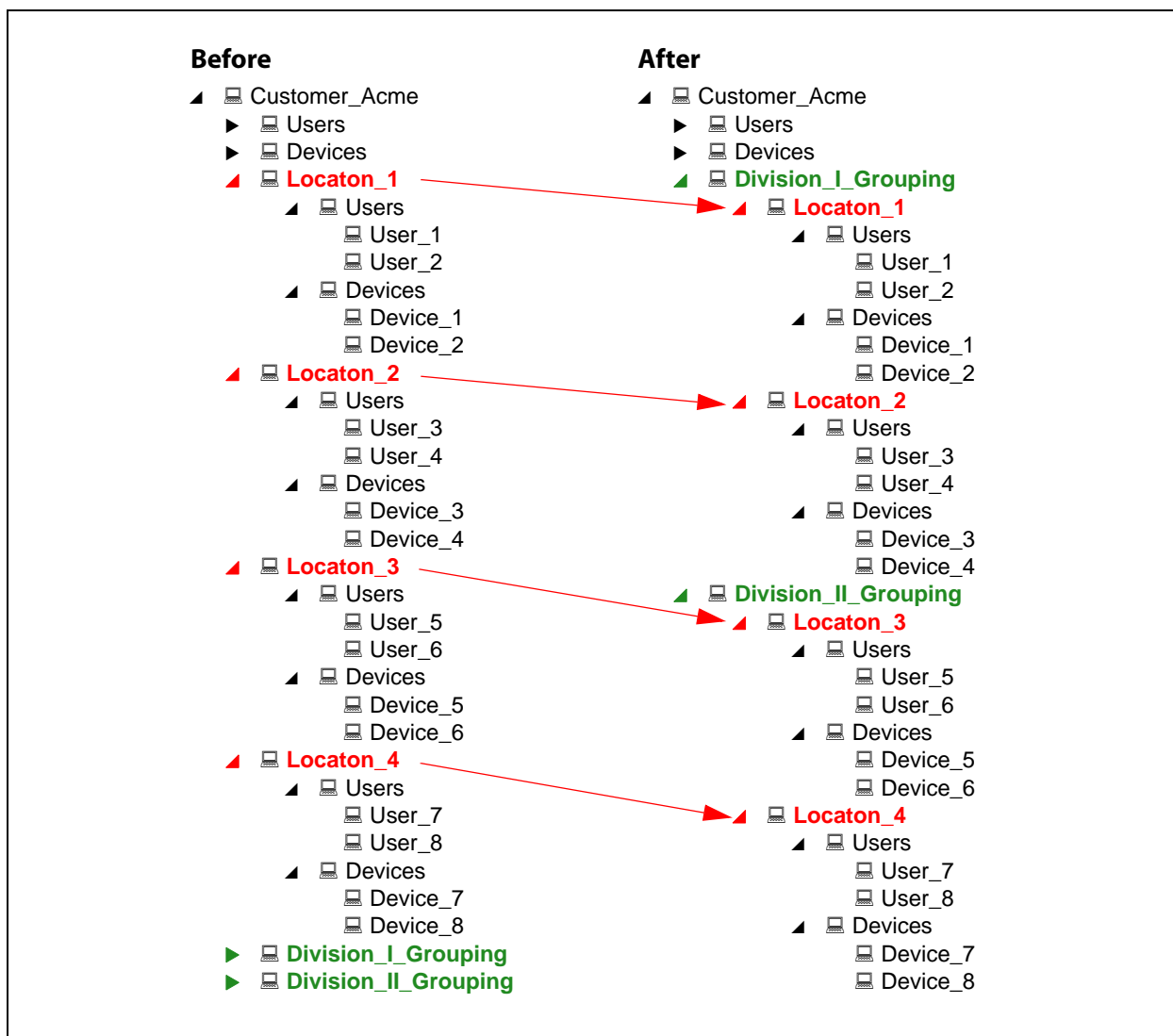
Figure 4-3. Moving Locations to a Grouping

To move a location:

1. Drag-and-drop a location into to a grouping. Locations can be moved between groupings or between the customer account and a grouping in either direction.

2. When prompted to confirm your intention to alter the hierarchy, click **YES, I'M SURE**; otherwise, click **CANCEL**.

3. In the Edit Location section, make changes to the location parameters, and then click **SAVE**. Otherwise, if there are no changes, click **CANCEL**.

4. Inspect the account tree to confirm the placement of the location in the grouping.

Managing Customer Accounts

> **NOTE**
>
> The functions described in this section are for resellers only. If you are not a reseller and find that you have the ability to create and delete customer accounts in INSIGHT, contact INSIGHT support at insightsupport@winland.com or call 800.635.4269.

 As a reseller, your user name has Customer Admin permission, which makes you the administrator of your account with the ability to add customer accounts. You can add User IDs with Customer Admin permission to your account, who can also manage the customer accounts. For example, Figure 4-4 shows a reseller's account tree (Winland Demo Main) and its customer's account tree (Winland Demo Sub). All users in the reseller's account should have Customer Admin permission and can manage the customer's account, though none of the users in reseller's account are found in the customer's account.

