wren SOLUTIONS™

HYPERION

User Guide

HMG1 Radio Module
Hyperion Version x

United States FCC Approval

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

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions.

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

Warning: Changes or modifications not expressly approved by the party responsible.

Canada IC Approval

English
This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

French
Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

FCC/IC Approved Antennas

This equipment uses the following Antennas and may not be used with other antenna types or with antennas of higher gain:

Manufacturer	Part Number	Type	Gain (dBi)
Data Alliance	A9D2RA	Omni-directional	2
L-com	HG908UP-NF	Omni-directional	8
Wren Solutions	HYP-HMG1WA2	Omni-directional	2.3

RF Exposure
FCC
This equipment complies with FCC RF Exposure requirements and should be installed and operated with a minimum distance of 20cm between the radiator and any part of the human body.

IC
This equipment complies with the ICES RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and any part of the human body.

Cet équipement est conforme aux limites d'exposition aux radiations ICES définies pour un environnement non contrôlé . Cet équipement doit être installé et utilisé à une distance minimale de 20 cm entre le radiateur et une partie de votre corps.

The HMG1 Module is not intended for OEM integrators and/or end-users. The module must be integrated by grantee authorized professional installers. Installers must be provided with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

Le HMG1 n'est pas destiné aux intégrateurs OEM et / ou aux utilisateurs finaux. Le module doit être intégré par des installateurs professionnels agréés. Les installateurs doivent disposer d'instructions d'installation d'antenne et des conditions de fonctionnement de l'émetteur afin de satisfaire à la conformité d'exposition RF.

The host product shall be properly labeled to identify the modules within the host product.
The host product must be labeled to display the FCC ID and ISED certification number for the module, preceded by the word "Contains" or similar wording expressing the same meaning, as follows:
Contains FCC ID: 2ARTD-HMG1
Contains IC: 24568-HMG1

Le produit hôte doit être correctement étiqueté pour identifier les modules qu'il contient.
Le produit hôte doit porter une étiquette indiquant le numéro de certification FCC et ISED du module, précédé du mot "contient" ou d'un libellé similaire exprimant le même sens, comme suit:
Contient: FCC ID: 2ARTD-HMG1
Contient: IC: 24568-HMG1

Contents

Product Overview

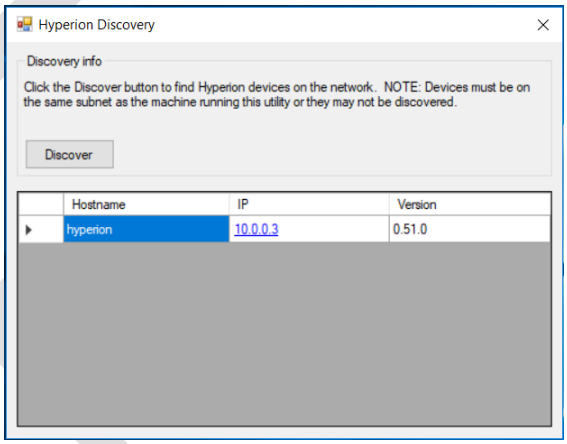
Hyperion enables automated control of various input and output devices for intelligent, automated response to events. This document outlines the setup and configuration of the Hyperion application. For hardware setup instruction, refer to the product specific installation guides that are provided with the equipment.

Gateway Configuration

Gateway Discovery

The Hyperion application is hosted on the Hyperion Gateway. The Hyperion Discovery Tool is used to initially find and connect to the gateway on the network.

1. Login to the Wren Solutions Support portal to download the discovery tool. The support portal is located at: http://www.wrensolutions.com/support
2. Extract the files in the Discovery zip file to a folder on a PC
3. Attach the PC to the same subnet on the local network as the gateway
4. Click on the hyperion-discover.exe file to run it
5. Click the Discover button
6. Click on the IP address next to the desired **Hyperion** host. This will launch a browser window to the Hyperion Log In page.



Note: Hyperion is certified on the latest version of Google Chrome and Mozilla Firefox. Microsoft Internet Explorer is not currently supported.

Log In

From the browser launched in Discovery or by entering the URL directly, log in to the Hyperion application using the administrative credentials provided with your Hyperion installation package.

Network

From the System menu, configure the Gateway's network settings. The default setting uses DHCP.

