

# **GRIDSMART®**

## **USERGUIDE V19.3**

## VERY IMPORTANT!

# PLEASE READ PRIOR TO INSTALLING VERSION 19.3

GS<sub>2</sub>'s must first be updated to 6.9. Legacy Processors (LPs) are not supported.

IMPORTANT NOTE: When upgrading from version 6.9 of the GS<sub>2</sub> software, any passwords used in the client to publish configuration changes WILL NOT BE CONVERTED. This is due to a necessary change in the password hashing scheme used. Any future upgrades will preserve usernames and passwords along with all other settings.

The following changes apply to version 19.3 and should be noted before applying the update:

- Passwords set and used in version prior to 19.3 for publishing are not preserved.
- To publish you must supply a username. The default publish user is "publish" and default password is "aldis#world9".
- Some functions related to the device were removed from the GS<sub>2</sub> Client software. These include network settings, and NTP Server Settings. THESE FUNCTIONS CAN ONLY BE DONE in the GS<sub>2</sub> Device Manager. To access these components, you MUST login with the ADMIN user account. The default ADMIN user "admin" and default password is "admin". It is highly recommended you change this password from the default value immediately and secure the password in a secure location or password vault.

LOSING THE PASSWORD TO THE ADMIN ACCOUNT MAY RESULT IN THE INABILITY TO ACCESS THE GS<sub>2</sub> PROCESOR.

## Changelog

### 19.3 (April 2019)

**PREREQUISITES:** GS<sub>2</sub>'s must first be updated to 6.9. Legacy Processors (LPs) are not supported.

**CRITICAL NOTE ABOUT THE UPDATE:** This update will take a longer time to complete than most prior releases, up to 15 minutes depending on the processor. It includes both low-level firmware updates as well as security updates to the underlying operating system. Upon reboot, it may take several minutes for the system to start up while the operating system updates are applied, with both the STATUS and CAMSTAT LEDs flashing during this time. **DO NOT DISRUPT THE SYSTEM DURING THIS TIME.**

**IMPORTANT NOTE ABOUT PUBLISH:** The publish workflow has changed to improve security features. We now require admin created usernames, roles, and passwords to publish or make changes. To publish by default, you must type `publish` for the user name and then the default `publish` account password, which is set to the GRIDSMART historical default password (`aldis#world9`). All current passwords will be reset to defaults upon updating to 19.3. The administrator of the Processor should create appropriate user accounts with appropriate roles and ensure secure passwords.

**NEW:** Bicyclist discrimination in the box that enables green extension for bikes. This new feature, available with the Performance Plus Module, satisfies the California MUTCD 2014 revision 3 and provides both improved safety and improved efficiency relative to stop-line bicycle discrimination.

**NEW:** Length-based counting now differentiates bicyclists as a fixed length of 6ft so that length-based reporting can be used for bike counts. The minimum recorded length for a vehicle is 11ft. Note that motorcycles may sometimes be recorded as bicycles or vehicles.

**NEW:** Basic device configuration such as network, date/time, and NTP is now done **\*\*only\*\*** via browser, providing a device-focused, secure alternative to the Client. Through this new interface, you can configure network/security settings, date/time, and location without requiring a connected camera. The GRIDSMART device manager is accessible via web browser, when connected to the processor laptop port, at <https://192.168.150.10:8900>. There is also a link on the processor desktop if you are connected via VNC. Using this device manager will require the default administrator account credentials; consult your user guide or ask support for that information and note that you should change those default credentials.

**NEW:** Enhanced security features are provided and configurable through the new browser interface. This includes client HTTPS support, user management, SSL certificate management, options to disable VNC and USB ports, and a self-audit security check.

**NEW:** An x64 Client installer is now available. This is the preferred installer, but an x86 client installer is also available for customers still running the client on an x86 architecture.

**NEW:** Processors running 19.3 can be updated remotely to subsequent versions via the new browser interface.

**IMPROVEMENT:** Length-based classification is now more accurate by taking advantage of the new bicycle discrimination capabilities.

**IMPROVEMENT:** Volume and Turning Movement reports by Approach can now optionally include empty columns to provide consistent exports for post-processing workflows.

**IMPROVEMENT:** Improved networking and Cloud connection management, particularly with the included cell modem.

**IMPROVEMENT:** During an update, call LEDs on the GS<sub>2</sub> front panel are used to indicate progress.

**IMPROVEMENT:** Changed the colors in the Client to better differentiate Road Masks from Object Masks.

**IMPROVEMENT:** Improved detection of bicyclists in low contrast stop-line zones.

**IMPROVEMENT:** Improved capture of nighttime counts that might have been missed if the headlights were obscured as the vehicle left a zone, such as by a luminaire or mast arm.

**IMPROVEMENT:** In some cases, certain zones – particularly occupancy count and permissive only zones – could remain activated after vehicles exited (stuck call). This issue has been improved.

**IMPROVEMENT:** In some cases, with advanced detection (traditional) cameras, zones with stopped queues could deactivate (drop calls) or fail to activate with tightly spaced vehicles. This issue has been improved.

**IMPROVEMENT:** All external communications adhere to TLS 1.2.

**FIX:** GS<sub>2</sub>'s now reads Canadian Fast Flash properly with TS2 controllers.

**FIX:** Fixed issue where some cameras would not supply an RTSP URL with the Performance Plus Module.

**FIX:** Fixed issue where processor might not recover properly after loss of power.

See: <https://support.gridsmart.com/solution/articles/27000052007-issue-gs2-processor-stuck-in-recoverymode>

**FIX:** Fixed issue where Client might crash when viewing fisheye in virtual PTZ (flattened) mode.

See: <https://support.gridsmart.com/a/solutions/articles/27000052002>

**FIX:** Changes to some traditional camera configuration parameters (camera height, compass heading, calibration rectangle) were not being applied after a publish, but only after a restart. This has been resolved.

**FIX:** Resolved rare issue that could cause unplanned Engine restarts when a camera connection was exhibiting communication failures.

**FIX:** Resolved a very rare condition that could trigger an engine restart in multi-camera systems.

**FIX:** Resolved a bug where incoming API requests, such as from a remote Client, could prevent a just-updated processor from starting correctly until the processor restarted itself a subsequent time.

**NOTICE:** This version includes support for a work-around to enable RTSP H.264 streams over TCP on non-standards-compliant implementations that rely on ping (e.g., Genetec).

**NOTICE:** This version removes the ability to use Publish to Drive on GS2 Processors. Publish to Drive is still available for version 6.9 or later.

**NOTICE:** The Pedestrian Module is no longer available, and that functionality is now included as part of the Performance Plus Module.

**NOTICE:** GRIDSMART 19.3 is the first to adopt the previously noted change to the release numbers to the YY.M format.

**NOTICE:** There are several changes in upcoming releases of which you should be aware:

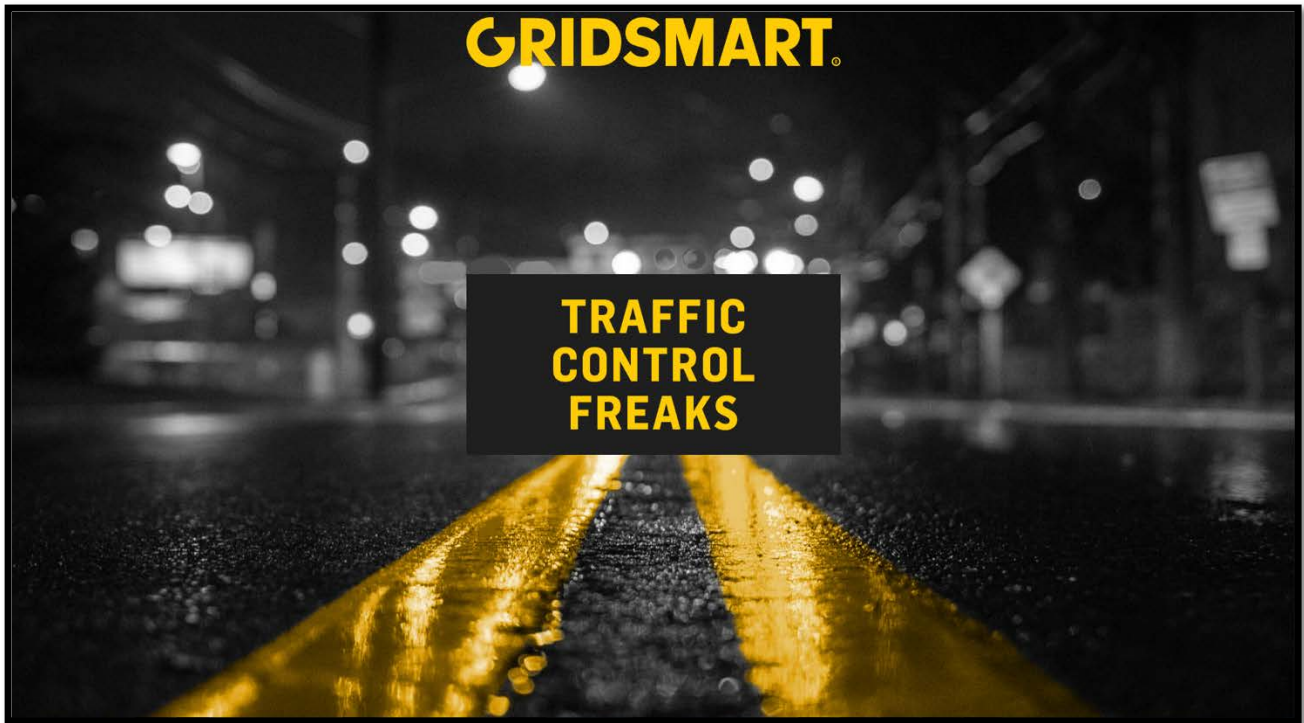
- The Engine display window(s) will be removed altogether.
- HTTP will be deprecated, and HTTPS will be required for all API use.
- VNC will be removed altogether.
- JSON will replace XML for serialized data exchange for all API use.
- Support for the previously deprecated quad-view API will be removed altogether. Flattening must be done in the GRIDSMART Client or third-party video management systems with the streams feature.

**SECURITY:** Operating system security updates included are:

KB4493467 <https://support.microsoft.com/en-us/help/4493467/windows-8-1-update-kb4493467>

KB4054566 <https://support.microsoft.com/en-us/help/4054566/microsoft-net-framework-4-7-2-forwindows-8-1-windows-rt-8-1-and-windo>

Please refer to the [GRIDSMART Box FAQ](#) for further information and notes.



Welcome to GRIDSMART!

GRIDSMART is your eye in the sky for actuation and data collection at intersections and on highways. Our unique solution tracks cars, trucks and bicycles while recording turning movements, vehicle counts, incidents and classifications. The GRIDSMART software, commonly referred to as the Client, lets you manage intersections in real-time. The Client is typically installed on a laptop and used to

configure the GRIDSMART Processor on-site during installation. If your cabinet is on a network, the Client can remotely access your system to view and configure sites, replay recorded video, calls and phases, generate reports and email alerts.

Your GRIDSMART system ships with an unlimited number of Client licenses, so feel free to install it on any number of computers in your office or traffic operations center.

Configuration changes made with the Client are easily undone. Nothing affects the operation of your site until you explicitly publish your changes. Even then, you can easily revert a site to a previous configuration, or even reset the GRIDSMART Processor to its original factory settings.



## Quick Reference

### Site Menu

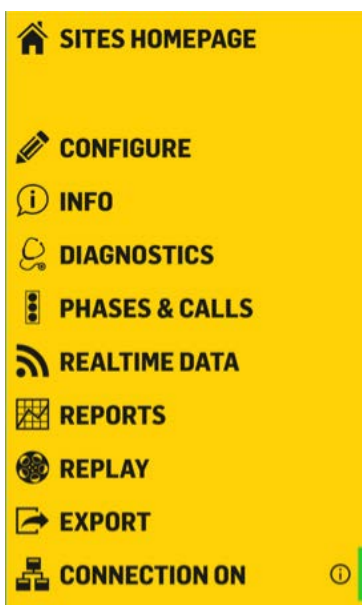
Intersection Setup

Temp, Power, etc.

Performance Data

Virtual DVR

Connection Status



Site Information

RYG & Detection

Volume, Arrivals, etc.

Export Site Card

### View Toolbar

Toggle Cameras

Custom Views



4-Panel View

Flatten Image

## TABLE OF CONTENTS

<b>PLEASE READ PRIOR TO INSTALLING VERSION 19.3.....</b>	<b>2</b>
<b><u>CHANGELOG .....</u></b>	<b><u>3</u></b>
<b><u>QUICK REFERENCE .....</u></b>	<b><u>7</u></b>
<b><u>1.0 CLIENT INSTALLATION &amp; CONFIGURATION .....</u></b>	<b><u>11</u></b>
1.1 DOWNLOAD THE CLIENT .....	11
1.2 INSTALL THE GRIDSMART CLIENT .....	13
<b><u>2.0 SITE CARDS AND THE SITES HOMEPAGE.....</u></b>	<b><u>14</u></b>
2.1 SITE CARDS .....	15
2.2 SITE VIEW MODES .....	17
2.3 CONFIGURE A NEW SITE FROM THE FACTORY DEFAULT SETUP .....	17
<b><u>3.0 SITE CONFIGURATION.....</u></b>	<b><u>20</u></b>
3.1 ROAD MASKS .....	21
3.2 VEHICLE ZONES .....	21
3.3 OBJECT MASKS .....	26
3.4 PEDESTRIAN ZONES .....	27
3.5 GRIDSMART BOX .....	28
3.5 FACTORY DEFAULT AND RESET TO FACTORY.....	29
3.6 QUAD VIEW .....	29
3.7 PHASES AND CALLS .....	29
3.8 MAKE OR CLEAR CALLS ON OPERATING ZONES.....	30
3.9 RECOMMISSION A FACTORY DEFAULT PROCESSOR .....	31
<b><u>4.0 PUBLISH .....</u></b>	<b><u>32</u></b>
4.1 SECURITY – ADMIN, PUBLISH AND READ-ONLY.....	32
4.2 DEFAULT CREDENTIALS.....	32
4.3 LEARNING MODE.....	33
4.4 MAKE CHANGES TO A SITE CONFIGURATION .....	33
4.5 PUBLISH HISTORY .....	33
4.6 MAKE CHANGES TO A SITE WITHOUT TAKING A LAPTOP INTO THE FIELD (PUBLISH TO DRIVE) .....	33
4.7 UNPUBLISHED CHANGES.....	34
<b><u>5.0 REVERT.....</u></b>	<b><u>36</u></b>
<b><u>6.0 SITE INFO.....</u></b>	<b><u>37</u></b>



<b>7.0 MODULES.....</b>	<b>38</b>
7.1 GRIDSMART DATA MODULES .....	38
7.2 ADD A MODULE .....	39
<b>8.0 REPORTS .....</b>	<b>39</b>
8.1 GET PERFORMANCE DATA WITH THE CLIENT .....	39
8.2 GET PERFORMANCE DATA WITH A USB STORAGE DEVICE .....	40
8.3 GENERATING REPORTS.....	41
8.4 AUTO REPORTS .....	49
<b>9.0 ALERTS .....</b>	<b>49</b>
<b>10.0 REPLAY .....</b>	<b>51</b>
10.1 RECORD AND REVIEW IMAGES AND/OR PERFORMANCE DATA .....	52
<b>11.0 GRIDSMART API .....</b>	<b>53</b>
<b>12.0 STREAMING H.264 STREAMS VIA RTSP .....</b>	<b>53</b>
<b>13.0 GS<sub>2</sub> DEVICE MANAGER.....</b>	<b>54</b>
13.1 NETWORK .....	55
13.2 CAMERAS .....	58
13.3 DIAGNOSTICS .....	58
13.4 MODULES .....	60
13.5 USERS .....	60
13.6 LOCATION .....	61
13.7 DATE/TIME .....	61
13.8 SECURITY .....	62
13.9 SYSTEM OPERATIONS.....	62
<b>14.0 SUPPORT .....</b>	<b>63</b>
14.1 SEND A SITE TO GRIDSMART SUPPORT FOR REVIEW OR ASSISTANCE .....	63
14.2 DATA STICK OR DATA DRIVE .....	63
14.3 IMPORT AND USE A MODIFIED SITE .....	63
14.4 VNC .....	64
14.5 UPGRADE A GRIDSMART PROCESSOR WITH AN UPDATE STICK .....	64
14.6 DIAGNOSTICS .....	65
14.7 REPLACE A CAMERA .....	65
14.8 UNINSTALL OR REPAIR THE GRIDSMART CLIENT .....	65
14.9 REMOTE SUPPORT .....	66

<b>GS<sub>2</sub> NETWORKING AND SECURITY .....</b>	<b>67</b>
INTRODUCTION .....	67
1.0 MODES OF OPERATION .....	67
2.0 GS <sub>2</sub> DEVICE MANAGER .....	68
2.1 UPGRADING FROM HTTP TO HTTPS .....	72
2.2 CLIENT/API SETTINGS.....	72
2.3 IMPORTING A SIGNED SSL CERTIFICATE.....	73
2.4 ROUTING CONSIDERATIONS .....	74
2.5 ADDING STATIC ROUTES.....	74
2.6 GRIDSMART CLOUD.....	74
2.7 RESTORING TO FACTORY DEFAULT NETWORK SETTINGS: .....	76
2.8 CHECKING CAMERAS .....	77
2.9 DIAGNOSTICS.....	78
2.10 MODULES .....	78
2.11 USER MANAGEMENT .....	79
2.12 MANUALLY SETTING THE CLOCK AND TIME ZONE. ....	79
2.13 SECURITY SELF AUDIT .....	80
2.14 REMOTE UPDATES .....	81
3.0 OTHER CONSIDERATIONS.....	82
4.0 NETWORK CONFIGURATIONS - BEST PRACTICES.....	85
5.0 CASE STUDY FOR USING STATIC ROUTES: .....	86
<b>FAQS.....</b>	<b>88</b>

## 1.0 Client Installation & Configuration

### 1.1 Download the Client

Download the latest version of the GRIDSMART Client from GRIDSMART Cloud.

1. Open a web browser and visit [gridsmart.com/support](https://gridsmart.com/support).
2. Sign in to GRIDSMART Cloud or click Sign Up to create a new account.
3. Click the Support dropdown, then click Downloads.

Welcome to GRIDSMART® Cloud, the online support center for [GRIDSMART](#) installers and customers.

Email

Password

[Log In](#)

[Need an account? Sign Up](#)

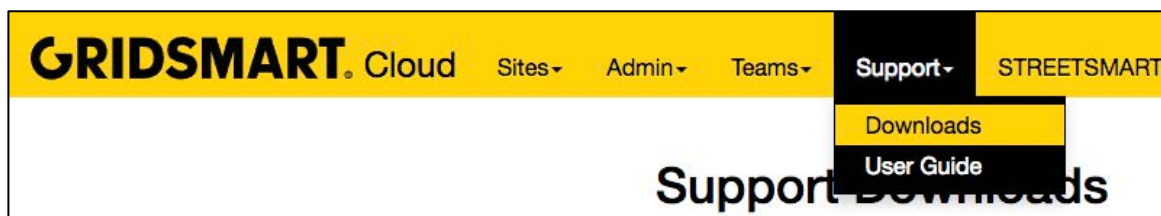
[Forgot your password? Reset Password](#)

Want to talk? Call us at +1 866.652.5347

Or email us at [support@gridsmart.com](mailto:support@gridsmart.com)

Just want the [User Guide](#)?

Here, you can always access the [GRIDSMART User Guide](#). When you log in above, you can access all your backed up site configurations from the GRIDSMART Client as well as the support downloads.



## 4. Select the Update Stick or the Client Installer and download the file.

Support Downloads

[Changelog](#)

Firmware Update Notice

**DO NOT UNPLUG OR MANIPULATE THE SYSTEM DURING AN UPDATE.** Updates for GS2 may often include firmware updates that put the system into a special programming mode. All front panel LEDs will go dark and the fan will operate loudly at its highest speed. This is expected. After roughly 30 seconds, the fan will return to normal speed. The phase LEDs will turn all red as the system exits the special programming mode and then all green when the update is complete.

Releases

19.3

Name	Description
v19.3 Update Stick	Processors must be a GS2 running GRIDSMART 6.9 Firmware or later to be updated. Download, unzip the archive, and then put the extracted contents (folder aldiss and GridSmartClientInstaller.exe) at the root level of a freshly formatted USB stick.

6.9

Name	Description
v19.3 Client Installer x64	Download and then double-click the *.exe to install. Fully backward-compatible, including Publish, with Processors running GRIDSMART 4.0 or later. This installer is for x64 computers only.
v19.3 Client Installer x86	Download and then double-click the *.exe to install. Fully backward-compatible, including Publish, with Processors running GRIDSMART 4.0 or later. This installer is for x86 computers only.

## 1.2 Install the GRIDSMART Client



Stay connected to the Internet while you install the Client on your laptop or desktop computer. The GRIDSMART Client is already installed on the GRIDSMART Processor. Please do not install the Client or any other software on the Processor.

Double-click the Setup Program or MSI Installer to open the GRIDSMART Client Setup.



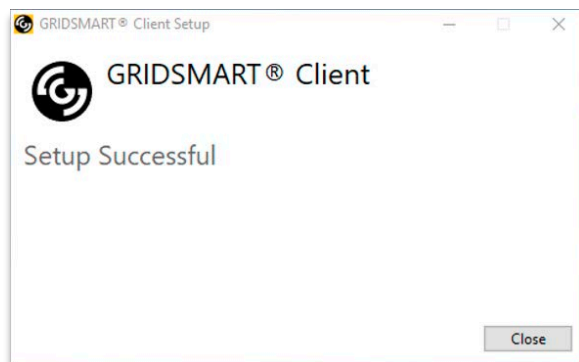
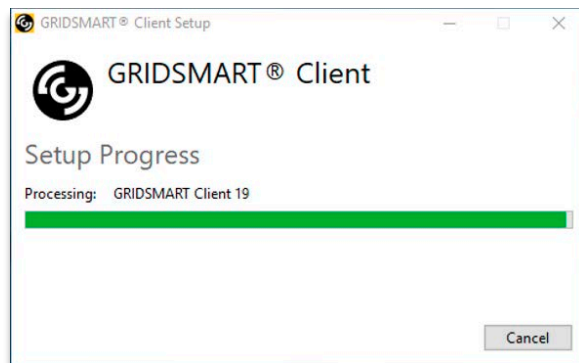
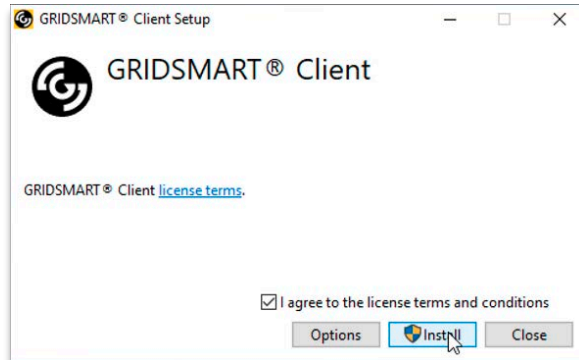
Accept the Terms and Conditions, then click Install.

The setup program creates shortcuts to the GRIDSMART Client on your Start Menu and Desktop.

A progress bar indicates the setup status.



A system restart may be required to complete the installation.



## 2.0 Site Cards and the Sites Homepage



The Sites Homepage appears after you launch the GRIDSMART Client. A Site Card represents an individual intersection, and the Sites Homepage displays a Site Card for each of your known sites. Additional Site Cards appear on the Homepage after you connect or import new sites.

## 2.1 Site Cards

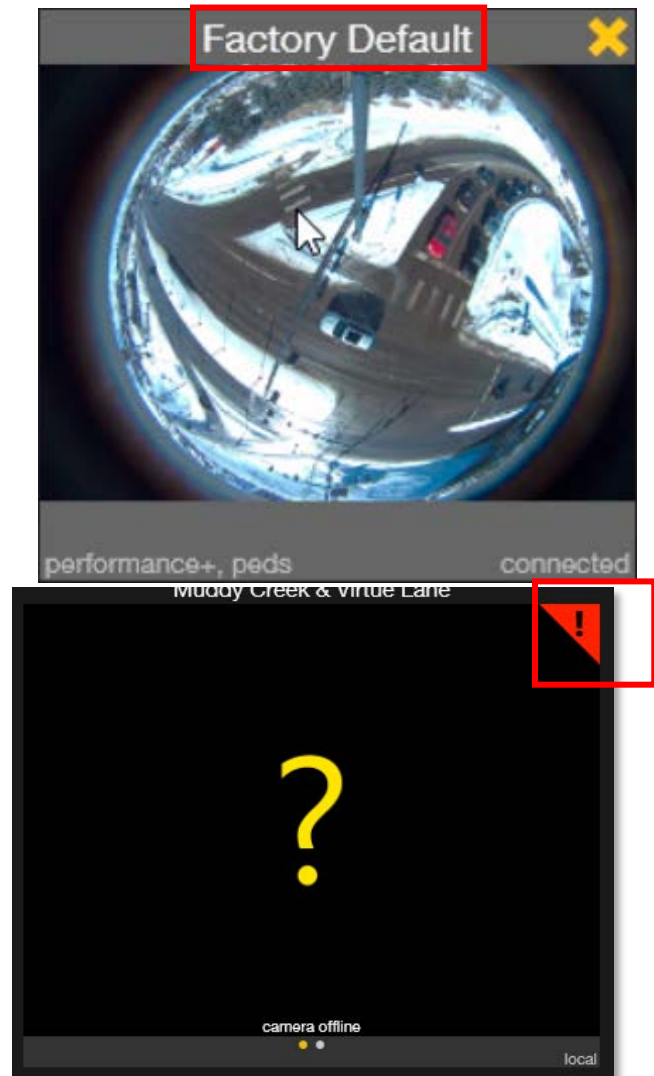
The Sites Homepage only displays one card the first time you configure a GRIDSMART system; the Factory Default card.