Reseller Account	Customer Account
◢ 🖥 Winland Demo Main	◢ 🖥 Winland Demo Sub
◢ 🖥 Users	◢ 🖥 Users
🖥 Gil Foresman	🖥 Adam Feinberg
🖥 Hal Geisen	🖥 Adam Sibarro
🖥 Lee Trillis	🖥 B Lawrence
🖥 Mike Hoffman	🖥 Brian Geggie
🖥 Ronda Marx	🖥 Chris Lanier
	◢ 🖥 Devices
	🖥 Winland Office
	◢ 🖥 Food Service Division
	◢ 🖥 Mankato - #5536
	◢ 🖥 Users
	🖥 Sub User
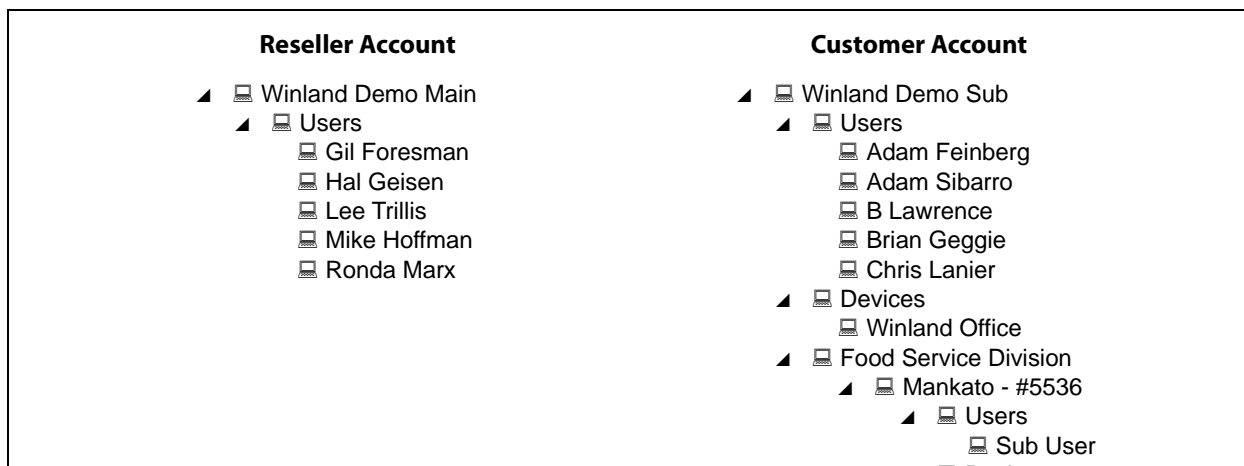
Figure 4-4. Reseller and Customer Accounts

To view the available customer accounts, click the **Account Administration** tab to open the Account Administration window, as shown in Figure 4-5.
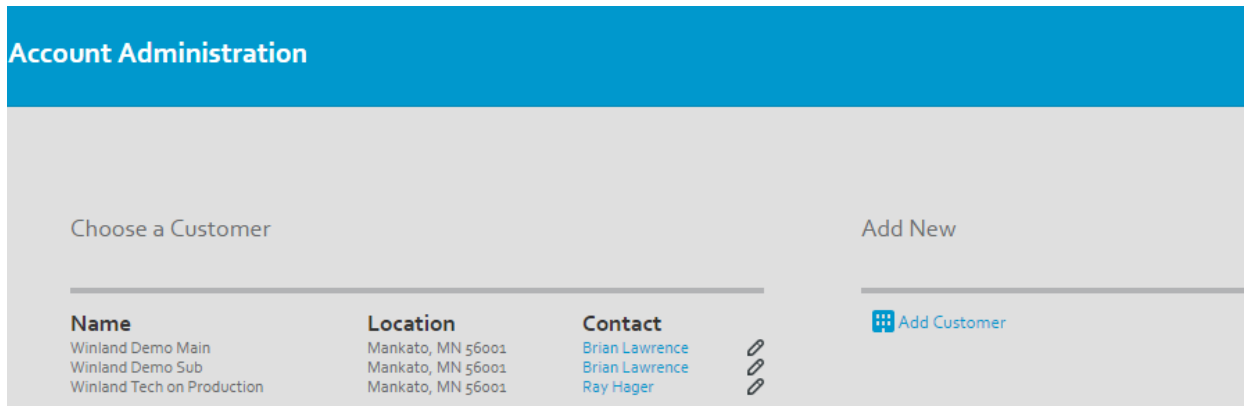
Figure 4-5. Account Administration—Customer Accounts

- To view customer details, click ✐ opposite the entry in the Choose a Customer section.

- To add a customer account, click ⊞ Add Customer in the Add New section. For more information about adding a customer account, see "Adding a Customer Account" on page 24.

- To manage User IDs, devices, and sensors for a specific customer, click the customer name in the Choose a Customer section. From the account tree in the Edit Accounts section (Figure 4-6), you can manage users, devices, locations, and groupings. In the Add New section, you can add new devices, groupings, locations, and users.
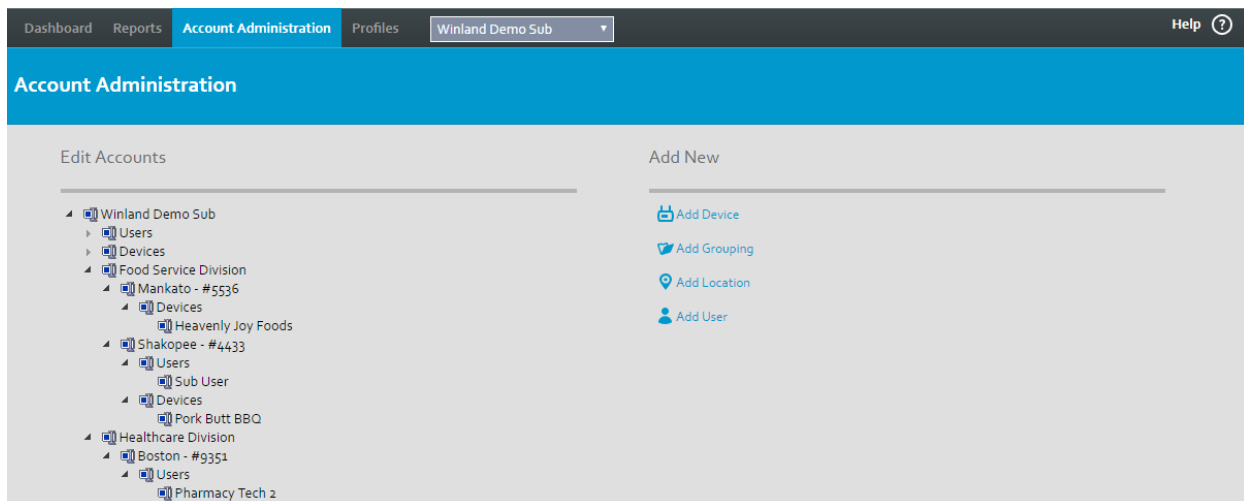
Figure 4-6. Account Administration—Edit Accounts

Adding a Customer Account

You must have Customer Admin permission to add a customer account.

