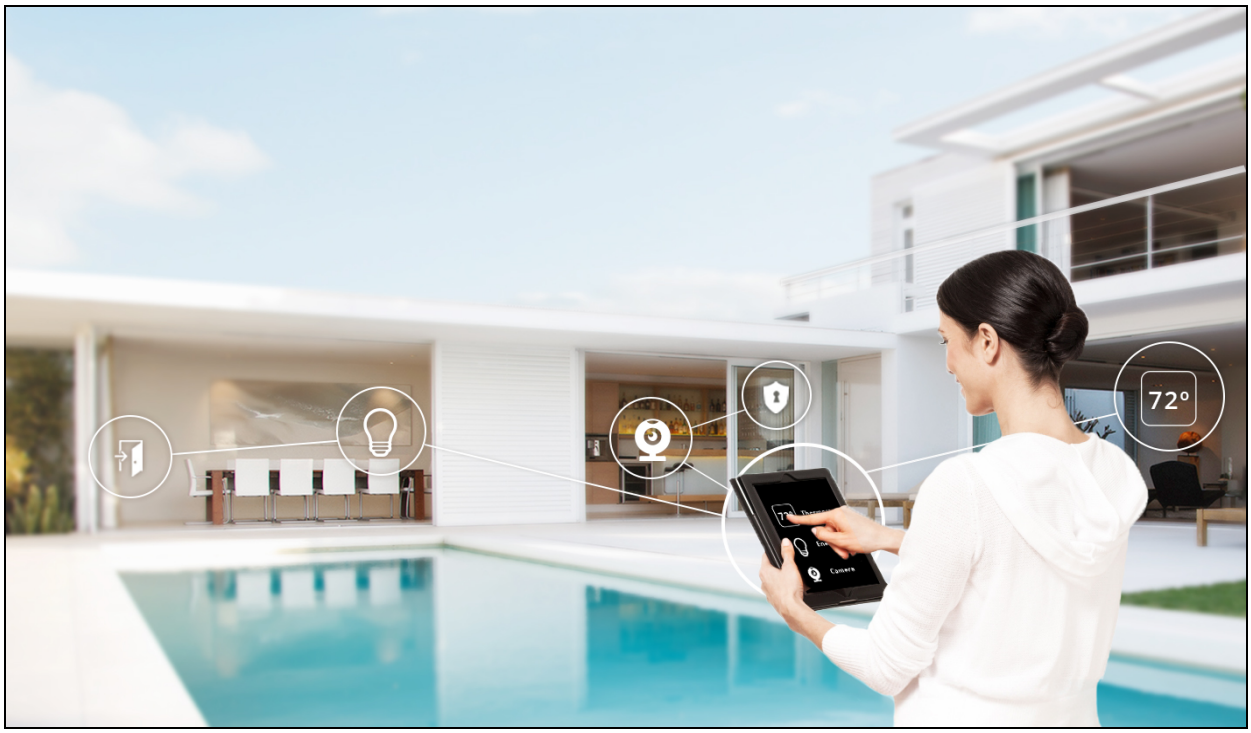
icontrol NETWORKS

Converge Feature Guide

7.3 Quadra



Document Information

Release version: 7.3 Quadra
Document name: Converge Feature Guide
Build date: 9/7/2016

Contents

Revision History

Release	Revisions
7.3 Quadra v2	Added the appendix Compliances on page 24
7.3 Quadra v1	Initial version

1 Welcome to Converge

The Converge platform allows subscribers to secure and monitor their home and control devices from anywhere with an Internet connection. For example, with the Converge touchscreen and Converge-compatible devices, the subscriber can:

- Arm and monitor the home for intruders when everyone is away
- Take video or snapshots of the home
- Turn lights on and off. If the light is dimmable, set the level of brightness
- Set the temperature in the home

In addition, the subscriber can create automations that tell the system what to do at certain times or when certain events happen (or don't happen). For example, the subscriber can create an automation that:

- Turns on lights every evening at 8:00 PM while the subscriber is on vacation
- Sends a text whenever the front door opens while everyone is away from home
- Sends an email if the front door is not opened on weekdays at the time children are expected to come home from school

This guide provides an overview of all the features available to the subscriber. It is not a comprehensive, step-by-step guide. It is up to the service provider to create a customized guide for its subscribers.

2 Signing In to User Interfaces

The Icontrol browser and apps give the user the ability to use many of the functions available via the touchscreen while being away from the touchscreen. The user must sign in to his Converge account each time the user accesses the account via the browser or apps.

