



Programming Manual

EN6091 Gateway Mark II

Preliminary

Table of Contents

Preface 4

Notice	4
Revision	4
Trademarks	4
Technical Services Contact Information	4
Document Conventions	5

Chapter 1 Inovonics Intrusion System Overview 6

1.1 Introduction	6
1.2 Inovonics Intrusion System Features	7
1.3 Inovonics Intrusion System Components	8
1.3.1 Gateway Mark II	8
1.3.2 IDTOUCH1 Touchpad	8
1.3.3 Inovonics Intrusion System Mobile App	9
1.3.4 Repeaters	9
1.3.5 EchoStream Hardware	9
1.3.6 Other Compatible Hardware	9
1.4 Software and Firmware Updates	10

Chapter 2 Dealer Organization Setup 11

2.1 Introduction	11
2.2 Accounts	11
2.2.1 Add Account	11

Chapter 3 System and Panel Setup 13

3.1 Add System	13
3.2 Add Panel	14

3.3 Enter/Exit Maintenance Mode	15
3.3.1 Enter Maintenance Mode	15
3.3.2 Exit Maintenance Mode	15
3.4 Update Gateway Mark II Firmware	15
3.5 Configure Onboard Hardwired Zone Module	16
3.6 Add Sounders	17
3.7 Add Central Station	18

Chapter 4 Partition and Zone Setup	19
---	-----------

4.1 Add Sub-Account	19
4.2 Add Partition	20
4.3 Add Touchpad	21
4.3.1 Configure Touchpad Wi-Fi	22
4.3.2 Configure Panel Connectivity	22
4.4 Update Touchpad Software	22
4.5 Configure Network Settings	23
4.5.1 Enable/Disable Network Connectivity	23
4.5.2 Configure Network Priority	24
4.6 Add Repeater	24
4.7 Add Wireless Zone	25
4.8 Add Wired Zone	27

Chapter 5 Configuration and Test	29
---	-----------

5.1 Dealer Users	29
5.1.1 Add Dealer User	29
5.1.2 Grant/Edit Access to Dealer User	30
5.2 System and Partition Users	31
5.2.1 Add System Administrator	31
5.2.2 Add Partition User or Administrator	32
5.3 Set Abort Window	33
5.4 Enable/Disable Exit Delay Restart	33
5.5 Enter/Cancel Test Mode	34
5.6 Access Activity Logs	34
5.7 View Overview Page	35
5.8 Reset E-Fuse	35

Chapter 6 Zone Type Behavior**36**

6.1 Introduction	36
6.2 Entry/Exit and Entry/Exit Extended	36
6.2.1 Programming Options (Default in Parentheses):	37
6.3 Perimeter/Instant	38
6.3.1 Programming Options (Default in Parentheses):	38
6.4 Interior/Follower	39
6.4.1 Programming Options (Default in Parentheses):	39
6.5 Trouble While Disarmed/Alarm While Armed	40
6.5.1 Programming Options (Default in Parentheses):	41
6.6 24-Hour Silent	41
6.7 24-Hour Audible	42
6.8 24-Hour Auxiliary	43
Chapter 7 Quick Reference	44
7.1 Quick Reference Chart	44

Preface

Notice

Copyright 2026 Inovonics

Inovonics intends this manual for use by Inovonics customers only. All comments concerning the contents of this manual should be directed to the Inovonics marketing department. No part of this work covered by copyright may be reproduced in any form either graphically, electronically or mechanically; including photocopying, recording, taping, or storing in an information retrieval system without prior written permission from Inovonics.

Revision

10.8.26 356-00006-01 Rev A

Trademarks

All brand names and product names used in this manual are trademarks, registered trademarks, or trade names of their respective holders.

Technical Services Contact Information

If you have any problems with this procedure, contact Inovonics technical support:

- E-mail: support@inovonics.com.
- Phone: (800) 782-2709.

Document Conventions

The following notices are used throughout this document:

Note: Emphasizes points, provides supplementary information, or indicates minor problems in an expected outcome.

Caution: Indicates possible damage to equipment or loss of data, as well as potential problems in an expected outcome.

Warning: Indicates the possibility of minor injury to oneself or others.

Danger: Indicates the possibility of serious or fatal injury to oneself or others.

Chapter 1

Inovonics Intrusion System Overview

1.1 Introduction

Note: For regulatory information see the *EN6091 Installation and Operation Manual*.

The Inovonics Intrusion System is the first hybrid, cloud native enterprise-grade security platform combining proven Inovonics wireless technology with optional hardwired zone support. Built for commercial environments, it delivers reliable wireless performance, built-in cellular connectivity, and mobile app control in a single integrated system.

Powered by Inovonics EchoStream® 900 MHz wireless mesh network, the Inovonics Intrusion System connects the Inovonics EchoStream commercial mesh network with the EN6091 Gateway Mark II, IDTouch1 touchpad, and Inovonics Cloud Services into one integrated system.

Note: Refer to the latest revision of applicable SIA and UL standards for your installation. Inovonics recommends CP-01 for SIA installations, and UL 2610 for UL listed installations.