Date/Time

From the System menu, set the local device time using preferred method.

Users
From the System menu, create and manage system users.

- The Administrator role can manage the gateway system configuration, device settings, events, and users.
- The User role can manage device settings, events, and create other users without Administrator permissions.

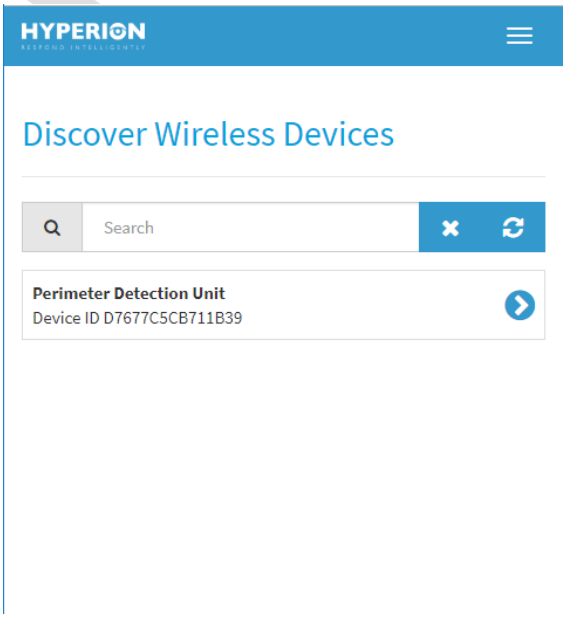
Users Add New

Username	Name	Administrator?	Actions
admin	Administrator	Yes	
bob.jones	Bob Jones	Yes	Delete
john.smith	John Smith	No	Delete
paul.wilson	Paul Wilson	Yes	Delete

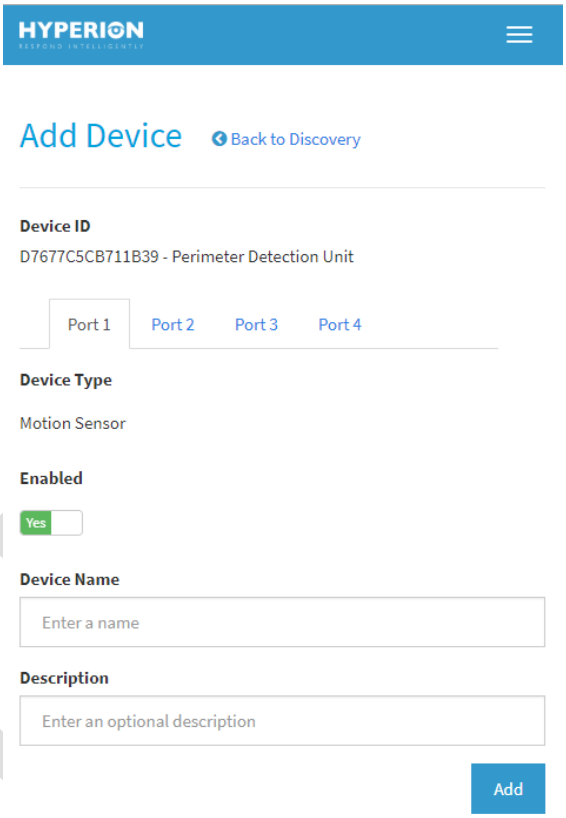
Device Configuration
This section details the steps to configure Hyperion devices and set up system operations.

Device Discovery
Discover Hyperion wireless devices at a location. Hyperion wireless devices utilize a 915 Mhz wireless signal to communicate with a local gateway. Locate wireless devices to add and configure in the system.

1. Power on a Hyperion wireless device and position it where desired.
2. Open the Discover Wireless Devices page from the Setup menu.
3. Select a Device to add.



