GRIDSMART®

USERGUIDE
V19.10

VERY IMPORTANT!

PLEASE READ PRIOR TO INSTALLING VERSION 19.10

GS_2'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_2 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 19.3, 19.10 and should be noted before applying the update:

- Passwords set and used in versions 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`**".
- Beginning in v19.10 the System will utilize a captive user account. This user account is unable to modify the network settings, NTP Server Settings or anything system related. THESE FUNCTIONS CAN ONLY BE DONE through the GS_2 Device Manager with ADMIN access. The default ADMIN user is "admin" and default password is "admin".
- Default passwords will now prompt to be changed on first log in. It is highly recommended you 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_2 PROCESSOR.

Changelog
19.10 (2019)

PREREQUISITES: GS2'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 19.10. The administrator of the Processor should create appropriate user accounts with appropriate roles and ensure secure passwords.

NEW: Channels-to-phases mapping for TS2 and ITS (ATC). The Phases view of the GRIDSMART Device Manager will show the current Phases and Channel Groups. From this view, pre-configured Flashing Yellow Arrow (FYA) mode maps (A-L) can be set on the processor, allowing the FYA states to be recognized, logged in archived data, and displayed in the Client. For non-standard scenarios, GRIDSMART can help generate a custom channel map you can push to the device in the Device Manager. Zones can be configured for FYA in the Client when the processor uses mapped FYAs.

NEW: The Device Manager's camera view has been updated to include historical frame rates. Lower-than-expected rates will be indicated with warning icons.

SECURITY: The ability to access the GRIDSMART Client from the device desktop has been disabled by default to improve security and comply with evolving state laws. If this type of access is required, it may be enabled in the Device Manager. Enabling this will allow users to log in to the device as user "GRIDSMART" with the password as configured in the Device Manager. Remote access with Remote Desktop Protocol (RDP) or VNC can also be enabled and disabled independently. As indicated in the notice below, VNC will be removed in the next release. As indicated in the additional notice below, all default passwords and default access will be disabled in the next release.

IMPROVEMENT: The Box for bicycle discrimination and Pedestrian zones are now included in the base GRIDSMART System product and no longer require the Performance Plus Module.

IMPROVEMENT: The false detection rate of bicycles in the box has been improved.

IMPROVEMENT: The Diagnostics view of the Device Manager has been streamlined and shows areas of concern with warning icons.

IMPROVEMENT: The Client now uses the same nomenclature for detector outputs as the cabinet standard.

IMPROVEMENT: The Client will indicate the version of firmware for the selected site in the title bar.

IMPROVEMENT: The Diagnostics button in the Client will now open the Device Manager directly when the site firmware supports it.

IMPROVEMENT: When an action in the Client requires a specific level of user privilege, the login dialog will indicate so. (Note: Admin access to a device always requires HTTPS and is never available over HTTP.)

IMPROVEMENT: After 19.10 has been installed, the Device Manager will indicate the status of the processor during a reboot or an update.

IMPROVEMENT: During an update, the front panel will show progress of the update on the phase lights, while showing stage of update on the call lights, providing more information about where the update is in process.

FIX: The processor will now perform a daily Time Sync. The Device Manager will also indicate whether the selected Time Zone supports Daylight Savings Time. This fix works around an OS issue that could prevent NTP time sync from working correctly in some circumstances.

FIX: Device Manager's camera view will no longer enter a refresh loop when a camera goes missing.

FIX: When navigating away from the Device Manager on the processor, the user will no longer be logged out.

NOTICE: VNC will be removed in the next release. Remote desktop access, if enabled, will use RDP.

NOTICE: All default passwords and default access to the device will be removed in a subsequent release to improve security and comply with evolving state laws. Accounts and credentials will need to be created as the first step of setup in the Device Manager.

NOTICE: The processor will no longer provide HTTP access to the API in the next release. API access will require the use of HTTPS

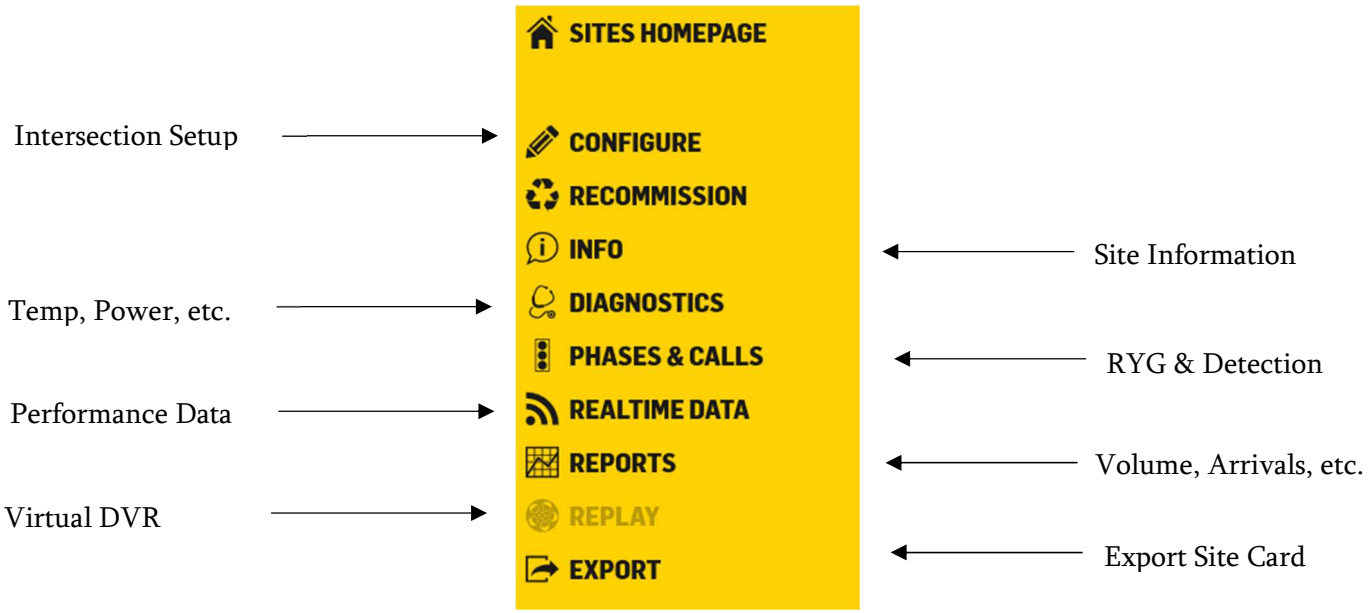
Welcome to GRIDSMART!

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



View Toolbar

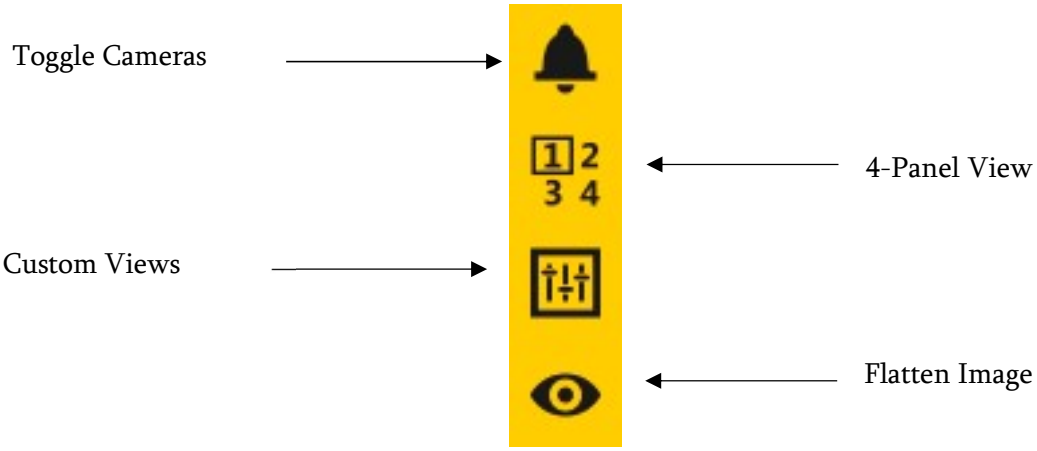


TABLE OF CONTENTS

PLEASE READ PRIOR TO INSTALLING VERSION 19.10 2

CHANGELOG 3
QUICK REFERENCE 6
1.0 CLIENT INSTALLATION & CONFIGURATION 10

1.1 DOWNLOAD THE CLIENT 10
1.2 INSTALL THE GRIDSMART CLIENT 12

2.0 GS_2 DEVICE MANAGER 13

2.1 NETWORK 14
2.2 CAMERAS 17
2.3 DIAGNOSTICS 18
2.4 MODULES 19
2.5 USERS 19
2.6 LOCATION 20
2.7 DATE/TIME 20
2.8 SECURITY 21
2.9 SYSTEM OPERATIONS 21

3.0 SITE CARDS AND THE SITES HOMEPAGE 22

3.1 SITE CARDS 23
3.2 SITE VIEW MODES 25
3.3 CONFIGURE A NEW SITE FROM THE FACTORY DEFAULT SETUP 25

4.0 SITE CONFIGURATION 29

4.1 ROAD MASKS 29
4.2 VEHICLE ZONES 30
4.3 OBJECT MASKS 34
4.4 PEDESTRIAN ZONES 35
4.5 GRIDSMART BOX 36
4.5 FACTORY DEFAULT AND RESET TO FACTORY 37
4.6 QUAD VIEW 37
4.7 PHASES AND CALLS 37
4.8 MAKE OR CLEAR CALLS ON OPERATING ZONES 38
4.9 RECOMMISSION A FACTORY DEFAULT PROCESSOR 39

5.0 PUBLISH 40

5.1 SECURITY – ADMIN, PUBLISH AND READ-ONLY 40
5.2 DEFAULT CREDENTIALS ..... ERROR! BOOKMARK NOT DEFINED.
5.3 LEARNING MODE 40
5.4 MAKE CHANGES TO A SITE CONFIGURATION 41
5.5 PUBLISH HISTORY 42
5.6 MAKE CHANGES TO A SITE WITHOUT TAKING A LAPTOP INTO THE FIELD (PUBLISH TO DRIVE) ERROR! BOOKMARK NOT DEFINED.
5.7 UNPUBLISHED CHANGES 41