1.2 Inovonics Intrusion System Features

Feature	Details
Access codes	Supports up to 500 users/codes, four/six/eight-digit length (eight is reserved for dealers).
Event history	Local event log saves last 1000 events; event log saves last 10,000 events.
Installer support	Inovonics programming menus and local application using WiFi.
Wireless sensors	Inovonics EchoStream wireless devices.
Zones	Up to 256 supervised zones: any combination of wired and Inovonics wireless devices. Eight hardwired zones supported on panel.
Zone characteristics	Entry/exit; entry/exit extended; perimeter/instant; interior follower; trouble while disarm/alarm while armed; 24-hour silent; 24-hour audible; 24-hour auxiliary.
Arming modes	Arm away, arm stay, arm maximum.
Wired zone types	Normally closed, single EOL, double EOL, triple EOL (anti-masking and doubling).
Users	500 users/codes; four/six/eight digit length (eight reserved for dealers); dealer admin, system admin; partition user and admin.
Partitions	Up to eight partitions; one partition can be designated as a common area; partitions can be independently armed and disarmed.
Interface(s)	One battery backed up touchpad, Android/iOS mobile application, dealer dashboard for configuration and management.
Firmware updates	Panel (mender); Touchscreen app (RMS); touchscreen OS (RMS); touchscreen MCU (RMS); mobile application (relevant app store).
False alarm mitigation	Remote arm cancel (remote arming and disarming of the Inovonics Intrusion System have not been evaluated by UL under UL 294 or UL 2610); alarm cancel on-premises; alarm abort on-premises; test mode (disable CMS for one-hour); recent closing; stay mode failover.

Feature	Details
Communication	Failover support, primary wired Ethernet, secondary built-in cellular and WiFi. Built-in EchoStream radio for communication with Inovonics wireless initiating devices.
Central station integrations	Rapid Response and Affiliated Monitoring (DC-09 connector).
Central station communication audit trail and activity log	ANSI/SIA DC-09-2019; activity log accessible through mobile app; event log saves last 10,000 events.
Bypass	Individual zone bypass; scheduled bypass.

1.3 Inovonics Intrusion System Components

Each Inovonics Intrusion System includes the following components:

1.3.1 Gateway Mark II

The Inovonics Gateway Mark II is a fully integrated and modular commercial security platform designed for unmatched reliability, rapid deployment, and effortless scalability. Built on Inovonics' industry-proven EchoStream® wireless mesh network, it delivers secure, long-range communication that thrives in demanding RF environments—without the complexity of wired infrastructure.

1.3.2 IDTOUCH1 Touchpad

The Inovonics IDTOUCH1 touchpad connects to the Gateway Mark II hybrid panel for reliable performance and intuitive control. Featuring a sleek, high-resolution seven-inch full-color display, it allows users to easily arm, disarm, and bypass the system while providing real-time system status and alerts.

1.3.3 Inovonics Intrusion System Mobile App

The Inovonics Intrusion System mobile app enables users to remotely manage and control their Inovonics Intrusion System and compatible devices. Users can perform various keypad functions, including arming and disarming the system, bypassing specific zones, checking system status, and viewing activity logs — all from their smartphone or tablet.

Note: Remote arming and disarming of the Inovonics Intrusion System have not been evaluated by UL under UL 294 or UL 2610.

1.3.4 Repeaters

Repeaters are an optional component of an Inovonics system that expand the coverage area of the network. Repeaters can be easily included in the initial installation or added as the system grows. Repeaters receive messages and retransmit them at high power, optimizing communication paths to effectively manage RF traffic.

1.3.5 EchoStream Hardware

The Inovonics Intrusion System manages delivery of alarm information from Inovonics mobile duress and security devices. Please refer to the Inovonics website or contact your account manager for details about Inovonics security components.

1.3.6 Other Compatible Hardware

The Inovonics Intrusion System supports third-party hardwired security sensors, NAC devices, and programmable components with specific current and voltage requirements.

Note: See the *EN6091 Gateway Mark II Installation and Operation Manual* for a list of approved Inovonics and third-party devices.

1.4 Software and Firmware Updates

Inovonics will periodically update the Inovonics Intrusion System mobile app software and Gateway Mark II firmware to include new functionality, fix bugs and incorporate customer feedback. Inovonics will provide notifications via a pop up page upon login prior to the new versions going live.

Preliminary

Chapter 2

Dealer Organization Setup

2.1 Introduction

If you do not have an existing Inovonics account and login to the Inovonics dealer dashboard, use our dealer organization web form to contact technical services.

Once a dealer organization is created in Inovonics Cloud Services, an email will be generated for the dealer to setup their password and login. This will be the dealer admin account, with complete configuration access to the dealer organization.

2.2 Accounts

Creating accounts allows the dealer admin to folderize systems, such that dealers with multiple accounts can group them together.

2.2.1 Add Account

To add a new account:

1. In the sidebar menu, click on *Accounts*.
2. Click *ADD ACCOUNT*.
3. Enter the name of the account.

Note: Account names cannot include capital letters or special characters.

4. Optionally, click the *Systems* dropdown menu to select all systems associated with this account.
5. Click *ADD ACCOUNT*.

The account will now appear in the system portfolio account list. The following options are available when hovering over the account name:

- View a list of the systems associated with the account.
- Update the account name and the list of systems associated with the account.
- Remove the account.

Preliminary

Chapter 3

System and Panel Setup

Once the dealer organization has been setup, the next step is to add and configure a system and associated Gateway Mark II panel.

Note: Any configuration change made to the system will sync with the panel. The panel will also sync every 60 seconds. If you need to expedite sync, click SYNC SNAPSHOT.

3.1 Add System

To add a new system:

1. In the sidebar menu, click on *All Systems*.
2. Click *ADD SYSTEM*.
3. Click the *System Type* dropdown menu to choose Residential or Commercial.
4. Enter the name of the system.
5. Enter the address for the system.
6. Click the *User Code Length* dropdown menu to choose a length of four or six.
 - The user code length will determine the length of codes that users will enter to access the touchpad, set the duress code, arm/disarm the system and dismiss silent alarms.
7. Click the *Time zone* dropdown menu to select the time zone in which the system is located.

8. Click the *Accounts* dropdown menu to select the accounts with which to associate this system.
9. As desired, enter any descriptive text you would like associated with the system.
10. Ensure authorization to setup this system in accordance with the Inovonics Cloud Services Agreement.
11. Click *ADD SYSTEM*.
12. When the prompt appears, click *CONFIGURE* to advance to the system configuration page or *CLOSE* to exit to the system list.