1. To sign in for the first time, the user uses the link, username, and password provided by the service provider.
2. The user is prompted to change the username and password to use in subsequent logins.
    - If the user does not complete the process, depending on when it is aborted, the new username and password are not be saved and the user needs the original username and password provided by the service provider.
    - The username and password provided by the service provider are valid for two weeks. If the user has not activated within that timeframe, a new username and password must be issued.

2.1 Failed Sign-In Attempts

The user is allowed five unsuccessful sign-in attempts before being locked out for 30 minutes. Within that timeframe, even a valid username and password combination will fail. If this happens, a message is displayed informing the user that the account has been locked and the user can not sign in for 30 minutes. These settings can be customized by editing the server properties:

- `subscriberPortal.login.max.retry`
- `subscriberPortal.login.lockTime`

See the "Properties" section in *System Operations Guide*.

2.2 Forgotten Username or Password

If the user has forgotten the username or password for the account, the link on the Sign In page can be used to begin the process of retrieving the username or resetting the password.

3 Arming/Disarming the Security System

The Converge system consists of a touchscreen, security sensors, optional cameras, and a remote user interface, such as a browser or app. Each security sensor paired with the touchscreen is assigned a zone function at the time of installation. The zone function indicates how the touchscreen should interpret the signals from the sensor when it is armed or disarmed. The system can be armed in the following modes:

- Arm Away
- Arm Stay
- Arm Night

The system is armed and disarmed in the same manner regardless of the mode. The user can arm the system via the touchscreen, the browser, or apps using a valid keypad code. Regardless of the user interface used to arm the system, if the user is leaving the premises, the user must leave during the exit delay period using the entry/exit door or disarm the system to prevent generating an alarm. The exit delay is the period of time after the user arms the system and the system is armed. If the entry/exit door remains faulted when the exit delay expires, an alarm is generated. To enter the premises, the user must use an entry/exit door and enter the correct keypad code using any user interface to disarm the system before the entry delay period expires. The entry delay begins when the entry/exit door is faulted, and an alarm is generated when the time expires and a valid keypad code is not entered.

When an alarm is generated, the touchscreen emits an audible alarm; however, the central monitoring station is not notified immediately. The period of time after the alarm is generated and when the system notifies the central monitoring station is the alarm transmission delay. The user can still enter a valid keypad code to disarm the system during this time and cancel the alarm. When the alarm transmission delay ends, the system notifies the central monitoring station. The user can disarm the system at any time, however once the central monitoring station receives the alarm transmission, the operator will attempt to contact the user to verify the alarm or dispatch authorities. For more information, see the section "Disarming the System & Understanding What Happens During an Alarm" in *Converge User Guide*.

Note: If the system is in the entry delay and the server loses all connectivity with the touchscreen, the system assumes an intruder has attempted to defeat the security system by destroying the touchscreen. For more information, see the "Understanding Smash & Grab" section in *System Operations Guide*.

Note: The service provider can configure the system so that the operator can attempt to contact the user through the touchscreen using two-way voice calling. If this is implemented, a series of ring tones sounds and then the voice of a monitoring operator comes through the touchscreen speaker. A dialog box is also displayed on the screen, alerting the user that a call is in progress on the touchscreen. For more information, see: https://share-icontrol.atlassian.net/wiki/display/CSKB/Touchscreen+Two-Way+Voice

IMPORTANT: Smoke alarms are reported without an alarm transmission delay or an entry delay

For more information on zone functions and arming modes, see Security Zones and Arming Modes on page 19.

3.1 System Status Headers

The status of the system is displayed on the touchscreen, the browser, and apps on two headers: the security status header and the trouble header.

The security status header indicates whether the system is armed, disarmed, or in alarm, it displays the countdown of the entry and exit delays, and it displays the name of the zone when a security sensor is faulted. Clicking on the security status header opens up the arming/disarming screen.

The trouble header displays troubles encountered by the system and paired devices. Clicking or tapping on the header displays additional information about the trouble(s).

3.2 Troubles

The troubles reported depend on the device and can include:

- Loss of connectivity
- Low battery
- Tampering

If a security sensor is reporting a trouble, it prevents the user from arming the system. If the trouble can not be remedied before the user wants to arm the system, the zone can be "turned off", or bypassed. When a zone is turned off, the zone events are still reported to the touchscreen, but they do not generate an alarm. The sensor remains turned off for the duration the system is armed. Once the system is disarmed, the sensor is "turned on". The user may turn the sensor off again after disarming. For more information, see the "System & Zone Trouble Header" section in *Converge User Guide*.