6.0 REVERT 43
7.0 SITE INFO 44
8.0 MODULES 45

8.1 GRIDSMART DATA MODULES 45
8.2 DESCRIPTION OF ALERTS 46
8.3 ADDING A MODULE 47

9.0 REPORTS 48

9.1 GET PERFORMANCE DATA WITH THE CLIENT 48
9.2 GET PERFORMANCE DATA WITH A USB STORAGE DEVICE 49
9.3 GENERATING REPORTS 50
9.4 AUTO REPORTS 58

10.0 ALERTS 58
11.0 REPLAY 61

11.1 RECORD AND REVIEW IMAGES AND/OR PERFORMANCE DATA 62

12.0 GRIDSMART API 62
13.0 STREAMING H.264 STREAMS VIA RTSP 63
14.0 SUPPORT 64

14.1 SEND A SITE TO GRIDSMART SUPPORT FOR REVIEW OR ASSISTANCE 65
14.2 DATA STICK OR DATA DRIVE 65
14.3 IMPORT AND USE A MODIFIED SITE 65
14.4 VNC 66
14.5 UPGRADE A GRIDSMART PROCESSOR WITH AN UPDATE STICK 66
14.6 DIAGNOSTICS 67
DEVICE MANAGER DIAGNOSTICS 67
14.7 REPLACE A CAMERA 68

14.8 UNINSTALL OR REPAIR THE GRIDSMART CLIENT 68
14.9 REMOTE SUPPORT 69

GS2 NETWORKING AND SECURITY 70

INTRODUCTION 70
1.0 MODES OF OPERATION 70
2.0 GS2 DEVICE MANAGER 72
2.1 UPGRADING FROM HTTP TO HTTPS 75
2.2 CLIENT/API SETTINGS 76
2.3 IMPORTING A SIGNED SSL CERTIFICATE 77
2.4 ROUTING CONSIDERATIONS 78
2.5 ADDING STATIC ROUTES 78
2.6 GRIDSMART CLOUD 79
2.7 RESTORING TO FACTORY DEFAULT NETWORK SETTINGS: 80
2.8 CHECKING CAMERAS 81
2.9 DIAGNOSTICS 82
2.10 MODULES 82
2.11 USER MANAGEMENT 83
2.12 MANUALLY SETTING THE CLOCK AND TIME ZONE. 83
2.13 SECURITY SELF AUDIT 84
2.14 REMOTE UPDATES 85
3.0 OTHER CONSIDERATIONS 86
4.0 NETWORK CONFIGURATIONS - BEST PRACTICES 89
5.0 CASE STUDY FOR USING STATIC ROUTES: 90

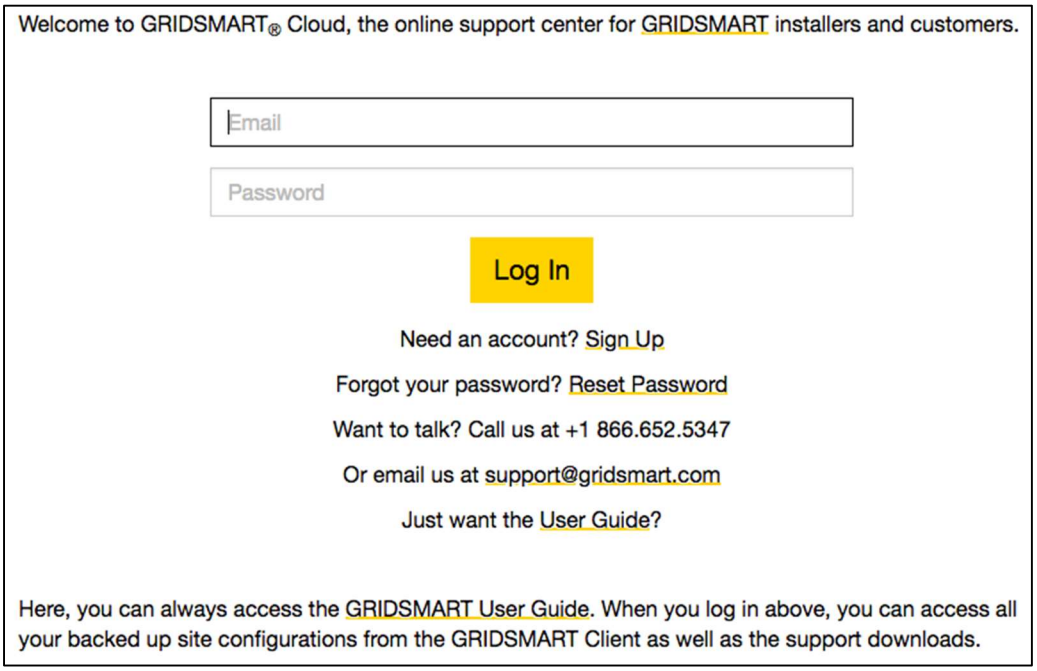
FAQS 92

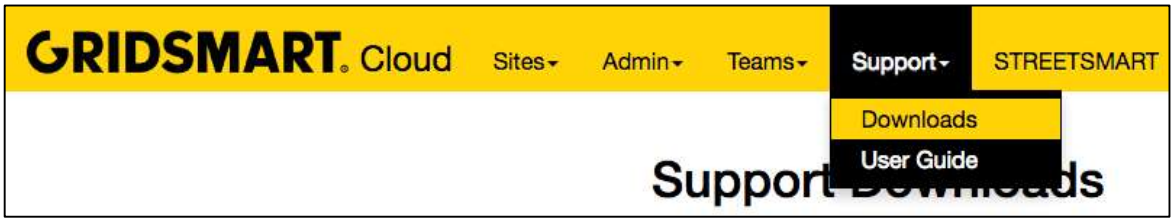
1.0 Client Installation & Configuration

1.1 Download the Client

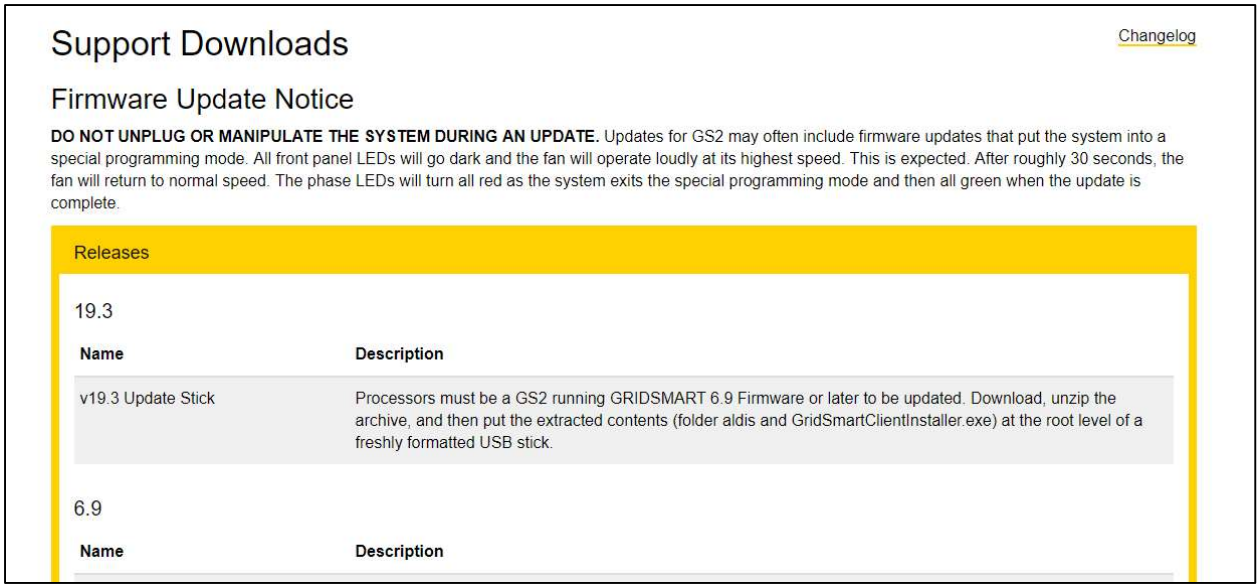
Download the latest version of the GRIDSMART Client from GRIDSMART Cloud.

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

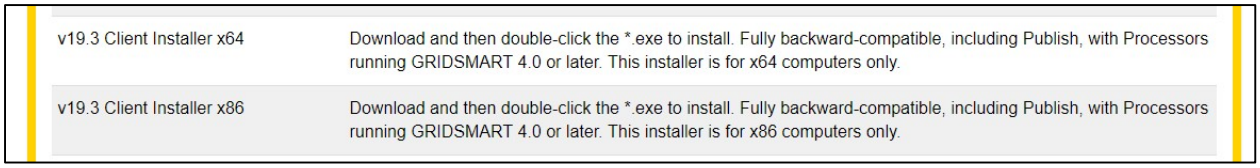
Releases

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 aldis and GridSmartClientInstaller.exe) at the root level of a freshly formatted USB stick.

6.9

Name	Description



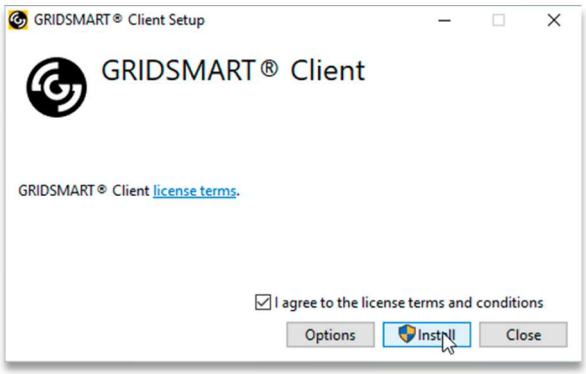
v19.3 Client Installer x64	Download and then double-click the *.exe to install. Fully backward-compatible, including Publish, with Processors running GRIDSMART 4.0 or later. This installer is for x64 computers only.
v19.3 Client Installer x86	Download and then double-click the *.exe to install. Fully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

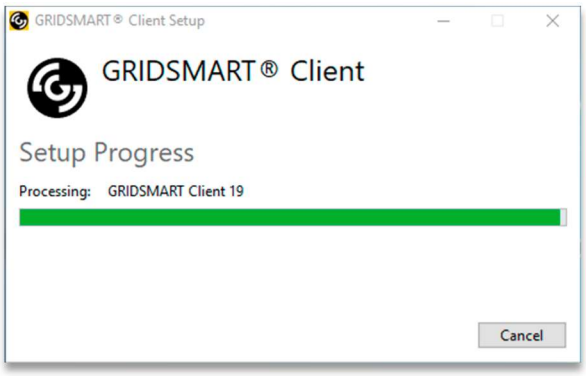
Double-click the Setup Program or MSI Installer to open the GRIDSMART Client Setup.