To add a customer account:

1. Click the **Account Administration** tab.

2. In the Add New section, click Add Customer.

3. In the Add Customer section, type values for the following fields:

   - Customer Name—Name of the customer's company

   - Primary Contact—Name of the individual who will administrate the EA800-ip device

   - Primary Phone—Telephone number of the primary contact

   - Primary E-mail—E-mail address of the primary contact

   - Company address, country, city, state/province, and zip code

   - Description—Optional details about the customer account

4. Click **SAVE** to save the customer account information; otherwise, click **CANCEL**.

Modifying or Deleting a Customer Account

You cannot modify or delete a customer account; neither can you merge two existing customer accounts. To create organizational divisions within a customer account, use locations and groupings. If you need to make changes to your customer account, contact INSIGHT support at insightsupport@winland.com or call 800.635.4269.

Managing Users IDs

User IDs determine who can log in to INSIGHT and what users can do in the customer account or location of which they are a member. For information about the factors that determine user access to elements in the account tree, see "Using the Account Tree" on page 18. This section describes how to add, modify, and delete a user ID.

Adding a User ID

When you add a User ID, an E-mail is sent to the primary E-mail address indicating the new user name and temporary password. You must have Customer Admin or Admin permission to add a user ID.

To add a user ID:

1. Click the **Account Administration** tab.

   ■ If you are a reseller, in the Choose a Customer section, click the customer account name.

   ■ If you are not a reseller, proceed to Step 2.

2. In the Add New section, click Add User.

3. In the Add User section, type values for the following fields:

   ■ Username—User name consisting of upper and lowercase alphanumeric characters, period (.), underscore (_), and @. The user name must be unique across the entire $\mathrm{INSIGHT}$ database; therefore, an E-mail address is recommended. Choose this name wisely; it cannot be changed except to delete the User ID and add a new one.

   ■ First Name, Last Name—Name of the person who owns the user ID.

   ■ Primary Email—E-mail address that receives the user name and temporary password. This E-Mail address also receives alert notifications.

   ■ Secondary Email—An alternate E-Mail address to receive alert notifications. This address can also be the number for a phone that can receive text messages. To find the E-Mail format for your wireless carrier, click here in the sentence:

   "Click here for common text message email formats."

   ■ Notification Profile—Click the pull-down menu, and then select from the list of notification profiles. A notification profile defines the sensors and conditions for which the user is to receive alert notifications. For more information about notification profiles, see "Notification Profiles" on page 42.

   > **NOTE**
   >
   > If you do not specify a notification profile in the user ID, the user will not receive alert notifications.

■ User Permission Level—Choose a permission level. For information about user access and user permission levels, see "Using the Account Tree" on page 18.

❑ Customer Admin (resellers only)—View/add/modify customer accounts, user IDs, devices, locations, and groups for multiple customers

❑ Admin—View/add/modify user IDs, devices, locations, and groups for a single customer

❑ User— View users, devices, locations, and groups for a single customer

■ Account Locked—Locks (checked) or unlocks (unchecked) the user ID. If the user ID is locked, the user cannot log in to INSIGHT.

■ Address, Country, City, State/Province, Zip/Postal Code

■ Primary Phone—Telephone number of individual who owns the user ID

4. Click **SAVE** to save the user ID information; otherwise, click **CANCEL**.

Modifying a User ID

To modify a user ID:

1. Click the **Account Administration** tab.

■ If you are a reseller, in the Choose a Customer section, click the customer account name.

■ If you are not a reseller, proceed to Step 2.

2. In the Edit Accounts section, click a user in the account tree.

3. In the Edit User section, make the necessary changes. The user name cannot be changed. For information about the user ID parameters, see "Adding a User ID" on page 25.

4. Click **SAVE** to save the user ID information; otherwise, click **CANCEL**.

Deleting a User ID

Deleting a user ID removes the User ID from the $\mathrm{INSIGHT}$ database. $\mathrm{INSIGHT}$ will no longer accept a login with the associated user name. You may want to consider the following alternatives:

■ To temporarily block access to $\mathrm{INSIGHT}$ while retaining the user ID, you can lock the User ID, as described in .

■ To remove a user ID from a location, see .

To delete a user ID:

1. Click the **Account Administration** tab.

   ■ If you are a reseller, in the Choose a Customer section, click the customer account name.

   ■ If you are not a reseller, proceed to Step 2.

2. In the Edit Accounts section, click a user in the account tree.

3. In the Edit User section, click **Delete User**.

4. In the User Delete Confirmation window, click **YES, I'M SURE** to confirm the deletion; otherwise, click **CANCEL**.

Managing Devices

A device is a EA800-ip console. Adding a device requires three pieces of information: a name, the serial number, and the device key. Having added the device to $\mathrm{INSIGHT}$, you can now remotely manage device parameters, such as the console password, date and time, buzzer, and several others. The following sections describe how to add, modify, and delete a device.