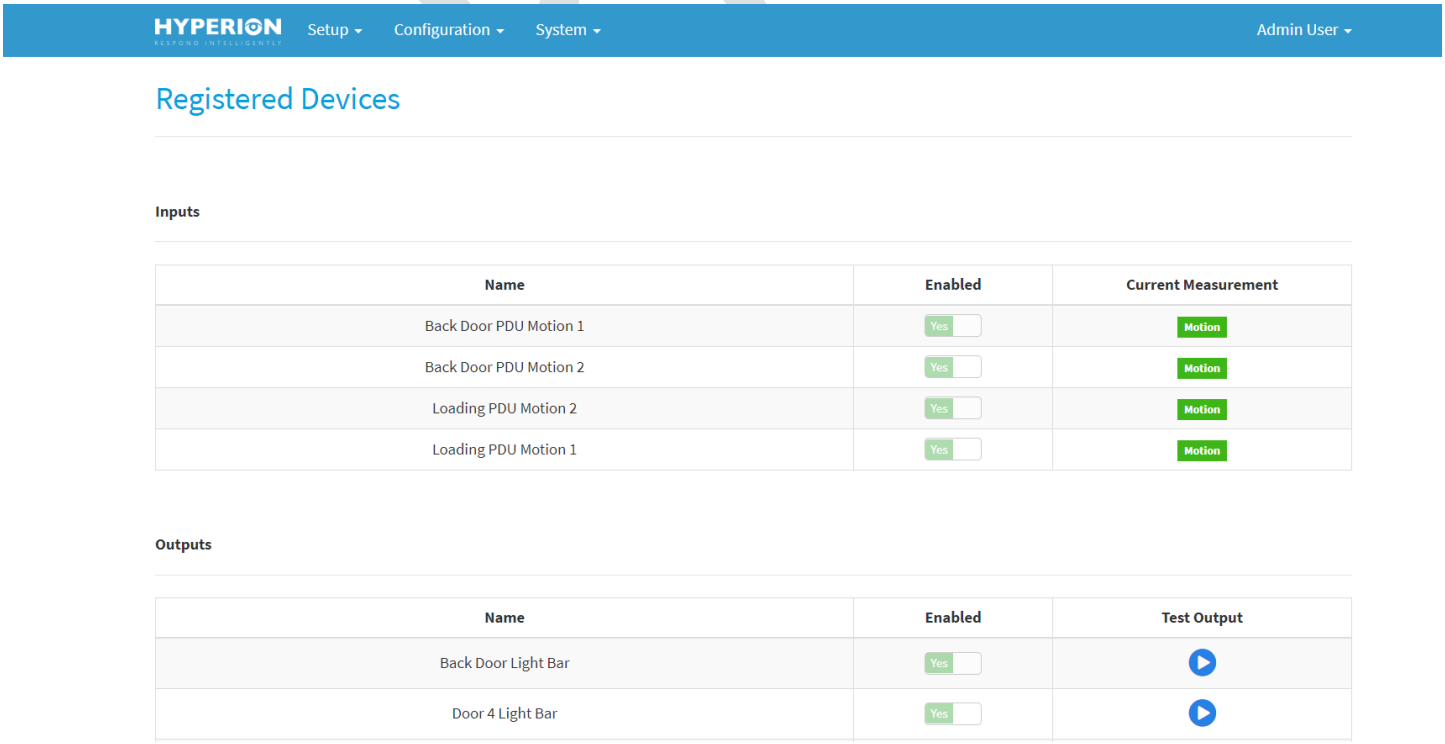
4. Enter the required information for all tabs (Ports), if applicable. Click Add.
5. Repeat steps 3 and 4 to add additional devices.



Registered Devices

From this default home page under the Setup menu, view the status and reading of connected devices.