Accept the Terms and Conditions, then click Install.

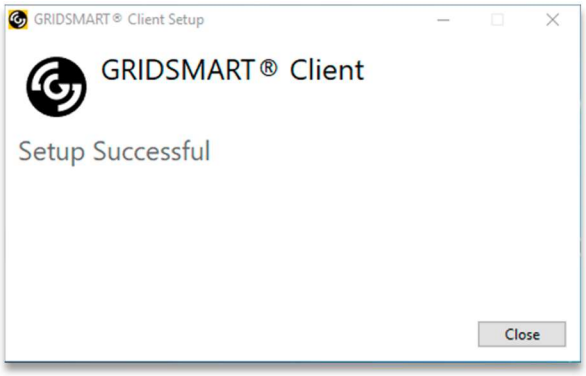


The setup program creates shortcuts to the GRIDSMART Client on your Start Menu and Desktop.

A progress bar indicates the setup status.

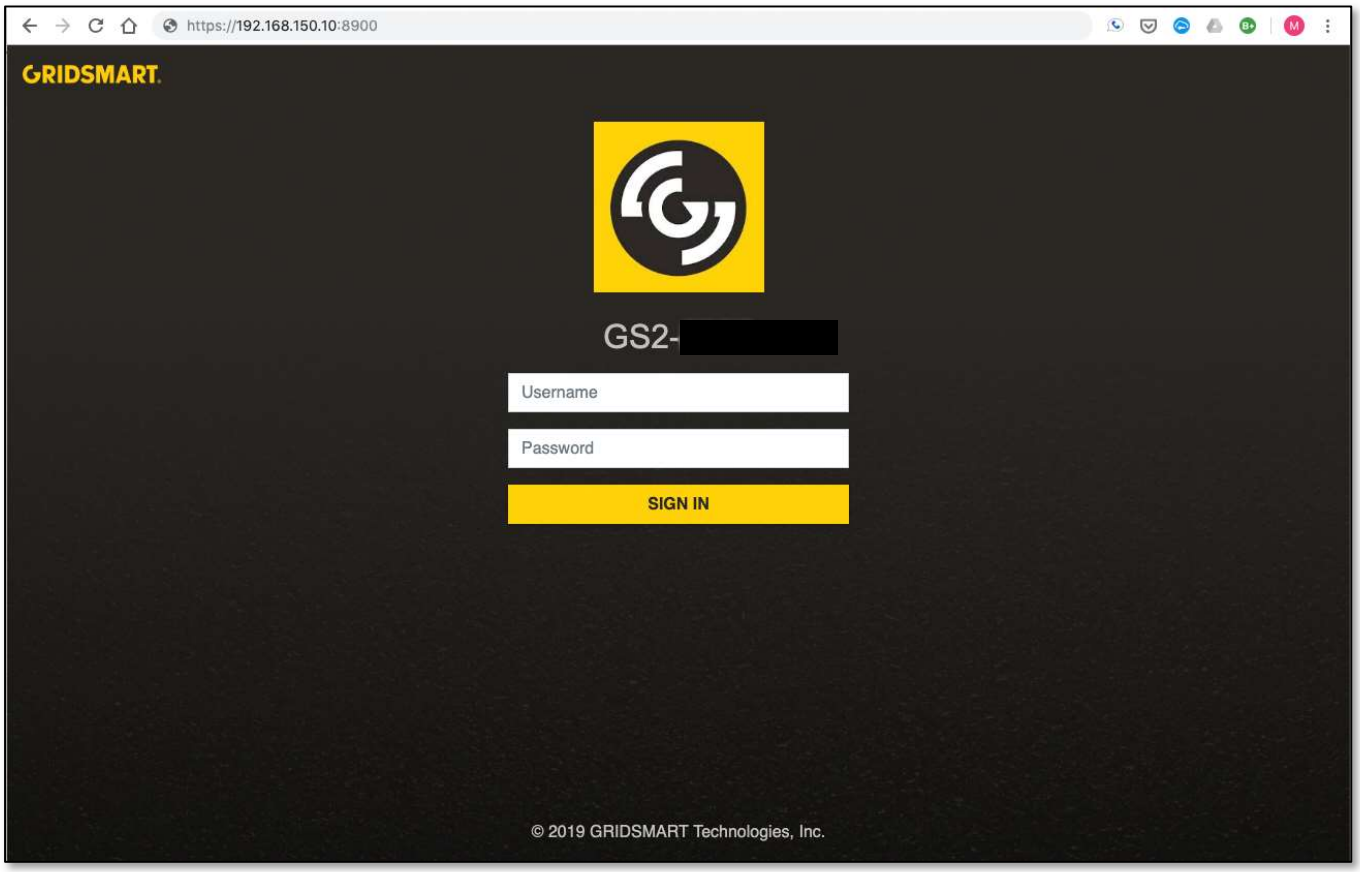


A system restart may be required to complete the installation.



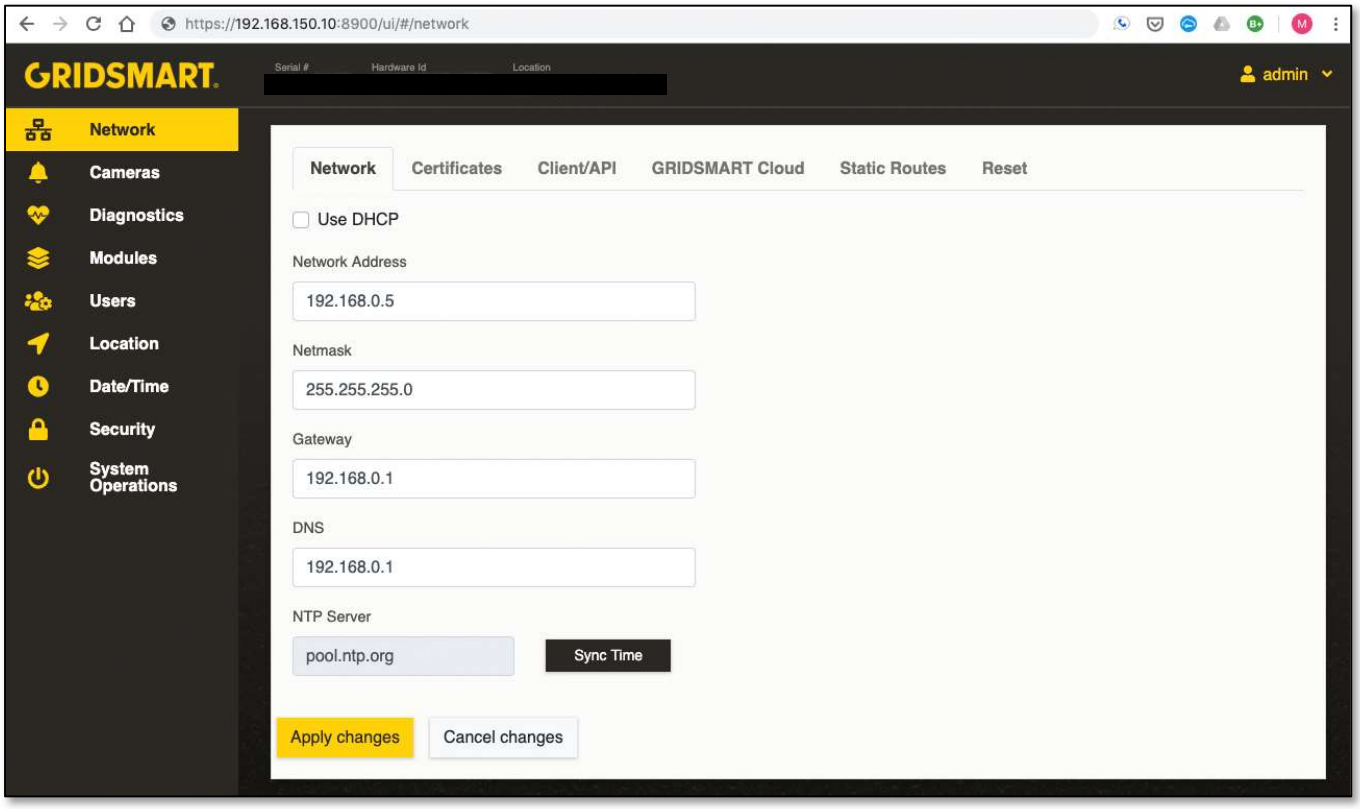
2.0 GS_2 Device Manager

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 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 or RDP. Using this device manager will require the default administrator account credentials.
The default administrator account is '**admin/admin**'.
GRIDSMART recommends changing the default accounts.



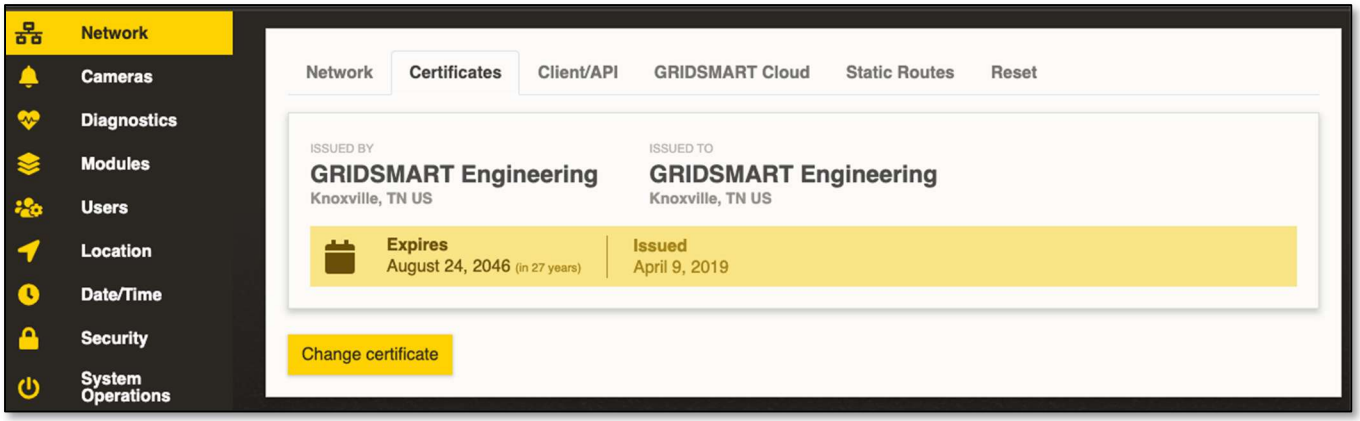
2.1 Network

Select the Network tab to configure the GS2 for your network.