IMPORTANT: Zones for smoke, carbon monoxide, and water detectors can not be turned off.

See Troubleshooting on page 22 for more information.

4 Managing Keypad Codes

Keypad codes are used to arm and disarm the system from the touchscreen, the browser, or apps. The Master keypad code is set during the installation of the security system, and the Duress code is added by default, but is not set. The user can create multiple keypad codes, but only the Master keypad code can be used to access the system settings.

The Master keypad code is required when creating, editing, and deleting keypad codes. The Master and Duress codes can be modified, but not deleted. Each keypad code is assigned a name, the arming level, a unique four-digit code, and the days of the week the code is active. The arming levels are:

- **Master**: Only the Master keypad code can have this level. The keypad code can be used to arm and disarm the system and to create, edit, and delete keypad codes.
- **Duress**: Only the Duress keypad code can have this level. The keypad code can be used to arm and disarm the system, but the touchscreen generates a silent alarm and notifies the central monitoring station.
- **Arm/Disarm**: The keypad code can be used to arm and disarm the system (available on Mobile and Web Apps only).
- **Standard**: The keypad code can be used to arm and disarm the system (available on touchscreen and legacy Subscriber Portal only).
- **Guest**: The keypad code can be used to arm and disarm the system (available on touchscreen and legacy Subscriber Portal only).
- **Arm Only**: The keypad code can only be used to arm the system.

Note: A keypad code added via the Mobile and Web Apps with the "Arm/Disarm" arming level is displayed with the "Standard" arming level on the touchscreen. A keypad code added via the touchscreen with "Standard" or "Guest" arming level is displayed with the "Arm/Disarm" arming level on the Mobile and Web Apps.

The Master and Duress codes are set to be active every day by default and can not be modified. The keypad codes added by the user can be set to be active every day or only on certain days. For example, a keypad code can be created to enable a cleaning service to arm and disarm the system only on Wednesdays. The code would be detected as invalid on any other day.

5 Monitoring Sensors and Environmental Devices

A maximum of 64 ZigBee devices are supported on Converge. This includes security sensors and environmental devices (up to four thermostats). It is up to the service provider to determine which devices are available to the subscriber, however the user interfaces delivered by Icontrol include all the device types supported by Icontrol. See https://share-icontrol.atlassian.net/wiki/display/CDA/Icontrol+Certified for more information on supported devices.

The following device types and actions are supported:

- Carbon monoxide detectors: monitor
- Cloud devices: monitor and control
- Door locks: monitor, lock, and unlock
- Door/window sensors: monitor
- Glass break sensors: monitor
- Lighting modules: monitor, turn on, turn off, and dim (if the device is capable)
- Motion sensors: monitor
- Smoke detectors: monitor
- Thermostats: monitor, set mode, and set temperature
- Water/flood sensors: monitor

IMPORTANT: If a device that is paired with the touchscreen is not displayed on the Mobile or Web App, the device may have been previously configured with another touchscreen and was not properly deleted from the touchscreen. The device must be deleted from the current touchscreen and another added.

Turning a Device On and Off

The user can "turn off", or bypass, a sensor so that the system does not report when the sensor is faulted or restored/cleared. Automations using a sensor that has been turned off do not execute. This is useful when a sensor is reporting too many events, such as a door opening and closing frequently due to a special event at the premises.

IMPORTANT: Zones for smoke, carbon monoxide, and water detectors can not be turned off.

6 Viewing Pictures and Videos

Viewing Live Video

The user can view live video from the camera on the browser and apps. If the user has more than one camera, they are displayed as thumbnail images and the image is updated every five seconds. When the user selects a camera, it is displayed on the live video screen.

IMPORTANT: Adobe Flash Player 14 or newer is required for viewing video.

Note: If the subscriber has both HD and VGA cameras, the HD cameras are displayed in 16:9 aspect ratio and the VGA cameras are displayed in 4:3 aspect ratio. The thumbnail images for VGA cameras may be "letter-boxed".

Viewing Saved Pictures and Video

Pictures and videos can be generated by:

- The user from the live video screen on the browser and apps
- Automations set to take a picture or video in response to an event or schedule
- An alarm (pictures only)

Only one picture is taken when the user takes a picture from the live video screen. Five pictures are taken when it is in response to an automation or an alarm. Video is saved in 15-second clips when it is triggered by the user or an automation.

Thumbnail images of the picture(s) and video(s) are displayed once the camera is done capturing the picture or video clip and are available for viewing, saving locally, and deleting. These pictures and video clips reside on the service provider's server and can only be accessed by logging on to the subscriber's account via the browser or apps. Saving the picture(s) or video(s) locally does not delete them from the service provider's server. The user must manually delete any pictures and video clips that are no longer needed via the browser or apps.