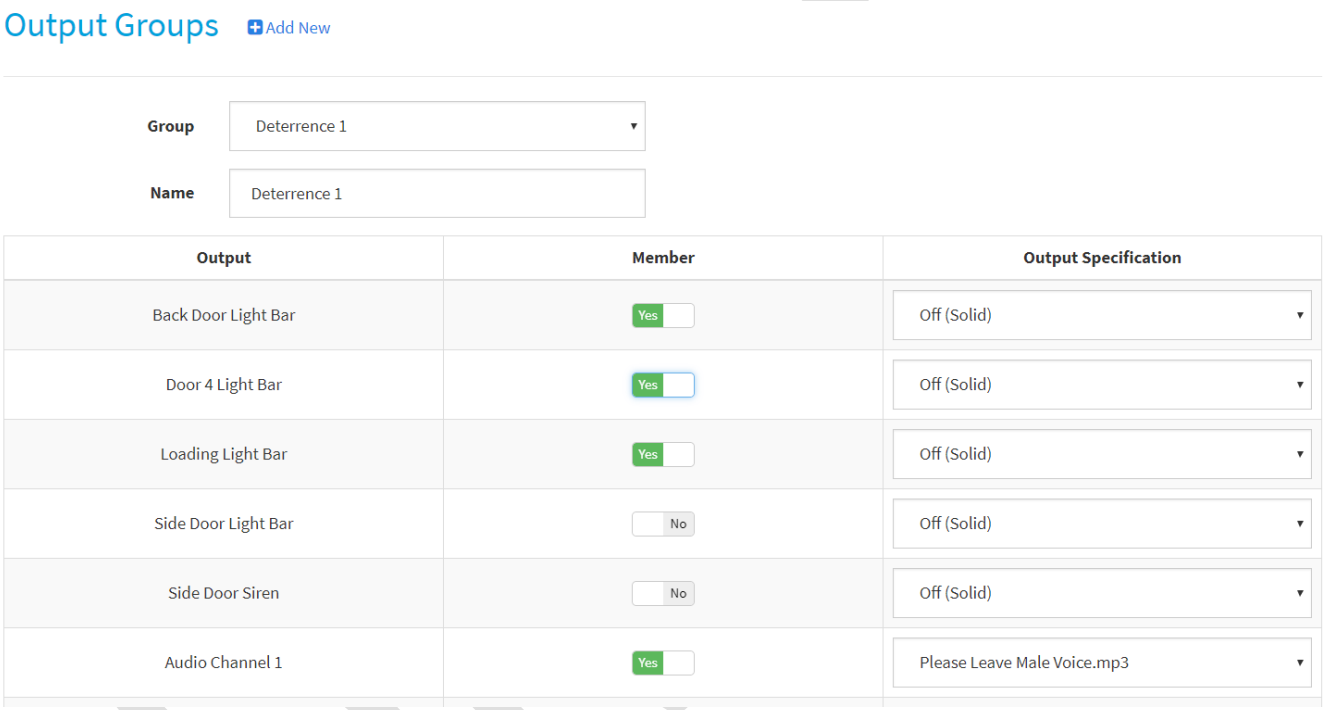
1. Click on an Input or Output to view and edit Device configuration.
2. Optionally, click the play icon next to an output device to test the output for 5 seconds.



Output Groups

Create and manage groups of output devices that are activated together in event response. These groups are used in Event setup to define the automated response for one or more devices at defined stages.

1. Open Output Groups from the Setup menu.
2. Click "+Add New"
3. When prompted, create a name for the new group and click Save.
4. Select the outputs to include by toggling Member status.
5. Select the audio file to be played when including an audio channel in the output group. Audio files are managed in the Audio page found under the Setup menu.
6. Optionally, Test the group output response.
7. Click Save to apply changes.



Audio

Add and manage audio files for use in audio channel output.

1. Open Audio from the Setup menu.
2. Click "+Add New"
3. Select an .mp3 file and click Upload.
   Note: .mp3 file format is required for all audio files.
4. Optionally, test the audio files on one or both audio channels for sound quality and volume.

   System Volume: In addition to audio volume controls on the back of the Gateway, system output volume sent to the internal amplifier can be adjusted. The default value for the system output volume is 9. This value can be adjusted from 1 to a maximum value of 11.

Audio Add New

File	Test Channel 1	Test Channel 2	Actions
Authorities have been notified and are responding.mp3	Yes	Yes	Play Once Stop Delete
Hakan Eriksson - Springtime Strings.mp3	Yes	Yes	Play Once Stop Delete
Please Leave Male Voice.mp3	Yes	Yes	Play Once Stop Delete

System Volume

Audio Channel 1 6

Audio Channel 2 6

Save

System Operations

Events

Define conditions with corresponding, escalating automated responses as well as scheduled system actions. Staged, conditional response operations can be activated by schedule or input devices.