If you are locally connected to the GRIDSMART Processor (Laptop Port), the Site Card appears at the top center of the Homepage.

The Processor cannot see this new Camera. The Site is connected, but the Camera is offline.

To remove a site from your Homepage, click the Yellow X in the upper right-hand corner of the card.

A yellow “!” indicates a new Camera has been found. A red “!” is camera offline or failed connection (which overrides yellow in the event you have both new camera and an offline camera).



### Open a Site

To open a site, click the appropriate Site Card on the Sites Homepage.

You can also use the search bar in the upper right-hand corner of the Sites Homepage to search your sites by street, city, state, postal code or IP address.



Site Cards display on the Homepage if the Client previously connected to the site and the IP address of the corresponding GRIDSMART Processor has not changed.



## Site View Manager

Click the View button on the top left of the homepage to toggle a new view. Next, select the site you want to view.



## Site Image View



## Lightweight View

17 AVE & 50 ST	320 & West Chester Pike	320 & West Chester Pike	Barbur Blvd & Capitol	Bernard & Gordon
Cherahala & Hardin Valley	Cherahala & Hardin Valley	Factory Default	Freedom & Commonwealth	Glenn & Gay

## Detail View

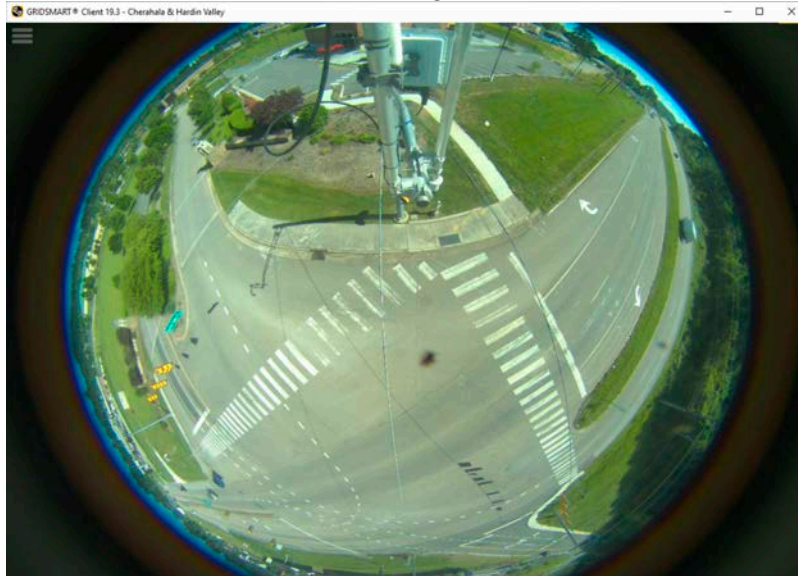
Site	Serial #	Location	Endpoint	Connection
17 AVE & 50 ST	GS2-2721	Calgary, Alberta		
320 & West Chester Pike	GS-U5-20126	Broomall, PA		
320 & West Chester Pike	GS-U5-4924	Broomall, PA	Show	Off
Barbur Blvd & Capitol	GS2-3171	Portland, OR		
Bernard & Gordon	GS-U5-5521	Kelowna, BC		
Cherahala & Hardin Valley	GS2-3963	Knoxville, Tennessee	Show	Off
Cherahala & Hardin Valley	GS2-2987	Knoxville, TN	Show	On

Select the Site you want to view or Select the top center “Factory Default” site card to configure a new site.



## 2.2 Site View Modes

**Fisheye**

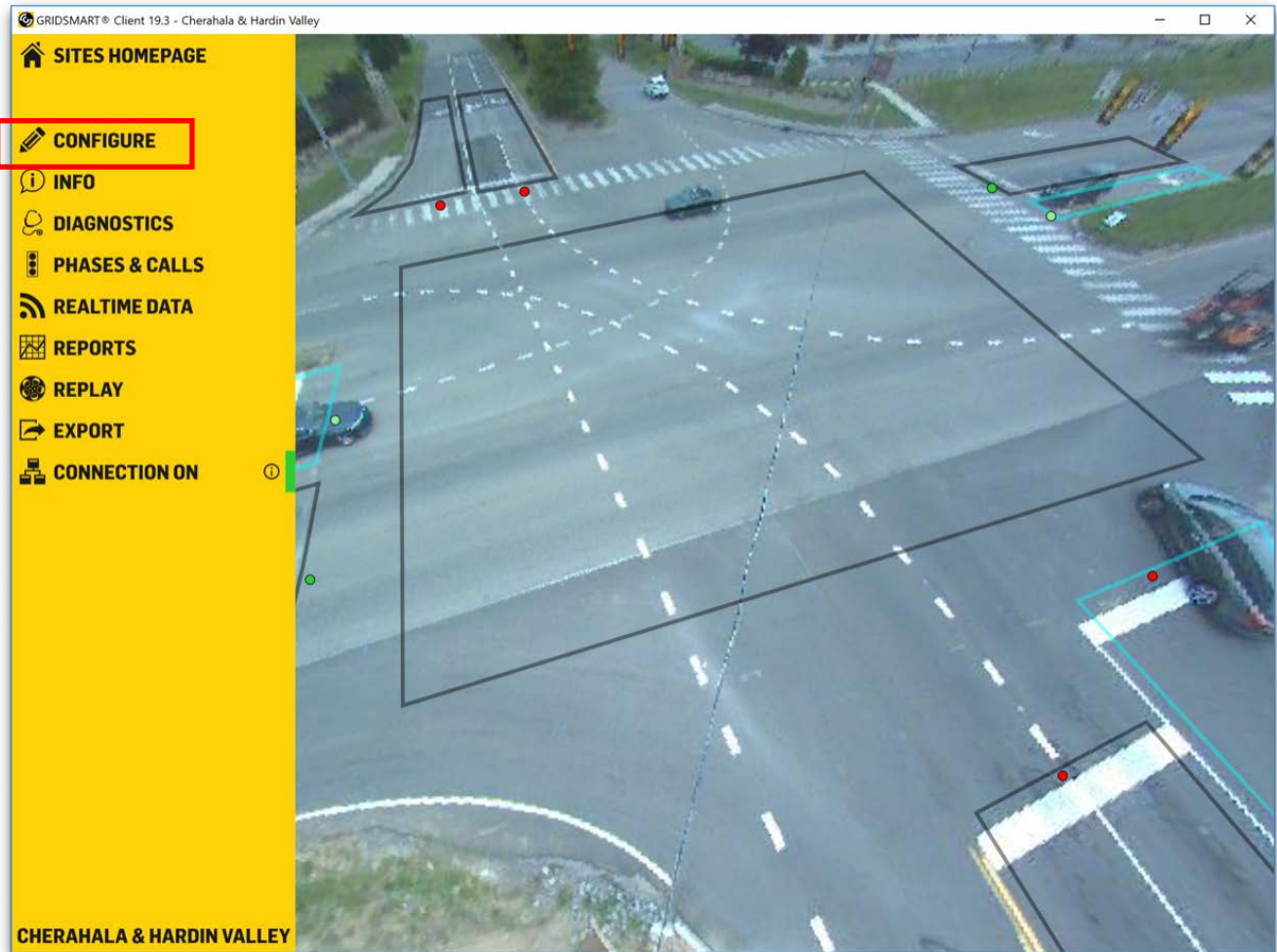


**Flattened**



## 2.3 Configure a New Site from the Factory Default Setup

Launch the Client and click the Factory Default Site Card. The Site Menu appears when the mouse hovers over the left-hand side of the Site View screen.



Click the Configure pencil on the Site Menu to start the setup wizard.



You must have a Camera connected to the System and have a picture to see the Configure option



You can now complete basic device configuration via a browser now as well.

## Location

Enter the site location information.  
For U.S. and Canadian sites, the Postal Code automatically populates the City, State, County, Latitude and Longitude fields.

If you are outside the US and Canada manually enter the Latitude and Longitude.

The screenshot shows the 'Location' tab selected. It contains input fields for:
 

- Postal Code: 37932
- City: Knoxville
- Country: USA
- Street 1: Cherahala
- County: Knox
- Latitude: 35.92
- Street 2: Hardin Valley
- State: Tennessee
- Longitude: -84.2

 There are also checkboxes for 'Metric' and 'Left Side Driving', both of which are currently unchecked. A 'Close' button is at the bottom.

## Control

The Control Mode will be automatically selected based on the installed Option Card, TS1, TS2 or ITS.

Generally, TS1 mode will also be used for 170/2070 and SCATS configurations.

The SCATS (Sydney Coordinated Adaptive Traffic System) option is available in the Control settings for TS1 sites licensed for the Performance Module.

BIU and SIU selections can be made at the time you draw the zones and assign outputs.

The screenshot shows the 'Control' tab selected. It contains:
 

- 'Cabinet Type' with three buttons: TS1 (highlighted in yellow), TS2, and ITS.
- 'SCATS' with 'On' and 'Off' buttons; 'Off' is highlighted in yellow.
- 'Max Recall Default' with 'On' and 'Off' buttons; 'Off' is highlighted in yellow.
- 'Delete Stationary After' with a slider bar set to 'Never'.

 A 'Close' button is at the bottom.

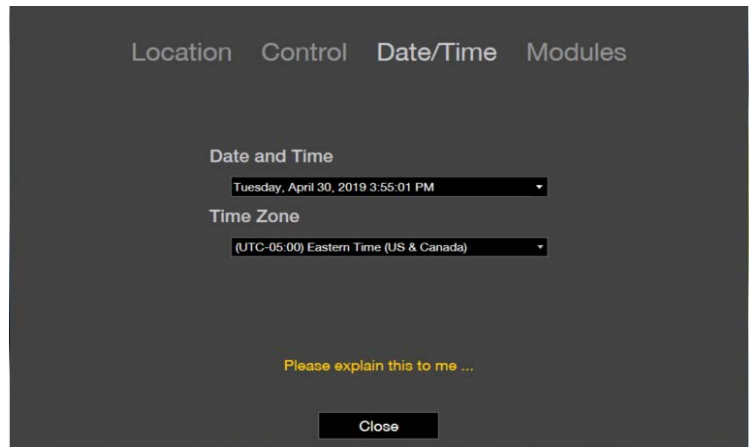
## Date and Time

Select the Date, Time and the Time Zone. The factory default is Eastern Time (US & Canada).



Date and time are important parameters for the Engine and must be set correctly for the site location.

The Processor will automatically adjust the time to the configured Time Server.

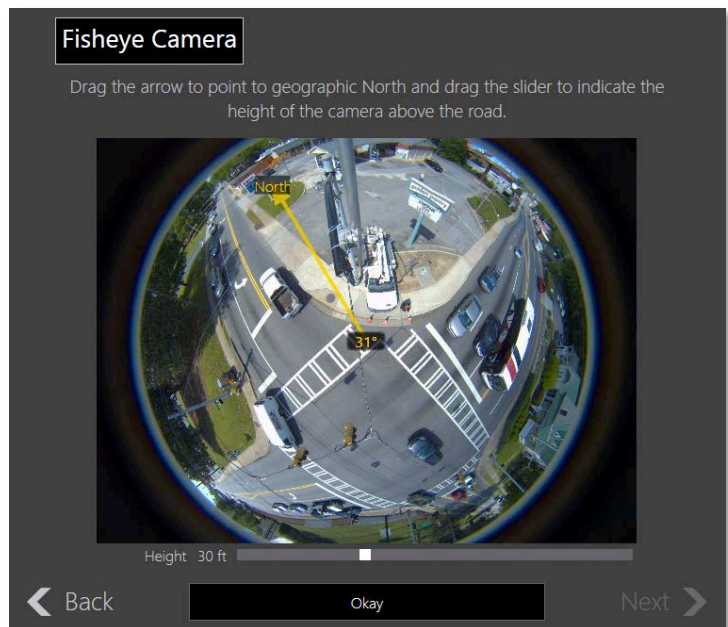


## North Heading and Camera Height

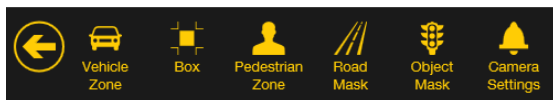
Set the North heading. Stand beneath the Camera with a compass and identify a structure in the North heading line of site. Click and drag the North arrow to point to that structure.

Measure the Camera height from the bottom of the camera housing to the roadway. Use the slider to set the correct height. We recommend at least 30 feet.

Click Okay.



## 3.0 Site Configuration

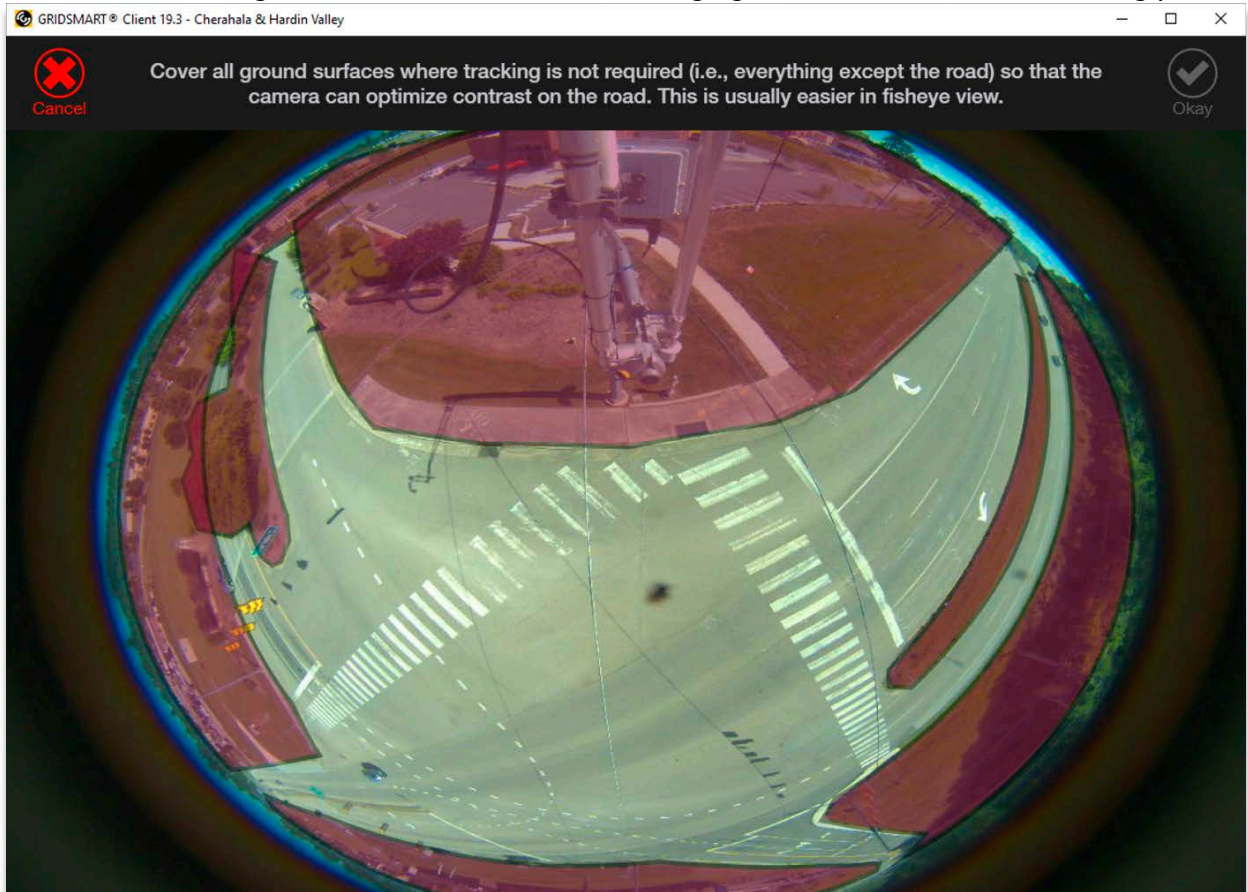


Use the Top Menu bar on the Site View screen to add and configure zones and masks.



## 3.1 Road Masks

1. Road Masks eliminate areas that do not require object tracking (i.e. everything except the road). You may find it easier to create masks in the Fisheye view.
2. Click Road Mask on the Top Menu bar.
3. Place the cursor at the edge of the roadway, then click to place the starting point.
4. Click around the edge of the area to be covered, bringing the cursor back to the starting point.



- 5.
6. Hover the cursor over the green starting point until the cursor turns into a pencil, then click the pencil to close the mask area.
7. Click Okay to complete.
8. Continue Masking out all other areas.

## 3.2 Vehicle Zones

A Vehicle Zone is the basic vehicle detection region. When you assign an output to a Vehicle Zone, GRIDSMART sends a signal to the controller when a vehicle is present in the area. Zones also collect vehicle data for Reports and Alerts.

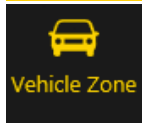
## Vehicle Zone recommendations:

1. Zones should be 3-4 car lengths.
2. Maintain a distance of 1-2 feet between each zone.
3. Zones should cover the entire movement region regardless the number of lanes.

## Create a Vehicle Zone

Click the Configure pencil, then click the Eye icon.

Click the Vehicle Zone icon.



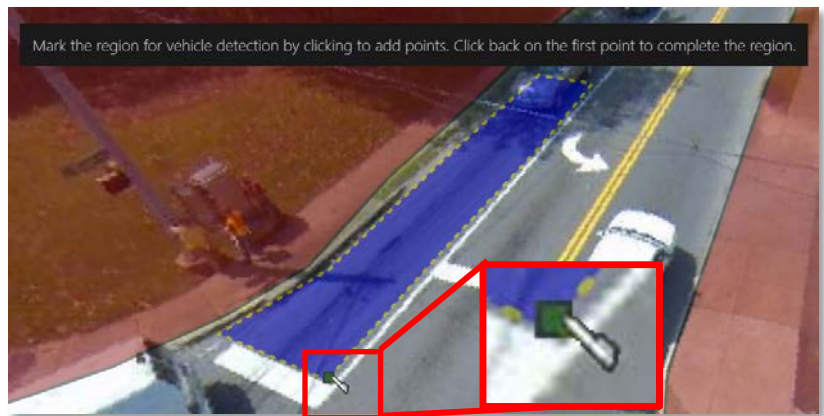
In flattened mode, the image becomes a virtual pan-tilt-zoom. Pan and zoom the image to the area where the zone will be created.



## Draw the Vehicle Zone

Mark the region for vehicle detection by clicking to add points.

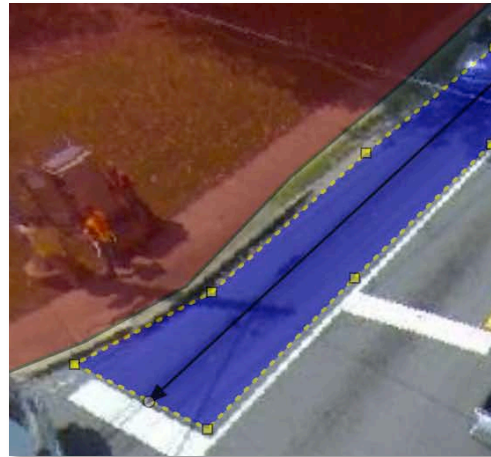
Click back on the first point to complete the region.



## Set the Flow Direction

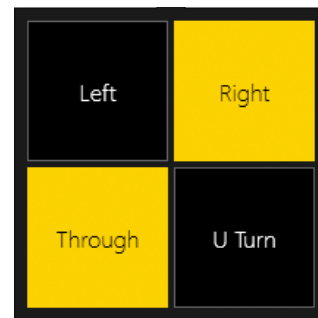
Left-click the front of the directional flow arrow.

Drag the arrow to indicate the flow of traffic.



## Turns

Select valid turns from the Vehicle Zone.



## Phase

Click the phase(s) associated with the Vehicle Zone.

Left turn zones can be Protected, Permissive or Protected/Permissive.

Only assign phases to zones that are located at the Stop Line and physically connected to the light state phase.



Do not assign phases to a setback/advanced detector zones.



## Output: TS1 / BIU / SIU

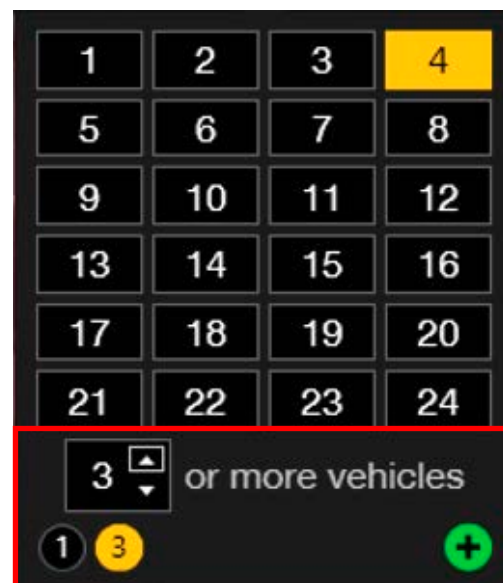
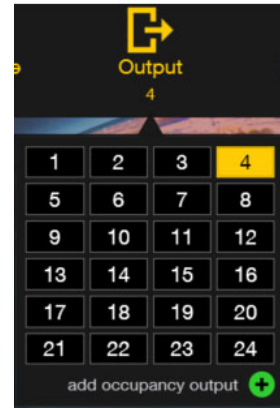
The output, or call, identifies the channel that the vehicle detector will send a signal to when activated. GRIDSMART supports Presence Mode only.

Multiple outputs may be assigned.

Occupancy Based Outputs can also be assigned.

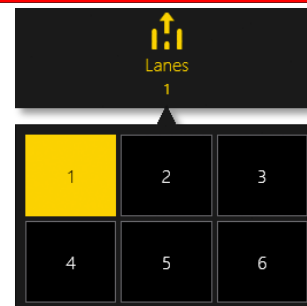
Occupancy Based Outputs can be configured while creating Zones. To Start, click the Green Plus icon under the output option for the zone. Select the number of cars desired (up to 6) for the new output. You can now add up to 6 different outputs for each zone.

**The Zone will only become active when there are the set number of vehicles in the zone.**



## Lanes

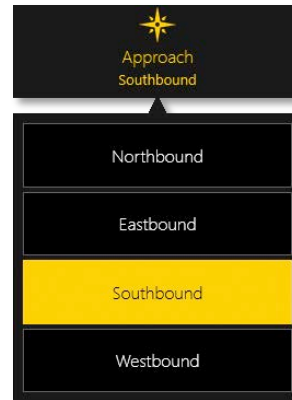
Assign the number of lanes covered by the zone.





## Approach

The Reports module aggregates vehicle data based on the approach.



## Options

**Zone Name** appears in the Reports module.

**Extension** extends a call to the controller in seconds.

**Delay** suspends the call to the controller in seconds (only during a Red sequence).

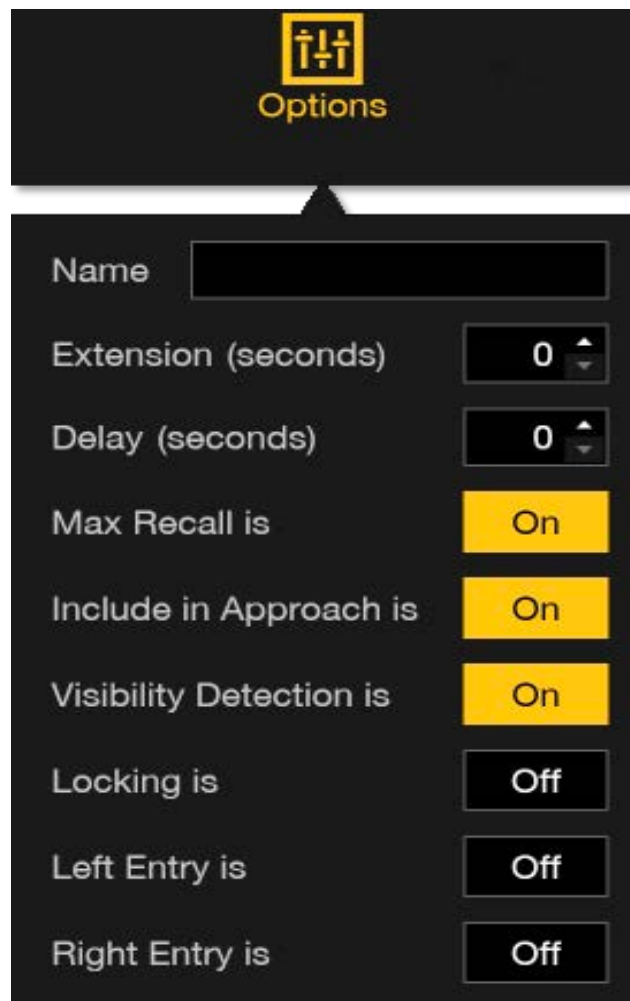
**Max Recall** is a failsafe. When On, the zone is placed in constant call during learning mode or a system failure event. When Off, the call only persists until the phase is serviced by a green sequence.