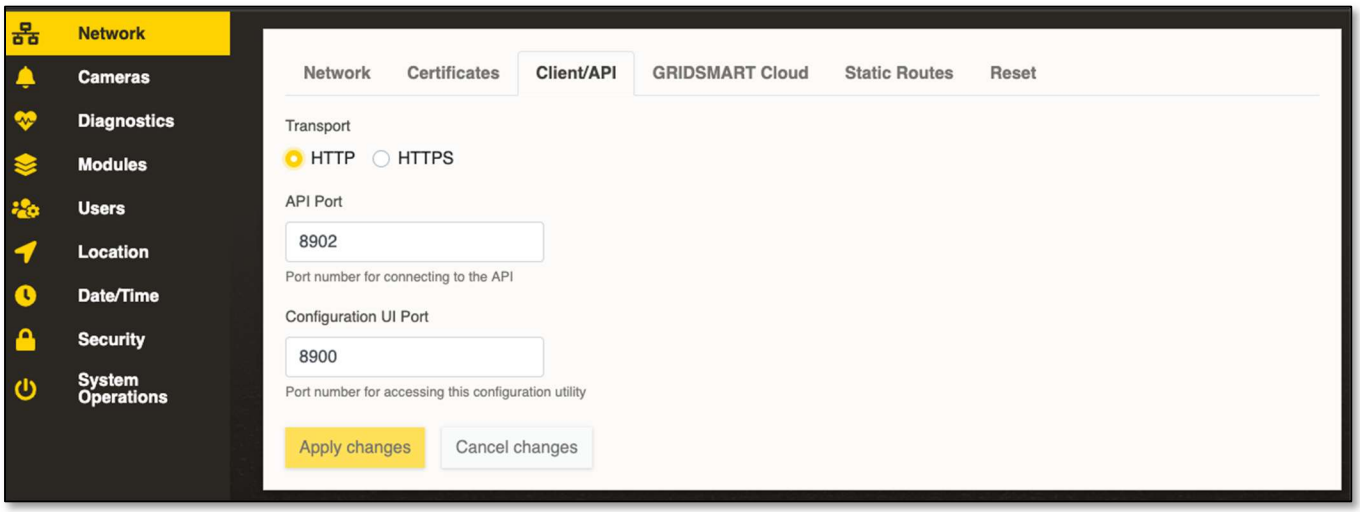


2.1.1 Certificates

GRIDSMART provides a self-signed SSL certificate to enable an encrypted connection. GRIDSMART recommends users install their own signed SSL certificate. Do not use wild card certificates.

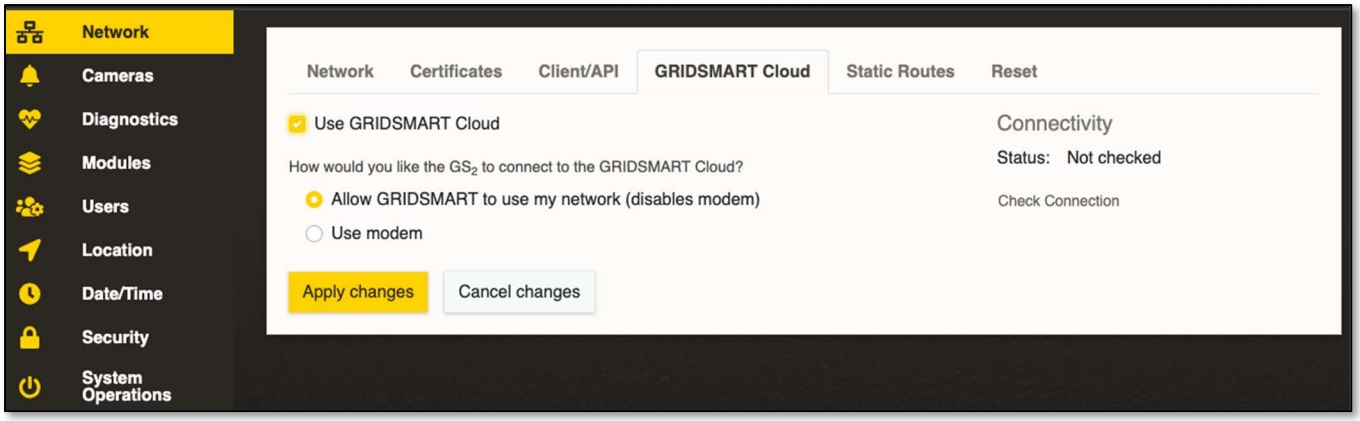


2.1.2 Client/API *(Users may now configure HTTPS and modify the API and UI ports.)*

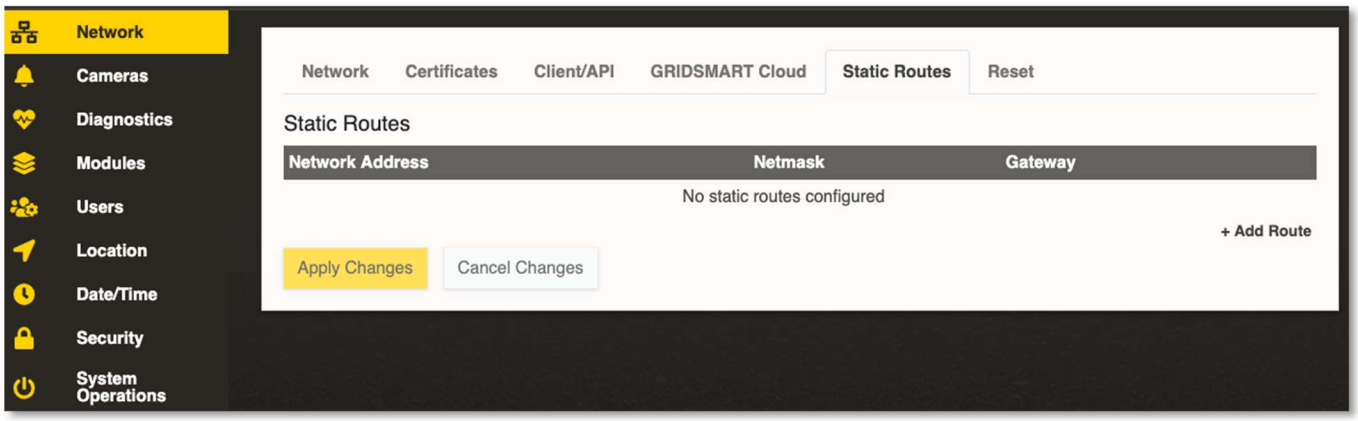


2.1.3 GRIDSMART Cloud

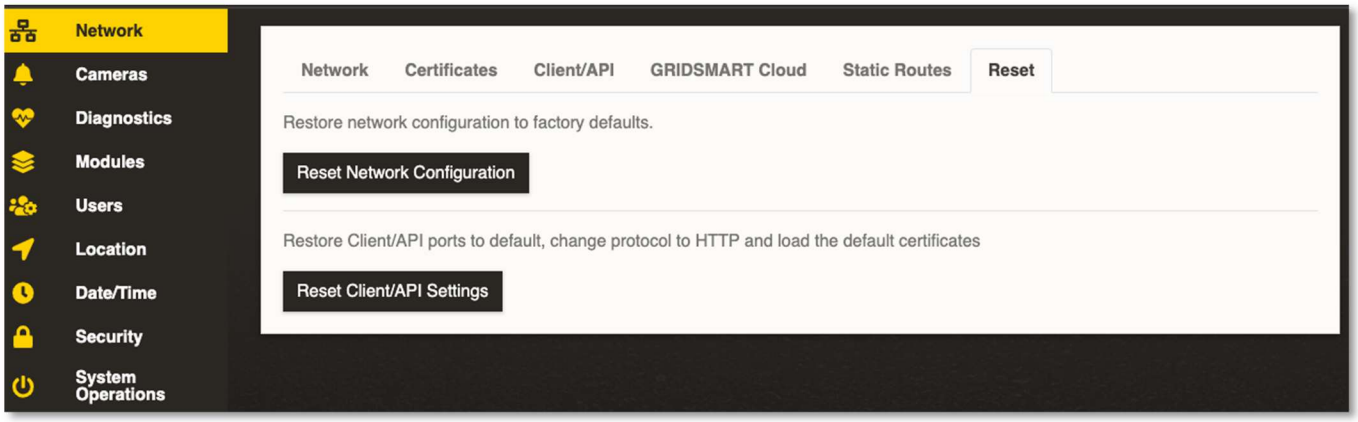
In order for GS_2 to communicate to GRIDSMARTCloud.com, Port 443 MUST be open and have outbound access to api.gridsmart.com.



2.1.4 Static Routes



2.1.5 Reset



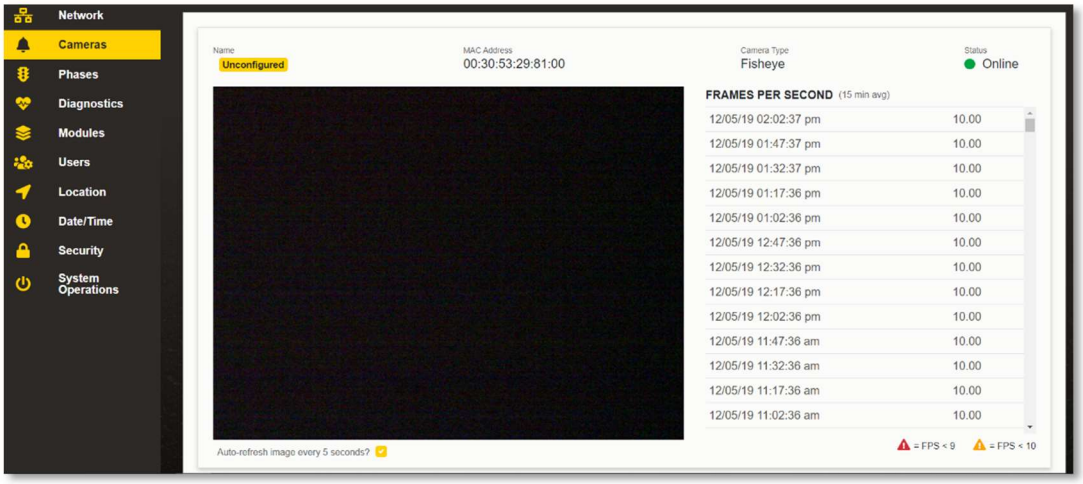
Reset Network Configuration:
Erases user defined network settings and sets the network to DHCP.