The system will now appear in the system portfolio list. The following options will be available when hovering over a system name:

- Configure the system configuration page.
- Remove the system.

3.2 Add Panel

Once a system has been created, a Gateway Mark II panel can be added to it. To add a panel to the system:

1. Hover over the name of the newly-created system and click *Configure*. This will bring up the system configuration page.
2. In the sidebar menu, click *PANELS*.
3. Click *ADD PANEL*.
4. Enter the authorization code for the panel.
 - The authorization code can be found on a sticker on the panel's printed circuit board.
5. Enter the location in the building where the panel is installed for future reference.
6. As desired, enter any descriptive text you would like associated with the panel.
7. Click *ADD PANEL*.

3.3 Enter/Exit Maintenance Mode

Once a panel has been added, you will need to activate maintenance mode to continue programming. In order to enter maintenance mode, all partitions must be disarmed. During maintenance mode no alarms will be sent to the central station. Maintenance mode will continue until exited by the user or the maximum time period of four hours is reached.

Note: Only one dealer user or dealer admin can be in maintenance mode in any given time; no other user will be able to activate it until it has been exited or the four hour time has expired.

3.3.1 Enter Maintenance Mode

To enter maintenance mode:

1. Click *Settings*.
2. Click *PROCEED TO MAINTENANCE*.
3. When the Activate Maintenance Mode prompt appears, click YES.

3.3.2 Exit Maintenance Mode

To exit maintenance mode:

1. Click *STOP MAINTENANCE*.
2. When the Deactivative Maintenance Mode prompt appears, click YES.

3.4 Update Gateway Mark II Firmware

Note: The procedure can only be performed in maintenance mode. To activate maintenance mode, see section 3.3, “Enter/Exit Maintenance Mode” on page 15.

To update the Gateway Mark II firmware:

1. Click *Panels* on the sidebar menu.
2. Click *VIEW* on your panel.

- If a firmware update is available, the **UPDATE FIRMWARE** button will be green; if there is not firmware update available, it will be gray.
- 3. Click **UPDATE FIRMWARE**.
- 4. When the Update Firmware Version prompt appears, enter your password and click **UPDATE FIRMWARE**.
- 5. When the loading indicator has cleared, a prompt will appear indicating that the firmware update has started. Click **CLOSE**.
 - A banner will appear at the top of the page indicating the firmware is updating with an option to **ABORT**.

Once the update is complete, the Gateway Mark II will restart.

3.5 Configure Onboard Hardwired Zone Module

Note: The procedure can only be performed in maintenance mode. To activate maintenance mode, see section 3.3, “Enter/Exit Maintenance Mode” on page 15.

The Gateway Mark II supports eight hardwired zones using an onboard hardwired zone module. Before adding hardwired zones, the onboard hardwired zone module will need to be registered with the system.

To add the onboard hardwired zone module:

1. In the sidebar menu, click on *Panels*.
2. Click *View* on the newly-created panel.
3. On the panel's configuration screen, click **MODULES**.
4. Click **ADD MODULE**.
5. Enter a name for the module.
6. Enter the onboard zone module's serial number.
 - The onboard hardwired zone module's serial number can be found on a sticker on the Gateway Mark II panel's printed circuit board.

Note: Module Type is set at the manufacturer.

7. As desired, enter any descriptive text you would like associated with the panel.
8. Click *ADD MODULE*.

3.6 Add Sounders

Note: For recommended sounders that have been tested with the Inovonics Intrusion System, see the *EN6091 Gateway Mark II Installation and Operation Manual*.

Note: The procedure can only be performed in maintenance mode. To activate maintenance mode, see section 3.3, “Enter/Exit Maintenance Mode” on page 15.

The Gateway Mark II can support two sounder loops. To add a new sounder:

1. In the sidebar menu, click on *Panels*.
2. Click *View* on the panel.
3. On the panel’s configuration screen, click *Sounders*.
4. Click *ADD SOUNDERS*.
5. Click the *Sounder 1* or *Sounder 2* tab.
6. Click the *Bell Timeout* dropdown menu to choose the duration for which the sounder will alarm.
7. Click the *Supervised* toggle button to choose whether the sounder will be supervised.

Note: Ensure the sounder is properly connected with a 1kohm EOL resistor before selecting supervision; if not, the panel will go into alarm.

- If the sounder has resistance and supervision is enabled, Inovonics will generate a trouble message if a change in resistance is detected.
 - If you are only using one of the two sounder loops, ensure that supervision is disabled on the sounder loop that is not being used.
8. Click *Steady* or *Pulsing* to select an audio output for the sounder.

- Choosing Steady will emit a continuous alarm tone; choosing Pulsing will pulse the alarm tone.
9. Click *ADD SOUNDER*.

3.7 Add Central Station

Note: The procedure can only be performed in maintenance mode. To activate maintenance mode, see section 3.3, “Enter/Exit Maintenance Mode” on page 15.

The central station menu option allows you to add or edit a monitoring service for the system.

To add a monitoring service:

1. In the sidebar menu, click on *Central Station*.
2. Click *ADD SERVICE*.
3. Use the *Monitoring Service* dropdown menu to select the monitoring service.
4. Add the account number from your monitoring service for the panel .
5. Click *ADD SERVICE*.

The monitoring service will now appear on the central station menu page. The following options are available:

- Update the monitoring service.
- Remove the monitoring service.

Once added, the connection can be verified by clicking the connectivity popup on the IDTOUCH1 touchpad home screen. Additionally, when CMS connectivity is active and configured, arming or disarming a partition will provide an auditory signal confirming receipt.

Note: For instructions on adding the touchpad, see section 4.3, “Add Touchpad” on page 21.

Chapter 4

Partition and Zone Setup

Now that the system and panel have been setup, partitions and their associated zones can be added.