Adding a Device

Before you can add a device to $\mathrm{INSIGHT}$, the EA800-ip console must be installed, connected to the Internet, and communicating with the host server. You will also need the device serial number and device key, which can be found in two places:

- On the Ethernet port mounted on the EA800-ip circuit board

- On the EA800-ip console Main Menu: select **About EA800**↵, select **ENET** (F2), and then find SN and Key in the display.

To add a device:

1. Click the **Account Administration** tab.

   - If you are a reseller, in the Choose a Customer section, click the customer account name.

   - If you are not a reseller, proceed to Step 2.

2. In the Edit Accounts section, click .

3. In the Add Device section, type values for the following fields:

   - Device Name—Descriptive name by which to identify the EA800-ip device in $\mathrm{INSIGHT}$.

     NOTE

     Choose this name wisely; it cannot be changed except to delete the device and add a new device with the same name.

   - Serial Number—Device serial number

   - Key—Device key

4. Click **SAVE** to save the device; otherwise, click **CANCEL**.

Modifying a Device

To modify EA800-ip device parameters:

1. Click the **Account Administration** tab.

   ■ If you are a reseller, in the Choose a Customer section, click the customer account name.

   ■ If you are not a reseller, proceed to Step 2.

2. In the Edit Accounts section, click a device in the account tree.

3. In the Edit Device section, make the necessary changes to the following parameters:

   ■ Password—Four-digit password used to unlock the EA800-ip console.

   ■ Date Format—Date format: **MM/DD/YYYY** or **DD/MM/YYYY**

   ■ Time Format—Time format: **12 hour or 24 hour**

   ■ Device Response Profile—Action plan to perform in response to an alert on any sensor connected to this device. For more information about response profiles, see "Response Profiles" on page 44.

   ■ Time Zone—Time zone.

   ■ Offline Alert Time—Time period that the EA800-ip device can be without communication with the host server before issuing an alert. Select **10 Minutes, 30 Minutes, 1Hour** or **2 Hours**. Select **Disabled** to send no alerts regarding offline status.

   ■ Alert Reminder Interval—Time period that INSIGHT waits to send a reminder alert E-mail after the first alert E-mail has been sent to users in the notification profile. Select **10 Minutes, 30 Minutes, 1Hour** or **2 Hours**. Select **Disabled** to send no alerts of any kind, including condition alerts, offline alerts, and alert reminders.

   ■ Buzzer—Enables (checked) or disables (unchecked) the audible alarm on the EA800-ip console.

   ■ Collection Frequency—Time interval at which to collect and store sensor log data in the INSIGHT database. Select **5 Minutes**, **15 Minutes**, **30 Minutes**,**1 hour** or **2 hours**.

   ■ Keypad Lock—Locks (checked) or unlocks (unchecked) the EA800-ip console keypad. If the keypad is locked, the EA800-ip device can be managed only with INSIGHT.

4. Click **SAVE** to save the device information; otherwise, click **CANCEL**.

Deleting a Device

Deleting an EA800-ip device deletes the device and its configured sensors from the INSIGHT database, including all past notifications and sensor log data associated with those sensors. References to the device and its sensors are also removed from notification profiles. However, the sensor configurations remain on the EA800-ip device.

> **NOTE**
>
> Consider creating a sensor detail log report as a backup before deleting a device. For information about creating a sensor detail log report, see "Creating a Report" on page 38.

To delete an EA800-ip device from the account tree:

1. Click the **Account Administration** tab.

    ■   If you are a reseller, in the Choose a Customer section, click the customer account name.

    ■   If you are not a reseller, proceed to Step 2.

2. In the Edit Accounts section, click a device in the account tree.

3. In the Edit Device section, click **Delete Device**.

4. In the Device Delete Confirmation window, click **YES, I'M SURE** to confirm the deletion; otherwise, click **CANCEL**.

Managing Sensors

INSIGHT enables you to modify wired and wireless sensor parameters from a remote location. You can also use INSIGHT to add and delete wired sensors; wireless sensors have to be added and deleted at the EA800-ip console.

Adding a Wired Sensor

For information about adding a wireless sensor, see the *EnviroAlert EA800-ip Installation/Owner's Manual*.

To add a wired sensor to a device:

1. Click the **Account Administration** tab.

    ■   If you are a reseller, in the Choose a Customer section, click the customer account name.

    ■   If you are not a reseller, proceed to Step 2.

2. In the Edit Accounts section, click a device in the account tree.

3.   Click **+Add a Sensor** or **+Add Another Sensor**.

4.   Under Add a New Sensor . . ., select or type values for the following sensor parameters. For details about the sensor parameters, see the *EnviroAlert EA800-ip Installation/Owner's Manual*.

■   Type—Select from the pull-down menu:

❑   **Temp White**, **Temp Blue**, **Temp Red** (temperature)

❑   **Ha III+** (Humidity)

❑   **WaterBug** (water presence)

❑   **NO Contact**, **NC Contact** (normally open/normally closed contact)

❑   **4 to20 mA**

■   Position—Sensor terminal position (1–4) on the EA800-ip circuit board. For information about sensor terminal positions, see the *EnviroAlert EA800-ip Quick Start Guide.*

■   Name/Location—Descriptive name by which to identify the sensor

■   Units—Unit of measure for the sensor. This value cannot be changed after you click **SAVE**, except to delete the sensor and add a new one.

■   Low Limit—Sensor value at or below which an alert is issued

■   High Limit—Sensor value at or above which an alert is issued

■   Alert Delay—Time period in minutes to wait before issuing an alert after an alert condition occurs. Values can be 0–120.

■   Alert Response Profile—Response profile to use in the event of an alert on this sensor. This profile has precedence over the response profile that is assigned to the connected device. Other than a specific response profile, values can be the following:

❑   **[Use This Device's Response Profile]**—Specifies the response profile that is assigned to the connected EA800-ip device.