Reset Client/API Settings:

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

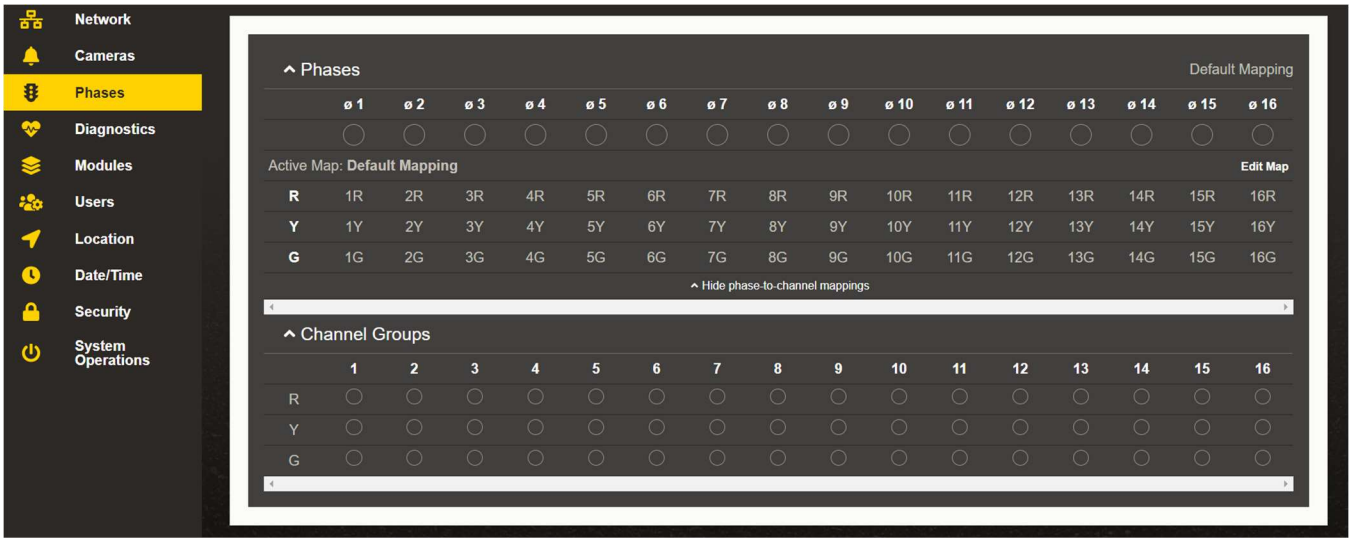
2.2 Cameras

The Cameras Page displays connected cameras, 1frame/5sec. The Auto-refresh may turned off by toggling the switch on the bottom right. This will also include a Diagnostic read out of frames/sec historically.



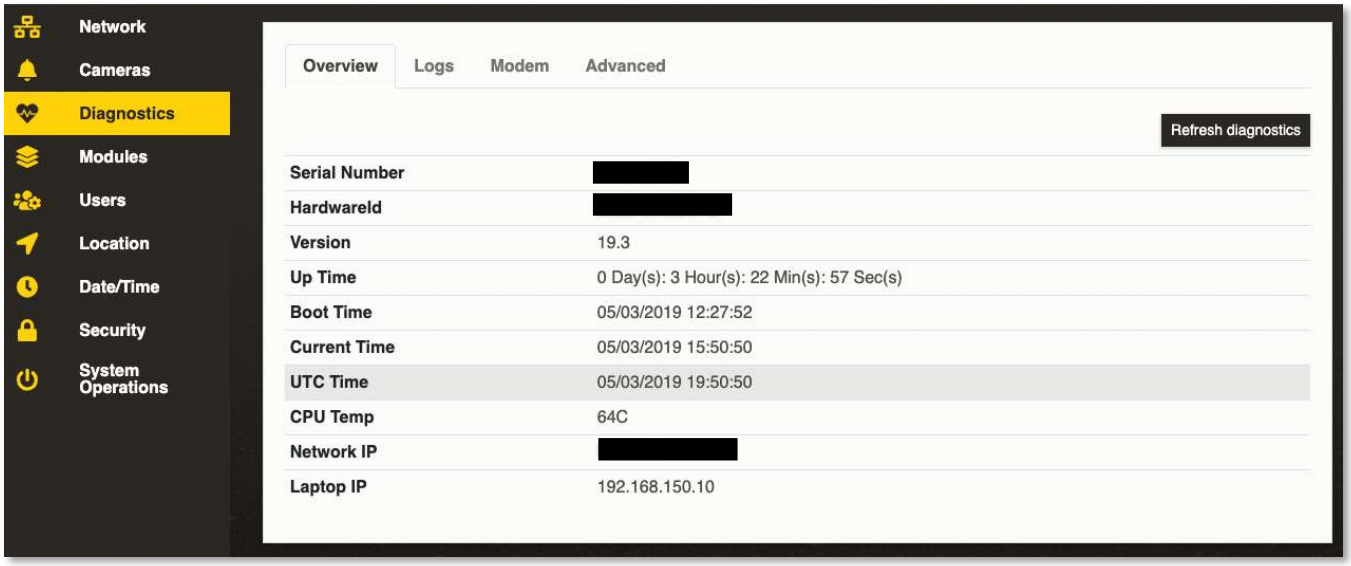
2.3 Phase Mapping

The Phases view of the GRIDSMART Device Manager will show the current Phases and Channel Groups. From this view, pre-configured Flashing Yellow Arrow (FYA) mode maps (A-L) can be set on the processor, allowing the FYA states to be recognized, logged in archived data, and displayed in the Client. For non-standard scenarios, GRIDSMART can help generate a custom channel map you can push to the device in the Device Manager. Zones can be configured for FYA in the Client when the processor uses mapped FYAs

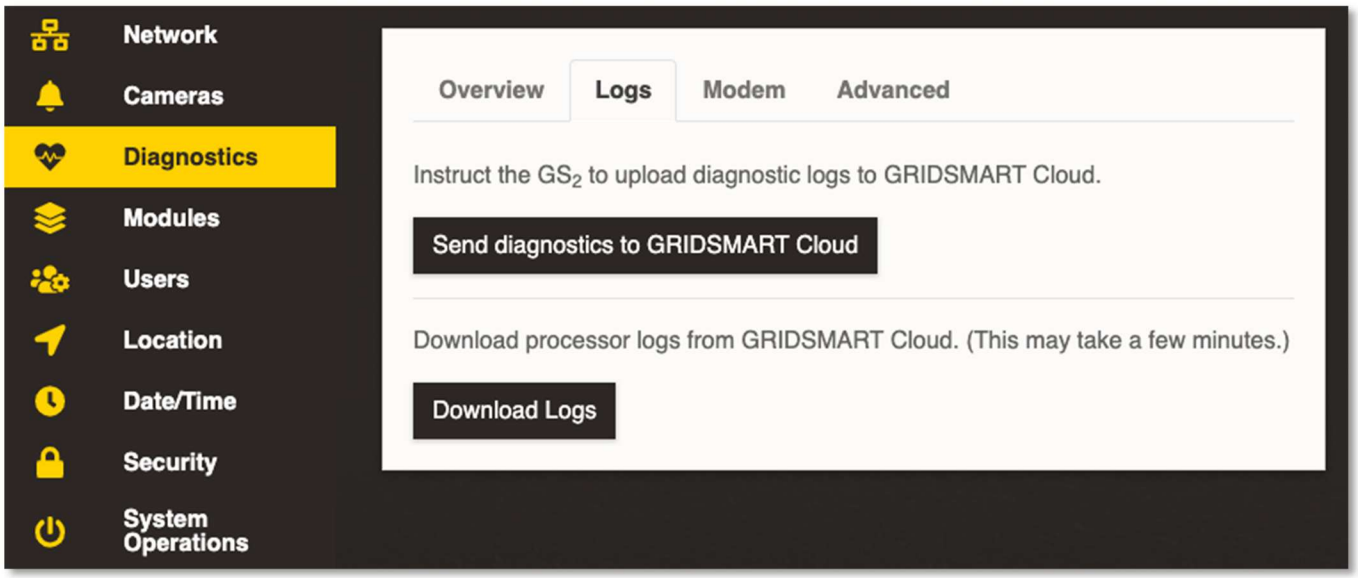


2.4 Diagnostics

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.

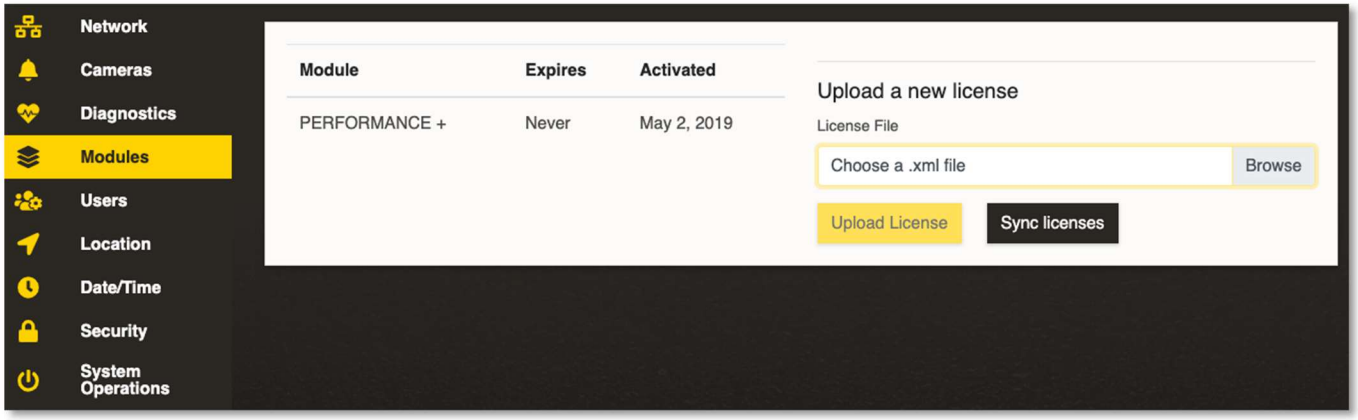


Diagnostic logs may be sent to Support through GRIDSMARTcloud.com.



2.4 Modules

This allows licenses to be uploaded or synced as needed.