4.1 Add Sub-Account

Note: The procedure can only be performed in maintenance mode. To activate maintenance mode, see section 3.3, “Enter/Exit Maintenance Mode” on page 15.

Sub-accounts can be added to folderize partitions in the same manner as accounts are used to folderize systems. They are optional.

To add a sub-account:

1. In the sidebar menu, click *Sub-Accounts*.
2. Click *ADD SUB-ACCOUNT*.
3. Enter a name for the sub-account.
4. As desired, enter a description for the sub-account.

The sub-account will now appear on the Sub-Account menu page.

4.2 Add Partition

Note: The procedure can only be performed in maintenance mode. To activate maintenance mode, see section 3.3, “Enter/Exit Maintenance Mode” on page 15.

Partitions can be armed and disarmed separately, allowing users to control different areas.

To add a partition:

1. In the sidebar menu, click *Partitions*.
 2. Click *ADD PARTITION*.
 3. Enter a name for the partition.
 4. In the Duress Code field, enter a unique four or six digit duress code.
 - When this code is entered on the touchpad, the user will be able to use the touchpad as a system administrator, but a silent alarm will also be automatically sent to the central station.
-

Note: The length of the duress and silent alarm dismissal code are set when adding a system, as shown in section 3.1, “Add System” on page 13.

5. In the Silent Alarm Dismissal Code field, enter a unique four or six digit code, different from the duress code.
 - When this code is entered on the touchpad after a silent alarm has been sent, it will dismiss the alarm.
 6. As desired, use the *Sub-Account* dropdown menu to assign the partition to a sub-account.
 7. As desired, enter a description for the partition.
 8. Click *Adjust Delays* and use the sliders, arrows, or number fields to choose delays for the partition.
 - The entry delay can be set between 30 and 240 seconds, with a default of 30 seconds.
 - The extended entry delay can be set between 30 and 240 seconds, with a default of 30 seconds.
 - The exit delay can be set between 45 and 120 seconds, with a default of 60 seconds.
-

- SIA requirements are:
 - Entry delay: 30 seconds to four minutes.
 - Exit delay: 45 seconds to two minutes.

9. Click *ADD PARTITION*.

The partition will now appear on the Partitions menu page.

4.3 Add Touchpad

Note: The procedure can only be performed in maintenance mode. To activate maintenance mode, see section 3.3, “Enter/Exit Maintenance Mode” on page 15.

1. Wire the touchpad to the panel per the touchpad’s installation instructions.
2. In the sidebar menu, click *Partitions*.
3. Click *VIEW* on the partition to which you want to add the touchpad.
4. Click *Add Device*.
5. Use the *Device Type* dropdown menu and to select Touchpad.
6. Enter a name for the touchpad.
7. Use the *Model* dropdown menu to select the touchpad model.
8. Enter the serial number of the touchpad.

Note: The touchpad’s serial number is located on a sticker on the backplate of the device. If the mounting bracket is installed, it will obscure the serial number.

9. As desired, enter a description of the touchscreen.
10. Click *ADD DEVICE*.

The touchpad will now appear on the partition’s list of devices and zones. It can take up to 30 seconds for the panel to recognize the touchpad. Once the touchpad is recognized, connection options will appear.

The panel’s Ethernet connection will be the primary connection to the cloud upon startup.

4.3.1 Configure Touchpad Wi-Fi

To configure Wi-Fi when the Configure Touchpad Wi-Fi message appears:

1. Click *Connect to Wi-Fi*.
2. Select your Wi-Fi network.
3. Enter the password.
4. Click *Connect*.
 - The touchpad screen will advance to the Ethernet connection screen.

Note: WiFi and Ethernet connectivity can be edited on settings page on the touchpad at any point.

4.3.2 Configure Panel Connectivity

To configure panel connectivity when prompted by the touchpad:

1. Click *Setup your Panel network*.
2. To use Ethernet only, click *Ethernet*; to setup panel Wi-Fi backup now, click *Wi-Fi*.
3. If using Wi-Fi, enter the network name and password.
4. Click *Connect*.

4.4 Update Touchpad Software

Note: The procedure can only be performed in maintenance mode. To activate maintenance mode, see section 3.3, “Enter/Exit Maintenance Mode” on page 15.

When there is an update available to the touchpad, the Update button will show on the home screen.

Note: Updates can also be accessed in Settings when available.

To update touchpad firmware:

1. Tap the *Update* button on the home screen.
2. When prompted, enter a dealer admin or dealer user passcode.

The touchpad will restart when the update is complete.

4.5 Configure Network Settings

Note: The procedure can only be performed in maintenance mode. To activate maintenance mode, see section 3.3, “Enter/Exit Maintenance Mode” on page 15.

Configure network settings allows you to enable/disable your Wi-Fi, Ethernet and cellular connections, as well as to arrange the priority of your connections.

Note: Wi-Fi and Ethernet connection parameters can be edited upon startup of the touchpad, or in Settings screen on the touchpad. For more information, see section 4.3, “Add Touchpad” on page 21.

4.5.1 Enable/Disable Network Connectivity

To enable/disable Wi-Fi, Ethernet or cellular connection:

1. In the sidebar menu, click on *Panels*.
2. Click *View* on the panel.
3. Click *Network Settings*.
4. Use the *Cellular Enabled* or *Wi-Fi Enabled* toggle buttons to enable or disable connectivity.

Note: Ethernet cannot be disabled.

4.5.2 Configure Network Priority

To change network priority for the connection options:

1. In the sidebar menu, click on *Panels*.
2. Click *View* on the panel.
3. Click and drag the connectivity options.
 - The panel will attempt to connect using the connectivity options in order from top to bottom.

4.6 Add Repeater

Note: The procedure can only be performed in maintenance mode. To activate maintenance mode, see section 3.3, “Enter/Exit Maintenance Mode” on page 15.