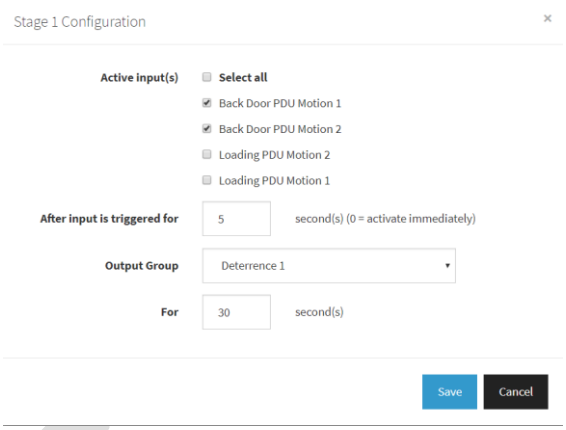
1. Open Events from the Configuration menu.
2. Click "+Add New"
3. Select the applicable Event Type and create a Name. Click Save.
4. Follow the steps below based on Event Type.

Event Configurations Add New

Configuration	Type	Actions
Back Door Exterior	Input	Edit Delete
Loading Exterior	Input	Edit Delete
Security Sweep Scheduled	Schedule Start/Stop	Edit Delete
Security Sweep Random	Random Schedule	Edit Delete

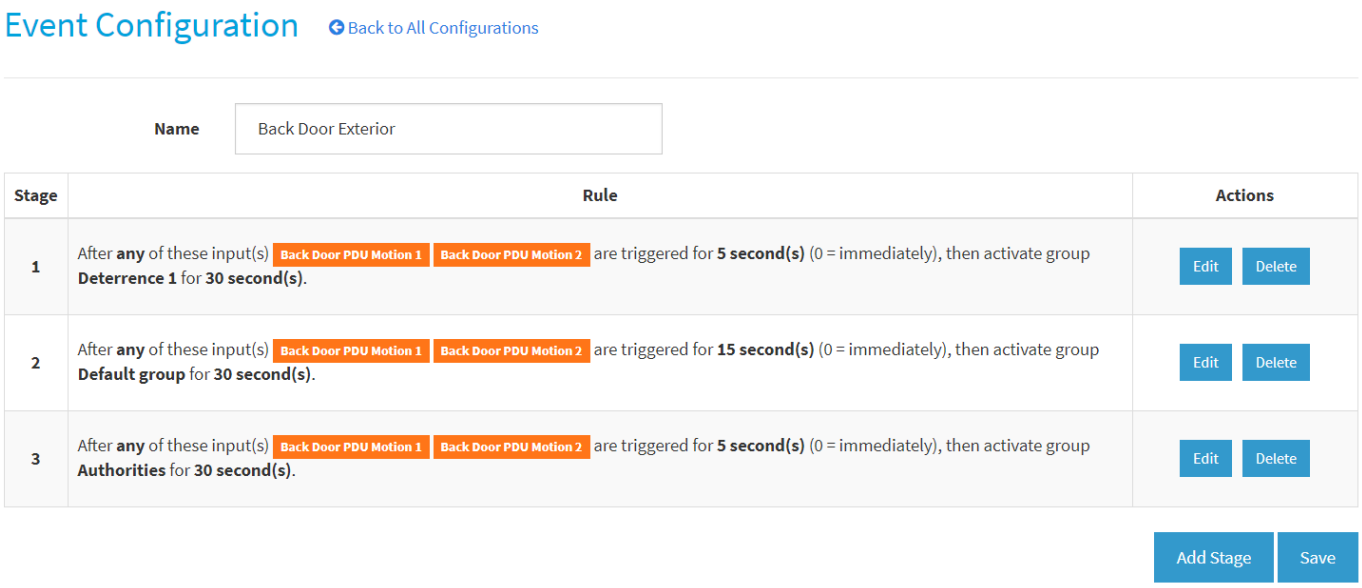
Input – One or more registered Input devices are used to trigger a system response.

a. For Input type events, click Edit next to Stage 1.
b. Select the Input(s) and associated duration an input should be active to trigger a response.
c. Select the Output Group to be used in the response and the duration of response.
d. Click Save.
e. Optionally, click Add Stage and repeat steps b – d.



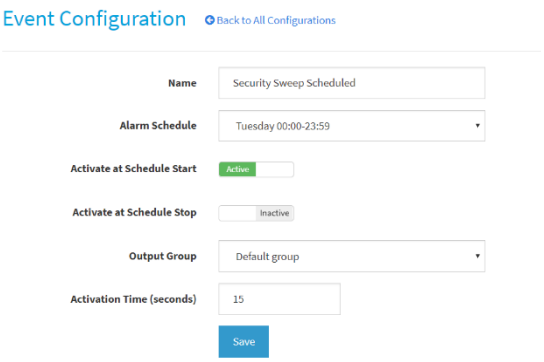
Note: Input type events must also be selected in Schedules to determine the active periods for each Event.