**Include in Approach** logs vehicle Counts. Usually Off for setback zones.

**Visibility Detection** is a threshold mechanism that enables the system to detect fog, glare or other similar events. If the Visibility Detection exceeds the threshold, a constant call is placed until the event clears.

**Locking** places a call to the controller until the phase receives a Green.

The **Left and Right Entry** options allow the user to specify if a side zone entry should activate the detector. This is used for driveway exits at or near the stop line where vehicles may not travel in the direction of the flow arrow.



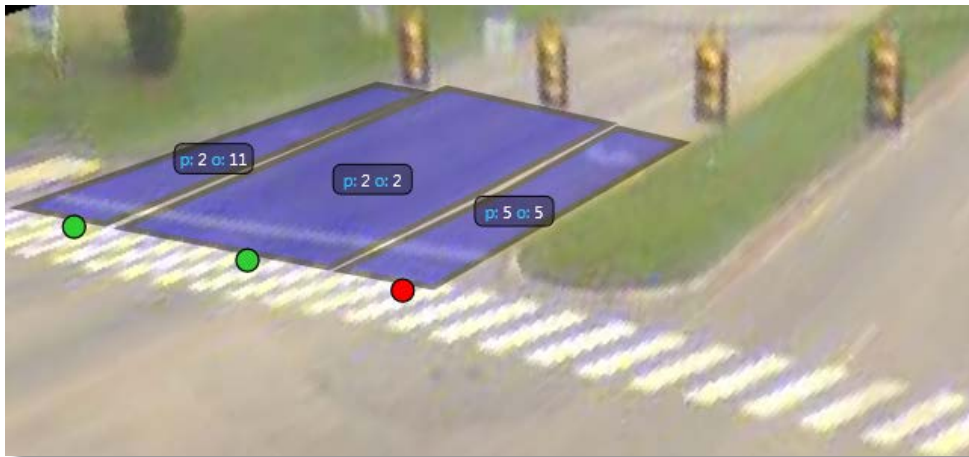
## 3.3 Object Masks

Draw Object Masks to cover objects that block or interfere with the camera view of the ground or road.

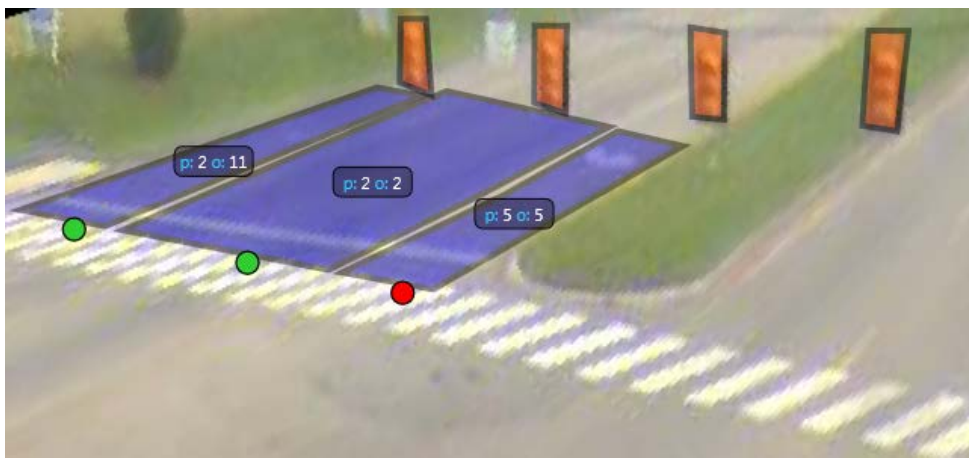
Object Masks are very important because they eliminate objects that may result in false calls (signal heads, mast arms); disrupt the image contrast because they are highly reflective (Luminaire heads, poles, mast arms); emit light at night (lighted signage).

To create Object Masks, click Object Masks on the Top Menu bar and follow the same instructions in the [Road Masks](#) section.

Unmasked signals:



Signals masked out:

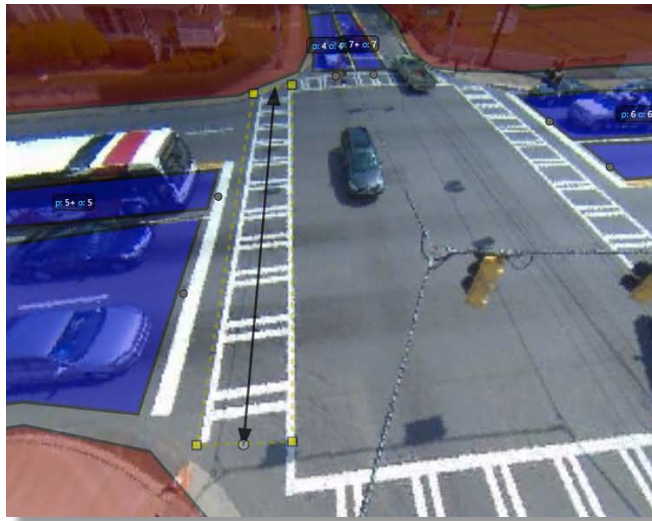


## 3.4 Pedestrian Zones

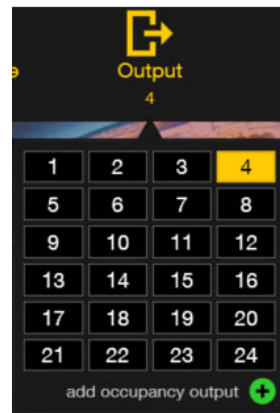
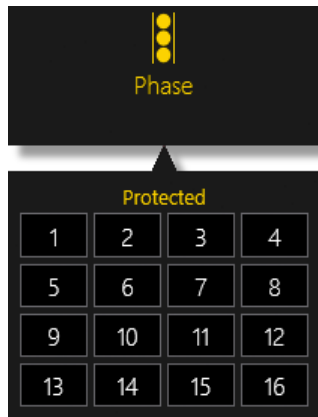


A Pedestrian Zone detects bi-directional pedestrian movement in crosswalks. Outputs signal the controller, or other devices, of pedestrian activity in the intersection.

1. Click the Pedestrian icon from the Top Menu bar.
2. Place the cursor at or near the corner of the crosswalk. Cover the detection zone by clicking around the area, then return to the starting point to close the zone.
3. Set the direction of crossing.



4. Select the Protected Pedestrian Phase and Output.

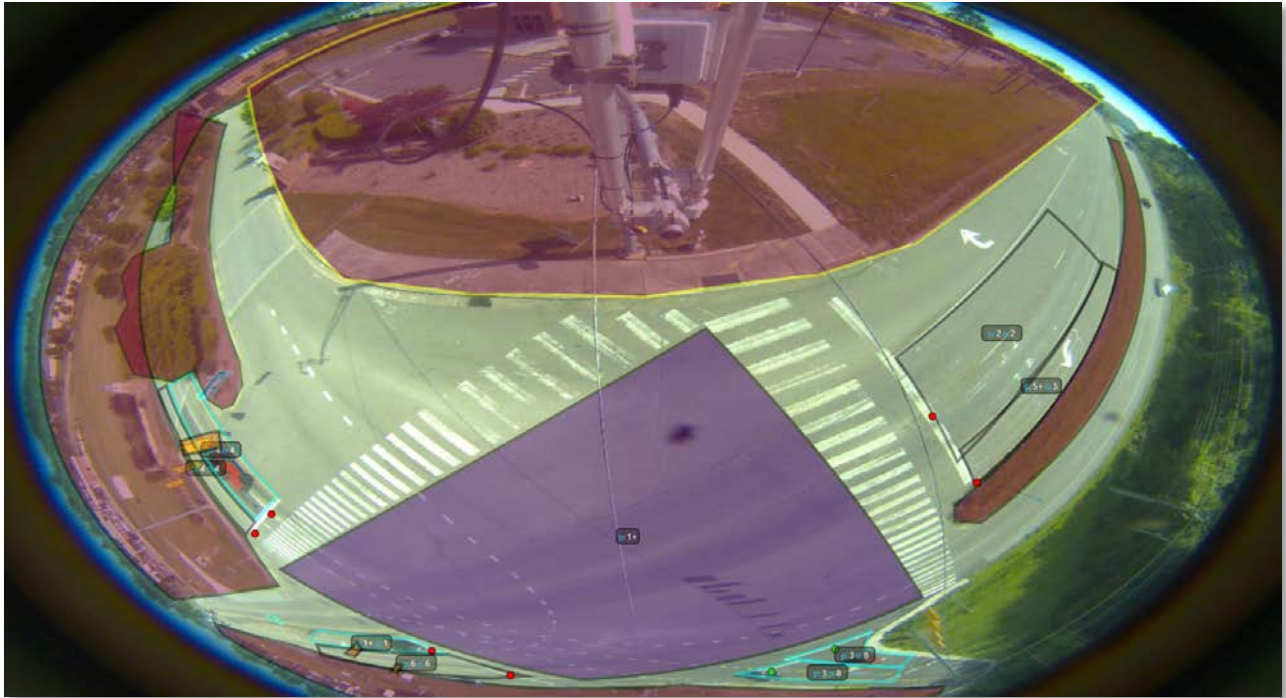


5. Select Alerts and Options as needed.


## 3.5 GRIDSMART Box

The GRIDSMART Box was created to allow extensions for Bicycles and/or Vehicles entering the intersection.


1. Click Box on the Top Menu bar.
2. Place the cursor at the middle of the intersection, then click to place the starting point.
3. Cover the detection zone by clicking around the area, then return to the starting point to close the zone.



4. Select the Extension Outputs for Bikes and Vehicles.

  
Extension Outputs

Bikes		Vehicles	
1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16
17	18	19	20
21	22	23	24

  
Extension Outputs

Bikes		Vehicles	
1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16
17	18	19	20
21	22	23	24



## 3.5 Factory Default and Reset to Factory

GRIDSMART Processors ship from the factory in the original “default” state, and the Site Card is labeled Factory Default. Resetting a Processor erases all configurations and history.



Reset to Factory cannot be performed remotely. You must either run the GRIDSMART Client on the Processor or run the Client on a laptop directly connected to the Processor through the local port.

Reset to Factory appears on the Site Configuration screen and requires Publish level privileges for the site.

1. Launch the GRIDSMART Client. The large Site Card appears as the Local Site on your Sites Homepage.
2. Click the Site Card to enter the Site View screen.
3. Click the Configure pencil on the Site Menu.
4. Click Revert on the Site Configuration screen, then click Reset to Factory.
5. Authenticate with the Publish password, then click Reset to Factory to complete the process.

Reset to Factory does not remove the original Site Card from the Sites Homepage. If you no longer need the old Site Card, you can safely delete it by clicking the Yellow X in the upper right-hand corner of the card.

## 3.6 Quad View

In Quad View, each of the four panels can display cameras in Fisheye view, pan-tilt-zoom view, and rectilinear view for traditional cameras.



## 3.7 Phases and Calls

Click the Traffic Signal icon in the Site Menu to display phases and calls during replay, as well as when viewing live, connected sites.



## 3.8 Make or Clear Calls on Operating Zones

To make or clear calls on operating zones, you must have connectivity to the site or be running GRIDSMART Client on the Processor. You must also have Admin or Publish level privileges.

1. Click to select a Site Card from the Sites Homepage.
2. Move the mouse pointer into a zone and directly above the phase/output label. The phase/output label content changes to action/info icons represented by a gear and the letter "i" respectively.




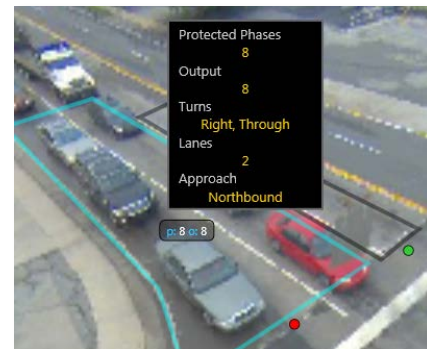
3. Click the Gear to open the Call and Clear buttons.
4. Click Call to activate a call on the zone. Click Clear to clear a call from the zone. You are required to authenticate with your username and password the first time you call or clear any zone.



For zones with designated phases, calls will persist until the light receives a green. Without a designated phase, calls will persist for 10 seconds.

Calls are not placed for two seconds when cleared in this manner. The zone will not reactivate until a new vehicle enters the zone or a vehicle already in the zone moves.

Click  to see zone phase information:



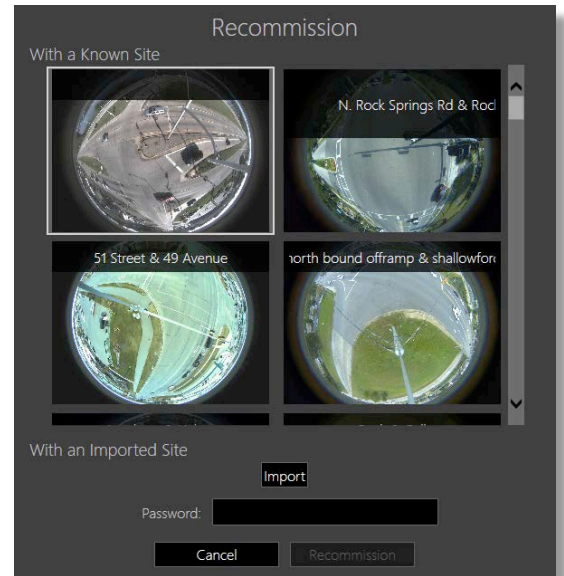
## 3.9 Recommission a Factory Default Processor



(Only appears on Factory Default systems)

To replace a Processor at an existing GRIDSMART site, use the Recommission feature.

1. Click the Recommission icon.
2. Authenticate with Admin or Publish credentials.
3. Select a Site Card to use with the new Processor, or, click Import to browse for the appropriate Site Card.
4. The Factory Default Processor will be configured with the selected Site configuration.



## 4.0 Publish

Publishing sends changes made in the GRIDSMART Client into live operation on the corresponding GRIDSMART Processor.



The Publish icon appears in the upper right-hand corner of the Site Configuration screen when you have unpublished changes. You must enter a username and password to Publish along with a brief description of the changes made.

Changes can be reviewed and/or reverted using the [Revert](#) feature.

All changes must be published to the Processor to be implemented.

The publish method has changed as we migrate towards improved security. To publish by default, if still using HTTP, you must type “publish” for the user name and then “aldis#world9” for the password. We strongly encourage that the administrator of the Processor creates appropriate user credentials.

### 4.1 Security – Admin, Publish and Read-only

There are three levels of security permissions in the GRIDSMART Client.

- **Publish** permission is required to [Publish](#) configuration changes.
- **Admin** permission is required to change. The Admin user also has Publish privileges.
- **Read-Only** provides access to view and troubleshoot but will be unable to publish.

### 4.2 Default Credentials

It is highly recommended to update these passwords on first login.

Permission Level	Username	Password	Capabilities using HTTP	Capabilities using HTTPS
<b>Admin</b>	admin	admin	Full access to GS <sub>2</sub> Device Manager, Admin account disabled in client software.	Full access to GS <sub>2</sub> Device Manager, Full access in client software.
<b>Publish</b>	publish	aldis#world9	Limited functionality in GS <sub>2</sub> Device Manager, can publish to site from client	Limited functionality in GS <sub>2</sub> Device Manager, can publish to site from client.
<b>Read-only</b>	aldis	aldis#world9	Limited functionality in GS <sub>2</sub> Device Manager, cannot publish in client.	Limited functionality in GS <sub>2</sub> Device Manager, cannot publish in client.

To change passwords, please refer to the Appendix - GS<sub>2</sub> Networking & Security.



## 4.3 Learning Mode

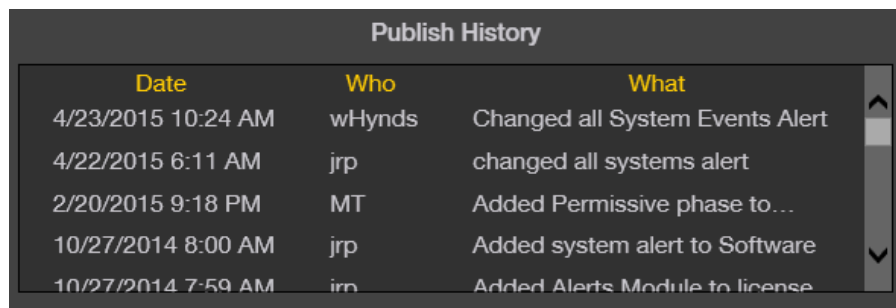
After the initial Configuration Publish, a System Reboot, Engine Restart or adding/replacing cameras, the GRIDSMART Processor will enter a Learning Mode for the first 4-6 minutes of system operation. The system operates in recall while the GRIDSMART Engine learns the scene.

## 4.4 Make Changes to a Site Configuration

Changing a site configuration is similar to configuring a new site as described in the [Factory Default](#) section.

1. Launch the GRIDSMART Client.
2. Click the appropriate Site Card on the Sites Homepage. The Site View screen appears.
3. Click the Configure icon on the Site Menu to enter the Site Configuration screen.
4. Make the desired changes.
5. Click Publish on the Site Configuration screen. If you are connected to the site, your changes are immediately placed into live operation after entering your username and password. If you are not connected and have a removable drive attached to your machine, you will be prompted to [Publish to Drive](#) (Only available if Site is running 6.9 or earlier).

## 4.5 Publish History



Date	Who	What
4/23/2015 10:24 AM	wHynds	Changed all System Events Alert
4/22/2015 6:11 AM	jrp	changed all systems alert
2/20/2015 9:18 PM	MT	Added Permissive phase to...
10/27/2014 8:00 AM	jrp	Added system alert to Software
10/27/2014 7:59 AM	irn	Added Alerts Module to license

Publish History displays all previously published changes made to a site configuration. Click the Info icon on the Site Menu to see the date, time, username and description of the changes.

Publish History is also displayed in the [Revert](#) panel on the Site Configuration screen.

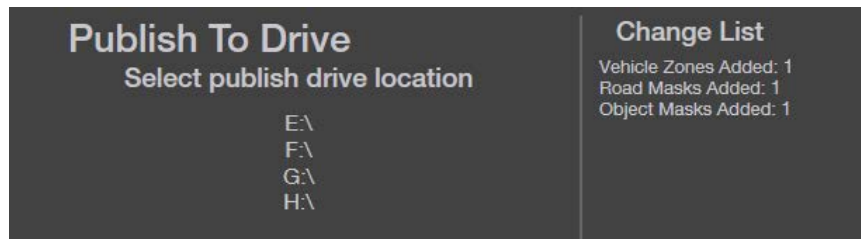
## 4.6 Make Changes to a Site without Taking a Laptop into the Field (Publish to Drive)

**Only available if Processor is running 6.9 or earlier**

This feature allows you to make changes to a site in your office or vehicle that can be put into field operation by simply connecting a USB storage device to the GRIDSMART Processor. When you have unpublished changes for a site to which you are not currently connected, clicking Publish on the Site Configuration screen will present the Publish to Drive dialog.

1. Make the desired changes to the site using the GRIDSMART Client.

2. Ensure that either an empty USB storage device or an already used Data Stick or Drive is connected to your Client computer.
3. Select Publish from the Site Menu, select the appropriate drive, and complete the publish procedure. If you began with an empty USB storage device, this process, once complete, will transform that device into a GRIDSMART Data Stick or Drive.
4. Take the USB device to the field and connect it to the corresponding GRIDSMART Processor. Observe the Processor front panel. Your changes will automatically be published onto the Processor. Additionally, data from the GRIDSMART Processor will be copied onto your Data Stick or Drive including log files, count data (if data-enabled), and image data.
5. Take the USB device from the field and connect it to your Client computer again. Until you do this, the changes you made will show as unpublished in your Client. This process will also copy count data from the Data Stick or Drive onto your Client computer for use within the Reports screen.



Publish to Drive will take your unpublished changes and put them onto the selected drive, making that drive a Data Stick or Drive. Your changes are published to the corresponding Processor when the Data Stick or Drive is connected to the Processor. The changes will continue to show as unpublished in your Client until the Data Stick or Drive is once again connected to your Client machine with the Client running.

## 4.7 Unpublished Changes

Unpublished changes are site modifications made in the Client that have not yet been put into operation. Unpublished mask and zone changes are indicated with a hash mark fill pattern in the Site View screen.



The Sites Homepage displays a hash mark fill pattern on Site Cards with unpublished changes.

Click Publish on the Site Configuration screen to save your changes.

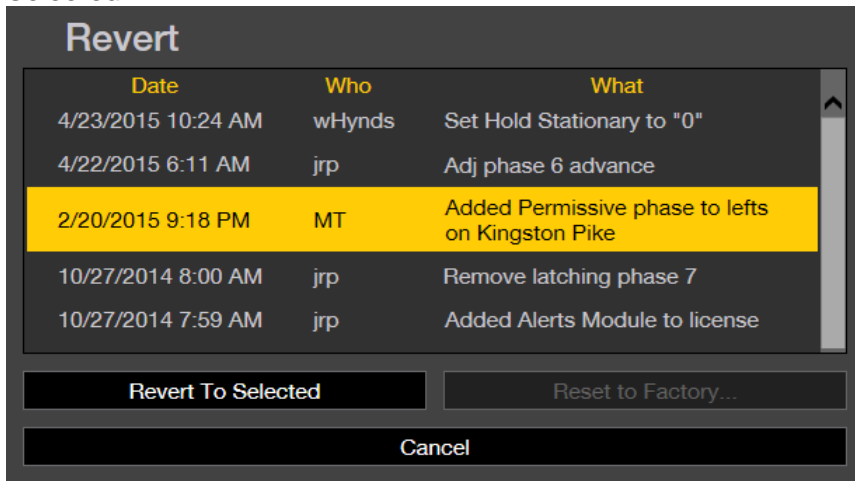


## 5.0 Revert



The Revert feature returns the GRIDSMART Processor to any previously published configuration.

1. To open the Revert panel, click the Configure pencil on the Site Menu, then click Revert to Selected.



2. Select a previously published configuration, then click the Revert to Selected button.
3. You must Publish a reverted configuration for it to take effect.

The current operational configuration is listed at the top of the Revert list. Revert to this configuration to remove any unwanted unpublished changes.

## 6.0 Site Info

Click the Info icon on the Site View screen to display location settings, including control settings, installed modules, cameras and publish history.

Site Info (v19.3)

Location Settings

Cherahala & Hardin Valley Knoxville Tennessee 37932 35.92 -84.2

Serial #

GS2-3963

Site Id

9de954a3-05bb-471e-9b7a-a06874f890ff

License Id

00E04B60BC16

IP Address

10.33.0.2

Date/Time

5/2/2019 1:17:17 PM (UTC-05:00) Eastern Time (US & Canada)

Control Settings

Full Control TS1

Modules

Performance+

Cameras

Proto RL

NE FE

257°/ 28 ft

37°/ 32 ft

Rectilinear

Fisheye

Show GRIDSMART API

Publish History

Date	Who	What
5/1/2019 5:43 PM	publish	removed box vehicle extension output
5/1/2019 1:57 PM	publish	
5/1/2019 1:54 PM	publish	
5/1/2019 1:54 PM	publish	
5/1/2019 1:52 PM	publish	

## 7.0 Modules

GRIDSMART offers add-on software modules that create your one-of-a-kind solution. Modules are independently licensed on each Processor and appear on the intersection Site Card.

### 7.1 GRIDSMART Data Modules

FEATURES	Performance Module	Performance Plus Module
<b>Client Reports</b>		
<b>Standard Reports</b>		
Volume	X	X
Turning Movement Count	X	X
Vehicle Classification	X	X
Incident	X	X
Raw Export	X	X
<b>Performance Reports</b>		
Seven Day Volume	X	X
Green Occupancy	X	X
Red Occupancy	X	X
Percent Arrivals on Green	X	X
Percent Arrivals on Red	X	X
Speed	X	X
<b>Auto Reports</b>	X <sup>1</sup>	X <sup>3</sup>
<b>GRIDSMART.cloud Reports</b>	X <sup>1</sup>	X <sup>3</sup>
<b>Alerts<sup>2</sup></b>		
All System Events	X <sup>1</sup>	X <sup>3</sup>
Loss of Visibility		X <sup>3</sup>
Volume Exceeded		X <sup>3</sup>
Loss of Green (Flash)		X <sup>3</sup>
Zone Activated		X <sup>3</sup>
<b>H.264 Streams</b>		X <sup>1, 4</sup>
<b>Minute by Minute Display</b>	X <sup>1</sup>	X <sup>1</sup>
<b>Vulnerable Road Users</b>		
Pedestrian Crosswalk Extensions		X <sup>4</sup>
Bicycle Clearance Extensions		X <sup>4</sup>

#### KEY

1 Requires WAN connectivity.

2 Alerts are delivered via email upon occurrence. Events shown in GRIDSMART Cloud are updated once daily, not upon occurrence.