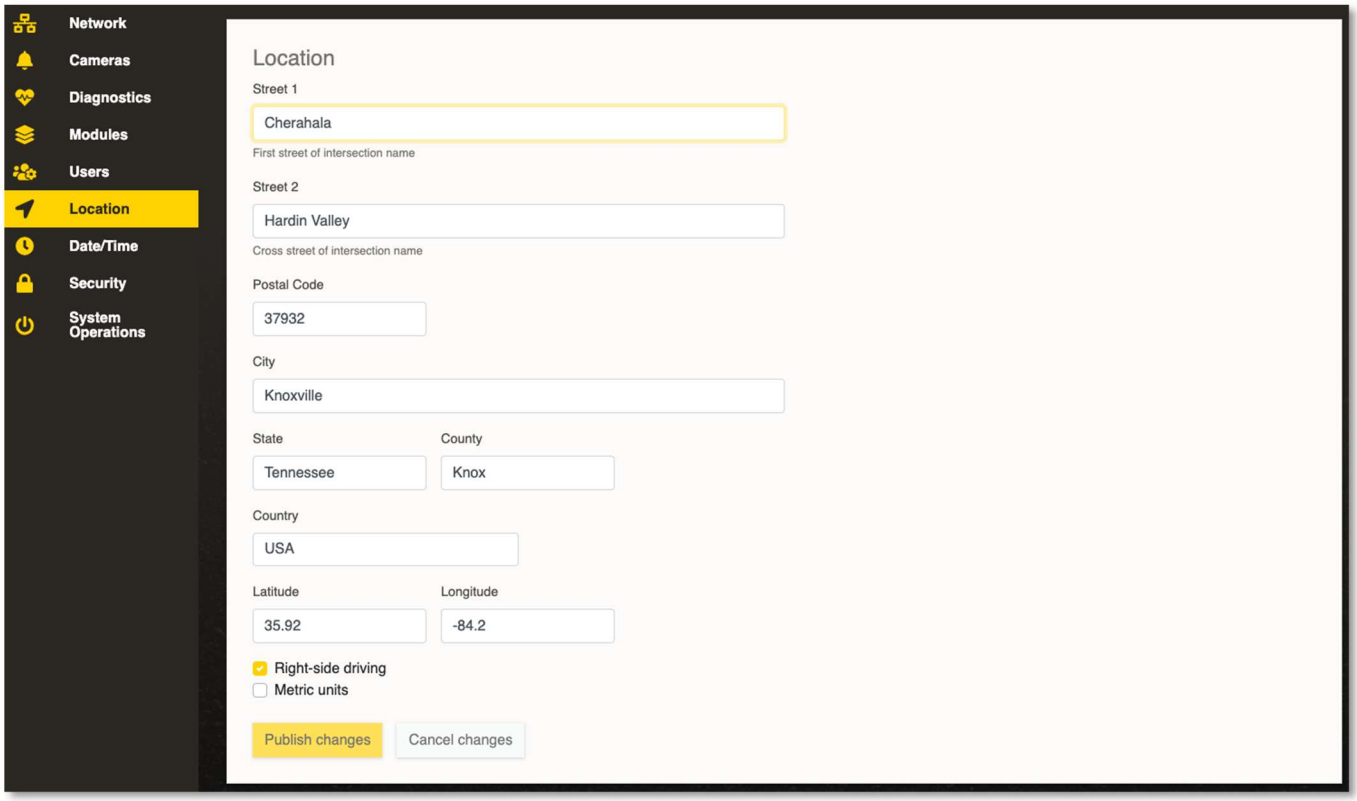
2.5 Users

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.

Refer to Section 4.2 for more details.

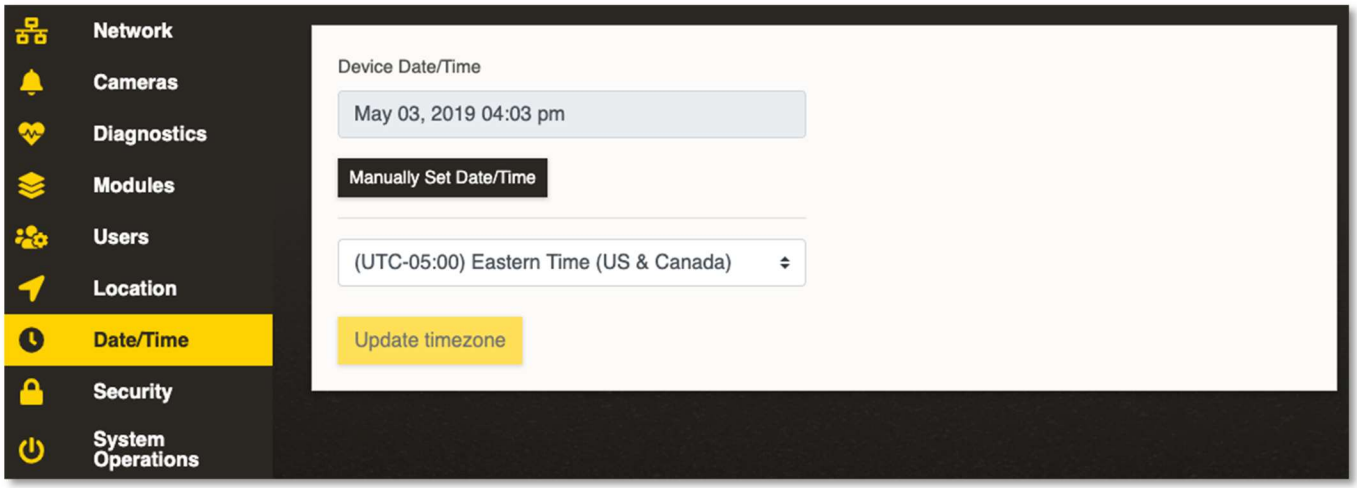
2.6 Location

This allows configuration of the location for the GS2 processor.



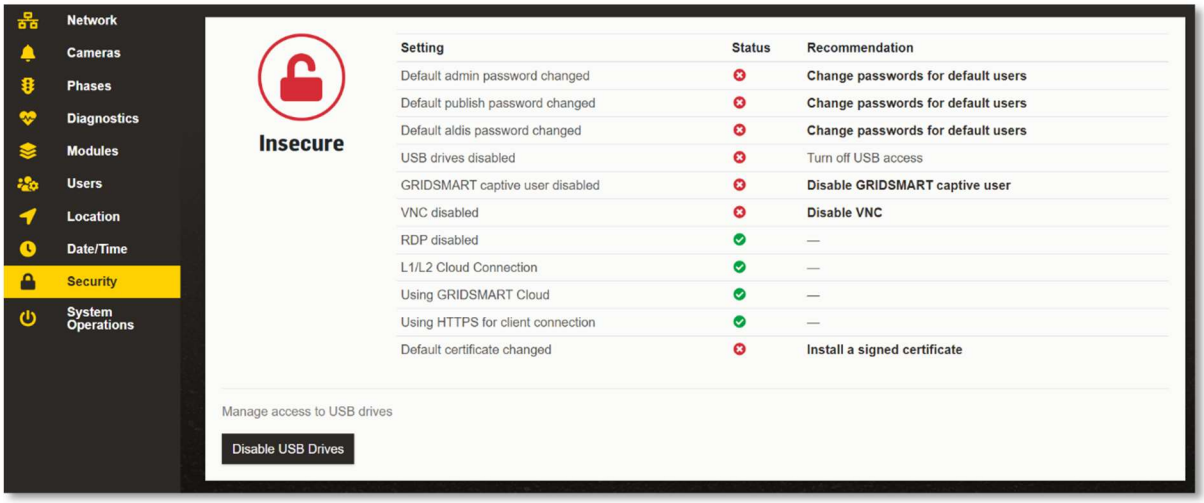
2.7 Date/Time

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



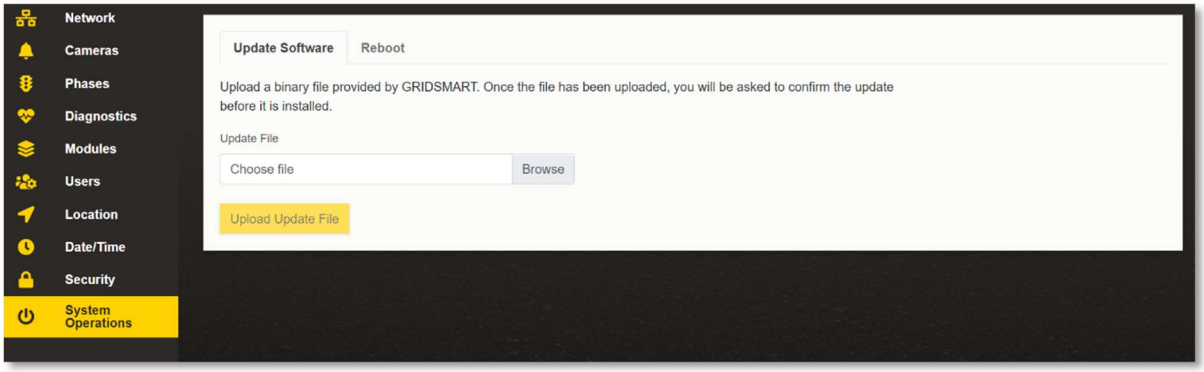
2.8 Security

This screen is a Self Audit of the GS2. The Self Audit function provides an easy way to ensure the equipment is as secure as possible. You can make changes by clicking the recommendation.



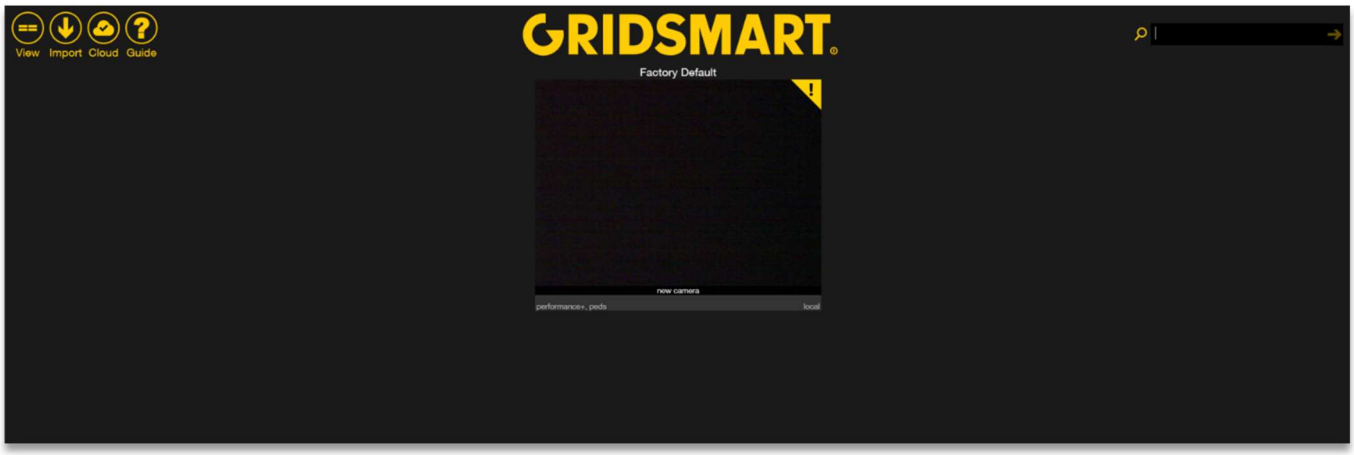
2.9 System Operations

This allows you update software by uploading a binary file and also to reboot the GS2 processor.