IMPORTANT: If the user saves pictures or videos to a local device, they are no longer secured by Icontrol.

7 Cameras with Motion Detection Capability

Some cameras are designed with integrated motion detection. The camera's sensitivity to detect motion can be modified at any time via the touchscreen, browser, and apps. The options are:

- **Off** - the camera does not report motion detection
- **Low** - the camera ignores most motion detected; i.e. medium pets, small children
- **Medium** - the camera ignores some motion detected; i.e. small pets
- **High** - the camera reports all motion detected

Once the touchscreen receives a motion event, there is a blackout period where the touchscreen does not acknowledge additional motion events from the camera that reported the first event. The default setting of the blackout period is three minutes. During this blackout period, live video can still be viewed and recorded. If another motion event is received immediately after the blackout period from that same camera, a new blackout period begins. This is designed to prevent overloading the network and servers.

Changes to the camera motion detection setting take effect immediately if the camera is not within the blackout period. If the setting was changed during the blackout period, the change will take effect once the blackout period expires.

8 Event History

The user can view all the events captured by the system from the Activity screen on the browser and apps. In addition to viewing the events by date, filters are available to narrow down the events displayed:

Filter	Description
All activity	Lists all recent events
Alarms	Lists the zone that generated an alarm
Camera Motion	Lists the events reported by cameras with motion detection enabled
Door Locks	Lists the lock and unlock events from door locks
Pictures/Videos	Lists the pictures and videos taken from the system, whether triggered by an alarm, an automation, or taken manually
Security System/System	Lists the arm, disarm, entry delay, and exit delay events
Troubles	Lists the troubles the system or devices have reported
Zones/Sensors	Lists the events reported by zones/sensors **Note:** Non-security events from motion detectors are not displayed

9 Managing Contacts

Contacts are listed in Converge's Trusted Circle as "call before police in emergency", "call after police in emergency", and "non-emergency contacts". The Trusted Circle can only be accessed via the browser and apps. The account email and phone number are listed in the Trusted Circle by default. The user can edit the information, but it can not be deleted. The user can add additional contacts to the Trusted Circle. The additional contacts are not associated with the account at the service provider and do not have access to the account.

Call Before Police in Emergency Contacts

The contacts listed under "call before police in emergency" are those that the user added when setting up the account with the service provider. These contacts are the persons the central monitoring station calls to verify the alarm before calling the authorities. These contacts can be modified, but cannot be deleted. By default, two contacts must be listed under "call before police in emergency".

Call After Police In Emergency Contacts

The contacts listed under "call after police in emergency" are optional. These contacts are the persons the central monitoring station calls to notify them of the alarm after calling the authorities. By default, the user can add a maximum of two contacts under "call after police in emergency", and they can be edited and deleted by the user.

Non-Emergency Contacts

The contacts listed under "non-emergency contacts" are for notification of automations only. The user selects one or more contacts listed as "non-emergency contacts" when creating an automation to send an email or a text message. For example, the user can add an adult who lives nearby to "non-emergency contacts" and select that contact in an automation that triggers when Converge is armed away and the user is out of town. Icontrol has not set a limit to the number of contacts a user can add as "non-emergency contacts". Service providers must consult with data center and database administrators to determine limitations, if any.

10 Automations

Automations allow the subscriber to define how Converge responds to events reported by sensors. They also allow the subscriber to control non-sensor devices, such as cameras, lights, and thermostats. Automations can only be created, viewed, and managed via the browser and apps.

Example automations include:

- Take a picture from my front door camera when Converge is armed away and the front door opens
- Send an email when any sensor reports a trouble
- Turn the front porch light on every night at 9 PM and off every morning at 6 AM

10.1 Types of Automations

There are two basic types of automations a user can create. Icontrol has not set a limit to the number of automations a subscriber can create. Service providers must consult with datacenter and database administrators to determine limitations, if any.

Type	Description
Scheduled Event	An action that should occur at a specified day and time, or range of days and times, and while a specified mode is set, regardless of other events.
Event	The automation executes when the specified event occurs during the specified day and time, or range of days and times, and while a specified mode is set.

10.2 Automation Actions

The purpose of an automation is to have the system perform an action under specific circumstances. To have multiple actions occur for the same event, multiple automations must be created. The table below lists all the actions that can occur when the desired time and/or event is detected.