3 Requires External Antenna or WAN connectivity.

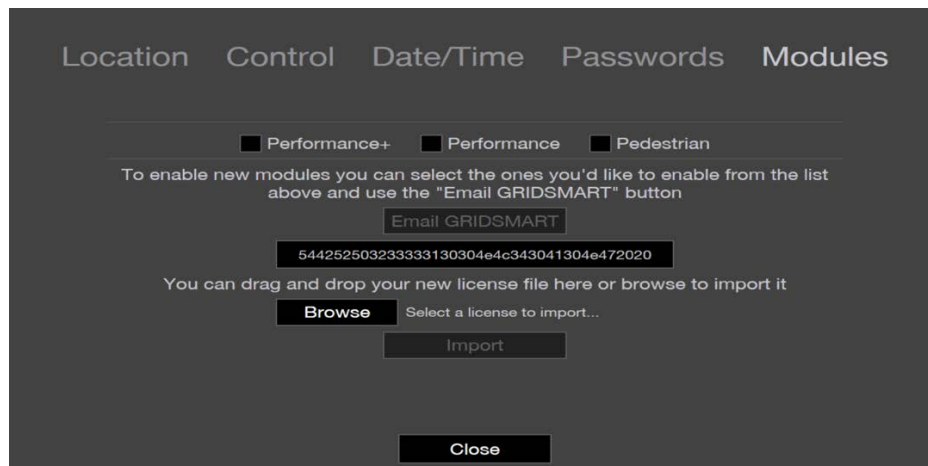
4 Requires GS2 Processor

## DESCRIPTIONS OF ALERTS

All System Events	On system events such as Publish, Startup, IP address change, Camera Offline/Online.
Loss of Visibility	When the camera visibility is lost for any zone. Includes snapshot.
Volume Exceeded	When the site volume exceeds a set amount.
Flash (Loss of Greens)	When the intersection is suspected to be in flash.
Zone Activated	When a zone is activated. Can be used for wrong-way detection.

## 7.2 Add a Module

1. Launch the GRIDSMART Client and click the appropriated Site Card.
2. Click the Configure pencil, then click Site Settings.
3. Click the Modules tab.
4. Follow the instructions to add a new Module license files.
5. Publish your changes after you receive and import the license files.



Note. If the GRIDSMART Processor is communicating to GRIDSMARTCloud.com, the license will be synced automatically.

## 8.0 Reports



### REPORTS

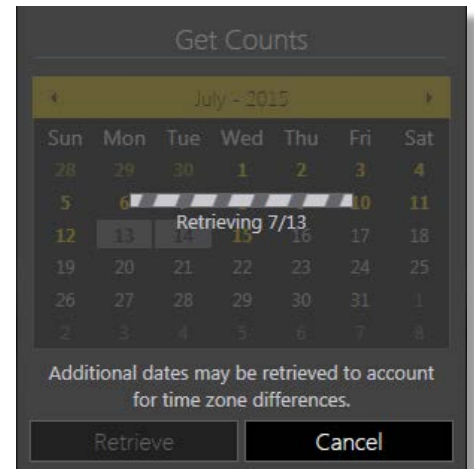
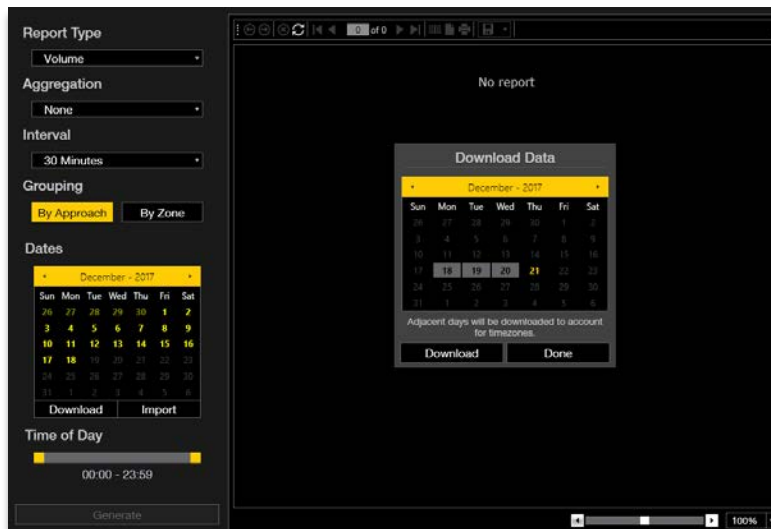
With the PERFORMANCE and PERFORMANCE PLUS Modules, GRIDSMART automatically logs vehicle counts for up to one year. Counts are stored on a first in, first out basis.

### 8.1 Get PERFORMANCE DATA with the Client

When connected to a site either locally or remotely, use the GRIDSMART Client to retrieve count data.

1. Click the appropriate Site Card on the Sites Homepage.
2. Click the Reports icon on the Site Menu.

3. On the Reports Screen, click the Download button under the calendar on the left. In the calendar that appears in the middle of the window, select one day or several days of data to retrieve.
4. Click the Download button under the middle calendar, then Done once the data has been downloaded. It may take a while to retrieve data over slow connections.



## 8.2 Get PERFORMANCE DATA with a USB Storage Device

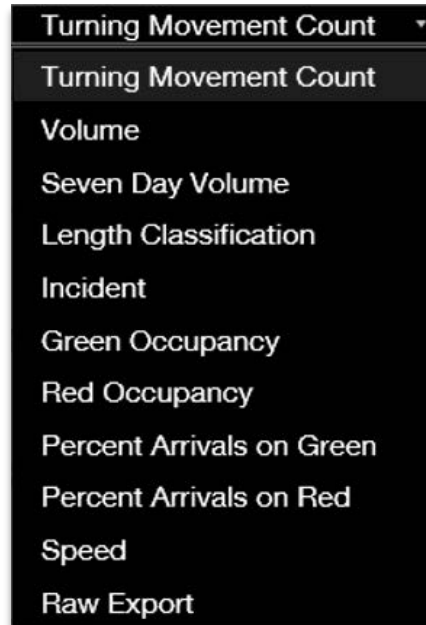
1. Begin with a freshly NTFS-formatted USB storage device or with a Data Stick or Drive that you have already used with GRIDSMART. If you are formatting a new device with greater than 128GB of storage, please select NTFS.
2. Ensure that there is enough free space on the device for your needs.
3. Connect the USB storage device to a USB port on the GRIDSMART Processor. Observe the front panel.
4. Images and other data – including counts for systems with the Data Module – are automatically copied onto the device. For large capacity devices (>128GB), images will be stored at approximately 5-10 images per second until the drive is full. For small capacity devices, images will be stored at approximately one image per second for only three minutes.
5. Once you have collected the data you need, and the Processor front panel indicates that it is safe to do so, disconnect the USB device from the Processor. This USB device is now a GRIDSMART Data Stick or Drive.
6. Connect your Data Stick or Drive to the computer where you intend to use the GRIDSMART Client for reporting.
7. Launch the Client, select the Site Card for your site of interest and then click Reports (chart icon) on the Site Menu.
8. The count data from your Data Stick or Drive will be automatically synchronized with your Client and available for use in the Reports Screen as indicated by highlighted dates in the calendar.



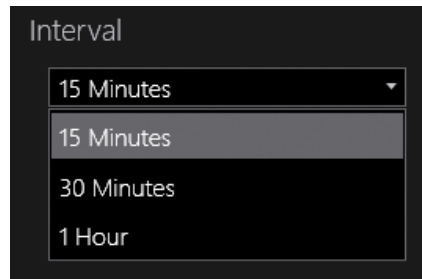
## 8.3 Generating Reports

Once the Counts have been downloaded or synced to the Client, click the Reports icon and choose your options.

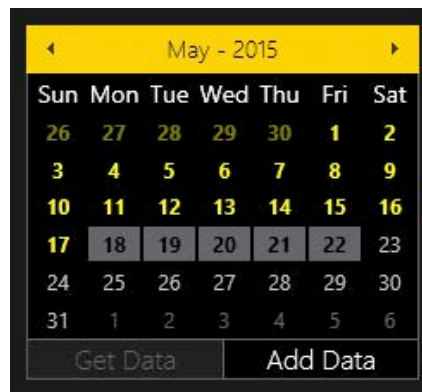
Select the Report Type.



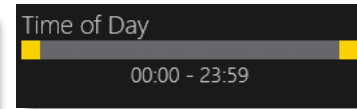
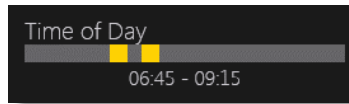
Select the Interval.



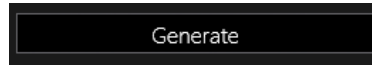
Click a date or drag the cursor to highlight a date range.



Use the slider to specify the Time of Day.



Click Generate.



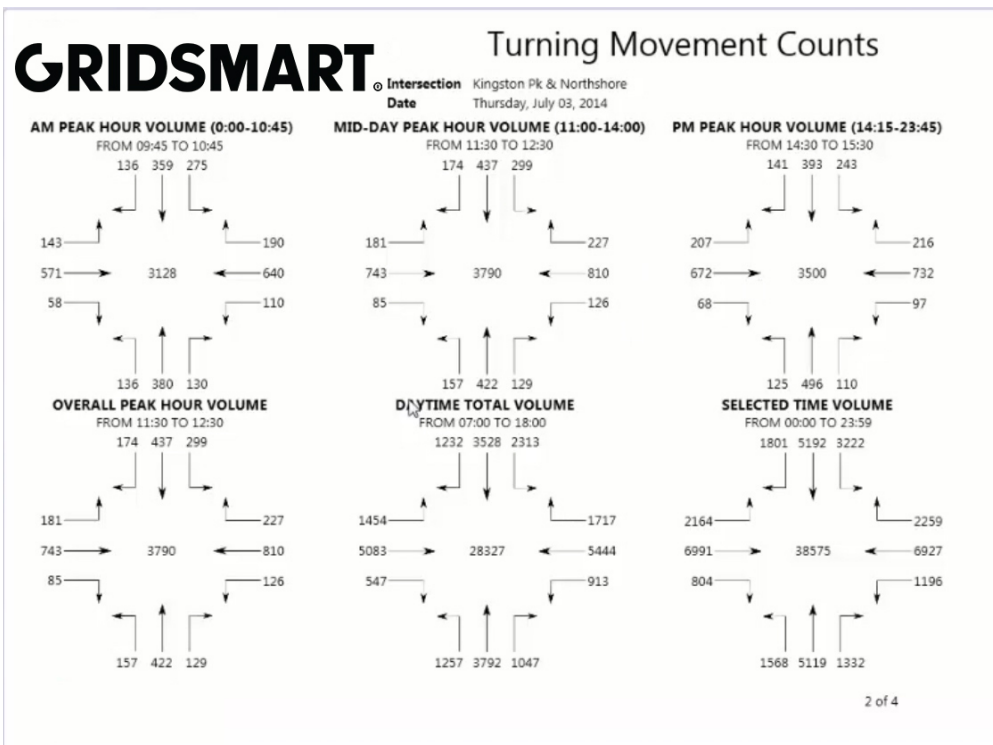
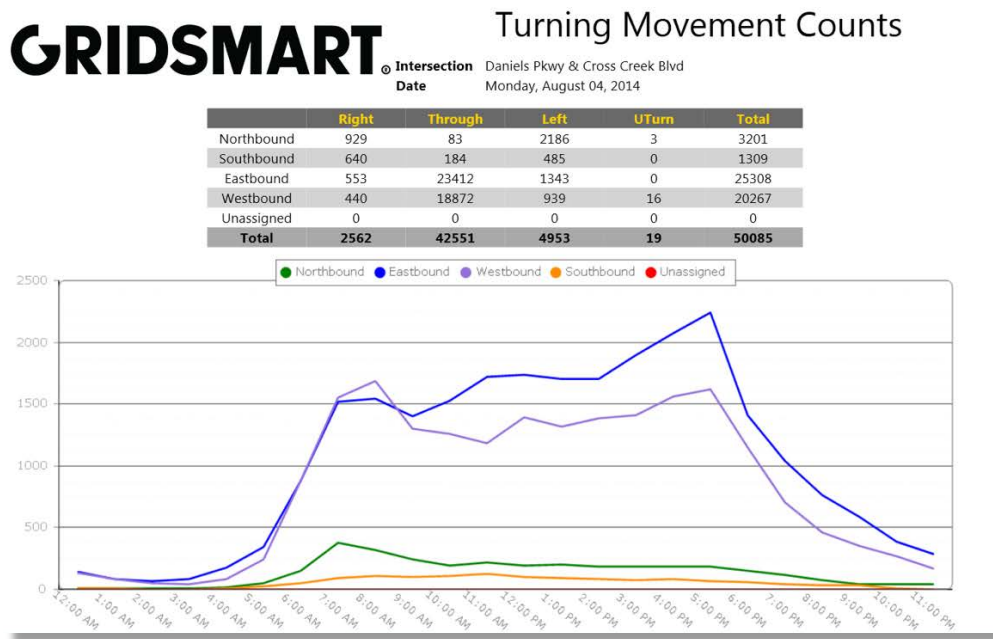
Use the header to Browse, Print, or Export pages.



Click the disk to save the report as:

1. PDF
2. Excel

## 8.3.1 Report – Turning Movement Counts



## 8.3.2 Report – Vehicle Classification

Use the sliders under Edit Bins to define customized vehicle length bins.

Report Type

Vehicle Classification

Edit Bins

Length Bins

Bin 1 0-9 ft

Bin 2 10-23 ft

Bin 3 24-35 ft

Bin 4 36-51 ft

Bin 5 52-73 ft

Defaults Okay

## GRIDSMART

Intersection  
Date

## Vehicle Classification Counts

Hardin Valley & Cherahala  
Tuesday, June 02, 2015

	Northbound				Southbound				
	0-9'	10-23'	24-35'	36-51'	0-9'	10-23'	24-35'	36-51'	0-9'
11:30 AM	4	20	2	2	6	54	11	6	26
11:45 AM	2	15	4	1	11	46	16	6	22
12:00 PM	6	26	1	0	12	63	13	8	28
12:15 PM	3	17	4	4	8	59	9	11	27
12:30 PM	4	16	3	1	7	36	5	5	29
12:45 PM	3	14	0	1	6	36	5	4	26
1:00 PM	1	16	3	1	5	43	7	5	20
1:15 PM	5	10	3	2	4	44	13	4	27
1:30 PM	3	10	5	0	6	59	17	11	34
1:45 PM	2	15	3	1	3	36	9	4	24
2:00 PM	4	6	2	1	4	29	8	9	32
2:15 PM	4	5	3	0	7	30	13	7	24
<b>Total</b>	<b>41</b>	<b>170</b>	<b>33</b>	<b>14</b>	<b>79</b>	<b>535</b>	<b>126</b>	<b>80</b>	<b>319</b>

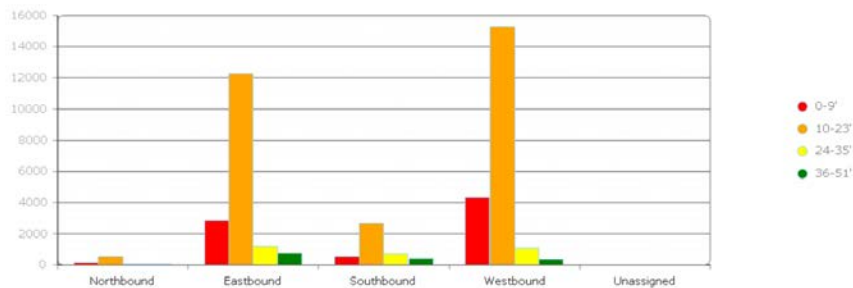
## GRIDSMART

Intersection  
Date

## Vehicle Classification Counts

Hardin Valley & Cherahala  
Tuesday, June 02, 2015

	Northbound	Southbound	Eastbound	Westbound	Unassigned	Total
0-9'	117	497	2844	4303	0	7761
10-23'	478	2717	12280	15233	0	30708
24-35'	79	662	1202	1090	0	3033
36-51'	38	456	745	354	0	1593
<b>Total</b>	<b>712</b>	<b>4332</b>	<b>17071</b>	<b>20980</b>	<b>0</b>	<b>43095</b>



## 8.3.3 Report – Incidents Excel Output

A1	:	X	✓	<i>fx</i>	10/26/2012							
	A	B	C	D	E	F	G	H	I	J	K	
1	10/26/2012	11:45.2	29505	1	ILLEGAL_LEFT	32.0511	0	T6	61	PG	SR	
2	10/26/2012	17:07.3	29827	1	ILLEGAL_LEFT	32.0552	0	T0	20	PG	SR	
3	10/26/2012	21:18.8	30078	1	ILLEGAL_LEFT	30.6899	0	T3	20	PG	SR	
4	10/26/2012	22:40.8	30160	4	ILLEGAL_LEFT	52.4821	0	T0	16	PG	S	
5	10/26/2012	30:14.0	30614	1	ILLEGAL_LEFT	29.6204	0	T0	17	PG	SR	
6	10/26/2012	30:59.8	30659	1	ILLEGAL_LEFT	37.7162	0	T2	55	PG	SR	
7	10/26/2012	31:20.7	30680	8	ILLEGAL_RIGHT	33.7939	0	T0	7	PG	S	
8	10/26/2012	32:03.9	30723	10	ILLEGAL_LEFT	48.3713	0	T0	11	PG	S	
9	10/26/2012	34:42.1	30882	2	ILLEGAL_RIGHT	32.044	0	T1	19	PG	LS	
10	10/26/2012	45:09.5	31509	1	ILLEGAL_LEFT	25.169	0	T1	20	PG	SR	
11	10/26/2012	50:46.5	31846	1	ILLEGAL_LEFT	30.6881	0	T6	73	PG	SR	
12	10/26/2012	53:43.3	32023	2	ILLEGAL_RIGHT	27.1043	0	T0	19	PG	LS	
13	10/26/2012	58:54.9	32334	1	ILLEGAL_LEFT	25.1757	0	T1	21	PG	SR	
14												

## 8.3.4 Report – Incidents Report

# GRIDSMART

## Incident Report

Intersection Kingston Pk & Northshore  
Date Monday, July 13, 2015

	Northbound	Southbound	Eastbound	Westbound	Total
Illegal Turn	14	6	13	19	52
Red Light	201	153	43	121	518

### Exits on Red

	Northbound	Southbound	Eastbound	Westbound	Total
11:30 AM	109	87	25	58	279
12:30 PM	92	66	18	63	239
<b>Total</b>	<b>201</b>	<b>153</b>	<b>43</b>	<b>121</b>	<b>518</b>

### Illegal Turns

	Northbound			Southbound			Eastbound			Westbound		
	R	T	L	R	T	L	R	T	L	R	T	L
11:30 AM	0	6	0	0	2	1	0	8	0	0	8	2
12:30 PM	0	8	0	0	0	3	0	5	0	0	8	1
<b>Total</b>	<b>0</b>	<b>14</b>	<b>0</b>	<b>0</b>	<b>2</b>	<b>4</b>	<b>0</b>	<b>13</b>	<b>0</b>	<b>0</b>	<b>16</b>	<b>3</b>

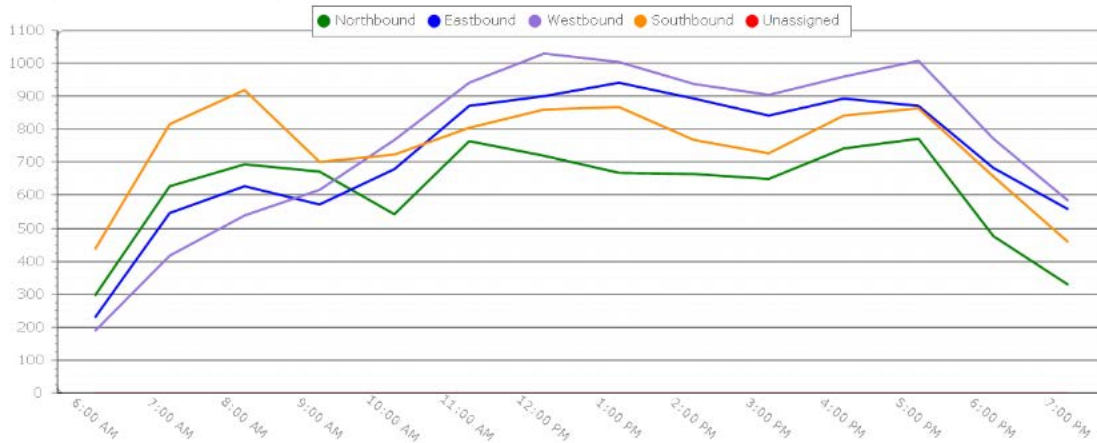
## 8.3.5 Report – Volume

# GRIDSMART

## Volume Report

Intersection: Kingston Pk & Northshore  
Date: Monday, July 13, 2015

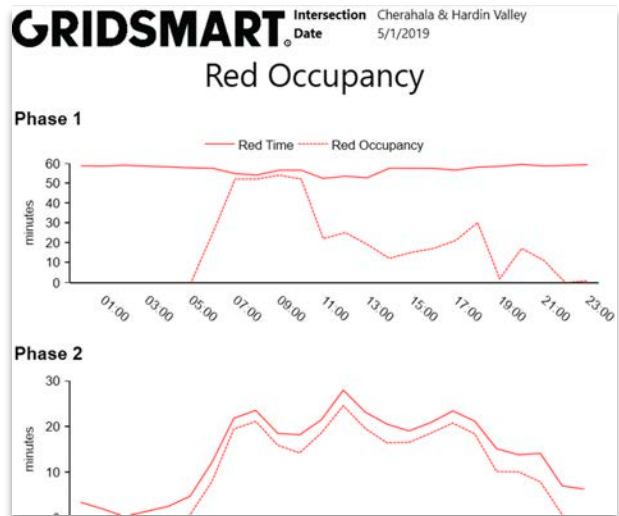
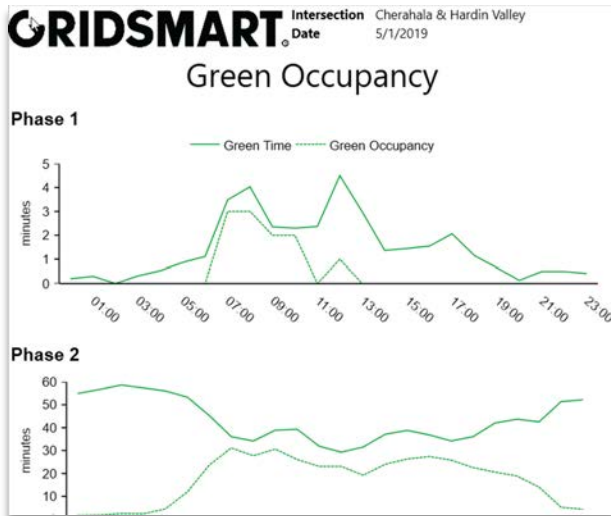
	Total
Northbound	8603
Southbound	10434
Eastbound	10106
Westbound	10663
Unassigned	0
<b>Total</b>	<b>39806</b>



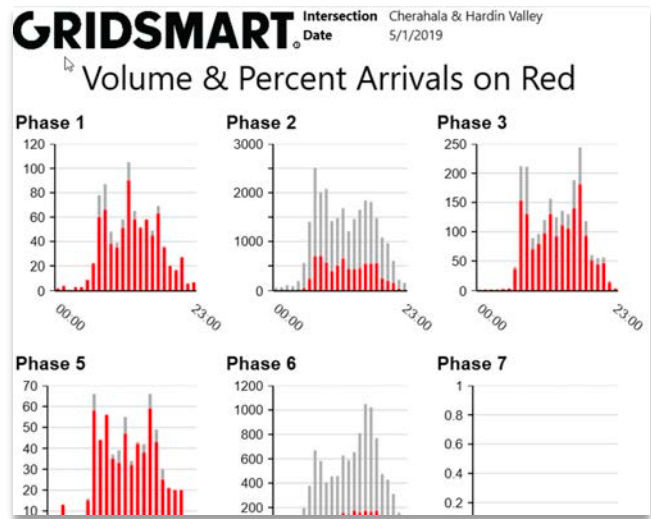
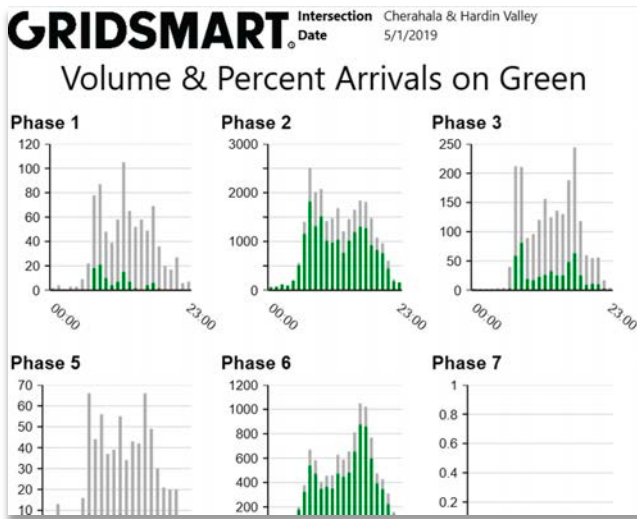
	Northbound	Southbound	Eastbound	Westbound	Total
6:00 AM	294	435	228	187	1144
7:00 AM	626	814	548	417	2405
8:00 AM	693	919	629	540	2781
9:00 AM	672	703	572	618	2565
10:00 AM	542	723	681	768	2714
11:00 AM	763	803	870	940	3376
12:00 PM	719	859	900	1029	3507
1:00 PM	667	866	942	1003	3478
2:00 PM	663	766	894	938	3261
3:00 PM	648	729	840	903	3120
4:00 PM	741	840	893	959	3433
5:00 PM	773	865	870	1008	3516
6:00 PM	475	656	683	770	2584
7:00 PM	327	456	556	583	1922
<b>Total</b>	<b>8603</b>	<b>10434</b>	<b>10106</b>	<b>10663</b>	<b>39806</b>