Each stage includes a selection of inputs to activate that stage. If an input is active after a stage is completed, the system will move to the next stage, using active inputs or repeat the current stage if it is the last defined stage.



Schedule Start / Stop – A user defined schedule is used to trigger a system response at the beginning or end of a scheduled period.

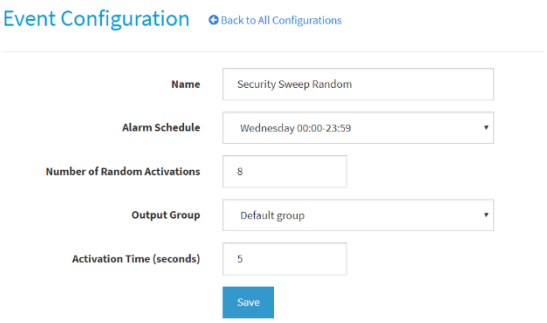
a. For Schedule Start / Stop type events, select an Alarm Schedule.
b. Select whether you'd like the response to activate at the beginning or end of the schedule using the toggles.
c. Select the Output Group to be used in the response and the duration of response.
d. Click Save.



Note: Alarm schedules are setup in Schedules under the Configuration menu.

Random Schedule – A user defined schedule is used to trigger a one or more random system response activities throughout a scheduled period.

a. For Random Schedule type events, select an Alarm Schedule.
b. Add the number of random response activations desired during the scheduled period.
c. Select the Output Group to be used in the response and the duration of response.
d. Click Save.



Note: Alarm schedules are setup in Schedules under the Configuration menu.

Schedules

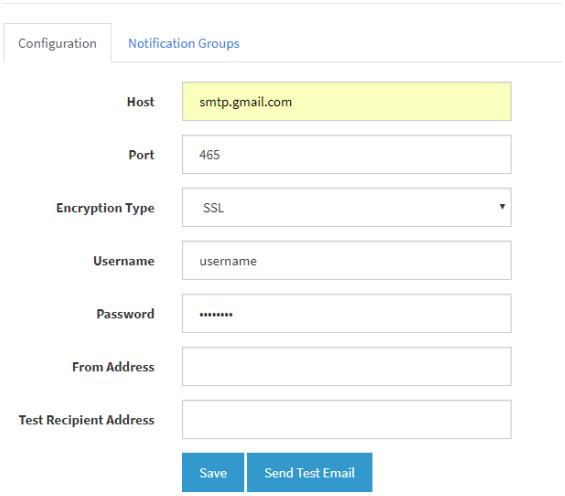
Schedules are used in defining the operational periods for Hyperion events and automated responses. Events can be triggered by a scheduled time period or external input. Additionally, input type events are set to only be active during scheduled periods. Multiple time periods can be setup for each day of the week but cannot overlap in time.

Active?	Day	Start Time (hh:mm)	End Time (hh:mm)	Event Configuration	Actions
☑	Sunday	00:00	06:00	Back Door Exterior	Delete
☑	Sunday	22:00	23:59	Back Door Exterior	Delete
☑	Monday	00:00	06:00	Back Door Exterior	Delete
☑	Monday	22:00	23:59	Back Door Exterior	Delete

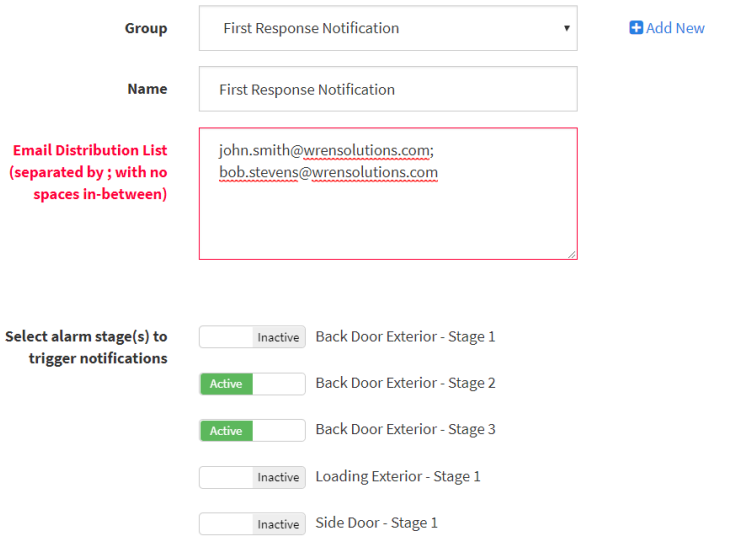
Notifications

Email Notifications can be configured to be sent when automated response events occur.