Inovonics high power repeaters can be added to a partition in cases where the RF signal needs amplification to reach the panel.

To add a repeater:

1. In the sidebar menu, click *Partitions*.
2. Click *VIEW* on the partition to which you want to add the repeater.
3. Click *ADD DEVICE*.
4. Use the *Device Type* dropdown menu to select Repeater.
5. Enter a name for the repeater.
6. Select the repeater model.
7. Enter the TXID of the repeater.

Note: The repeater’s TXID number is located on a sticker on the housing as well as on the printed circuit board.

8. As desired, enter a description of the repeater.
9. Click *ADD DEVICE*.

The repeater will now appear on the partition’s list of devices and zones. The following options will be available when hovering over the repeater:

- Update the repeater.
- Remove the repeater.

4.7 Add Wireless Zone

Note: The procedure can only be performed in maintenance mode. To activate maintenance mode, see section 3.3, “Enter/Exit Maintenance Mode” on page 15.

Note: For a full list of compatible Inovonics wireless devices, see the *EN6091 Gateway Mark II Installation and Operation Manual*.

To add a wireless zone:

1. In the sidebar menu, click *Partitions*.
2. Click *VIEW* on the partition to which you want to add the wireless zone.
3. Click *Add Zone*.
4. Use the *Device Type* dropdown menu to select *Wireless*.
5. Enter a name for the wireless zone.
6. Select the wireless zone model.
7. Select the wireless zone behavior.
 - For more information about zone behaviors, see “Zone Type Behavior” on page 36.
8. Enter the TXID of the wireless zone.
9. If the behavior chosen is Entry/Exit, Entry Extended/Exit, Perimeter Instant or Interior, you will have the option to cross zone. As desired, click *Cross Zone* to select another zone to connect this zone with.
 - When cross zone is enabled between two zones, neither zone will register an alarm unless both zones are triggered. This can be used to help prevent false alarms. For example, cross zoning two motion detectors will ensure motion is detected by both before sending an alarm.
10. If the behavior chosen is Entry/Exit, Entry Extended/Exit, Perimeter Instant or Interior, you will have the option for an abort window. As

desired, click the *Abort Window* toggle to enable or disable the abort window.

- When the abort window is enabled, an alarm will not be transmitted to the central station if it is cleared within a predetermined period. The abort window is enabled by default.
- The default abort window is 30 seconds; to adjust the abort window, see section 5.3, “Set Abort Window” on page 33.

11. As desired, enter a description of the wireless zone.

12. Click *Advanced Settings* to display the chime and swinger suppression options.

13. As desired, choose a chime tone.

- If a chime tone is enabled, it will sound each time a zone is activated. For example, if set for a door contact, the touchpad will chime each time the door is opened. Chime is disabled by default.

14. As desired, enable swinger suppression.

- Swinger suppression will stop reporting alarms to the central station if a set number of alarms has already been sent. This will avoid overwhelming the central station with duplicate alarms. Swinger suppression is disabled by default.

15. If swinger suppression has been enabled, select an alarm threshold for the number of alarms that can occur before alarms sent to the central station are suppressed.

- Six is the maximum allowable alarm threshold.

16. Click *ADD ZONE*.

The wireless zone will now appear in the partition’s list of devices and zones. The following options will be available when hovering over the zone name:

- Update the zone configuration.
- Remove the zone.

4.8 Add Wired Zone

Note: For a full list of recommended wired devices that have been tested with the Inovonics Intrusion System, see the *EN6091 Gateway Mark II Installation and Operation Manual*.

Note: The procedure can only be performed in maintenance mode. To activate maintenance mode, see section 3.3, “Enter/Exit Maintenance Mode” on page 15.

1. In the sidebar menu, click *Partitions*.
 2. Click *VIEW* on the partition to which you want to add the wireless zone.
 3. Click *Add Zone*.
 4. Use the *Device Type* dropdown menu to select *Wired*.
 5. Enter a name for the wired zone.
 6. Click *Zone Type* to select the type of zone.
 7. Select the wired zone behavior.
-

Note: For more information about zone behaviors, see “Zone Type Behavior” on page 36.

8. Click the *Hardwired Zone Expander* dropdown menu to select the hardwired zone module to which the zone is attached.
 9. Select the contact type of the wired zone.
 10. If a contact type with a resistance value has been chosen, click the *Resistance Value(s)* dropdown menu to choose the resistance value.
 11. Select a port for the wired zone.
 - The port indicates the hardwired zone module zone terminals to which the wired zone is connected on the panel.
 12. If the behavior chosen is Entry/Exit, Entry Extended/Exit, Perimeter Instant or Interior, you will have the option to cross zone. As desired, click *Cross Zone* to select another zone to connect this zone with.
-

- When cross zone is enabled between two zones, neither zone will transmit an alarm unless both zones are triggered. This can be used to help prevent false alarms. For example, cross zoning two motion detectors will ensure motion is detected by both before sending an alarm.
- 13.** If the behavior chosen is Entry/Exit, Entry Extended/Exit, Perimeter Instant or Interior, you will have the option for an abort window. As desired, click the *Abort Window* toggle to enable or disable the abort window.
- When the abort window is enabled, an alarm will not be transmitted to the central station if it is cleared within a predetermined period. The abort window is enabled by default.
 - The default abort window is 30 seconds; to adjust the abort window, see section 5.3, “Set Abort Window” on page 33.
- 14.** As desired, enter a description of the wired zone.
- 15.** Click *Advanced Settings* to display the chime and swinger suppression options.
- 16.** As desired, choose a chime tone.
- If a chime tone is enabled, it will sound each time a zone is activated. For example, if set on a door contact, the touchpad will chime each time the door is opened. Chime is disabled by default.
- 17.** As desired, enable swinger suppression.
- Swinger suppression will stop reporting alarms to the central station if a set number of alarms has already been sent. This will avoid overwhelming the central station with duplicate alarms. Swinger suppression is disabled by default.
- 18.** If swinger suppression has been enabled, select an alarm threshold for the number of alarms that can occur before alarms sent to the central station are suppressed.
- Six is the maximum allowable alarm threshold.
- 19.** Click ADD ZONE.