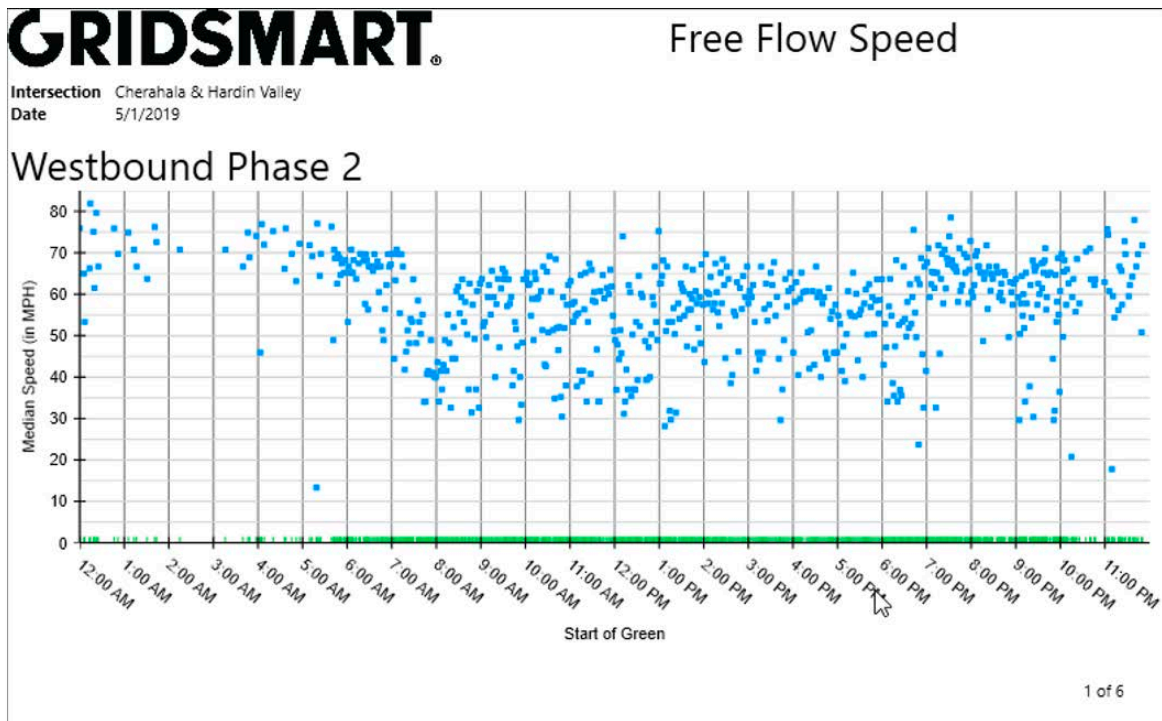
## 8.3.6 Report – Green/Red Occupancy



## 8.3.7 Report – Percent Arrivals On Green/Red



## 8.3.8 Report – Speed



## 8.3.9 Report – Raw Data Export

Creates a CSV file with raw count data.

A1													

## 8.4 Auto Reports



Automatically email reports to a group of contacts on a schedule. This functionality is included as part of the Counts Module and requires a connected Processor.

1. Launch the GRIDSMART Client and click on the appropriate Site Card.
2. Click the Configure pencil to open the Site Configuration screen.
3. Click the Auto Reports icon in the upper right-hand corner of the Site Configure screen, then click New.
4. Set the desired report parameters, then click Next.
5. Enter the recipients' email addresses or select them from the list of known contacts.
6. Publish your changes.

## 9.0 Alerts



The Alerts Module sends emails to a user-defined set of contacts when the GRIDSMART Processor detects certain events.

Site Alerts include All System Events, Loss of Visibility, Volume Exceeded and Flash (Loss of Greens). All System Alerts are included with your GRIDSMART system and do not require the Alerts Module.

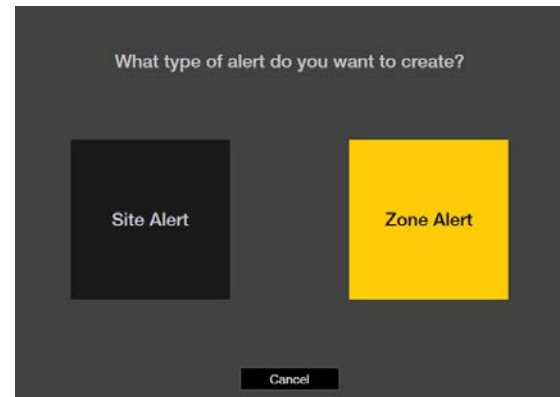
Zone Alerts include Volume Exceeded and Zone Activated, where Zone Activated alerts can be used to detect wrong way travel or breakdown lane occupancy.

To create an Alert, click the Configure pencil on the Site Menu, then click Alerts in the upper right-hand corner.

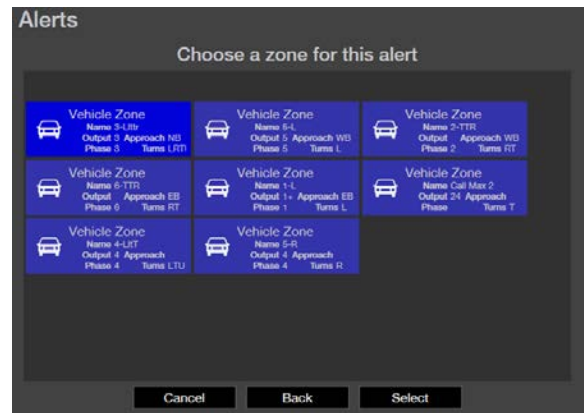
Click New.



Click Site Alert or Zone Alert.

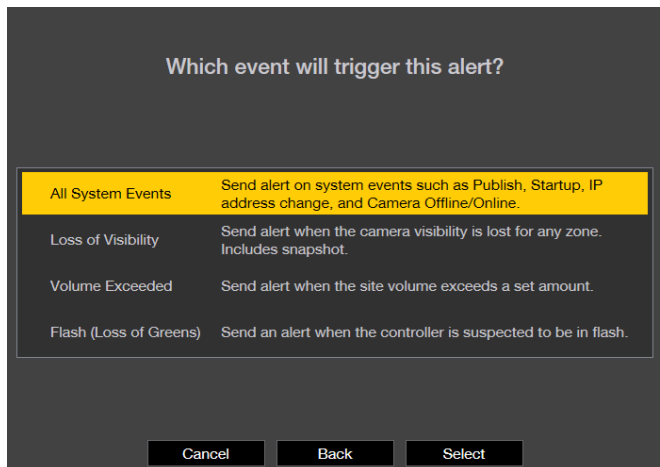


If you are creating a Zone Alert, choose a vehicle zone, then click Select.



Choose an event to trigger the alert, then click Select.

The intersection is determined to be in flash if twelve seconds pass without the GRIDSMART system receiving any green lights from the controller.



Add users to notify. Enter a new email address or select from a list of your existing contacts.

Optionally add an alert name. The name defaults to the event type.

Enter the maximum volume for Volume Exceeded alerts.

Select an approach for Site Alerts.

Use the slider to indicate the active time period.

Zone Activated alerts are generally used for breakdown lane or wrong way detection.

Camera images are attached to the email. Up to twelve emails will be sent per hour.

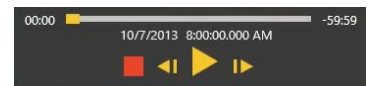
Publish your changes.

## 10.0 Replay



The Replay feature enables playback of data (images, phases, calls) acquired from a GRIDSMART Processor by connecting a Data Stick or Drive.

The Replay function (movie reel icon) is accessible on the Site Menu.



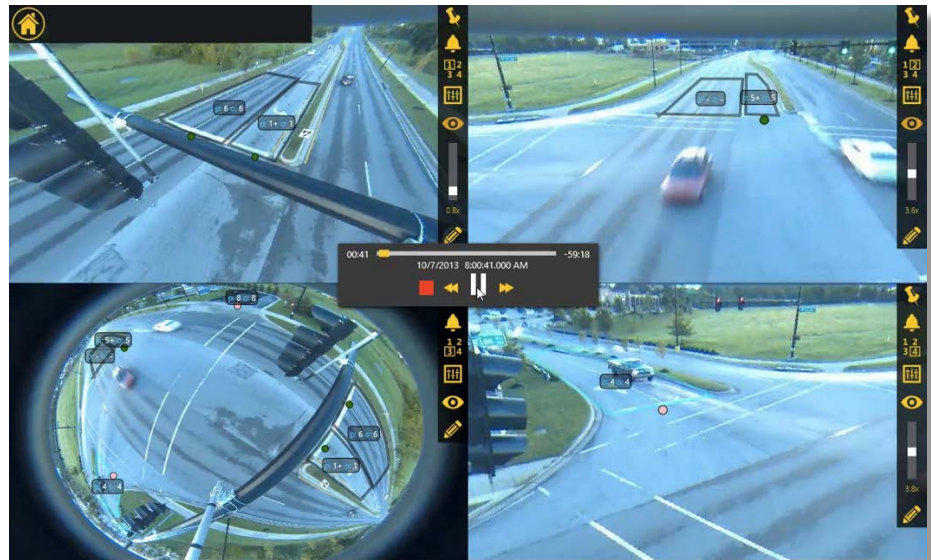
1. Connect the Data Stick or Data Drive to your GRIDSMART Client computer, then launch the Client.
2. Click the appropriate Site Card, then click Replay from the Site Menu. The Select Data to Display window opens.
3. Click Select the Day and Hour of data from the connected Data Drive. Or Browse to a Counts Folder if not using the original data drive.
4. Use the playback controls to review the data. Press the red Stop button when you have finished.



Fisheye View  
Replay



Quad View  
Replay



## 10.1 Record and Review Images and/or Performance Data

1. Begin with a freshly NTFS-formatted USB storage device obtained from GRIDSMART Support or a Data Stick or Drive that you have previously used with GRIDSMART.
2. Ensure that the device has enough free space to support your needs. A single Fisheye Camera requires approximately 100 GB per day.
3. Connect the USB storage device to a USB port on the GRIDSMART Processor and observe the front panel. Images and other data, including logs and counts, are automatically copied onto the device. On large capacity devices (>128GB), images are stored at a rate of 5-10 images per second until the drive is full. On small capacity devices, images are stored at approximately one image per second for three minutes only.
4. After collecting the data, disconnect the USB storage device from the Processor. This storage device is now a GRIDSMART Data Stick or Data Drive.

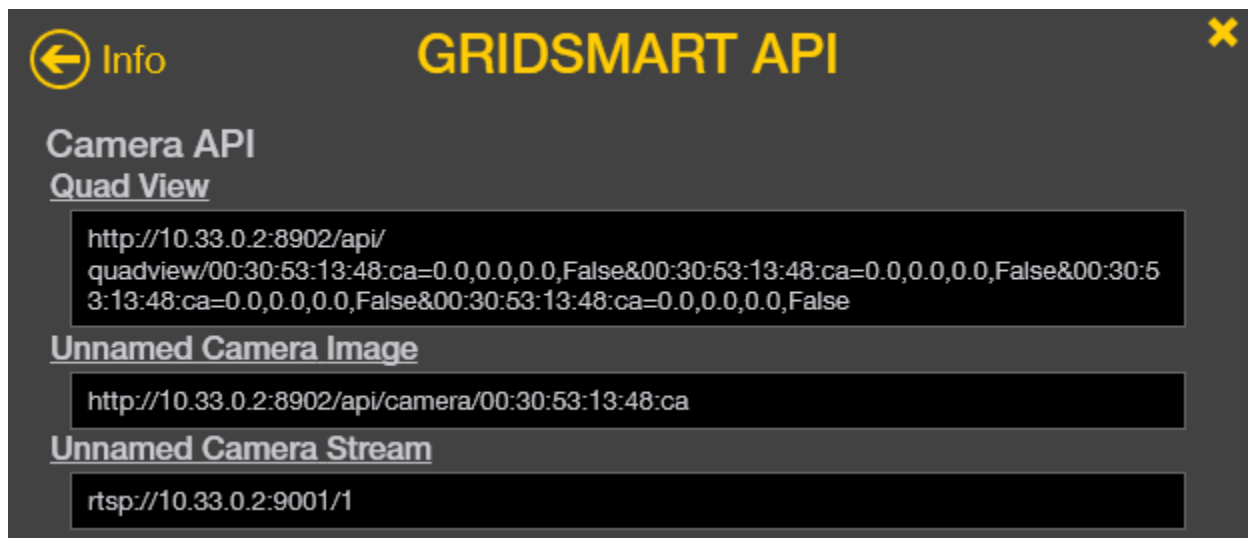


## 11.0 GRIDSMART API

The GRIDSMART Application Programming Interface (API) retrieves data and images from GRIDSMART Processors using HTTP or HTTPS. To view examples of the camera API calls, click Info, on the Site Menu, then click Show GRIDSMART API.

With the API, you can:

1. See live Quad View and single camera images in a web browser
2. Automate the retrieval of Counts and Realtime data.
3. View site history, current configuration and camera status.
4. And much more...



See the [API documentation](#) on the GRIDSMART Support Portal for more details.

## 12.0 Streaming H.264 streams via RTSP

Streaming is now possible with the purchase of a Performance Plus module and with a high-speed connection to the GS2 processor and video management or network video system software and/or hardware. The customer and/or customer's vendor are responsible for de-warping the images, if desired, as well as for integration into their existing system. GRIDSMART will supply instructions for accessing the streams.

1. Streams are 10 frames per second (FPS) for both Bell and Traditional Cameras.
2. The image resolution for a Bell Camera is 1280 X 960 while the Traditional Camera is 640 X 480.
3. Each Bell Camera stream requires approximately 10Mb/s and each Traditional Camera stream requires approximately 5 Mb/s.
4. You can access the streaming link by going to the GRIDSMART API and finding the Stream Link. To open the API Panel, click Info, on the Site Menu, then click Show GRIDSMART API. From here you will see the Stream link that can be copied.
5. Port 9000 – 9007 MUST be open.

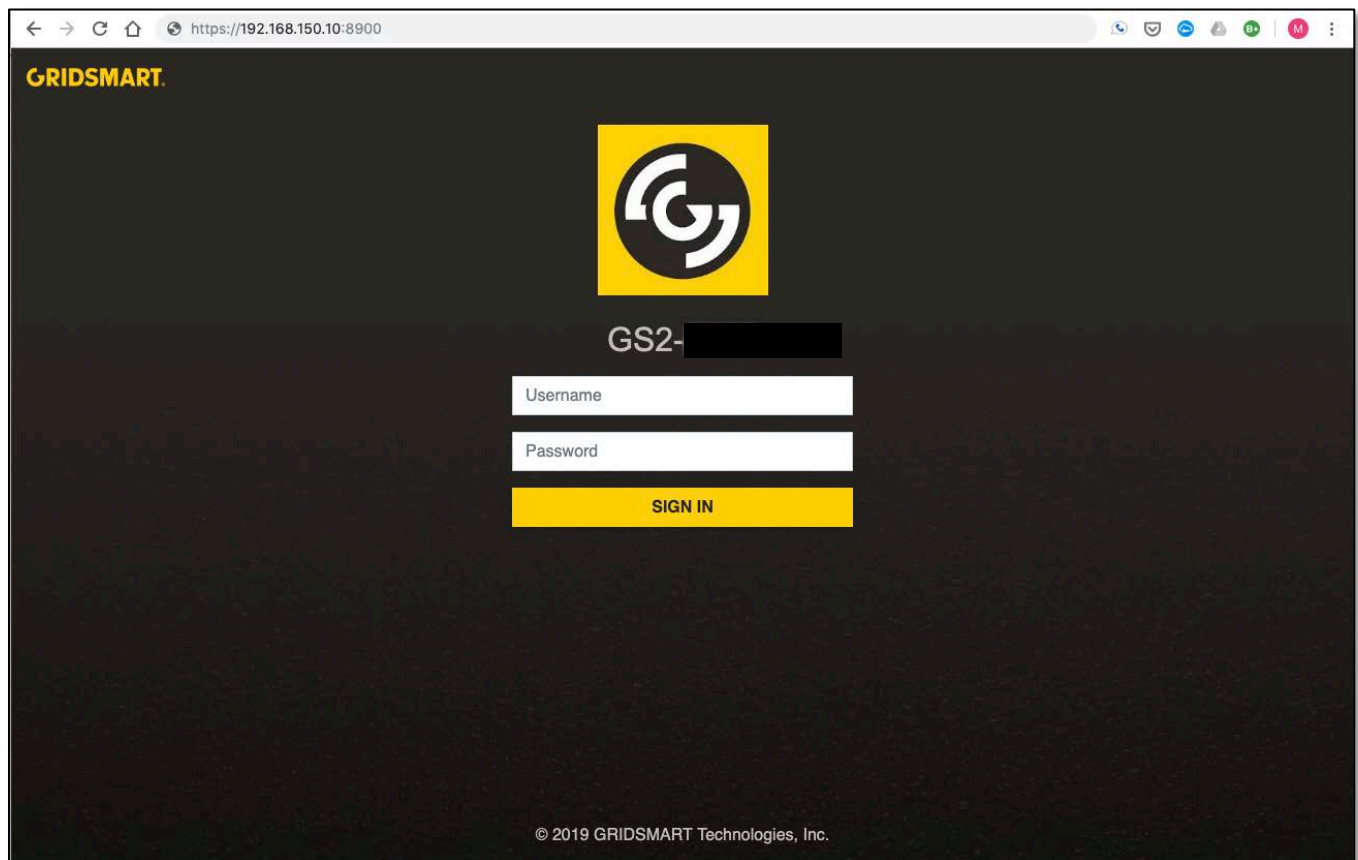
## 13.0 GS<sub>2</sub> Device Manager

Basic device configuration such as network, date/time, user management, and NTP is now done only via browser, providing a device-focused, secure alternative to the Client. Also, through this new interface, you can configure network/security settings, date/time, and location without requiring a connected camera.

The GRIDSMART device manager is accessible via web browser, when connected to the processor laptop port, at **https://192.168.150.10:8900**. There is also a link on the processor desktop if you are connected via VNC. Using this device manager will require the default administrator account credentials.


The default administrator account is '**admin/admin**'.

GRIDSMART recommends changing the default accounts.



← → ↻ 🏠 🔍 https://192.168.150.10:8900

**GRIDSMART.**



GS2- [REDACTED]

Username

Password

**SIGN IN**

© 2019 GRIDSMART Technologies, Inc.

## 13.1 Network

Select the Network tab to configure the GS<sub>2</sub> for your network.

In order for GS<sub>2</sub> to sync to an NTP Time Server, Port 123 MUST be open.

GRIDSMART. Serial # Hardware Id Location admin

**Network** Certificates Client/API GRIDSMART Cloud Static Routes Reset

☐ Use DHCP

Network Address  
192.168.0.5

Netmask  
255.255.255.0

Gateway  
192.168.0.1

DNS  
192.168.0.1

NTP Server  
pool.ntp.org Sync Time

Apply changes Cancel changes

### 13.1.1 Certificates

Version 19.3 contains a self-signed SSL certificate to provide a secure connection. Users may use their own SSL certificate.

**Network** Certificates Client/API GRIDSMART Cloud Static Routes Reset

ISSUED BY  
**GRIDSMART Engineering**  
Knoxville, TN US

ISSUED TO  
**GRIDSMART Engineering**  
Knoxville, TN US

Expires  
August 24, 2046 (in 27 years)

Issued  
April 9, 2019

Change certificate

## 13.1.2 Client/API (Users may now configure HTTPS and modify the API and UI ports.)

**Network**

Cameras

Diagnostics

Modules

Users

Location

Date/Time

Security

System Operations

Network Certificates **Client/API** GRIDSMART Cloud Static Routes Reset

Transport

☒ HTTP ☐ HTTPS

API Port

8902

Port number for connecting to the API

Configuration UI Port

8900

Port number for accessing this configuration utility

Apply changes Cancel changes

## 13.1.3 GRIDSMART Cloud

In order for GS<sub>2</sub> to communicate to GRIDSMARTCloud.com, Port 443 MUST be open and have outbound access to api.gridsmart.com.

**Network**

Cameras

Diagnostics

Modules

Users

Location

Date/Time

Security

System Operations

Network Certificates Client/API **GRIDSMART Cloud** Static Routes Reset

☒ Use GRIDSMART Cloud

How would you like the GS<sub>2</sub> to connect to the GRIDSMART Cloud?

☒ Allow GRIDSMART to use my network (disables modem)

☐ Use modem

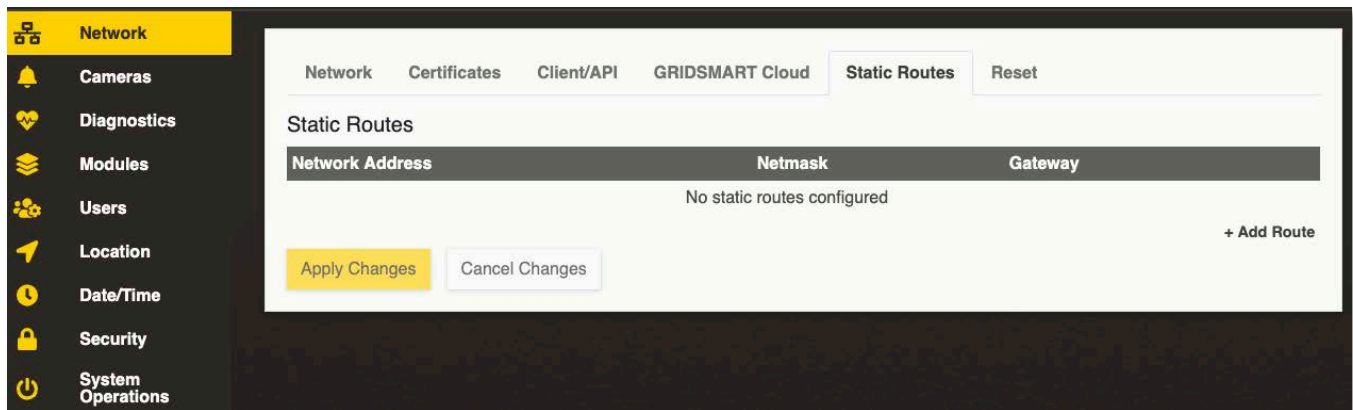
Connectivity

Status: Not checked

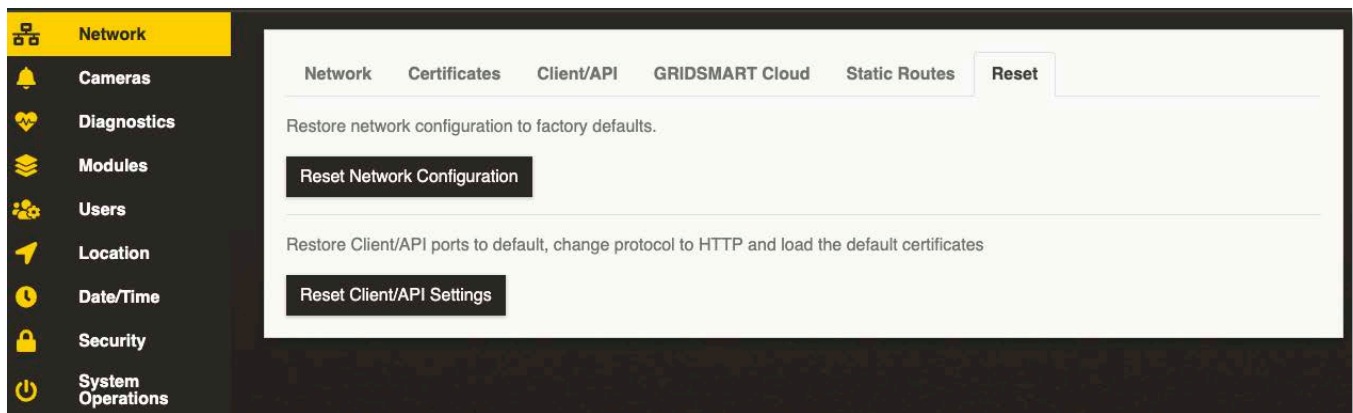
Check Connection

Apply changes Cancel changes

## 13.1.4 Static Routes



## 13.1.5 Reset



### Reset Network Configuration:

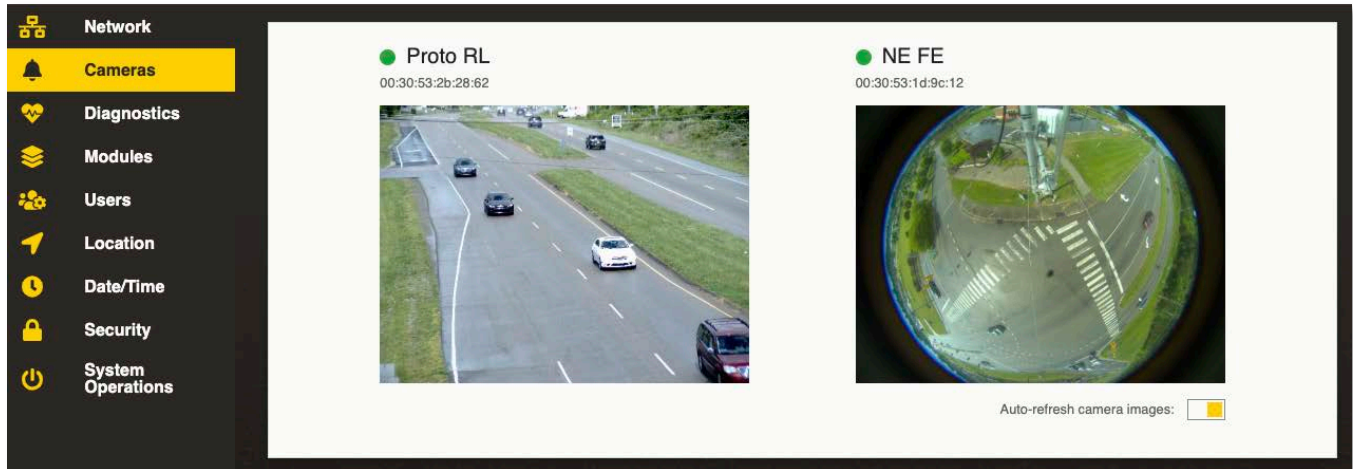
Erases user defined network settings and sets the network to DHCP.