Action	Description
Arm System	Arm the system in the selected mode (no keypad code required).
Disarm System	Disarm the system (no keypad code required).
Send Email	Send an email notification to the email address(es) in the subscriber's Trusted Circle with a description of the automation triggered. **Note:** It is up to the service provider to allow whether a picture or video can be attached to the email message.
Send Text Message	Send an SMS notification to the phone number(s) in the subscriber's Trusted Circle with a description of the automation triggered. **Note:** It is up to the service provider to allow whether a picture or video can be attached to the SMS message.
Take Picture	The selected camera takes five pictures in quick succession. The pictures are available under event history.
Take Video Clip	The selected camera takes a 15 second video clip. The video clip is available under event history.
Play Sound	Play the selected sound from the touchscreen.
Turn on/Turn off Light	Turn the selected light(s) on or off.
Set Thermostat to Cool	Have the thermostat cool the premises to the specified temperature.
Set Thermostat to Heat	Have the thermostat heat the premises to the specified temperature.
Turn Thermostat Off	Turn the thermostat off so that it is not maintaining the premises temperature.
Lock/Unlock a Door Lock	Lock or unlock the selected door lock.

10.3 Default Automations

The following automations are created by default.

Default Automation	Description	Created When
Alarm Alert via Email and Text Message	If the system goes into alarm, an email and text message is sent to the contacts listed under "non-emergency contacts" in the Trusted Circle. **Note:** This automation can not be turned off or deleted. Only the contact information can be edited.	The touchscreen is activated (see note below)
Security System Armed, Send Email	Send an email to the contacts listed under "non-emergency contacts" in the Trusted Circle when the system is armed in any mode.	
Security System Disarmed, Send Email	Send an email to the contacts listed under "non-emergency contacts" in the Trusted Circle when the system is disarmed.	

Note: The default automations created by the server when a touchscreen is first activated vary slightly by Tier. All three are created for accounts in Gold and Silver tiers, but only the "Alarm Alert via Email and Text Message" automation is created for accounts in the Bronze tier. For more information on tiers, see the "Understanding Tiers, Tier Properties, and Packages" section in *Management Portal Guide*.

10.4 Creating Automations

The automations wizard guides the user in creating automations. The steps differ slightly depending on the automation type, device, and desired action, but the basic steps are:

- **When My** device/system

  This device/system is called the "trigger". If there is more than one device per category, the subscriber can only pick one device to use as a trigger per automation.

- **Reports** an event

  The list of expected events depends on the device selected as the trigger. Only one event per automation is supported.

  For some devices, there is a "non-event" option. This option sets the automation to expect an event to occur at a certain time/day and triggers if it **does not** occur by the end of the time range specified. For example, for the automation "When my front door sensor does not report 'open', text me, every weekday between 3:00 PM and 3:30 PM and the system is armed 'Away'", if the system detects the front door sensor reporting "open" between 3:00 PM and 3:30 PM during the week and the system is armed "Away", it does not send a text message. If by 3:30 PM the system has not detected an "open" event, it sends a text message to the contact(s) specified in the automation.

- **Do This** action

  The actions available depend on the devices paired to the system; i.e., send email, take picture.

- **On** this day

  The options available are Sunday through Saturday and every day.

- **During** these times

  The subscriber must select a start and end time that the system should react to the trigger.

- **And Home Security Mode Is Set**

  The mode can be any mode, armed, or disarmed.

10.5 Modifying Automations

Once created, the automations can be edited, "turned off", or deleted, except for the default "Alarm Alert via Email and Text Message" automation. The automations wizard guides the user when editing the automation. All the items in the automation can be modified when editing the automation.

When an automation is "turned off", the automation is disabled and it does not run when the system detects the trigger. Deleting an automation removes it completely from the system and the action can not be reversed. A new automation would need to be created. Turning the automation off, back on, or deleting it takes effect immediately. Turning off or deleting the automation does not affect the functionality of the sensor.

10.6 Thermostat Scheduler

Users can manually set the temperature of the thermostat(s) or set up a schedule that maintains the desired temperatures. If the subscriber has more than one thermostat, each thermostat must have its own schedule.

By default, there are four times in each day that the system can adjust the thermostat. The user can change the times to meet the needs of the premises on a daily basis.