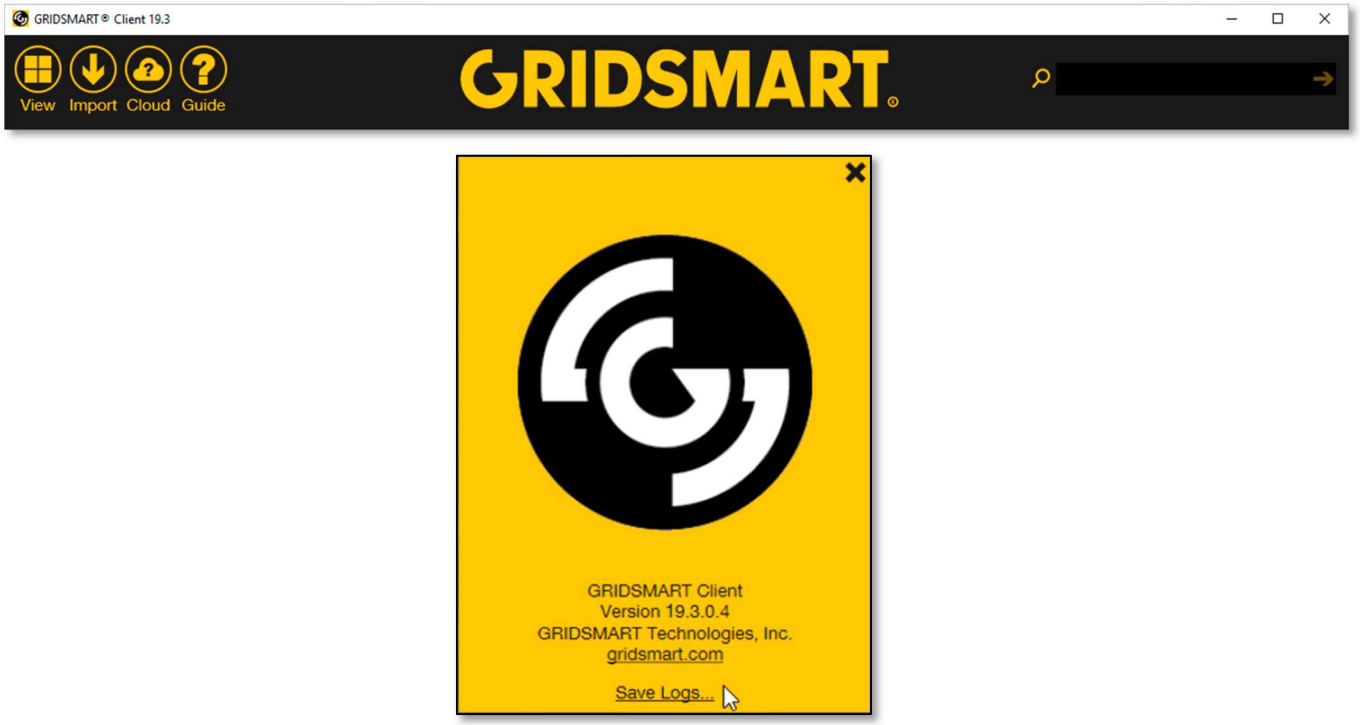
For more detail regarding the Networking and Security features, please refer to the **GS2 Network and Configuration Appendix.**

3.0 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.

GRIDSMART Client logs may be collected from double-clicking "GRIDSMART" in the Client. These may be requested by Support to help diagnose issues. Once you have the zip file attach it to an email and send it to support@gridsmart.com



3.1 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

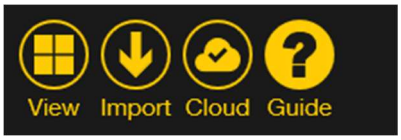
To open a site, click the appropriate Site Card on the Sites Homepage.

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.

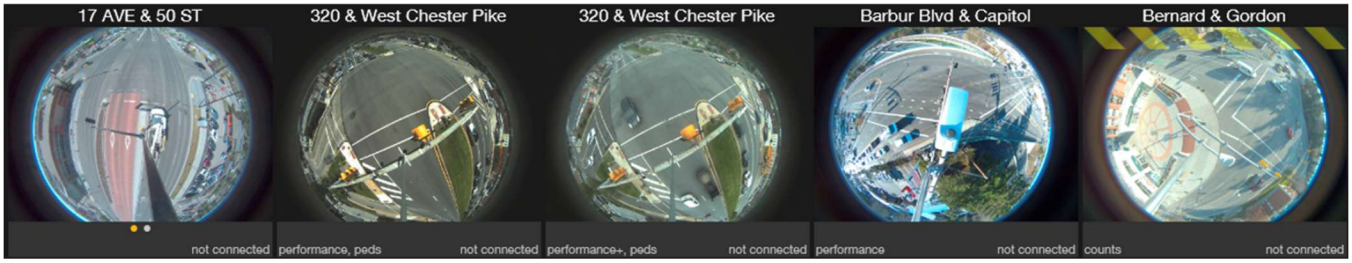
Site Cards display on the Homepage if the Client previously connected to the site and the IP address of the corresponding GRIDSMART Processor has not changed.

Site View Manager

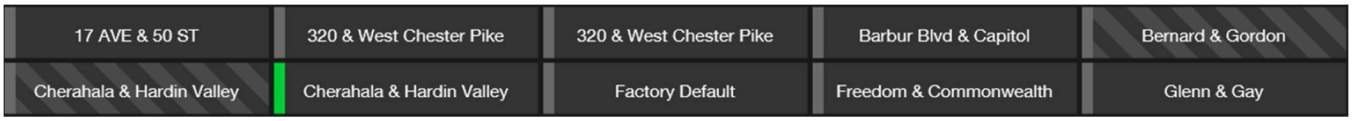
Click the View button on the top left of the homepage to toggle a new view. Next, select the site you want to view.



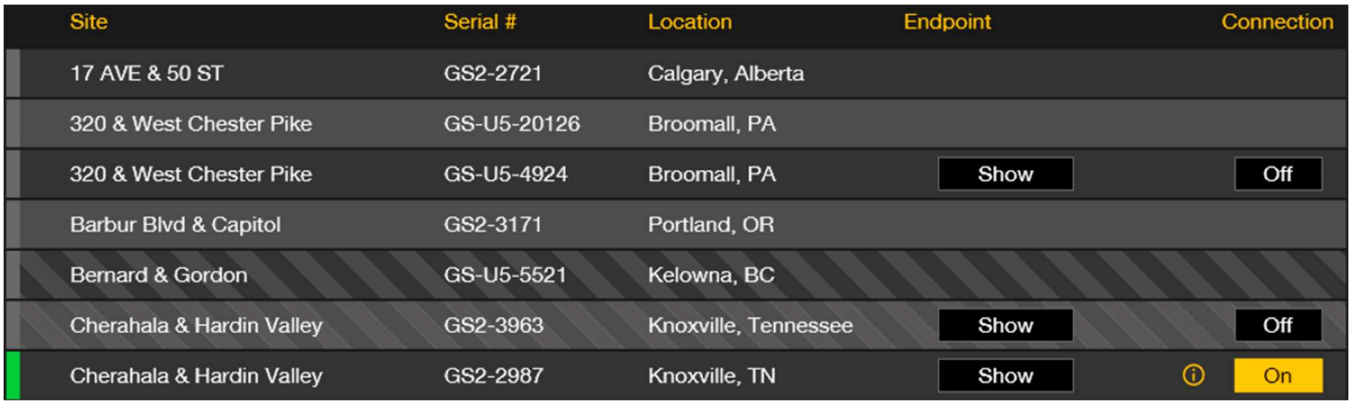
Site Image View



Lightweight View



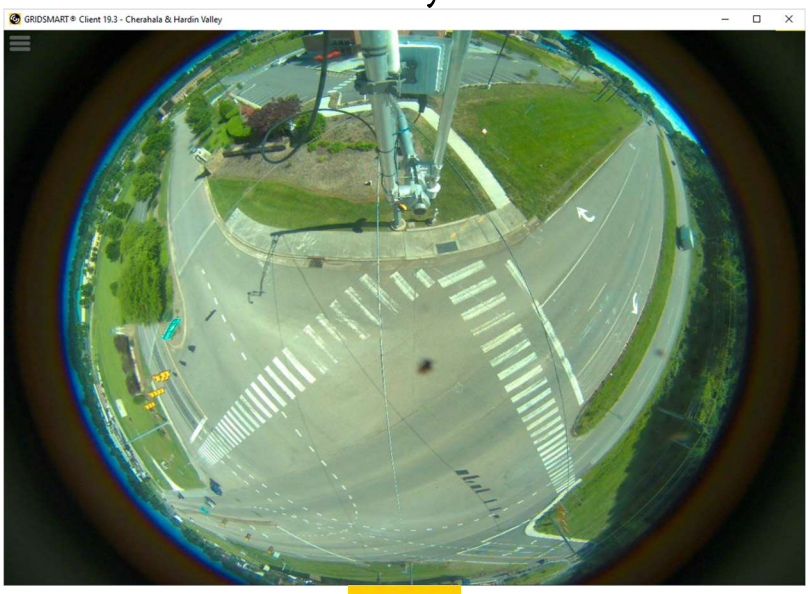
Detail View



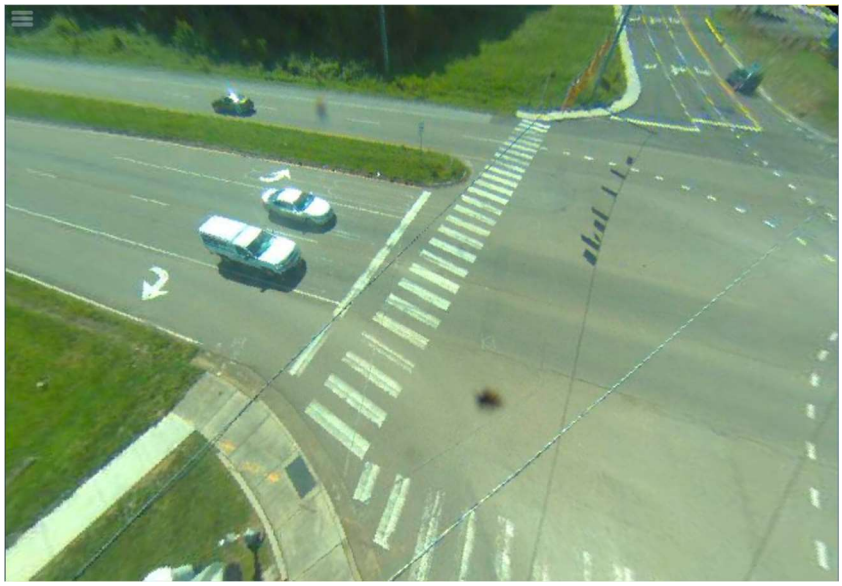
Select the Site you want to view or Select the top center “Factory Default” site card to configure a new site.