The wired zone will now appear in the partition’s list of devices and zones. The following options will be available when hovering over the zone name:

- Update the zone configuration.
- Remove the zone.

Chapter 5

Configuration and Test

With the Inovonics Intrusion System now setup, the following options are available.

5.1 Dealer Users

Dealer users are created by the dealer admin, who can provide the dealer user temporary time-bounded access to specific systems. Once a dealer user is created, an email will be generated for the dealer user, who will then setup a password for access. There is a maximum of ten dealer users per system.

5.1.1 Add Dealer User

To add a new dealer user:

1. In the sidebar menu, click on *Dealer Users*.
2. Click **ADD USER**.
3. Enter an eight-digit user code in the User Code field.
 - This eight-digit user code is created by the dealer admin; the dealer user will use it to access the system through the touchpad or mobile app.
4. Enter the user's email address in the Email field.
5. Confirm the user's email address in the Confirm Email field.
6. Click **ADD USER**.

The user will now appear in the user list viewable by clicking Dealer Users and an email will be sent inviting them to register. By hovering over the dealer name, the following actions can be performed:

- Edit the fields setup in the add user process.
- Remove the dealer user from the dealer organization.
- Reset the password by generating a password to the dealer user.

5.1.2 Grant/Edit Access to Dealer User

Time-bound access to individual systems can be granted to dealer user.

To grant time-bound access:

1. In the sidebar menu, click on *Dealer Users*.
2. Expand the user dealer information.
3. Click *ADD ACCESS*.
4. Use the *Select Systems* dropdown menu to select the systems you will add access for.
5. Select a date range for which you will grant them access in the System Access Date Range field.
6. Click *ADD SYSTEM ACCESS*.

The dealer user will now have access to the selected system for the date range provided.

5.2 System and Partition Users

Each system can include up to 500 administrators and users total. There are three types of system and partition administrators and users available:

- The system administrator, who has access to all partitions, and can arm and disarm all partitions in a system. The system administrator can also create partition administrators and users. There is no limit to the number of system administrators.
- The partition administrator, who can arm and disarm their assigned partition, and create partition users. There can be up to five partition administrators per partition.
- The partition user, who can arm and disarm their assigned partition. There can be as many partition users as will bring the total of users and administrators to 500.

5.2.1 Add System Administrator

Note: The procedure can only be performed in maintenance mode. To activate maintenance mode, see section 3.3, “Enter/Exit Maintenance Mode” on page 15.

To add a new system administrator:

1. In the sidebar menu, click *All Systems*.
2. Navigate to system to which you want add a user and click *CONFIGURE*.
3. In the sidebar menu, click on *System Users*.
4. Click *ADD SYSTEM USER*.
5. Enter a unique arm/disarm code for this user.

Note: The length of the arm/disarm code was set when adding a system, as described in section 3.1, “Add System” on page 13.

6. Enter the user’s email address.
7. Confirm the user’s email address.
8. Click *ADD SYSTEM USER*.

The system administrator will now appear in the System Users list and an email will be sent inviting them to register. By hovering over the system administrator's name, the following actions can be performed:

- Resend the registration email.
- Reset the password by generating a password to the dealer user.
- Edit the fields setup in the add user process.
- Remove the user from the System Users list.

5.2.2 Add Partition User or Administrator

To add a new partition user or administrator:

1. In the sidebar menu, click *All Systems*.
2. Navigate to system to which you want add a user and click *CONFIGURE*.
3. In the sidebar menu, click on *System Users*.
4. Click *ADD PARTITION USER*.
5. Enter a unique arm/disarm code for this user.

Note: The length of the arm/disarm code was set when adding a system, as shown in section 3.1, "Add System" on page 13.

6. Enter the user's email address.
7. Confirm the user's email address.
8. Click *CONTINUE*.
9. Click *MANAGE ACCESS*.
10. Select the partitions you are giving this user access to:
 - Select *Admin* to allow the partition user the ability to make edits to the partition.
 - Select *User* to restrict the partition user so that they can only arm and disarm the partition without being able manage users.
11. Click *ADD PARTITION ACCESS*.

The partition administrator or user will now appear in the System Users list and an email will be sent inviting them to register. By hovering over the partition administrator or user's name, the following actions can be performed:

- Resend the registration email.
- Reset the password by generating a password to the dealer user.
- Edit the fields setup in the add user process.
- Remove the user from the System Users list.

5.3 Set Abort Window

Note: The procedure can only be performed in maintenance mode. To activate maintenance mode, see section 3.3, “Enter/Exit Maintenance Mode” on page 15.

The abort window determines the period during which an alarm will not be transmitted to the central station if it is cleared before the window expires.

To set the abort window:

1. In the sidebar menu, click on *Settings*.
2. Click *Update* under System Configuration.
3. Select a value of up to 45 seconds.
4. Click *UPDATE SYSTEM SETTINGS*.

5.4 Enable/Disable Exit Delay Restart

Note: The procedure can only be performed in maintenance mode. To activate maintenance mode, see section 3.3, “Enter/Exit Maintenance Mode” on page 15.

When exit delay restart is enabled, a zone triggered during an exit delay will restart the countdown from the beginning. Exit delay restart is enabled by default.

To enable/disable exit delay restart:

1. In the sidebar menu, click on *Settings*.
2. Click *Update* under System Configuration.
3. Use the toggle to enable/disable exit delay restart.