For example, while on cool mode on weekdays:

- Set temperature at 74 degrees at 6:00 AM when everyone is expected to wake up
- Set temperature at 86 degrees at 9:00 AM after everyone has left the house
- Set temperature at 75 degrees at 3:30 PM when the children return from school
- Set temperature at 78 degrees at 10:00 PM when everyone is going to bed

The schedule can be edited at any time. When the schedule is edited, the changes do not take effect until the next scheduled time. Using the example above, if the schedule was edited so that the temperature is set to 83 degrees at 8:00 AM and it is currently 9:15 AM, the thermostat remains at 86 degrees. It will be set to 83 degrees at 8:00 AM the next weekday.

The thermostat schedule can also be disabled, leaving the thermostat at the last set mode and temperature. It does not turn the thermostat off. The thermostat can still accept manual commands at the thermostat, the touchscreen, and via the browser and apps.

11 Touchscreen Apps

Touchscreen apps are third-party software applications installed on the touchscreen. Service providers determine the apps available to the subscribers via the Management Portal. See the "Managing Apps (Converge Only)" section in *Management Portal Guide* for more information.

From the browser interface, the user can view, install, delete, and reposition apps on the touchscreen. The app may be configurable from the browser, however most are only configurable from the touchscreen; i.e., setting location and account preferences. For more information, see the "Managing Touchscreen Apps" section in *Converge User Guide*.

IMPORTANT: The Security, Settings, Cameras, Lights, and Thermostats apps are native to the touchscreen and can not be deleted or repositioned.

12 Managing Account Information

The user can access some of the account information from the browser and apps, such as username, address, timezone and quotas. The user can change the username and password, however the account address, timezone, and quotas are for informational purposes only.

Note: It is up to the service provider to allow the user to change the username and password. If the service provider requires that the username or password must be changed via another method, they will be displayed for informational purposes only.

12.1 Change Username

The username for the account must be 20 characters or less. By default, it can contain numbers (0-9), English uppercase and lowercase letters (a-z, A-Z), as well as the following non-English characters:

Ä, ä, É, é, Ö, ö, Ü, ü, ß, À, à, Â, â, Æ, æ, Ç, ç, È, è, Ê, ê, Ë, ë, Î, î, Ï, ï, Ô, ô, Œ, œ, Ù, ù, Û, û, Í, í, Ò, ò, Ó, ó, Ú, ú, Ñ, ñ, ¿, ¡

The following special characters are also supported:

! . # $ % ' * + - ? ^ _ ` { | } & / = ~

Spaces cannot be used in a username, and usernames are not case-sensitive.

12.2 Change Password

The account password must be 20 characters or less and can contain any character, and passwords are case-sensitive.

12.3 Quotas

The account quotas are displayed so the user can manage usage. These quotas are set by the service provider via the Management Portal. The quotas displayed are:

- Pictures saved per day
- Videos saved per day
- SMS messages sent per day

The quotas are refreshed daily. When a quota is met, the system will stop processing the action for the rest of the day. Increasing the quota for the account allows the action(s) to continue, but deleting pictures or videos does not clear the quota.

12.4 Managing the Security Secret Word

The security secret word (also known as the central station passcode) is used in alarm situations when the central monitoring station calls the emergency contact(s) to verify an alarm. It validates that the person answering the telephone is authorized to take the call.

The secret word can be set when the account is created or during installation of the security system. The user can modify the secret word via the touchscreen, browser, or apps. The user must provide the Master keypad code to view or modify the secret word.

12.5 Managing the Alarm Ordinance and Permit Registration

Some accounts may require a permit for the security system. The account is flagged as requiring a permit when it is created, but the Alarm Permit Number and expiration date are added via the browser or apps after account activation is complete.

Appendix A: Security Zones and Arming Modes

The system uses the arming mode to determine how to react to events sent by the sensors. Depending on the arming mode, the system can delay sending an alarm and wait for the user to disarm, trigger an alarm immediately, report a trouble, or take no action when it receives an event. At least one door is set as an entry/exit zone when the system is installed. This is usually the door the user most frequently uses to enter and exit the premises. Entry and exit delays are associated with the sensors assigned to entry/exit zones. The delays allow the user to enter or exit the premises without triggering the alarm. See Arming/Disarming the Security System on page 7 for more information.