### Reset Client/API Settings:

- sets API Port to 8902
- sets Configuration UI Port to 8900

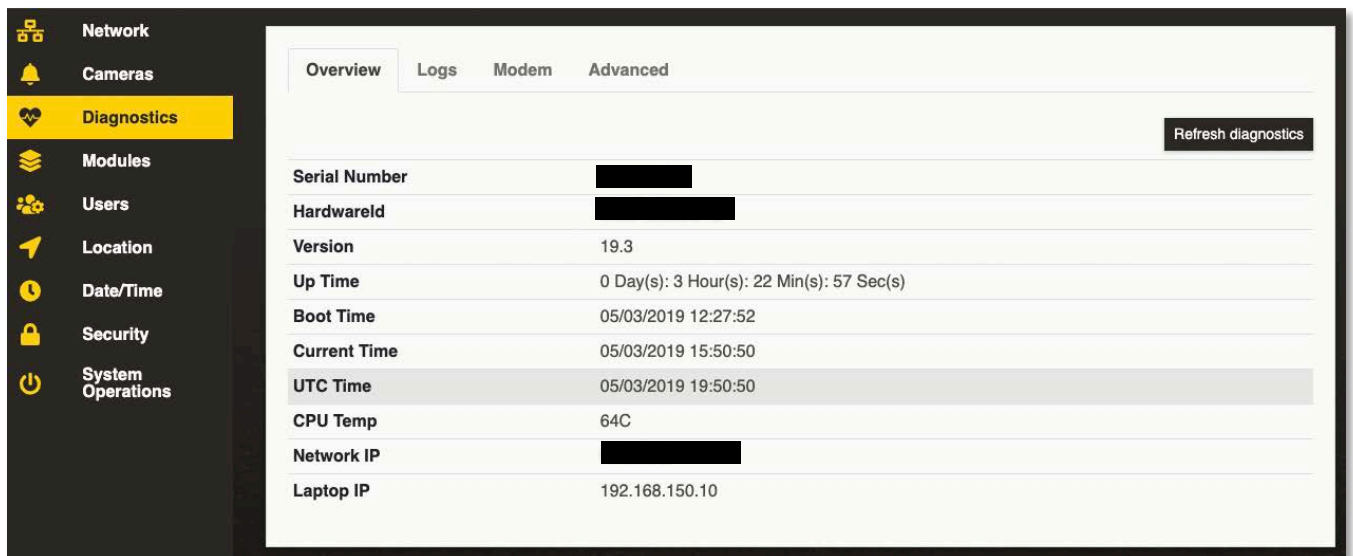
## 13.2 Cameras

The Cameras Page displays connected cameras, 1frame/5sec. The Auto-refresh may be turned off by toggling the switch on the bottom right.



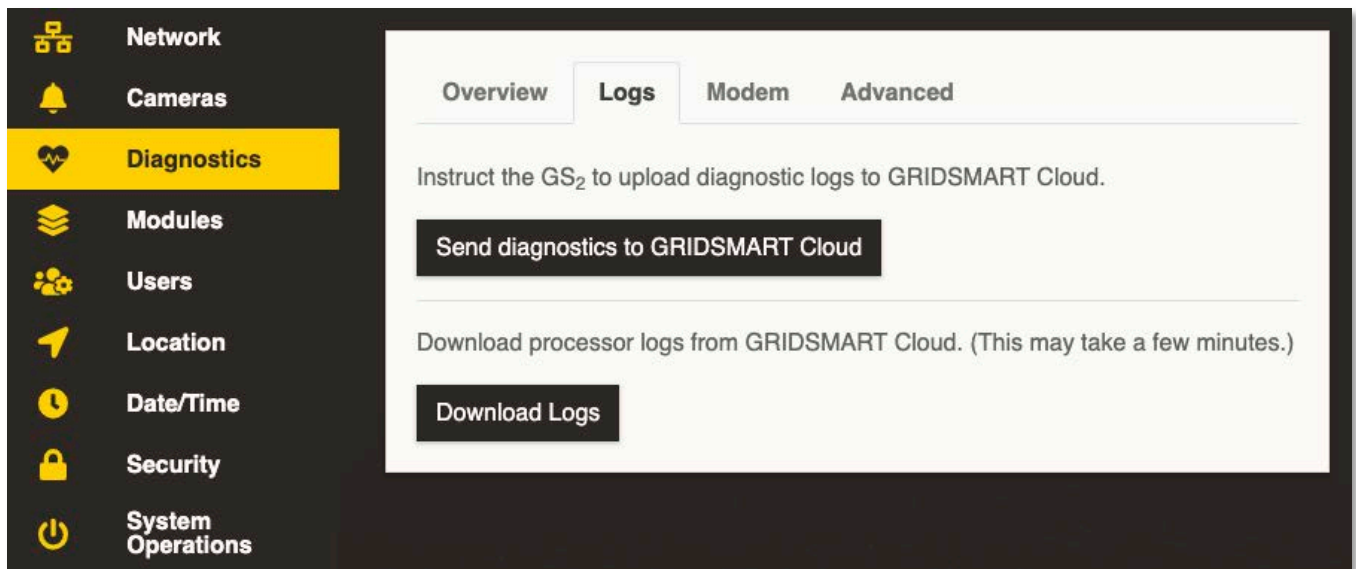
## 13.3 Diagnostics

This will give you an overview of network information, the ability to download logs or send logs to the GRIDSMART Cloud, view modem information, and advanced network information.





Diagnostic logs may be collected from GRIDSMARTcloud.com.



GRIDSMART Client logs may be collected from double-clicking "GRIDSMART" in the Client.



## 13.4 Modules

This allows licenses to be uploaded or synced as needed.

Module	Expires	Activated
PERFORMANCE +	Never	May 2, 2019

Upload a new license

License File

Choose a .xml file Browse

Upload License Sync licenses

## 13.5 Users

A new feature that allows the Processor Admin to create new users and assign roles based on needs.

Note: A 'publish' username and password is required to Publish changes to a GRIDSMART Site.

Username	Role	Description		
publish	publish	publish account		
admin	admin	admin account		
aldis	readonly	default user		

Add new user

Refer to Section 4.2 for more details.

## 13.6 Location

This allows configuration of the location for the GS<sub>2</sub> processor.

**Location**

Street 1  
Cherahala  
First street of intersection name

Street 2  
Hardin Valley  
Cross street of intersection name

Postal Code  
37932

City  
Knoxville

State  
Tennessee

County  
Knox

Country  
USA

Latitude  
35.92

Longitude  
-84.2

☒ Right-side driving  
☐ Metric units

**Publish changes** **Cancel changes**

## 13.7 Date/Time

This displays the current Date/Time and allows setup as well as time sync.

**Device Date/Time**

May 03, 2019 04:03 pm

**Manually Set Date/Time**

(UTC-05:00) Eastern Time (US & Canada) ▾

**Update timezone**

## 13.8 Security

This screen allows for disabling and enabling of USB drives and the VNC server as well as displaying status of security recommendations.

Setting	Status	Recommendation
Default admin password changed	✓	—
Default publish password changed	✓	—
Default aldis password changed	✗	Change passwords for default users
USB drives disabled	✓	—
VNC disabled	✗	Turn off VNC access
L1/L2 Cloud Connection	✓	—
Using GRIDSMART Cloud	✓	—
Using HTTPS for client connection	✓	—
Default certificate changed	✗	Install a signed certificate

Manage access to USB drives: **Enable USB drives**

Manage remote access via VNC: **Disable VNC server**

## 13.9 System Operations

This allows you update software by uploading a binary file and also to reboot the GS<sub>2</sub> processor.

Update software on the GS<sub>2</sub> by uploading a binary file provided by GRIDSMART.

Update File

Choose update file

Reboot the entire system, taking the GS<sub>2</sub> offline for up to several minutes while the system reboots.

For more detail regarding the Networking and Security features, please refer to the **GS<sub>2</sub> Network and Configuration Appendix**.

## 14.0 Support

Before contacting GRIDSMART Support, please prepare the following:

1. Connect a Flash/USB Drive to the problem Processor to collect diagnostic data;
2. Or export your site configuration AGS file, Client Logs and Processor Logs.

Email GRIDSMART Support or your regional GRIDSMART Field Application Engineer.

There are three ways to contact GRIDSMART Support:

Email: [support@gridsmart.com](mailto:support@gridsmart.com)

Web: [gridsmart.freshdesk.com](http://gridsmart.freshdesk.com)

Phone: +1 866 652 5347

### 14.1 Send a Site to GRIDSMART Support for Review or Assistance

If you would like GRIDSMART Support to review your site configuration, you can easily Export a site from the GRIDSMART Client and email it to GRIDSMART Support as follows.

1. Launch the Client and click the appropriate Site Card.
2. Click the Export icon from the Site Menu.
3. Save the file with a valid Windows filename. Make sure the file has the GRIDSMART \*.ags extension.
4. Email the \*.ags file to GRIDSMART Support – [support@gridsmart.com](mailto:support@gridsmart.com).

### 14.2 Data Stick or Data Drive

A USB stick or external hard drive can be used to collect and synchronize data and site configurations between GRIDSMART Processors and the Client. These USB devices must be formatted as NTFS volumes. Make sure there is enough free space on the drive before use. Otherwise, data may not be synchronized.

### 14.3 Import and Use a Modified Site

If you experienced problems with your site and requested GRIDSMART Support to review the site configuration, you will likely receive an email from GRIDSMART with your modified site configuration attached as a GRIDSMART \*.ags file. Follow this procedure to review that configuration and put it into operation on your site.

1. Save the \*.ags file from the email onto your hard drive.
2. Launch the GRIDSMART Client and click Import in the top right-hand corner of the Sites Homepage.
3. Navigate the Windows file system to find the \*.ags file. Select the file and click Open.
4. The appropriate Site Card on the Sites Homepage will have a hash mark fill pattern indicating unpublished changes. Click that Site Card to enter the Site View screen.
5. Review the changes. If they are significant, these changes may be hard to visualize as the unpublished changes may significantly overlap the current published configuration.



6. Click the Configure pencil on the Site Menu to enter the Site Configuration screen. There you will be able to see the new configuration without seeing the existing configuration overlaid.
7. If you are connected to the site, you can Publish the changes. If you are not connected and do not wish to take a laptop into the field, consider using the [Publish to Drive](#) feature.

## 14.4 VNC

Virtual Network Computing (VNC) enables you to remotely access the GRIDSMART Client resident on the Processor as well as the Processor's Windows operating system.



[Log onto GRIDSMART Cloud](#) for instructions.

## 14.5 Upgrade a GRIDSMART Processor with an Update Stick

A GRIDSMART Update Stick is a zip file available for download from [GRIDSMARTCloud.com](#). Extract the contents of the zip file to the root of a formatted USB flash drive before attempting to update a Processor.

1. If you have previously been using VNC, you must ensure that there are no windows or files open on the GRIDSMART Processor.
2. Disconnect everything from the GRIDSMART Processor except the camera(s), power cable and controller connections. You must disconnect your laptop and all network cables as well as any peripherals such as mouse, monitor and/or keyboard.
3. Insert the provided Update Stick into one of the USB ports.

### GS<sub>2</sub> Processor

The GS<sub>2</sub> Front Panel LEDs will display three LEDs “walking” from left to right.

After a few minutes, the GS<sub>2</sub> phase LEDs will turn GREEN. You may remove the USB stick once all the phase states are GREEN.

### Legacy Processor

Observe the front panel display of the GRIDSMART Processor. The Legacy Processor will display the update status. Once complete, the front panel will instruct you to remove the Update Stick.

Once the update is complete, the GRIDSMART Processor will reboot. After several minutes, your site will return to normal operations.


You may now reconnect any previously disconnected peripherals or network cables.



## 14.6 Diagnostics

Click the Diagnostics icon on the Site Menu to see data for the current site.


Temperature and voltages displayed are updated every 30 seconds.  
Select Extended Diagnostics to open the Device Manager for additional diagnostics.

Diagnostics 	
Temp	118.4 F
Uptime	23.13:43:53
3.3 V	3.27
5 V	5.15
12 V	12
48 V	48.79
Serial #	GS2-2987
IP Address	10.33.0.3
Cabinet (SWC)	Shadow
EB ADC	Day
Expanded Diagnostics	

## 14.7 Replace a Camera


1. Disconnect the non-functioning camera from the GRIDSMART Processor, then connect the replacement camera.
2. Wait four minutes before continuing to the next step.
3. Connect to the Processor, launch the GRIDSMART Client, and then click the appropriate Site Card.
4. Click the Configure pencil on the Site Menu. The Site Configuration screen displays a Replace Cameras option.
5. Click Replace Cameras and proceed by pairing the zones from your missing camera with the images from your new camera. Configure the camera heading and height when prompted.
6. Adjust your zones and masks as needed.
7. Publish the changes.

## 14.8 Uninstall or Repair the GRIDSMART Client

1. Open Programs and Features by clicking the Start button , clicking Control Panel, and then clicking Programs and Features.
2. Select the GRIDSMART Client, then click Uninstall.



3. To repair the Client, click Repair. To remove the Client, click Uninstall.

 If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

## 14.9 Remote Support

To request remote support from a GRIDSMART Support Technician, please download and install the Remote Desktop application from <https://remotedesktop.google.com/> before contacting support at 866-652-5347.

At GRIDSMART, your satisfaction is our top priority. We value your feedback and want to hear from you.

Please stay in touch!

Thank You

Twitter: <https://twitter.com/GRIDSMARTTech>

Facebook: <https://www.facebook.com/pages/Gridsmart/906447382729795?ref=hl>

Vimeo: <https://vimeo.com/gridsmart>

YouTube: [https://www.youtube.com/channel/UC6Cyj0ORFNOAI3rno2u6\\_xQ](https://www.youtube.com/channel/UC6Cyj0ORFNOAI3rno2u6_xQ)

LinkedIn: <https://www.linkedin.com/company/gridsmarttech/>

Support: <https://support.gridsmart.com>

Copyright © 2019 GRIDSMART Technologies, Inc.  
10545 Hardin Valley Road, Knoxville, Tennessee 37932 USA  
[gridsmart.com](http://gridsmart.com)

All rights reserved. GRIDSMART is a registered trademark of GRIDSMART Technologies, Inc. All other marks are property of their respective owners.

MADE IN THE USA

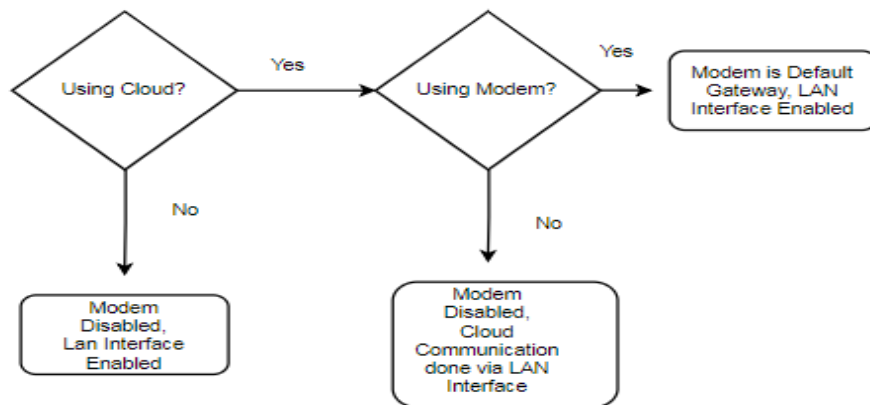
## GS<sub>2</sub> Networking and Security

### Introduction

The GRIDSMART GS<sub>2</sub> Processor is an enterprise appliance that has the flexibility to operate in a variety of network configurations. In version 19.3, the GRIDSMART Device Manager utility has been added to allow configuration of and management of the GS<sub>2</sub> device without the need to have a camera attached to the processor. The utility is used to configure both network and security settings as well as perform basic troubleshooting.

### 1.0 Modes of Operation

The GS<sub>2</sub> processor can run in a standalone “off network” configuration or be connect to a Local Area Network (LAN) along with the GRIDSMART Cloud. The GRIDSMART Cloud is a platform that can be used to automatically backup configuration changes, upload data and diagnostic logs, download license keys, provide access to software patches, updates, automatic reports, alerts and other system information. GRIDSMART is committed to continue to expand the capability of the GRIDSMART Cloud. For processors without customer network connectivity, a built-in cellular modem can be used to interconnect with the GRIDSMART cloud. When enabled, the modem operates a private APN using a non-public facing IP address which only allows outbound connections that are limited to specific ports required for use by the processor.



In addition to the modem, the processor has a 100Mbps Ethernet Interface that can also be used to connect the processor to a Local Area Network (LAN). The above diagram shows the combination of connection options available. The GRIDSMART cameras are connected to the GS<sub>2</sub> processor on a private LAN that is optimized specifically for transmission of video to the GS<sub>2</sub> processor.

### 1.1 Security Features

One of the key emphasis of the software release 19.3 was to provide many of the security features requested and required today in the enterprise computing environment. To maintain backwards compatibility many of the security features are disabled by default. The GRIDSMART GS<sub>2</sub> Processor with software release 19.3 contains a feature rich set of security features including:

- The GS<sub>2</sub> Device Manager is a new application for easy configuration of network and security settings, use management and advance diagnostics.
- HTTPS connectivity for client and API connections using TLS V1.2
- HTTPS signed URLs for communication with the GRIDSMART cloud.
- Support for Signed SSL Certificates on the processor.
- Role based user management system with three distinct user roles (Admin, Publish and View Only) that can be easily managed and assigned as required by the organization.
- Security Self-Auditing Tool within the GS<sub>2</sub> Device Manager.
- Signed Updates using a SHA-2 digital signature to ensure that the updates are GRIDSMART genuine.
- New ability to enable/disable VNC connections to the processor so they are only available when they are needed.
- Ability to enable/disable certain operations to USB drives until they are needed.
- An Updated Operating System Patching System that contains updates for each software release.
- A dynamically configured application firewall with specific rules for inbound and outbound services required.
- Processor Data encrypted at rest.
- Extensive Audit Logging of all security related functions, system access and system configuration changes.

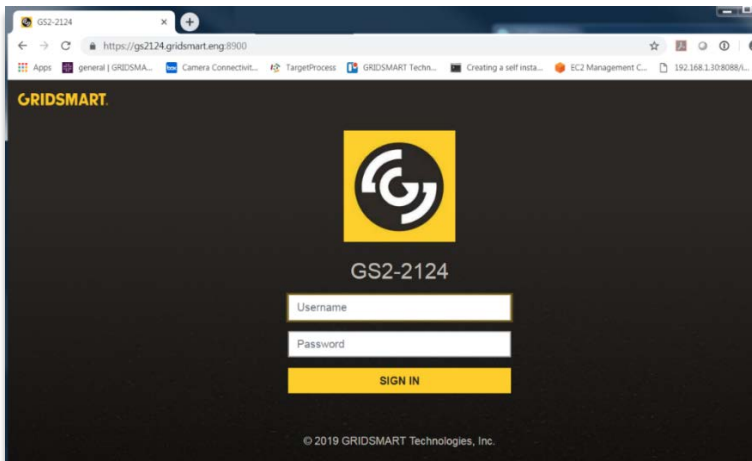
In addition to these features, the GS<sub>2</sub> process undergoes intense penetration testing during each software cycle to ensure vulnerabilities are minimized as much as possible.

## 2.0 GS<sub>2</sub> Device Manager

### 2.0.1 Connecting to Device Manager

The GS<sub>2</sub> Device Manager is a web application and will run on most modern browsers. The site will work with Internet Explorer but will have limited functionality. It currently is not designed to work on a mobile platform, but this will be supported in a future version of this utility. To access the GS<sub>2</sub> Device Manager open a browser and enter.

[https://\[ip address of GS2\]:\[port\]](https://[ip address of GS2]:[port])



If you are connected through the laptop port, access will be done using the following URL:

<https://192.168.150.10:8900>

The GS<sub>2</sub> Device Manager uses Transport Layer Security Version (TLS) version 1.2 (formally known as Secure Socket Layer or SSL) for all communication. System configuration and changes must be done by a user that has the “admin” role. Initially during installation of the system, a self-signed SSL certificate will get generated with GRIDSMART Engineering as the Certificate Authority. Because of this there will be a warning message. This can be ignored. The traffic being transmitted to the processor is encrypted but the certificate on the processor cannot be verified. Once a signed certificate is installed you will see the “key” in the upper right-hand corner of the URL pane as shown in the example login screen above.

From the processor desktop you can also access the GS<sub>2</sub> Device Manager by clicking on the following icon.



## 2.0.2 Default Credentials

The following default accounts will be configured as defaults in version 19.3.

If you choose to enable HTTPS transport for the client traffic, a password is required for ALL processor operations. It is highly recommended you enable HTTPS transport for all production systems.

Permission Level	Username	Password	Capabilities using HTTP	Capabilities using HTTPS
Admin	admin	admin	Full access to GS <sub>2</sub> Device Manager, Admin account disabled in client software.	Full access to GS <sub>2</sub> Device Manager, Full access in client software.
Publish	publish	aldis#world9	Limited functionality in GS <sub>2</sub> Device Manager, can publish to site from client	Limited functionality in GS <sub>2</sub> Device Manager, can publish to site from client.
Read-only	aldis	aldis#world9	Limited functionality in GS <sub>2</sub> Device Manager, cannot publish in client.	Limited functionality in GS <sub>2</sub> Device Manager, cannot publish in client.

**It is highly recommended that default credentials be changed immediately.**

Due to the California “Information Privacy: Connected Devices” bill that comes into effect on January 1, 2020, future versions of the GS<sub>2</sub> software will require default passwords to be changed before the device can be placed into service.

## 2.0.3 Network Settings

The GS<sub>2</sub> processor supports a variety of network configurations including DHCP, static IPV4 addressing, and static routes. The GS<sub>2</sub> processor does not support IPV6.

All Network settings for the processor **must be done in the GS<sub>2</sub> Device Manager**. Any changes done outside of the utility are not supported and could lead to unstable processor operation. This includes connection to devices on the private 192.168.150.0 network as well as any configuration or modification of any camera settings.

By default, the public interface is set to DHCP. In the GS<sub>2</sub> Device Manager, go to ‘Network’ → ‘Network’ and deselect ‘Use DHCP’ to enter a static address. If you select a static address, you must make sure the DNS server is working. Once you have applied changes, you can verify DNS is working by checking the DNS status on the “Advanced Diagnostic Page”.