❑   **None**—Specifies no response profile.

For more information about response profiles, see .

■   Relay—Relay terminal number (1–8) on the EA800-ip circuit board to use for output to an external alarm panel. An asterisk (*) next to the relay number means that relay is assigned to at least one other sensor. You can assign a relay to more than one sensor.

■   Resolution—For 4–20mA sensors, this parameter specifies accuracy of sensor readings to whole numbers, tenths, hundredths, or thousandths. Values can be 1, .1, .01, or .001.

- ■ Hysteresis—Value subtracted from the high limit and added to the low limit defining the thresholds for canceling an alert, thus minimizing recurring alerts. The default is the same as the Resolution parameter, and is generally a good value to use. Avoid using zero (0).

- ■ 4mA Value—For 4–20mA sensors, the sensor measurement value (usually the lowest) that corresponds to a current output of 4mA

- ■ 20mA Value—For 4–20mA sensors, the sensor measurement value (usually the highest) that corresponds to a current output of 20mA

- ■ Calibration—Positive or negative value applied to a sensor to correct a nominal difference between the sensor readings and a certified measurement or reference standard. This parameter is not available for all sensors, and the acceptable values are dependent on the sensor resolution. For temperature sensors, differences of more than 0.5° F may indicate a sensor malfunction.

- ■ Description—Sensor description

5. Click **SAVE and ADD** to save the sensor information; otherwise, click **CANCEL**.

6. Click **SAVE** to save the device information; otherwise click **CANCEL**.

Modifying Wired and Wireless Sensors

To modify a wired or wireless sensor on a device:

1. Click the **Account Administration** tab.

   - ■ If you are a reseller, in the Choose a Customer section, click the customer account name.

   - ■ If you are not a reseller, proceed to Step 2.

2. In the Edit Accounts section, click a device in the account tree.

3. Under Sensors:, click ✎ adjacent to a sensor in the sensor list.

4. Under Edit sensor details below. . ., make the necessary changes. For more information about the sensor parameters, see "Adding a Wired Sensor" on page 30.

5. Click **SAVE and ADD** to save the sensor information; otherwise, click **CANCEL**.

6. Click **SAVE** to save the device information; otherwise click **CANCEL**.

Deleting a Wired Sensor

Deleting a wired sensor deletes the sensor from the EA800-ip device; the device no long collects data from the sensor. Furthermore, all past notifications and log data associated with that sensor are removed from the $\mathrm{INSIGHT}$ database. The sensor is also removed from notification profiles. To delete a wireless sensor, you must use EA800-ip keypad as described in the *EnviroAlert EA800-ip Installation/Owner's Manual*.

> **NOTE**
>
> Consider creating a sensor detail log report as a backup before deleting a sensor. For information about creating a sensor detail log report, see "Creating a Report" on page 38.

To delete a wired sensor from a device:

1. Click the **Account Administration** tab.

   ■ If you are a reseller, in the Choose a Customer section, click the customer account name.

   ■ If you are not a reseller, proceed to Step 2.

2. In the Edit Accounts section, click a device in the account tree.

3. Under Sensors:, click ✎ adjacent to a sensor in the sensor list.

4. Under Edit sensor details below. . . ,click **Delete Sensor**.

5. In the Sensor Delete Confirmation window, click **YES, I'M SURE** to confirm the deletion; otherwise, click **CANCEL**.

Managing Locations

A location is a named set of devices and users that enable you to control access to devices. Locations can be added to groupings to create another layer of organization (see "Managing Groupings" on page 35). The following sections describe how to add, modify, and delete a location.

Adding a Location

To add a location:

1. Click the **Account Administration** tab.

   ■ If you are a reseller, in the Choose a Customer section, click the customer account name.

   ■ If you are not a reseller, proceed to Step 2.

2. In the Add New section, click 📍 Add Location.

3.   In the Add Location section, type values for the following fields:

   ■   Location Name—Descriptive name identifying the location

   ■   Primary Contact—Name of the individual at this location who will administrate the EA800-ip device

   ■   Primary Phone—Telephone number of the primary contact

   ■   Primary Email—E-mail address of the primary contact

   ■   Location Address, Country, City, State/Province, Zip/Postal Code

   ■   Description—Optional details about the location

4.   Click **SAVE** to save the location; otherwise click **CANCEL**.

5.   In the account tree, drag-and-drop users and devices into the location. For more information about moving users and devices into a location, see "Working with Locations" on page 20.

Modifying a Location

To modify a customer location:

1.   Click the **Account Administration** tab.

   ■   If you are a reseller, in the Choose a Customer section, click the customer account name.

   ■   If you are not a reseller, proceed to Step 2.

2.   In the Edit Accounts section, click a location in the account tree.

3.   In the Edit Location section, make the necessary changes. For detailed information about the location parameters, see "Adding a Location" on page 33.

4.   Click **SAVE** to save the location; otherwise click **CANCEL**.

Deleting a Location

Deleting a location deletes all member users, devices, and sensors configured to those devices from the INSIGHT database. Furthermore, all past notifications and sensor log data associated with the sensors is also deleted. However, the sensor configurations remain on their respective EA800-ip devices.

> **NOTE**
>
> Before deleting a location, move all member users and devices to the customer account or another location. Otherwise, create a sensor detail log report as a backup. For information about moving users or devices from a location, see "Working with Locations" on page 20. For information about creating a sensor detail log report, see "Creating a Report" on page 38.

To delete a location from the account tree:

1. Click the **Account Administration** tab.

   ■ If you are a reseller, in the Choose a Customer section, click the customer account name.

   ■ If you are not a reseller, proceed to Step 2.