4. Click *UPDATE SYSTEM SETTINGS*.

5.5 Enter/Cancel Test Mode

Note: The procedure can only be performed in maintenance mode. To activate maintenance mode, see section 3.3, “Enter/Exit Maintenance Mode” on page 15.

When in test mode, the system will behave normally, but will not send alarms to the central station. This allows each zone to be alarmed to ensure an appropriate response.

To put the system into test mode:

1. In the sidebar menu, click on *Partitions*.
2. Use the Test Mode toggle to activate test mode.
3. When testing is complete, use the Test Mode toggle to deactivate test mode.
 - Test mode will run for 60 minutes; a timer will appear on the touchpad indicating the time left.
 - Test mode can be canceled at any time by returning to this page and clicking *EXIT TEST MODE*.

5.6 Access Activity Logs

The activity logs are primarily used for troubleshooting. All activity in the system will be captured here, including any configuration changes, alarms and faults by zone, and arms and disarms.

To access the activity log, click on *Activity Logs* in the sidebar menu.

By default, activity logs are displayed in order of occurrence. There are three filters that can be used to sort the activity logs — by activity category, partition, and/or by specific date range — as well as a search bar to search for specific activity.

5.7 View Overview Page

The overview page allows viewing of configured partitions, zones, devices and activity log from a central location. The overview page can be accessed from the sidebar menu.

5.8 Reset E-Fuse

In the event of lightning strike or malfunction, resetting the e-fuse restore functionality to devices connected to all buses, including notification appliances, wired zones connected to the onboard hardwired zone expander and other devices, such as touchpads. To reset the e-fuse:

1. Click *Overview*.
2. Click *RESET E-FUSE*.
3. Confirm by clicking *YES*.
4. When the Reset E-Fuse confirmation screen, click *CLOSE*.

Chapter 6

Zone Type Behavior

6.1 Introduction

Note: All Inovonics wireless models referenced in this chapter are UL Listed.

The zone type behavior defines how the panel interprets activity from the sensor connected to that zone.

6.2 Entry/Exit and Entry/Exit Extended

Entry/exit provides entry delay whenever the zone is faulted while the interior and/or exterior zones are armed. It provides an exit delay whenever the control panel is armed in any arming mode except instant.

Entry/exit extended operates in the same manner as entry/exit, but provides a different set of entry/exit delay times and should be assigned to zones that require a longer delay to enter or exit the premises (e.g., a garage, loading dock, etc.).

Note: Entry and exit delays are programmable as shown in section 4.2, “Add Partition” on page 20.

Default characteristics:

State	Hardwired Zone
Response to open when armed all	Alarm after delay.
Response to short when armed all	Alarm after delay.
Response to open when armed perimeter only	Alarm after delay.
Response to short when armed perimeter only	Alarm after delay.
Response to open when disarmed	Fault.
Response to short when disarmed	Fault.
Keypad sound	Burglary.
Bell sound	Burglary.
Inovonics wireless models that participate	EN1215EOL, EN1215WEOL.

6.2.1 Programming Options (Default in Parentheses):

- Allow to bypass: (Yes) / No.
- Limit alarm reports, per zone, per arming cycle: (Yes) / No.
- Swinger suppression: Yes / (No); if yes, select one through ten.
- Chime enable: Yes / (No); if yes, choose from chime one through five.
- Send activity events to ICS/CMC: Yes / (No).
 - If Yes, additional charges may apply.

6.3 Perimeter/Instant

Provides an instant alarm if the zone is faulted and the system is armed in any mode. Assign this zone type to all exterior doors and windows.

Default characteristics:

Response to open when armed all	Alarm after delay.
Response to short when armed all	Alarm after delay.
Response to open when armed perimeter only	Alarm after delay.
Response to short when armed perimeter only	Alarm after delay.
Response to open when disarmed	Fault.
Response to short when disarmed	Fault.
Keypad sound	Burglary.
Bell sound	Burglary.
Inovonics wireless models that participate	EN1215EOL, EN1215WEOL.

6.3.1 Programming Options (Default in Parentheses):

- Allow to bypass: (Yes) / No.
- Limit alarm reports, per zone, per arming cycle: (Yes) / No.
- Swinger suppression: Yes / (No); if yes, select one through ten.
- Chime enable: Yes / (No); if yes, choose from chime one through five.

6.4 Interior/Follower

Provides a delayed alarm (using the programmed entry delay time) if an entry/exit zone is faulted first. Otherwise, it produces an instant alarm. It is active when interior zones are armed.

Assign this zone type to a zone covering an area such as a foyer, lobby, or hallway through which one must pass to and from the keypad upon entry or exit.

Default characteristics:

Response to open when armed all	Alarm after delay if entry zone violated first; otherwise instant alarm.
Response to short when armed all	Alarm after delay if entry zone violated first; otherwise instant alarm.
Response to open when armed perimeter only	Fault.
Response to short when armed perimeter only	Fault.
Response to open when disarmed	Fault
Response to short when disarmed	Fault
Keypad sound	Burglary
Bell sound	Burglary
Inovonics wireless models that participate	EN1261HT.

6.4.1 Programming Options (Default in Parentheses):

- Allow to bypass: (Yes) / No.
- Limit alarm reports, per zone, per arming cycle: (Yes) / No.
- Swinger suppression: Yes / (No); if yes, select one through ten.
- Follow entry/exit delay time: (1) / 2; programmable in partition-specific options.

6.5 Trouble While Disarmed/Alarm While Armed

Provides an instant alarm if the zone is faulted and the system is armed in any mode. During the disarmed state, the system annunciates a latched trouble sounding from the keypad, and sends a central station report, if desired.

Assign this zone type to a rear door in a store, or to a zone covering a sensitive area such as a stock room or drug supply room. It can also be used in an area where immediate notification of an entry is desired, such as on a vault vibration sensor.