DNS Working

True



The screenshot shows the 'Network' configuration page in the GRIDSMART interface. The left sidebar contains icons for Network, Cameras, Diagnostics, Modules, Users, Location, Date/Time, Security, and System Operations. The main content area has tabs for Network, Certificates, Client/API, GRIDSMART Cloud, Static Routes, and Reset. Under the 'Network' tab, there is a checkbox for 'Use DHCP' which is unchecked. Below it are input fields for 'Network Address' (10.8.0.46), 'Netmask' (255.255.255.0), 'Gateway' (10.8.0.1), and 'DNS' (8.8.8.8). There is also an 'NTP Server' field with 'pool.ntp.org' and a 'Sync Time' button. At the bottom are 'Apply changes' and 'Cancel changes' buttons.

For static addressing, enter an IP address, net mask and DNS address. The gateway is optional. The NTP server can be updated if the modem is not enabled. If the modem is enabled NTP settings will be default to an NTP server reachable on the Private Cellular APN. **Modifying any of these settings outside the GS<sub>2</sub> Device Manager will void your support warranty and could cause the system operation to become unstable.**

## 2.0.4 Keeping Time

In order to have consistent reporting and audit logs it is essential the GS<sub>2</sub> processor time be accurate. The preferred way to do this is using NTP. If the modem is configured for use (default setting) the NTP server cannot be updated. (See Section on configuring GRIDSMART Cloud for more details). This is done to make sure a known NTP server is reachable from the modem. The NTP client on the processor will automatically synchronize time daily but this can be also forced using the “Sync Time” button on the Network tab. The time can be verified on the “Diagnostic” page.

In the GS<sub>2</sub> Device Manager go to ‘Network’ → ‘Network’ and you will find where you can enter an NTP server as a domain or IP address, or request a time sync. Once you have entered your NTP server, select Apply Changes.

This screenshot shows the 'Network' configuration page, similar to the one above, but with the 'Use DHCP' checkbox checked. The 'NTP Server' field contains 'pool.ntp.org' and the 'Sync Time' button is visible. The 'Apply changes' and 'Cancel changes' buttons are at the bottom.

## 2.1 Upgrading from HTTP to HTTPS

It is highly recommended to upgrade any GS<sub>2</sub> processor to use HTTPS. With HTTPS all network traffic between the GRIDSMART client software and processor is encrypted. Without this any data being sent between systems could be inadvertently monitored and collected by a third party. This includes passwords and sensitive information.

**If you choose to enable HTTPS transport for the client traffic, a password is required for ALL processor operations.** It is highly recommended you enable HTTPS transport for all production systems.

## 2.2 Client/API Settings

In the GS<sub>2</sub> Device Manager go to 'Network' → 'Client/API' and choose HTTPS, select Apply Changes. If the client was connected to the site previously, you may have to restart the client in order to connect using HTTPS.

You can also change the default port used by the client and the GS<sub>2</sub> Device Manager. If you have site cards in the client, they will default to use the default port number of 8902. To use a different port number, you must specify it using a URL format in the client.



In 19.3, the GRIDSMART client will automatically detect the transport type and connect to the site using the proper transport.

## 2.3 Importing a signed SSL Certificate

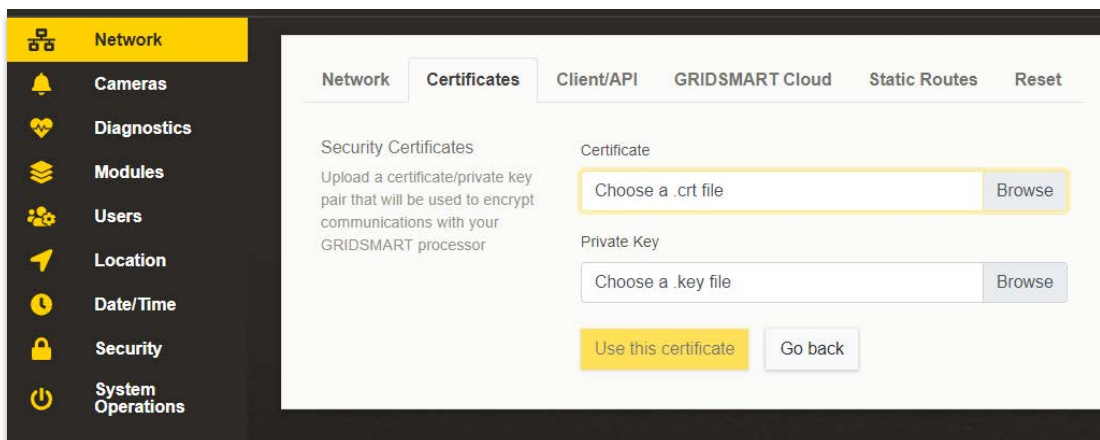
The GS<sub>2</sub> Processor will generate a “GRIDSMART” self-signed certificate during the update. Since the certificate is not signed by a Certificate Authority, it will not be validated by your web browser. If you have a signed certificate you can load it into the processor, and a warning will not be issued when accessing the GS<sub>2</sub> Device Manager or the GRIDSMART Client software.

In the GRIDSMART Device Manager, go to ‘Network’ → ‘Certificates’ and select ‘Change Certificate’.



You will be brought to a page where you can browse and select the corresponding .crt and .key file to import.

**NOTE: The .crt and .key files ARE NOT BACKED as part of the configuration to the GRIDSMART cloud.** As a best practice it is recommended not to use a wild card certificate. Each certificate should contain a separate private key. Any certificates loaded are digitally validated before they are applied to the processor.



## 2.4 Routing Considerations

For the most part the routing setup on the GS<sub>2</sub> processor is straightforward. There are a few caveats to understand and consider before you deploy your system.

When the modem is enabled it is the default gateway (0/0 route) for the processor. The WAN interface will have a 0/0 route but at a higher metric, so the modem is always preferred for outbound traffic. If this is not desired, then the modem can be disabled, or static routes can be used for routes that need to be accessed with the local area network. (See the Case Study Section for a real-life example of how this might work)

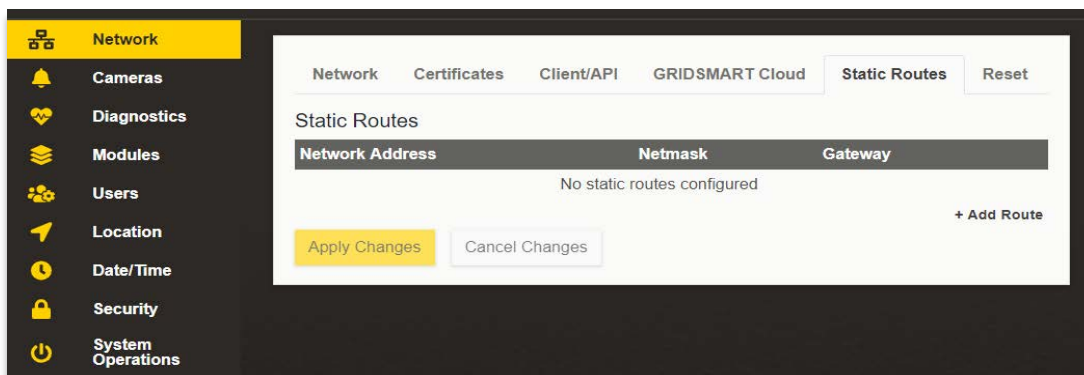
Standalone devices with no external connectivity can be setup with modem only access. In this mode, all traffic will be routed to the Cloud except for DNS, and NTP traffic.

In summary:

- The modem is the default gateway with the lowest metric and the preferred outbound connection when enabled.
- The Network LAN interface has a higher metric and will not route default traffic. If the modem is disabled all outbound traffic is routed across the Network LAN.
- DNS and NTP services must be reachable for the unit to function properly.
- Use the Diagnostic tools in the GS<sub>2</sub> Device Manager to ensure they are working.

## 2.5 Adding Static Routes

For Networks with multiple subnet and routed VLANs, static routes can be used in conjunction with the modem to ensure subnets are reachable from the GS<sub>2</sub> Processor. Setting up static routes should be done by a qualified networking professional who has knowledge of the local network setup.



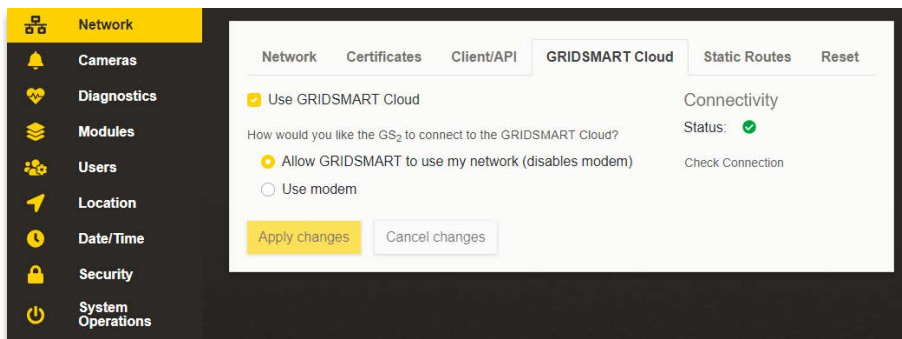
## 2.6 GRIDSMART Cloud

As stated earlier, there are two ways to connect to the GRIDSMART Cloud. This includes the LAN Network (preferred method) or the cellular modem. Optionally in 19.3 there is an option to disable the GRIDSMART Cloud. While we do not recommend this, if you do not wish to have your processors connect to the GRIDSMART cloud you should disable it in the GS<sub>2</sub> Device Manager, so no attempts

are made to connect. Even if the antenna is not connected, the processor will attempt to connect to the GRIDSMART cloud unless it is disabled in the GRIDSMART Device Manager.

## 2.6.1 Using your network to connect to GRIDSMART Cloud

In the GRIDSMART Device Manager, go to 'Network' → 'GRIDSMART Cloud' and select 'Allow GRIDSMART to use your network'

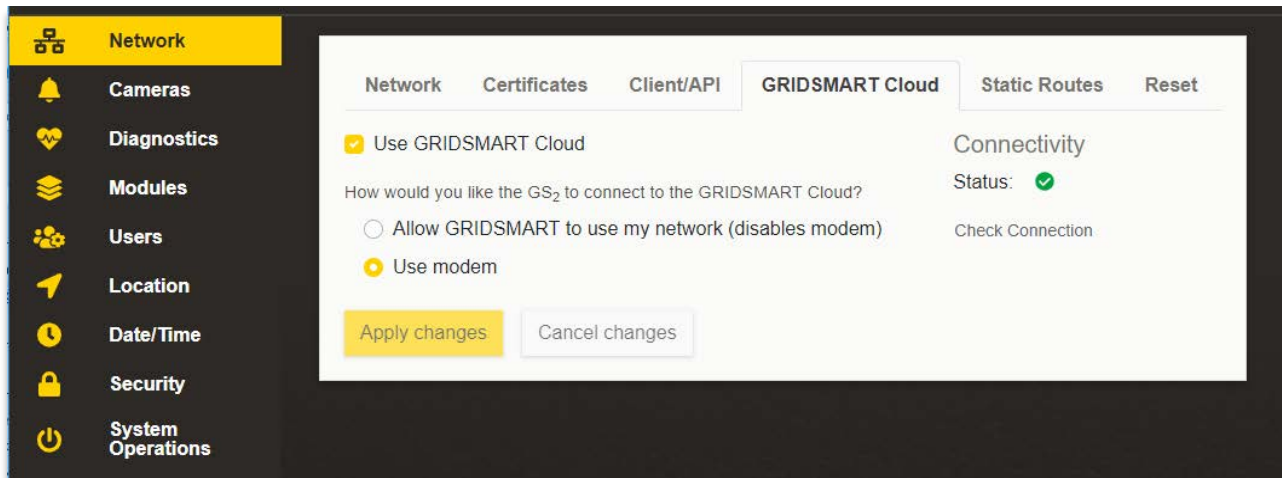


## 2.6.2 Using the modem to connect to GRIDSMART Cloud

If you wish to use the modem be sure to connect the antenna using best practices described in the installation guide and verify the signal strength on the modem diagnostic page.

Overview	Logs	Modem	Advanced
Modem Type	ZTE		
Modem Status	Enabled		
Signal Strength	Fair		
Model	MC2718		
Firmware	M6085_LM9BDB11		

In the GRIDSMART Device Manager, go to 'Network' → 'GRIDSMART Cloud' and select 'Use modem'. To verify connection to the GRIDSMART cloud click on "Check Connection" to verify the network is properly configured. If the Connectivity Status shows a green check mark, the processor is connected to GRIDSMART Cloud.

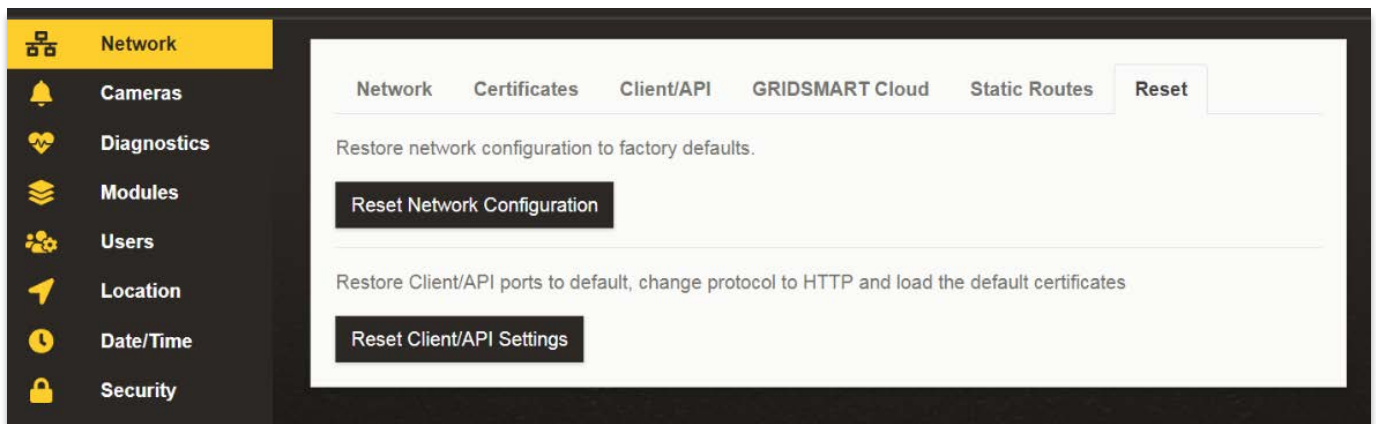


**If you do not get a green check mark, check the following:**

- Network Settings. Verify the IP address is correct. Use the Diagnostic page to verify the address is set properly.
- Cloud Settings. Verify Cloud is enabled.
- Verify the Modem is working. (if applicable). Check the antenna and signal strength.
- Verify DNS is working. Check the DNS Status on the “ADVANCED DIAGNOSTICS” page.
- More Advanced Diagnostics can be done on the “ADVANCED DIAGNOSTIC PAGE”

## 2.7 Restoring to Factory Default Network Settings:

In the GRIDSMART Device Manager, go to ‘Network’ → Reset and select the appropriate option.

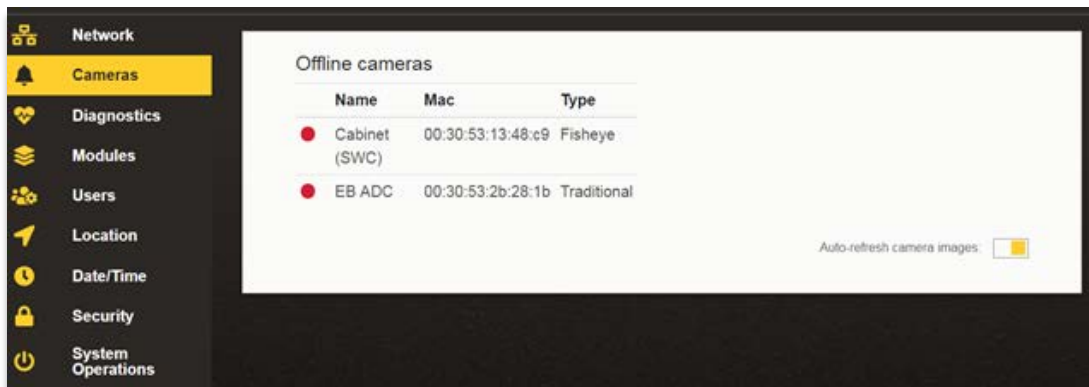




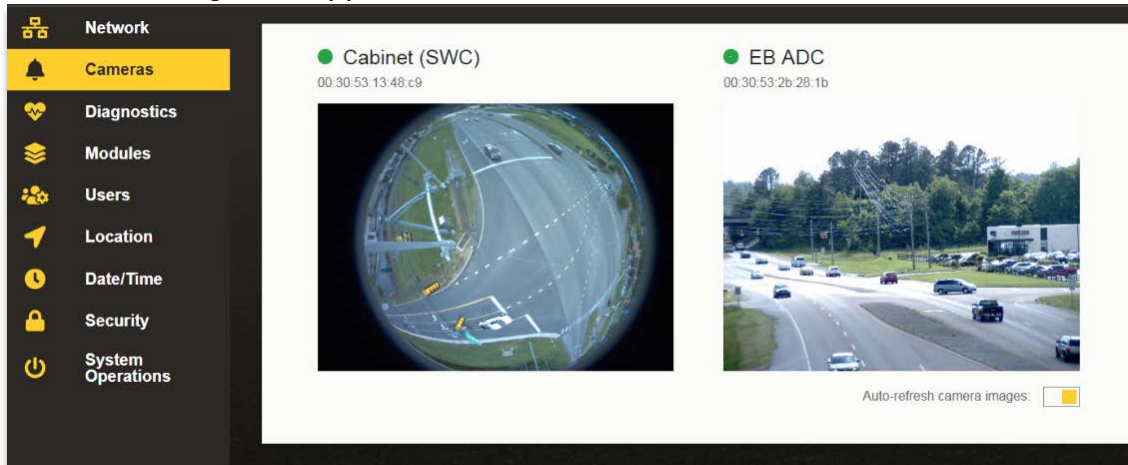
## 2.8 Checking Cameras

The GRIDSMART Device Manager allows configuration of the processor without any cameras connected. It can also be used to do basic camera troubleshooting without having to use the GRIDSMART client. This tool is meant only for troubleshooting and only refreshes the camera image every 5 seconds. For slow connections this can be disabled using the yellow toggle button on the bottom right of this screen. To stream video, use the STREAMS function which allow H.264 video to be delivered over a RTSP stream.

If the cameras are not communicating the following will be displayed.

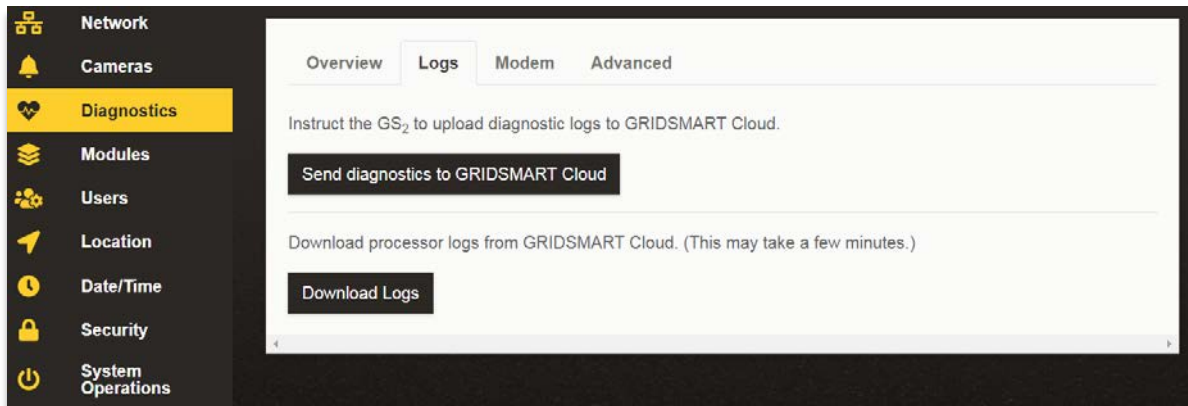


The camera images will appear as shown below when the cameras are online.



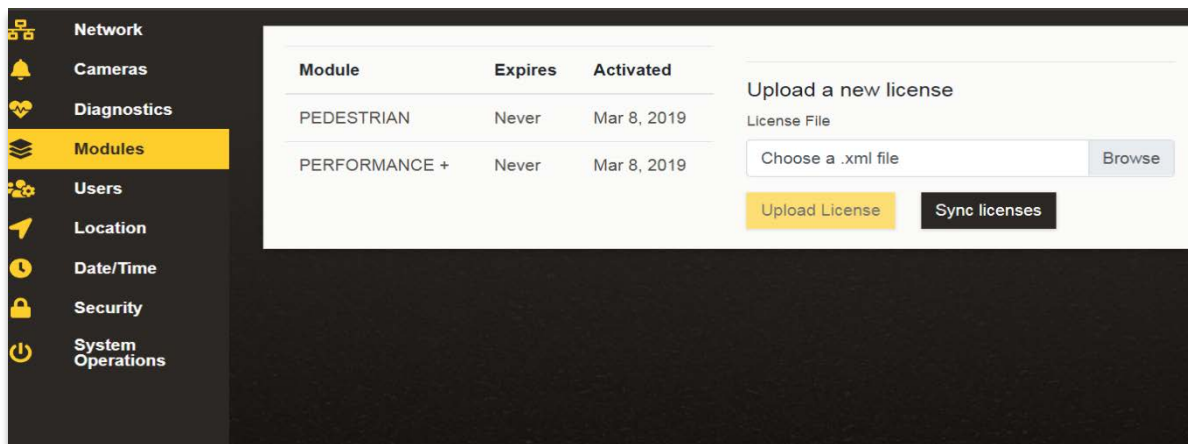
## 2.9 Diagnostics

The GRIDSMART Device Manager provides extensive diagnostic information that can be used to troubleshoot a processor. It also allows the ability to download diagnostics data or send them automatically to the GRIDSMART CLOUD.



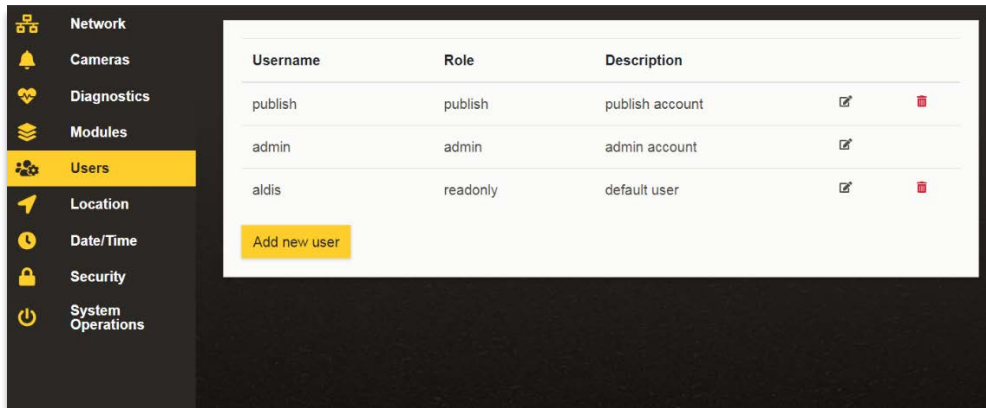
## 2.10 Modules

The GRIDSMART Device Manager allows the ability to sync licenses from the GRIDSMART Cloud or manually load them.



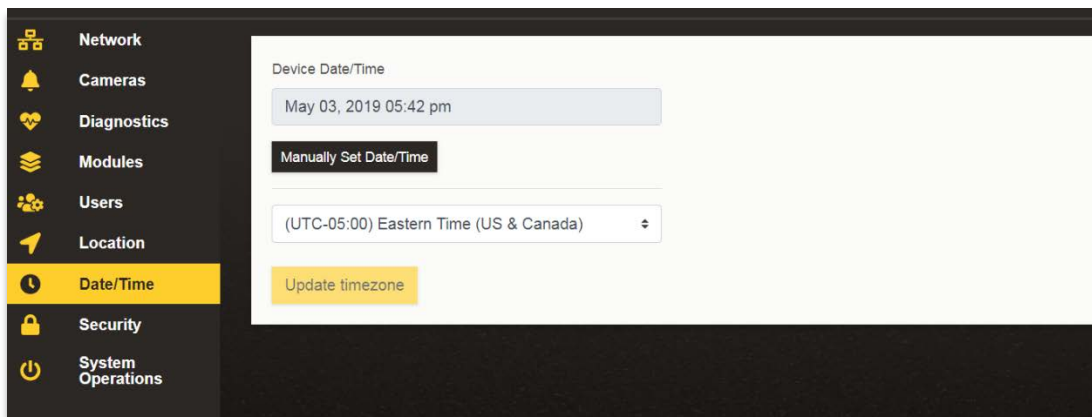
## 2.11 User Management

Users can be added in the GRIDSMART Device Manager. When HTTPS is enabled, users will be granted privileges based on their roles.



It is highly recommended to change the default passwords and to assign each user an account based on the role they are expected to perform. The “admin” account cannot be deleted from the processor.