2. In the Edit Accounts section, click a location in the account tree.

3. In the Edit Location section, click **Delete Device**.

4. In the Location Delete Confirmation window, click **YES, I'M SURE** to confirm the deletion; otherwise, click **CANCEL**.

Managing Groupings

A grouping is a named set of one or more locations that help you organize your account tree. For example, you might create a grouping of all locations in a geographical region. The following sections describe how to add, modify, and delete a grouping.

Adding a Grouping

To add a grouping:

1.   Click the **Account Administration** tab.

     ◼   If you are a reseller, in the Choose a Customer section, click the customer account name.

     ◼   If you are not a reseller, proceed to Step 2.

2.   In the Add New section, click Add Grouping.

3.   In the Add Group section, type a name for the grouping.

4.   Click **SAVE** to save the grouping; otherwise click **CANCEL**.

5.   In the account tree, drag-and-drop locations into the grouping. For more information about moving locations into a grouping, see "Working with Groupings" on page 21.

Renaming a Grouping

To rename a grouping:

1.   Click the **Account Administration** tab.

     ◼   If you are a reseller, in the Choose a Customer section, click the customer account name.

     ◼   If you are not a reseller, proceed to Step 2.

2.   In the Edit Accounts section, click a grouping in the account tree.

3.   In the Edit Grouping section, type the new name.

4.   Click **SAVE** to save the grouping; otherwise click **CANCEL**.

Deleting a Grouping

Deleting a grouping deletes all member locations from the INSIGHT database. This includes all member users, devices, and the sensors configured on those devices. Furthermore, all past notifications and sensor log data associated with the sensors are deleted also. However, the sensor configurations remain on their respective EA800-ip devices.

> **NOTE**
>
> Consider creating a sensor detail log report as a backup before deleting groupings. For information about creating a sensor detail log report, see "Creating a Report" on page 38.
>
> For information about removing a location from a grouping without deleting the location from the INSIGHT database, see "Working with Groupings" on page 21.

To delete a grouping from the account tree:

1. Click the **Account Administration** tab.

   ■ If you are a reseller, in the Choose a Customer section, click the customer account name.

   ■ If you are not a reseller, proceed to Step 2.

2. In the Edit Accounts section, click a grouping in the account tree.

3. In the Edit Grouping section, click **Delete Grouping**.

4. In the Grouping Delete Confirmation window, click **YES, I'M SURE** to confirm the deletion; otherwise, click **CANCEL**.

5   Managing Reports

INSIGHT provides several sensor log and alert reports with which to track the activity of your monitored environments. You can create reports on-demand for selected sensors, or you can automatically generate and deliver reports periodically to interested users by E-mail.

Report creation or modification is a three-step process characterized by the step buttons on the Reports page. Click on these buttons as needed to move back and forth in the process to review or change settings.
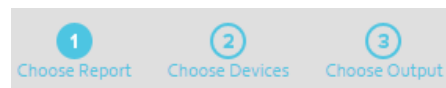
Creating a Report

To create a report:

1.   Click the **Reports** tab.

2.   In the Choose Report step, under Create a New Report, type a name in the Report Name field.

3.   Under Choose a new report type, click one of the report types, and then click **CREATE**. The following report types are available:

   ■   **Sensor Detail Log**—Lists the readings for the selected sensors at the data collection interval over the specified time period (1–31 days). A summary of the minimum, maximum, and average readings is included.

   ■   **Sensor Summary Log**—Plots the readings in a graph for the sensors on a selected device over the specified time period (1–31 days). The graph also shows the low and high limits. A summary of the minimum, maximum, and average readings is included.

   ■   **Sensor Acknowledgment Log**—Lists information about acknowledged readings for the selected sensors over the specified time period (1–31 days) including: time and date, user name, sensor reading, reading units, sensor status, and acknowledgment notes.

- **Alert Report By Location**—Plots a bar graph showing the number of alerts per EA800-ip device at selected locations over the specified time period (1–31 days). For HTML output only, click a bar to show a graph of the number of alerts per sensor at that location.

- **Alert Report By Device**—Plots a bar graph showing the number of alerts against each sensor on the selected device over the specified time period (1–31 days). Click a bar to show detailed alert information for that sensor.

- **Alert Response Summary**—Lists the alerts for which a response profile was performed for selected sensors over the specified time period (1–31 days). The report includes the responder's user name, actions completed, actions not completed, and responder's notes.

4. In the Choose Devices step, select one or more sensors in the device tree by customer account, by all devices, by device, by grouping, by location, or by individual sensor. Click **CONTINUE**.

5. In the Choose Output step, choose the report output type. Click **PDF**, **HTML**, or **CSV**.

    - CSV output is available only for Sensor Detail Log reports and Alert reports by device. Users must have Customer Admin or Admin permission.

    - CSV and PDF files are created in a folder according to your browser download settings.

6. Click the Start Date and End Date fields to specify the time period for which to collect sensor data from the INSIGHT database. The reports starts at 12:00 AM on the start date and ends at 12:00 AM on the end date.

7. Select a time zone from the Time Zone pull-down menu that corresponds to the dates you entered in Step 6. Consider the locations of your report recipients when choosing a time zone.

8. To save this report, check the **Save Report** check box. Saved reports appear in the Saved Reports table.

9. Click **CREATE REPORT**.

Scheduling a Report

To schedule a report:

1. Click the **Reports** tab.

2. In the Choose Reports step, do one of the following:

    - Under Create a New Report, type a name in the Report Name field. Under Choose a new report type, click one of the report types, and then click **CREATE**.

    - Under Saved Reports, click on a report.

3.   In the Choose Devices step, select one or more sensors in the device tree by customer account, by all devices, by device, by grouping, by location, or by individual sensor. Click **CONTINUE**.