A.1 Security Zone Functions

The sensors are assigned a type when the sensor is paired with the touchscreen via the installer menu. The subscriber can view the sensor type, label, and events, but can not view or change the zone function of the sensors. The following is a list of the supported zone functions:

Zone Function	Description	Sensor
Entry/Exit	Used to monitor doorways from which users enter and exit the premises. Depending on how the system is armed, faulting this sensor generates an audible alarm.	Door/Window
Perimeter	Used to monitor windows or doorways that are not used to enter or exit an armed premises. Faulting this sensor generates an audible alarm immediately.	Door/Window Glass Break Detector
24-Hour Inform	Used in areas that need monitoring, but faulting the sensor does not generate an alarm if the system is armed.	Door/Window Glass Break Detector Motion Detector Water Detector
Trouble Day/Alarm Night	Used on doors or windows that need monitoring only when the system is Armed Night. It generates an alarm if the sensor is faulted or tampered when the system is Armed Night.	Door/Window
Silent 24-Hour	Used in areas that need monitoring and generates an alarm if the sensor is faulted, whether the system is armed or disarmed, but there is no sound from the touchscreen, keypad(s), or siren to indicate the alarm has been generated.	Door/Window
Audible 24-Hour	Used in areas that need monitoring and generates an audible alarm if the sensor is faulted, whether the system is armed or dis-armed.	Door/Window Carbon Monoxide Detector Water Detector

Zone Function	Description	Sensor
Interior Follower	Used to monitor large areas inside the premises. Depending on how the system is armed, faulting this sensor generates an audible alarm.	Motion Detector
Interior with Delay	Used to monitor areas near entry and exit points. Depending on how the system is armed, faulting this sensor generates an audible alarm.	Motion Detector
Interior Follower Arm Night	Used to monitor large areas inside the premises. Depending on how the system is armed, faulting this sensor generates an audible alarm.	Motion Detector
Interior Delay Arm Night	Used to monitor large areas inside the premises. Depending on how the system is armed, faulting this sensor generates an audible alarm.	Motion Detector
Fire 24-Hour	Used only for smoke detectors and generates an audible alarm when smoke is detected, whether the system is armed or dis-armed.	Smoke Detector

A.2 Arm Away Mode

The Arm Away mode is used when everyone leaves the premises. The following rules apply:

- Exit delay starts when the user enters the correct key code to arm the system.
- An alarm is generated immediately when a monitored zone (non-entry/exit door or window) is faulted.
- The entry delay starts when an entry/exit zone or an interior follower with delay zone is faulted.
- An alarm is generated if the system is not disarmed before the entry delay expires.

During the Arm Away entry and exit delays:

- The touchscreen beeps once per second during the entry and exit delays. During the last ten seconds of the entry and exit delays, the touchscreen beeps twice per second until it expires.
- A timer displayed on the touchscreen, browser, and apps indicates how much time remains in the exit delay.
- After the exit delay expires, the security status header on the touchscreen, browser, and apps displays **Armed Away** and the touchscreen emits two short beeps.
- If an entry/exit door is opened, closed, and then opened again prior to the end of the exit delay, then the exit delay is restarted. This only occurs once.
- If an entry/exit door is not opened and closed during the exit delay, the arming mode changes to **Armed Stay**.

A.3 Arm Stay Mode

The Arm Stay mode is used to arm the system when there are still people in the premises. The following rules apply:

- Exit delay starts when the user enters the correct key code to arm the system.
- An alarm is generated immediately when a monitored zone (non-entry/exit door) is faulted, except interior follower function types.
- Interior follower function types do not generate an alarm when faulted.
- The entry delay starts when an entry/exit zone is faulted.
- An alarm is generated if the system is not disarmed before the entry delay expires.

During the Arm Stay entry and exit delays:

- The touchscreen beeps once per second during the entry delay period. During the last ten seconds of the entry delay, the touchscreen beeps twice per second until it expires.
- The exit delay is twice the length of the Arm Away exit delay.
- The touchscreen does not beep during exit delay.
- A timer displayed on the touchscreen, browser, and apps indicates how much time remains in the exit delay.
- After the exit delay expires, the security status header on the touchscreen, browser, and apps displays **Armed Stay** and the touchscreen emits three short beeps.

A.4 Arm Night Mode

The Arm Night mode is used when there are people in the premises, but no one is expected to be moving about the premises, i.e., everyone is going to bed. The following rules apply:

- Exit delay starts when the user enters the correct key code to arm the system.
- An alarm is generated immediately when a monitored zone is faulted, except Interior follower, interior with delay, and interior delay arm night function types.
- Interior follower and interior with delay function types do not generate an alarm when faulted.
- The entry delay starts when an interior delay arm night zone is faulted.
- An alarm is generated if the system is not disarmed before the entry delay expires.

During the Arm Night entry and exit delays:

- The touchscreen beeps once per second during the entry delay period. During the last ten seconds of the entry delay, the touchscreen beeps twice per second until it expires.
- The exit delay is twice the length of the Arm Away exit delay.
- The touchscreen does not beep during exit delay.
- A timer displayed on the touchscreen, browser, and apps indicates how much time remains in the exit delay.
- After the exit delay expires, the security status header on the touchscreen, browser, and apps displays **Armed Night** and the touchscreen emits three short beeps.