1. Configure the Email Service
2. From the Configuration Menu open Notifications.
3. Enter the account information for the email account that will be used to send notifications. Ensure the gateway can communicate with the email server across the network.
4. Save and optionally test the setup with a test email.



5. Under the Notification Groups tab, create Groups to define the Email distribution list(s) for automated response notification.
6. Select the Event stages to trigger the notifications for each Group.



Reporting

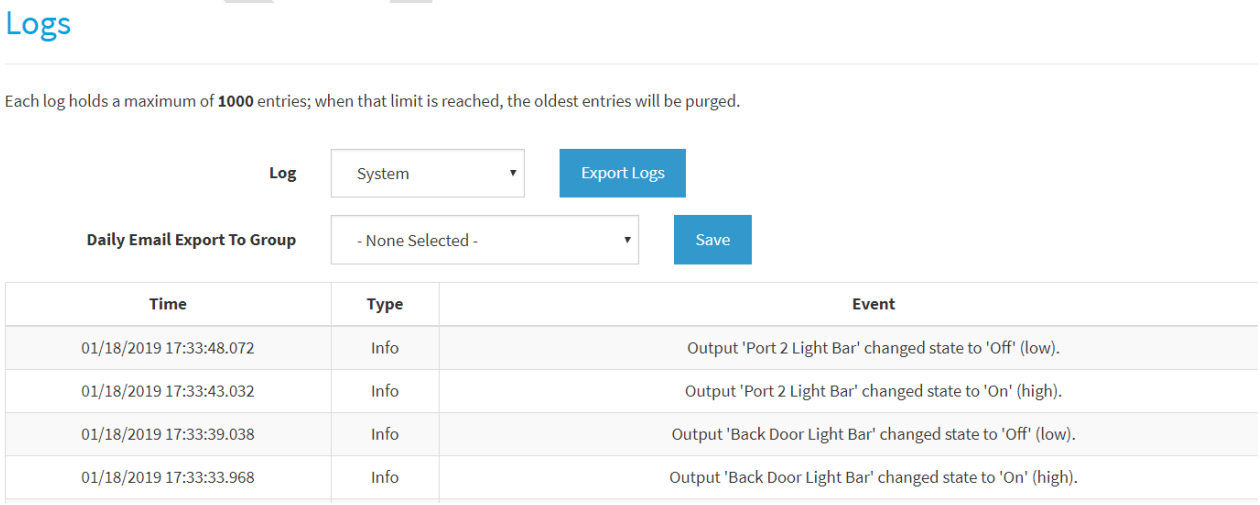
Data logs for a variety of system events and activities are stored in the database up to a certain number of records. Once the maximum number of records is reached, the records are overwritten by the most recent activities. The amount of time information is retained is dependent on the amount of activities occurring on each gateway. Logs can be exported from the app to be used for event investigation, system troubleshooting, and reporting purposes.

Logs

There are 3 types of logs used to capture different types of system activities.

- **Event Log**: Includes device input and output activity. This log can be used for investigation purposes and operational verification.
- **Users**: Lists user access activity.
- **System**: Includes system details, configuration changes and event activation details. This log can be used to view and report on event activation and automated response.

1. From the System menu, Select Logs.
2. Choose the Log type to view the specified logs in the App.
3. Click Export Logs to download a .zip compressed file that includes all three current log files in .csv format.
4. Optionally, set an Email notificaiton group to receive a daily copy of the logs via email and click Save.



System Updates

Hyperion Software App

The Update page under the System menu allows the user to view the current version of the software and load a software update.

1. To update the software, select the software update file.
   Note: The update will be in a .zip file and will be compressed. Do not extract.
2. Click the update button to update the software.
   The gateway will reboot during this process and will return to the Log In screen when update is complete.