4.   In the Choose Output step, click **Schedule**.

5.   In the Frequency field, choose the schedule frequency. Select **Daily**, **Weekly**, or **Monthly** from the pull-down menu.

For a daily schedule:

a.   In the Time to Run field, choose the time of day to create the report. Select the hour and time zone from their respective pull-down menus.

b.   In the Report Start/End Time field, choose the time from which to collect sensor data from the INSIGHT database for the previous 24 hours. Select the hour and time zone from their respective pull-down menus. The Report Start/End Time should be before the Time to Run.

c.   In the Subscribers pull-down menu, select the users who will receive the PDF report by E-mail.

For a weekly schedule:

a.   In the Time to Run field, choose the time of day to create the report. Select the hour and time zone from their respective pull-down menus.

b.   In the Day to Run pull-down menu, select the day to create the report.

c.   In the Report Start/End Time field, choose the time of day from which to collect sensor data for the previous week. Select the hour and time zone from their respective pull-down menus. The Report Start/End Time should be before the Time to Run.

d.   In the Subscribers pull-down menu, select the users who will receive the PDF report by E-mail.

For a monthly schedule:

a.   In the Time to Run field, choose the time of day to create the report. Select the hour and time zone from their respective pull-down menus.

b.   In the Day to Run pull-down menu, select the day of the month to create the report.

c.   In the Report Start/End Time field, choose the time of day to begin collecting sensor data for the previous month. Select the hour and time zone from their respective pull-down menus. The Report Start/End Time should be before the Time to Run.

d.   In the Subscribers pull-down menu, select the users who will receive the PDF report by E-mail.

6.   Click **SCHEDULE REPORT**.

Modifying a Saved or Scheduled Report

To modify a saved or scheduled report:

1.   Click the **Reports** tab.

2.   In the Choose Reports step, under Saved Reports or Scheduled Reports, click on a report.

3.   In the Choose Devices step, modify the sensor selections in the device tree as needed, and then click **CONTINUE**.

4.   In the Choose Output step, make changes to the output type, time period, time zone, and subscribers as needed.

5.   Click **CREATE REPORT**.

Deleting a Saved or Scheduled Report

To delete a saved or schedule report:

1.   Click the **Reports** tab.

2.   In the Choose Reports window, under Saved Reports or Scheduled Reports, choose a report you want to delete, and click next to the entry.

3.   In the Report Delete Confirmation window, click **YES, I'M SURE** to confirm the deletion; otherwise, click **CANCEL**.

6   Managing Profiles

A profile is a named set of data that can be referenced and reused in the configuration of User IDs, devices, and sensors. The INSIGHT platform uses two types of profiles: notification profiles and response profiles.

Notification Profiles

A notification profile is a named list of sensors for which a user can receive an E-Mail notification when an alert condition occurs. To implement a notification profile, you must specify a notification profile in the User ID, either when you add the User ID or by modifying the User ID. For more information about adding and modifying User IDs, see "Managing Users IDs" on page 24.

> **NOTE**
>
> If you do not specify a notification profile in the User ID, the user will not receive any notifications, including condition alerts, offline alerts, and alert reminders.

The following subsections describe how to add, modify, and delete a notification profile.

Adding a Notification Profile

To add a notification profile:

1. Click the **Profiles** tab.

2. In the Create or edit profiles section, under Notification Profiles, click **+Add Profile**.

3. In the Add Notification Profile column, type a descriptive name in the Notification Profile Name field.

4. In the Description field, type optional details about the profile's purpose and use.

5. In the device tree, check the check boxes next to the sensors for which you want to send alert notifications by E-mail. You can select individual sensors, or you can select all sensors associated with the customer account, with a device, with a location, or with a grouping.

6. Click **SAVE** to save the notification profile; otherwise, click **CANCEL**.

Modifying a Notification Profile

To modify a notification profile:

1. Click the **Profiles** tab.

2. In the Create or edit profiles column, under Notification Profiles, click on a profile name in the list of notification profiles.

3. In the Edit Notification Profile column, make the necessary changes to the profile parameters. For more information about the notification profile parameters, see "Adding a Notification Profile" on page 42.

4. Click **SAVE** to save the changes; otherwise, click **CANCEL**.

Deleting a Notification Profile

Deleting a notification profile removes that notification profile from User ID configurations, affecting what notifications users receive. If necessary, update your User IDs configurations before deleting a notification profile. For information about modifying a User ID, see "Modifying a User ID" on page 26.

To delete a notification profile:

1. Click the **Profiles** tab.

2. In the Create or edit profiles column, under Notification Profiles, click on a profile name in the list of notification profiles.

3. In the Edit Notification Profile column, click **Delete Profile**.

4. In the Delete Profile Confirmation column, click **YES, I'M SURE** to confirm the deletion; otherwise, click **CANCEL**.

Response Profiles

A response profile is a named list of actions that you are prompted to perform when an alert condition occurs involving one or more sensors (see "Responding to an Alert" on page 16). The response profile also enables you to specify which actions are required according to your SOP. The following subsections describe how to add, modify, and delete a response profile.

To implement a response profile, you must specify the profile as part of a device or sensor definition. You can specify a response profile for all sensors connected to a device or for individual sensors. The former profile is called a *device response profile*, and the latter is called a *sensor response profile*. When an alert condition occurs, a sensor response profile has precedence over the device response profile.

■　For information about specifying a device response profile, see "Modifying a Device" on page 29.

■　For information about specifying a sensor response profile, see "Adding a Wired Sensor" on page 30 and "Modifying Wired and Wireless Sensors" on page 32.