Default characteristics:

State	Hardwired Zone
Response to open when armed all	Alarm.
Response to short when armed all	Alarm.
Response to open when armed perimeter only	Alarm.
Response to short when armed perimeter only	Alarm.
Response to open when disarmed	Trouble.
Response to short when disarmed	Trouble.
Keypad sound	Alarm when armed; trouble when disarmed.
Bell sound	Alarm when armed; none when disarmed.
Inovonics wireless models that participate	EN1249.

6.5.1 Programming Options (Default in Parentheses):

- Limit alarm reports, per zone, per arming cycle: (Yes) / No.
- Swinger suppression: Yes / (No); if yes, select one through ten.
- Send activity events to ICS/CMC: Yes / (No).
 - If Yes, additional charges may apply.
- Report to CMS when disarmed: Yes / (No).

6.6 24-Hour Silent

Sends a report to the central station but provides no keypad display or sounding. Assign this zone type to a zone containing a duress button. Zone type cannot be bypassed.

Default characteristics:

State	Hardwired Zone
Response to open when armed all	Alarm.
Response to short when armed all	Alarm.
Response to open when armed perimeter only	Alarm.
Response to short when armed perimeter only	Alarm.
Response to open when disarmed	Alarm.
Response to short when disarmed	Alarm.
Keypad sound	None.
Bell sound	None.
Inovonics wireless models that participate	EN1223D, EN1235SF, EN1235DF, EN1249.

6.7 24-Hour Audible

Sends a report to the central station and provides an alarm sound at the keypad and an audible external alarm. Assign this zone type to a zone containing a duress button. Zone type cannot be bypassed.

Default characteristics:

State	Hardwired Zone
Response to open when armed all	Alarm.
Response to short when armed all	Alarm.
Response to open when armed perimeter only	Alarm.
Response to short when armed perimeter only	Alarm.
Response to open when disarmed	Alarm.
Response to short when disarmed	Alarm.
Keypad sound	Burglary.
Bell sound	Burglary.
Inovonics wireless models that participate	EN1223D, EN1235SF, EN1235DF, EN1249.

6.8 24-Hour Auxiliary

Sends a report to the central station and provides an alarm sound at the keypad only. No other notification appliance circuit is activated. Assign this zone type to non-critical monitoring functions. Zone type cannot be bypassed.

Default characteristics:

State	Hardwired Zone
Response to open when armed all	Alarm.
Response to short when armed all	Alarm.
Response to open when armed perimeter only	Alarm.
Response to short when armed perimeter only	Alarm.
Response to open when disarmed	Alarm.
Response to short when disarmed	Alarm.
Keypad sound	Trouble.
Bell sound	None.
Inovonics wireless models that participate	EN1223D, EN1235SF, EN1235DF, EN1249.

Chapter 7

Quick Reference

7.1 Quick Reference Chart

This quick reference chart lists the programming location and testing procedure for each ANSI/SIA CP-01:2019 False Alarm Reduction feature implemented by the Inovonics Intrusion System. Features not implemented by the system are not included.

The following programming options are available:

Function	Section
Add an account	2.2.1, "Add Account" on page 11
Add a central station	3.7, "Add Central Station" on page 18
Add a dealer user	5.1.1, "Add Dealer User" on page 29
Add a panel	3.2, "Add Panel" on page 14
Add a partition	4.2, "Add Partition" on page 20
Add a partition administrator or user	5.2.2, "Add Partition User or Administrator" on page 32
Add a repeater	4.6, "Add Repeater" on page 24
Add a sounder	3.6, "Add Sounders" on page 17
Add a sub-account	4.1, "Add Sub-Account" on page 19
Add a system	3.1, "Add System" on page 13
Add a system administrator	5.2.1, "Add System Administrator" on page 31
Add a touchpad	4.3, "Add Touchpad" on page 21
Add a wired zone	4.8, "Add Wired Zone" on page 27
Add a wireless zone	4.7, "Add Wireless Zone" on page 25

Function	Section
Adjust entry/exit delay	4.2, "Add Partition" on page 20
Enter/exit maintenance mode	3.3.1, "Enter Maintenance Mode" on page 15
Configure hardwired zone modules	3.5, "Configure Onboard Hardwired Zone Module" on page 16
Configure panel's Wifi and Ethernet connections	4.3.2, "Configure Panel Connectivity" on page 22
Configure touchpad's WiFi connection	4.3.1, "Configure Touchpad Wi-Fi" on page 22
Enable or disable a cross zone in a wired zone	4.8, "Add Wired Zone" on page 27
Enable or disable a cross zone in a wireless zone	4.7, "Add Wireless Zone" on page 25
Enable or disable an abort window in a wired zone	4.8, "Add Wired Zone" on page 27
Enable or disable an abort window in a wireless zone	4.7, "Add Wireless Zone" on page 25
Enable or disable an exit delay restart	5.4, "Enable/Disable Exit Delay Restart" on page 33
Enable or disable swinger suppression in a wired zone	4.8, "Add Wired Zone" on page 27
Enable or disable swinger suppression in a wireless zone	4.7, "Add Wireless Zone" on page 25
Enable or disable the panel's Wi-Fi, Ethernet or cellular connection	4.5.1, "Enable/Disable Network Connectivity" on page 23
Enter or cancel test mode	5.5, "Enter/Cancel Test Mode" on page 34
Grant or edit access to a dealer user	5.1.2, "Grant/Edit Access to Dealer User" on page 30
Set an abort window	5.3, "Set Abort Window" on page 33
Set panel Wi-Fi/Ethernet/cellular connection priority	4.5.2, "Configure Network Priority" on page 24
Update panel firmware	3.4, "Update Gateway Mark II Firmware" on page 15
Update touchpad software	4.4, "Update Touchpad Software" on page 22
View activity logs	5.6, "Access Activity Logs" on page 34