## 2.12 Manually setting the clock and Time Zone.



## 2.13 Security Self Audit

As a best practice each GS<sub>2</sub> processor should be hardened as required by your organization. The Self Audit function provides an easy way to ensure you have met best practices. If a deficiency is detected it can be easily corrected by clicking on the recommendation.

Here we see a system that has not enabled HTTPS for the GRIDSMART client software and has VNC and the USB drive scanning enabled.

Setting	Status	Recommendation
Default admin password changed	✓	—
Default publish password changed	✓	—
Default aldis password changed	✓	—
USB drives disabled	✗	Turn off USB access
VNC disabled	✗	Turn off VNC access
L1/L2 Cloud Connection	✗	Contact FAE
Using GRIDSMART Cloud	✓	—
Using HTTPS for client connection	✗	Enable HTTPS for client
Default certificate changed	✓	—

Manage access to USB drives: [Disable USB drives](#)

Manage remote access via VNC: [Disable VNC server](#)

After these conditions were corrected the system indicates it has been hardened.

Setting	Status	Recommendation
Default admin password changed	✓	—
Default publish password changed	✓	—
Default aldis password changed	✓	—
USB drives disabled	✓	—
VNC disabled	✓	—
L1/L2 Cloud Connection	✓	—
Using GRIDSMART Cloud	✓	—
Using HTTPS for client connection	✓	—
Default certificate changed	✓	—

Manage access to USB drives: [Enable USB drives](#)

Manage remote access via VNC: [Enable VNC server](#)

## 2.14 Remote Updates

Starting in 19.3 remote updates can be applied from the GS<sub>2</sub> Device Manager.

The screenshot displays the GridSmart GS<sub>2</sub> Device Manager interface. On the left is a dark sidebar with a vertical list of menu items, each preceded by a yellow icon: Network (gear), Cameras (bell), Diagnostics (heart), Modules (stack), Users (people), Location (location pin), Date/Time (clock), Security (lock), and System Operations (power button). The 'System Operations' item is highlighted with a yellow background. The main content area has a dark background with a light yellow rectangular panel for updates. At the top of this panel, text reads: 'Update software on the GS<sub>2</sub> by uploading a binary file provided by GRIDSMART.' To the right of this text is a warning: 'Reboot the entire system, taking the GS<sub>2</sub> offline for up to several minutes while the system reboots.' Below the main text is the label 'Update File'. There is a text input field containing the placeholder 'Choose update file', followed by a 'Browse' button. Below the input field is a 'Send Update File' button. To the right of the 'Browse' button is a 'Reboot System' button.

## 3.0 Other Considerations

### 3.1 Monitoring the GS<sub>2</sub>

The GS<sub>2</sub> will not respond to ICMP echo requests, i.e. ping. Enabling this feature on the GS<sub>2</sub> will void your warranty and could render the system unstable. The supported way to monitor the system is to use HTTP Ping. HTTP ping can be enabled using the following URL which will return a status code 200 on success.

<http://x.x.x.x:9009/>

where x.x.x.x is the IPV4 address of the GS<sub>2</sub> processor

### 3.2 Firewall Ports

The following ports should be reachable within the network for each GS<sub>2</sub> processor:

#### Inbound Ports

5900 (Cannot be changed)

8900 (default) – GS<sub>2</sub> Device Manager Port (Configurable)

8902 (default) – GRIDSMART API Port (Configurable)

9000-9009 – STREAMS Module using RTSP (9009 required for Genetec Support)

#### Outbound Ports

TCP 443 – Cloud

UDP 123 – NTP Service

UPD/TCP 53 – DNS

### 3.3 Accessing Video using STREAMS

GRIDSMART supports RTSP streams from the GRIDSMART cameras using the STREAMS module included in the *Performance+ module*. Any other method used to stream video from the cameras other than using the GRIDSMART client or STREAMS module voids the system warranty and **WILL BE DETECTED** and Disabled in a future release. Any unsupported Streaming methods will affect video processing and affect the operation of the intersection. Any connection of a device on the private Network other than a laptop used for field configuration violates the system warranty and is not supported.

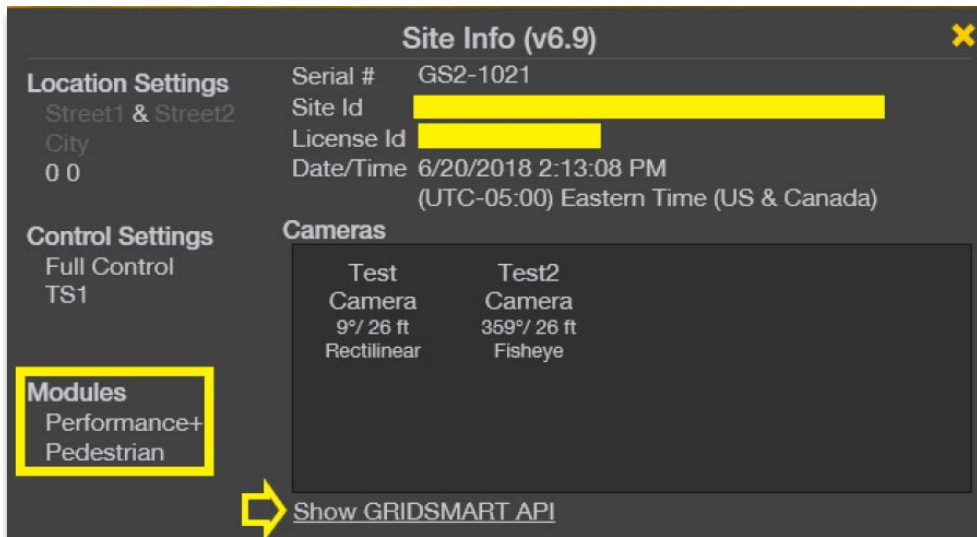
### 3.4 GRIDSMART STREAMS Requirements

To setup STREAMS you must setup a static IP on the GS<sub>2</sub> processor. As a Best Practice it is recommend to setup a static IP on the processor with a DHCP reservation. See section 2.0.3 on how to configure a static IP address. Additionally, any client connecting to the video stream must be able to reach the GS<sub>2</sub> Processor on ports 9000-9009.

### 3.5 RTSP Endpoints

From the site's homepage menu in the GRIDSMART client, click Info. Ensure the Performance+ module is installed. If the Performance+ module is not installed, the RTSP endpoints will NOT be displayed.





**Site Info (v6.9)**

**Location Settings**  
 Street1 & Street2  
 City  
 0 0

**Control Settings**  
 Full Control  
 TS1

**Serial #** GS2-1021  
**Site Id** [Redacted]  
**License Id** [Redacted]  
**Date/Time** 6/20/2018 2:13:08 PM  
 (UTC-05:00) Eastern Time (US & Canada)

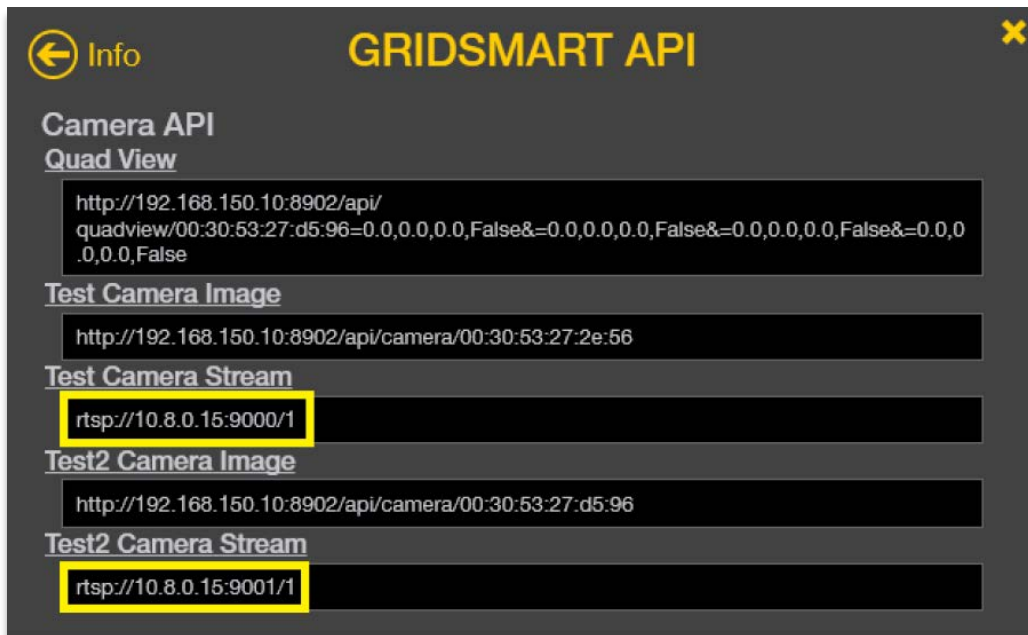
**Cameras**

Test	Test2
Camera	Camera
9°/ 26 ft	359°/ 26 ft
Rectilinear	Fisheye

**Modules**  
 Performance+  
 Pedestrian

[Show GRIDSMART API](#)

Click on **Show GRIDSMART API** to bring up API endpoints. Your screen should look similar to the following screenshot, but the IP address should reflect what you set as your static IP.



**GRIDSMART API**

**Camera API**  
**Quad View**  
<http://192.168.150.10:8902/api/quadview/00:30:53:27:d5:96=0.0,0.0,0.0,False&=0.0,0.0,0.0,False&=0.0,0.0,0.0,False&=0.0,0.0,0.0,False>

**Test Camera Image**  
<http://192.168.150.10:8902/api/camera/00:30:53:27:2e:56>

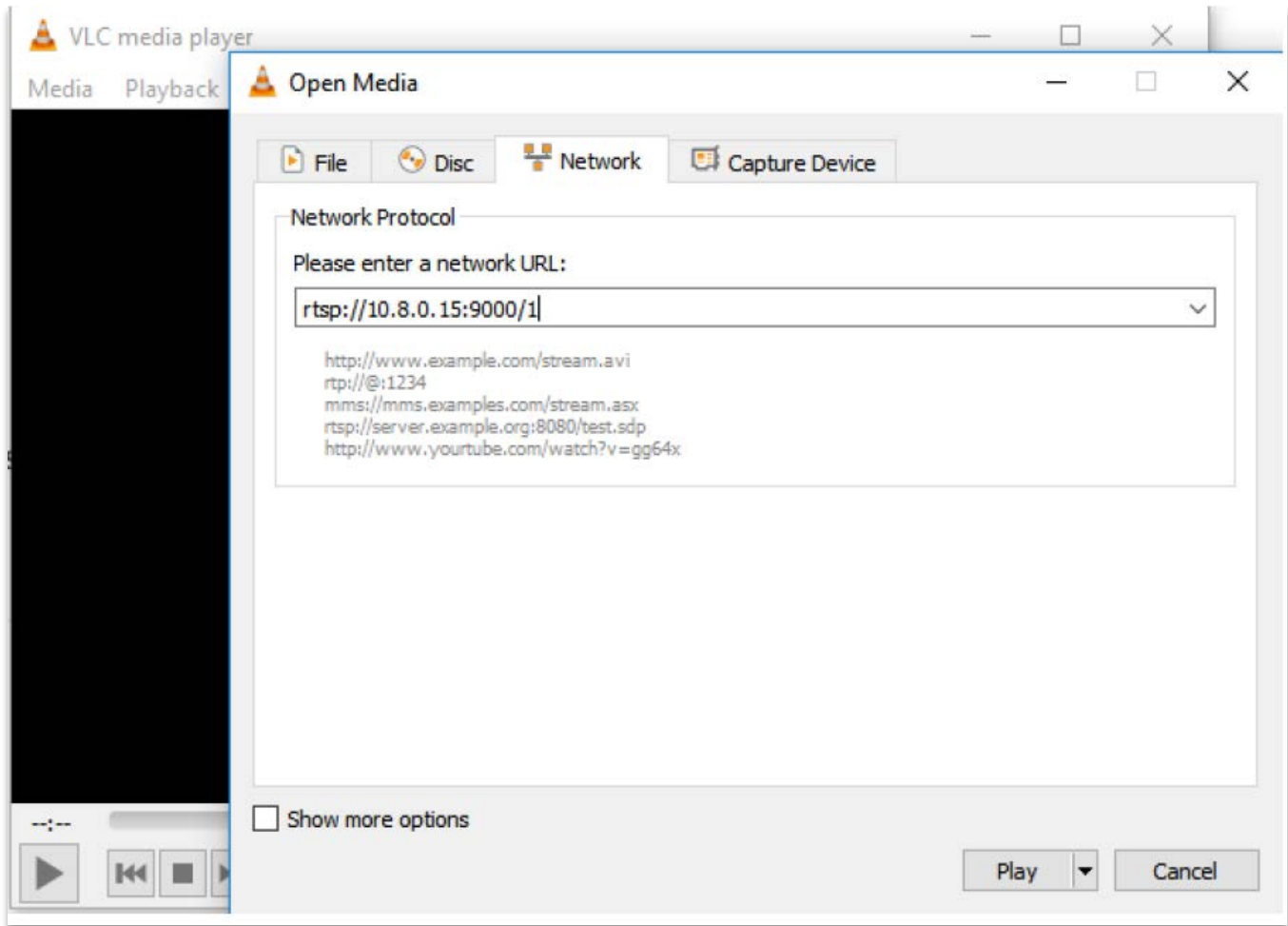
**Test Camera Stream**  
<rtsp://10.8.0.15:9000/1>

**Test2 Camera Image**  
<http://192.168.150.10:8902/api/camera/00:30:53:27:d5:96>

**Test2 Camera Stream**  
<rtsp://10.8.0.15:9001/1>

### 3.6 Testing STREAMS Using VLC

VLC is a free open-source media player that supports RTSP. Install VLC on a client machine. Open VLC, then select menu Media→Open Network Stream and copy/paste the full Camera Stream URL as the network URL (ex. rtsp://10.8.0.15:9000/1).



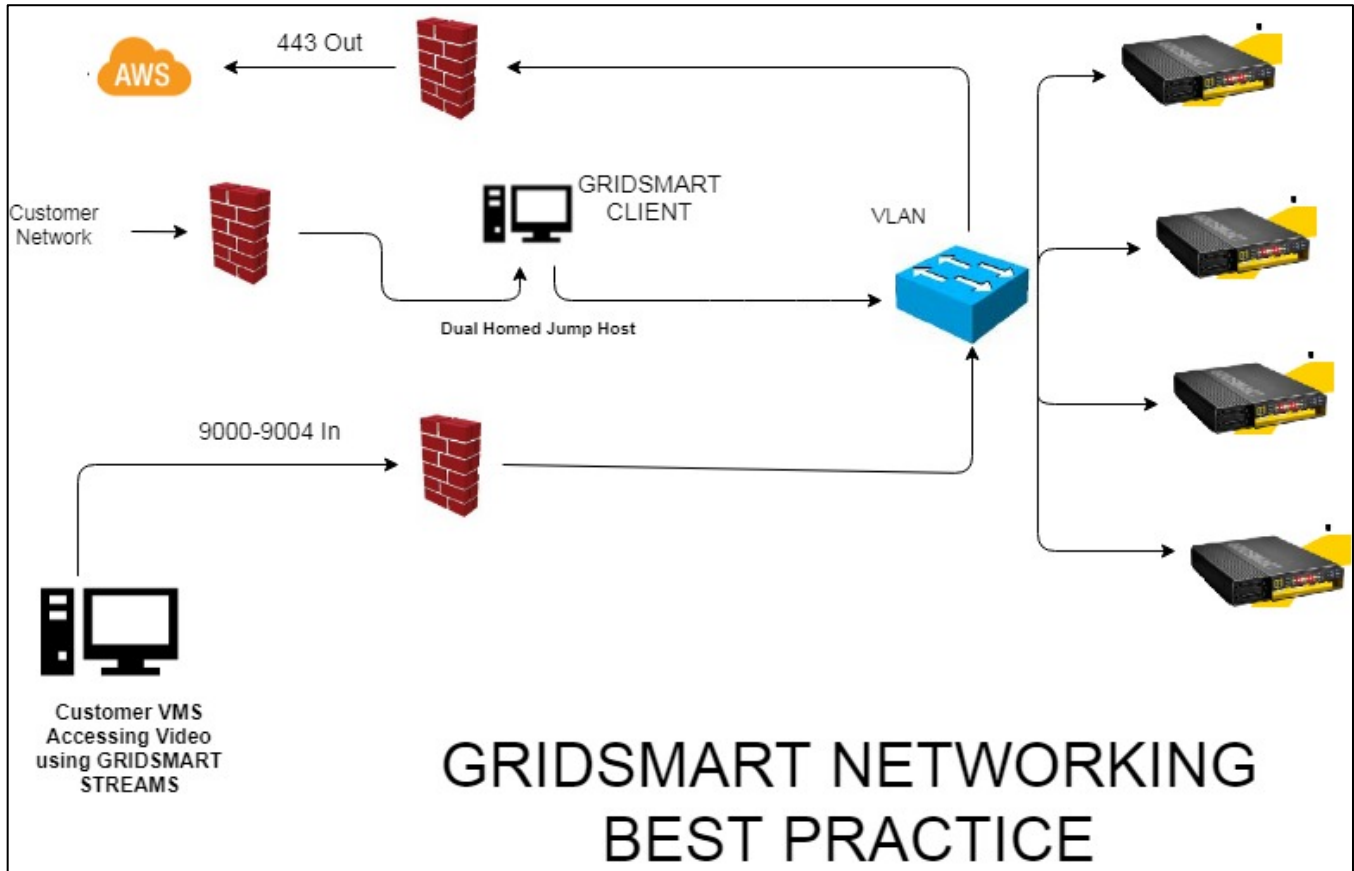
### 3.7 Private LAN connection (Laptop Port)

It is highly recommended, as a best practice, that any device connected via the Laptop port use IP address 192.168.150.250/32. Avoid using addresses in the ranges of 192.168.150.11 thru 192.168.150.19 and avoid using DHCP when possible. Any laptops connected to the laptop port should be used temporarily for configuration and removed as soon as the intersection is operating properly.

## 4.0 Network Configurations - Best Practices

As a best practice it is recommended connecting all GS<sub>2</sub> processors on a separate VLAN with a jump host client used to directly access the GS<sub>2</sub> processors. It is not recommended to use the GRIDSMART client for monitoring video. For video streaming and monitoring use the Streams Module.

DO NOT CONNECT a GS<sub>2</sub> Processor directly to the Internet on a public facing IP address.



## 5.0 Case Study for using Static Routes:

Consider the following example:

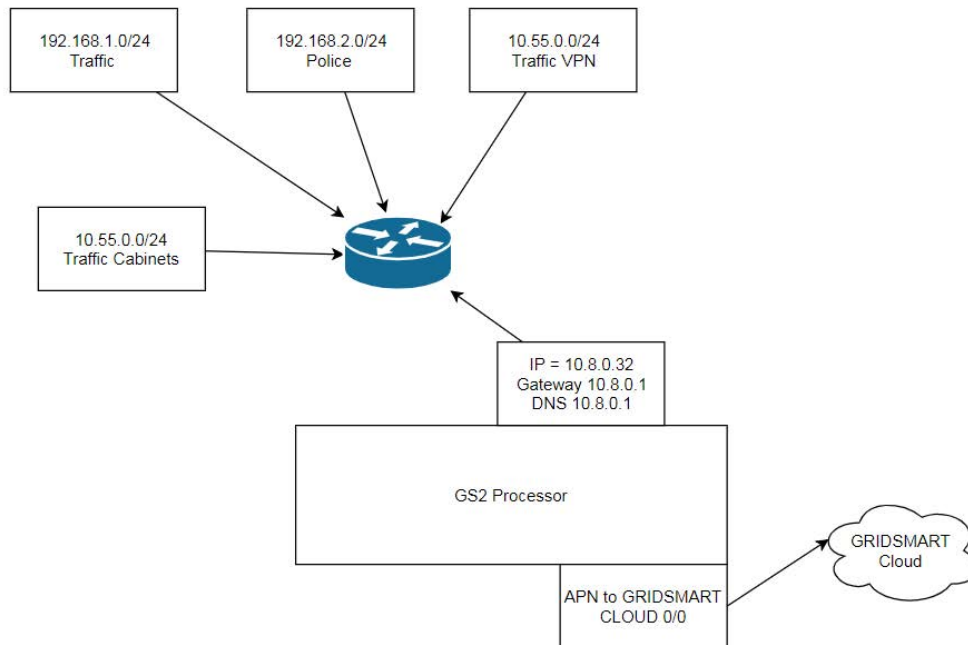
**Local Area Network contains the following subnets:**

Traffic Department: 192.168.1.0/24

Police Department: 192.168.2.0/24

Traffic VPN: 10.55.0.0/24

Traffic Cabinets: 10.55.0.0/23 (Router Address 10.8.0.1)



The connection to the traffic cabinet is done via 900 MHz radios running at 10Mbps.

The police department wishes to stream video to their operations center. The traffic department would like to upload configuration changes and send alerts using the GRIDSMART cloud. They have decided the modem can be used for cloud communications to save bandwidth instead of using the limited bandwidth of the radio. Additionally, the traffic department wants to access the GS<sub>2</sub> Processor to run reports and to make configuration changes from the local area network using the GRIDSMART Client software.

Since the modem is enabled on the GS<sub>2</sub> and the default route will be the modem, two static routes are needed on the GS<sub>2</sub> processor to allow traffic to the police and traffic department's network.

The Cloud configuration would be set as follows:

Network
Certificates
Client/API
**GRIDSMART Cloud**
Static Routes
Reset

☒ Use GRIDSMART Cloud

How would you like the GS<sub>2</sub> to connect to the GRIDSMART Cloud?

☐ Allow GRIDSMART to use my network (disables modem)

☒ Use modem

Connectivity

Status: ✔

Check Connection

Apply changes
Cancel changes

The static Routes would be setup as follows:

Network
Certificates
Client/API
GRIDSMART Cloud
**Static Routes**
Reset

Static Routes

Network Address	Netmask	Gateway		
192.168.2.0	255.255.255.0	10.8.0.1		
192.168.1.0	255.255.255.0	10.8.0.1		
10.55.0.0	255.255.255.0	10.8.0.1		

+ Add Route

Apply Changes
Cancel Changes

With this configuration, cloud traffic will be routed via the modem and all the stakeholders involved will have connectivity to the GS<sub>2</sub> processor.

## FAQs

**Q: Can antivirus/firewall software be installed on the GS<sub>2</sub> Processor?**

A: No. GRIDSMART takes several measures to prevent malware/viruses from installing or running on processors, however it's important to clarify how we handle anti-virus software. Our software repositories are scanned continuously for viruses. All system images are built and provisioned in a sanitized environment on a dedicated private network. However, once a processor is in the field, no active anti-virus scanning is performed. This is because the processor needs to operate in real time to process video at an acceptable rate. Additionally, any storage device (e.g. thumb drives, hard drives) attached to the processor to collect images or install an update should be scanned before connecting to the processor.

**Q: Does your system support any patch management software such as SCCM or Blade Logic?**

A: No. The GS<sub>2</sub> is an embedded appliance. We cannot guarantee the GS<sub>2</sub> processor will work properly until the patch management software has undergone extensive testing. Patches are automatically included in software updates after they have been thoroughly tested.

**Q: Can Local user accounts be added to the operating system or can the system be part of a Domain?**

A: No. The device is an embedded appliance and any system administration or management done on the processor voids the support warranty.

**Q: Can I disable Cloud or the Modem on the GS2 Processor.**

A: Yes, using the GRIDSMART Device Manager.

**Q: Can I do remote updates?**

A: Yes, beginning with version 19.3, use the GRIDSMART Device Manager to push updates to a networked GS<sub>2</sub> Processor. **Note, the GS<sub>2</sub> MUST be running version 19.3 or later.**

**Q: Why is ping not enabled on the processor?**

A: Ping is not enabled for both performance and security reasons.

**Q: Why is VNC installed on the processor? Is it secure?**

A: VNC is used to run the GRIDSMART Client locally on the processor and for specific field diagnostics and troubleshooting performed by authorized GRIDSMART personnel. VNC traffic is encrypted but it is recommended VNC be disabled in the GRIDSMART Device Manager when not being used.

**Q: I'm seeing a "Contact FAE" under Level 1/Level 2 Connection the Security Audit? What does this mean?**

A: You may have an unsupported or outdated modem. Contact your FAE for more details.

**Q: Can I connect an NVR directly to the Private LAN segment?**

A: No. This is not supported and violates the warranty. This could affect operation of the image processing algorithm. This may also not work in future releases of the software.



**Q: Does the processor support SNMP?**

A: Not at this time but it is being considered for a future release.

**Q: Can I access the GS<sub>2</sub> processor using the modem?**

A: No. The modem is for outbound connections to GRIDSMART Cloud only.

**Q: Can I do RTSP streaming without using the STREAMS module?**

A: No. This is not supported and violates the warranty. This could affect operation of the image processing algorithm. This may also not work in future releases of the software.

**Q: What NVRs do you support with STREAMS?**

STREAMS will work with any RTSP Version 2.0 (RFC 7826) compliant software.