Adding a Response Profile

To add a response profile:

1.　Click the **Profiles** tab.

2.　In the Create or edit profiles column, under Response Profiles, click **+Add Profile**.

3.　In the Add Response Profile column, descriptive name in the Responses Profile Name field.

4.　In the Description field, type additional optional profile details.

5.　Choose whether to require that all actions be performed to complete the profile.

　　■　If the check box is unchecked, all required actions must be performed to complete the profile.

　　■　If the check box is checked, required actions need not be performed to complete the profile.

6.　In the Action 1 field, type the first action. Indicate in the corresponding check boxes whether this action is required, and whether a comment is required.

7.　If additional actions are required, click **+Add Another Action**, and then repeat Step 6. To delete an action, click 　.

8.　Click **SAVE** to save the response profile; otherwise, click **CANCEL**.

Modifying a Response Profile

To modify a response profile:

1.   Click the **Profiles** tab.

2.   In the Create or edit profiles section, under Response Profiles, click on a profile name in the list of response profiles.

3.   In the Edit Response Profile section, make the necessary changes to the response profile parameters. For more information about the response profile parameters, see "Adding a Response Profile" on page 44.

4.   Click **SAVE** to save the changes; otherwise, click **CANCEL**.

Deleting a Response Profile

Deleting a response profile removes that response profile from device and sensor configurations. If necessary, update your device and sensor configurations before deleting a response profile. For information about specifying a response profile, see "Modifying a Device" on page 29 and "Modifying Wired and Wireless Sensors" on page 32.

To delete a response profile:

1.   Click the **Profiles** tab.

2.   In the Create or edit profiles section, under Response Profiles, click on a profile name in the list of response profiles.

3.   In the Edit Response Profile section, click **Delete Profile**.

4.   In the Delete Profile Confirmation window, click **YES, I'M SURE** to confirm the deletion; otherwise, click **CANCEL**.

Glossary

Account Tree

The hierarchical representation of users, devices, locations, and groupings associated with a customer account.

Acknowledgment

The validation of a sensor reading by a human being.

Admin Permission

The permission assigned to a user ID that enables a user to manage User IDs, devices and sensors, locations, groupings, and profiles for a single customer account. See Customer Admin Permission and User Permission.

Alert

The status assigned to a sensor, or the device to which it is connected, when an abnormal condition occurs.

Customer

A company or an individual that purchases the INSIGHT platform for use.

Customer Account

The customer name and supporting information that identifies the customer to the INSIGHT platform. A reseller's account can add customer accounts.

Customer Admin Permission

Permission assigned to a User ID that enables a reseller to create and manage customer accounts. This permission grants the most control. See Admin Permission and User Permission.

Dashboard

Graphic presentation of the EA800-ip devices in your monitored environment showing device and sensor status. The dashboard has three views: Device Overview, Device List View, and Map View.

Device

The EA800-ip console and its connected sensors.

Grouping

A named set of locations that aid in visually organizing the account tree.

Location

A named set of users and devices associated with a street address. Users assigned to a location have access only to those devices assigned to the same location.

Notification Profile

A named set of sensors for which a user may request to receive an E-mail in the event of an alert.

Reseller

An individual or company that purchases the INSIGHT service from Winland Electronics for resale to its customers.

Response

An action or procedure performed in response to an alert.

Response Profile

A named sequence of actions to perform in the event of an alert. You can specify a response profile for individual sensors (sensor response profile) or for all sensors connected to an EA800-ip device (device response profile).

Sensor

An instrument that measures an environmental condition, such as temperature, humidity, or electrical continuity. Sensors can be wired or wireless.

Standard Operating Procedures (SOP)

Approved and documented procedures that an organization uses to conduct its business.

User ID

The user name and supporting information that gives an individual access to the INSIGHT platform.

User Permission

Permission assigned to a User ID that enables a user to monitor sensors and generate reports. This is the most restrictive permission level. See Admin Permission and Customer Admin Permission.

Index

DNS address 5
domain name server, See DNS
Dynamic host configuration protocol, See DHCP

E

EA800-ip
  buzzer 29
  circuit board 31
  collection frequency 29
  device key 28
  installation 4
  keypad lock 29
  memory capacity 3
  normal 13
  offline 13
  remote control 2
  serial number 10, 28
E-mail
  address 25
  notification 1
equipment serial number, see ESN
ESN 10, 28
Ethernet cable 5

F

filter buttons 9, 13
frequency, data collection 29, 38

G

gateway address 5
grouping
  add 8, 36
  delete 37
  description 21, 35
  move a location 22
  rename 36

H

help 7
high limit 14, 31
HTML output 3, 39
hysteresis 32

I

INSIGHT
  configuration 8
  database 3
  login 6
  logout 7
  overview 1
  request 4
Internet connection 5
IP address 5

K

key, device 28
keypad lock 29

L

license agreement 6
limit 14
location
  add 8, 33
  delete 35
  description 2, 20, 33
  modify 34
  move to a grouping 22
  move user or device 20
  parameters 34
  user access 18

S

scheduled report 3
security
  company 4
  question 6
sensor
  4-20mA values 32
  accuracy 31
  acknowledgment log 38
  add 8, 30
  detail log 38
  information 14
  log data 3
  management 30
  modify 32
  name 14, 31
  parameters 31
  remote control 2
  response profile 16, 31, 44
  status 9
  summary log 38
  type 31
  wired or wireless 14
  wired, delete 33
serial number 28
SOP 1, 44
standard operating procedure, see SOP
subnet mask 5
subscribers, report 40
summary, alert response 39

T

technical support ix
text message 1
threshold 31
time zone 29

U

unit of measure 14, 31

user
  access 18
  move to location 20
  name 4, 6
  permission 18, 26
User ID
  add 8, 25
  delete 27
  description 2
  locked 26
  management 24
  modify 26
  parameters 25
  permission level 26

V

view buttons 9

W

weekly report 40