Appendix B: Troubleshooting

The following sections provide information about the trouble messages you may see and what you can do to resolve them.

B.1 General System and Communication Troubles

Most communication errors are temporary. If the tips for resolving communication problems listed do not help, try restarting your home router or gateway, then restart your system, if applicable.

IMPORTANT: Do not reset your system to default factory settings unless instructed by a Customer Care representative.

Message	Cause	Resolution
An issue is affecting the system.	Unknown	Contact Customer Care if the condition persists.
Communications to the system are lost.	The system servers can not connect to the system.	❑ Verify the system is powered on ❑ Verify the system is connected to the Internet
System Upgrade in Progress	Firmware update currently in progress.	No action required. Message will go away when the update is completed.

B.2 Sensor Troubles

Message	Cause	Resolution
Sensor Communication Failure	The system cannot communicate with the identified sensor. Possible causes include low battery and RF connectivity failure.	Replace the battery with a battery of the same size and capacity. Refer to the documentation that came with the sensor. If you have any electronics on your home network that communicate with RF or Bluetooth, make sure they are not being used near the sensor. Installing a light module between the system and the sensor might improve communication.
Sensor is tampered	The cover of the identified sensor has been removed.	Make sure that the sensor cover is securely attached to the sensor base. If the problem persists, contact Customer Care.
Low Sensor Battery	The battery in the sensor is getting low.	Replace the battery with a battery of the same size and capacity. Refer to the documentation that came with the sensor.

B.3 Camera Trouble

Message	Cause	Resolution
Having difficulty communicating with camera	The system cannot communicate with one of your cameras.	Ensure that the camera is powered on, and that it is in range of the system. The power indicator light on the camera should be solid. If the camera is on, then disconnect the power source, wait a few minutes, then reconnect the power source.

B.4 Lighting Trouble

Message	Cause	Resolution
Having difficulty communicating with a light module	The system cannot communicate with one of your light modules.	If you have any electronics in your home network that communicate with RF or Bluetooth, make sure they are not being used near the light. If your light module is movable, place it in another location and see if the problem resolves itself. If so, move the light module back to the original location. If the error message returns, the RF signal may be weak in that part of your home.

B.5 Thermostat Troubles

Message	Cause	Resolution
Having difficulty communicating with a thermostat module	The system cannot communicate with your thermostat	If you have any electronics in your home network that communicate with RF or Bluetooth, make sure they are not being used near the thermostat. Installing a light module between the system and the thermostat might improve communication.
Low Thermostat Battery	The battery in the sensor is getting low.	Replace the battery with a battery of the same size and capacity. Refer to the documentation that came with the thermostat.

Appendix C: Compliances

C.1 FCC Notice

This device has been designed, constructed, and tested for compliance with FCC rules that regulate intentional and unintentional radiators. As the user of this device, you are not permitted to make any alterations or modifications to this equipment or use it in any way that is inconsistent with the information described in this guide without the expressed, written permission of the manufacturer. Doing so will void your authority to operate this equipment.

This device complies with FCC rules part 15 and Industry Canada RSS-210. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

This Class B digital apparatus complies with Canadian ICES-003.

The term "IC" before the equipment certification number only signifies that the Industry Canada technical specifications were met.

RF Exposure Information: This device is only authorized for use in a mobile or fixed application. At least 20 cm (8 inches) of separation distance between the touchscreen and the user's body must be maintained at all times to ensure compliance with the FCC and Industry Canada RF Exposure Requirements.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

C.2 Device Purpose

Household Fire/Alarm Central Panel

C.3 UL and ULC Notices

This device complies with UL 985, UL1023, UL1635, ULC S545, ULC C1023.

IMPORTANT: The rechargeable battery is only available through the service operator. If your battery needs to be replaced, contact your service operator to arrange for replacement.

C.4 ETL Notice

This device complies with all ETL and ETLC safety requirements.

C.5 Limitations of Security Products

Security products and alarm systems do not offer guaranteed protection against burglary, fire, or other emergencies. They may fail to warn for diverse reasons, including (but not limited to): power failure, dead batteries, improper installation, coverage, coverage areas overlooked during installation, defeat by technically sophisticated intruders, component failure, or inadequate maintenance. Alarm systems should be checked weekly to ensure that all devices are working properly.

AN ALARM SYSTEM IS NOT A SUBSTITUTE FOR INSURANCE.