3.2 Site View Modes

Fisheye

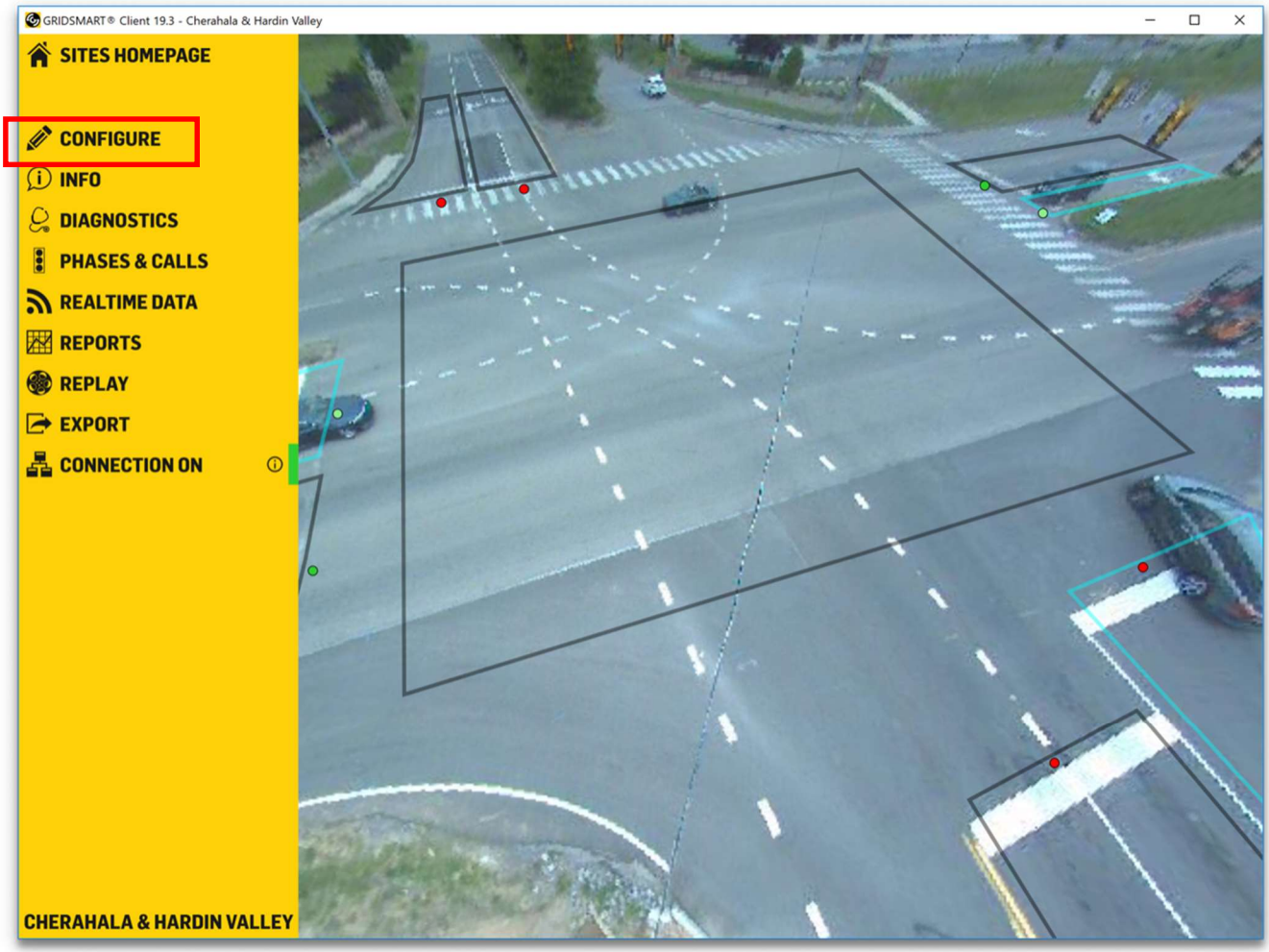


Flattened



3.3 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.

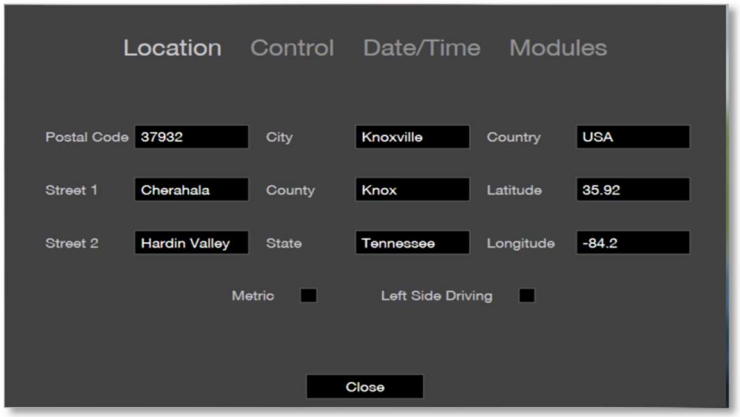


Click the Configure pencil on the Site Menu to start the setup wizard.

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

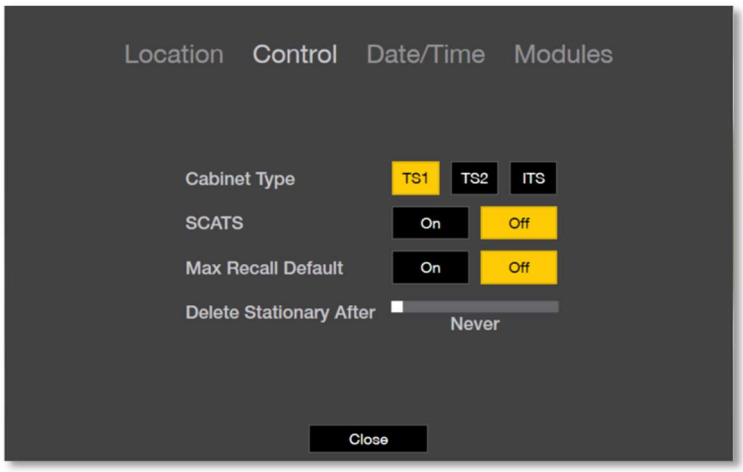
You can now complete basic device configuration via a browser now as well.

Location



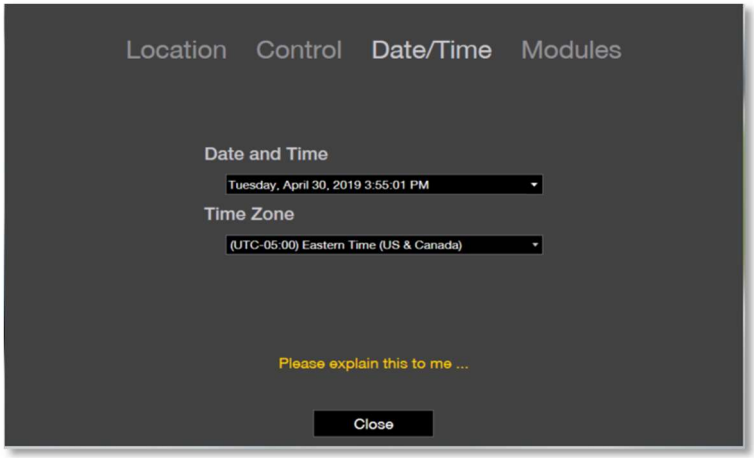
Enter the site location information.
For U.S. and Canadian sites, the Postal Code automatically populates the City, State, County, Latitude and Longitude fields.
If you are outside the US and Canada manually enter the Latitude and Longitude.

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.

Date and Time

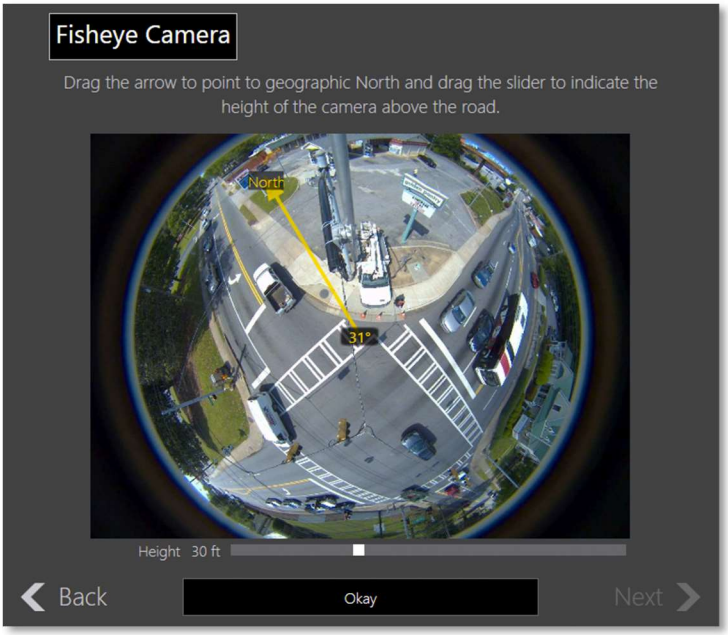


Select the Date, Time and the Time Zone. The factory default is Eastern Time (US & Canada).

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.

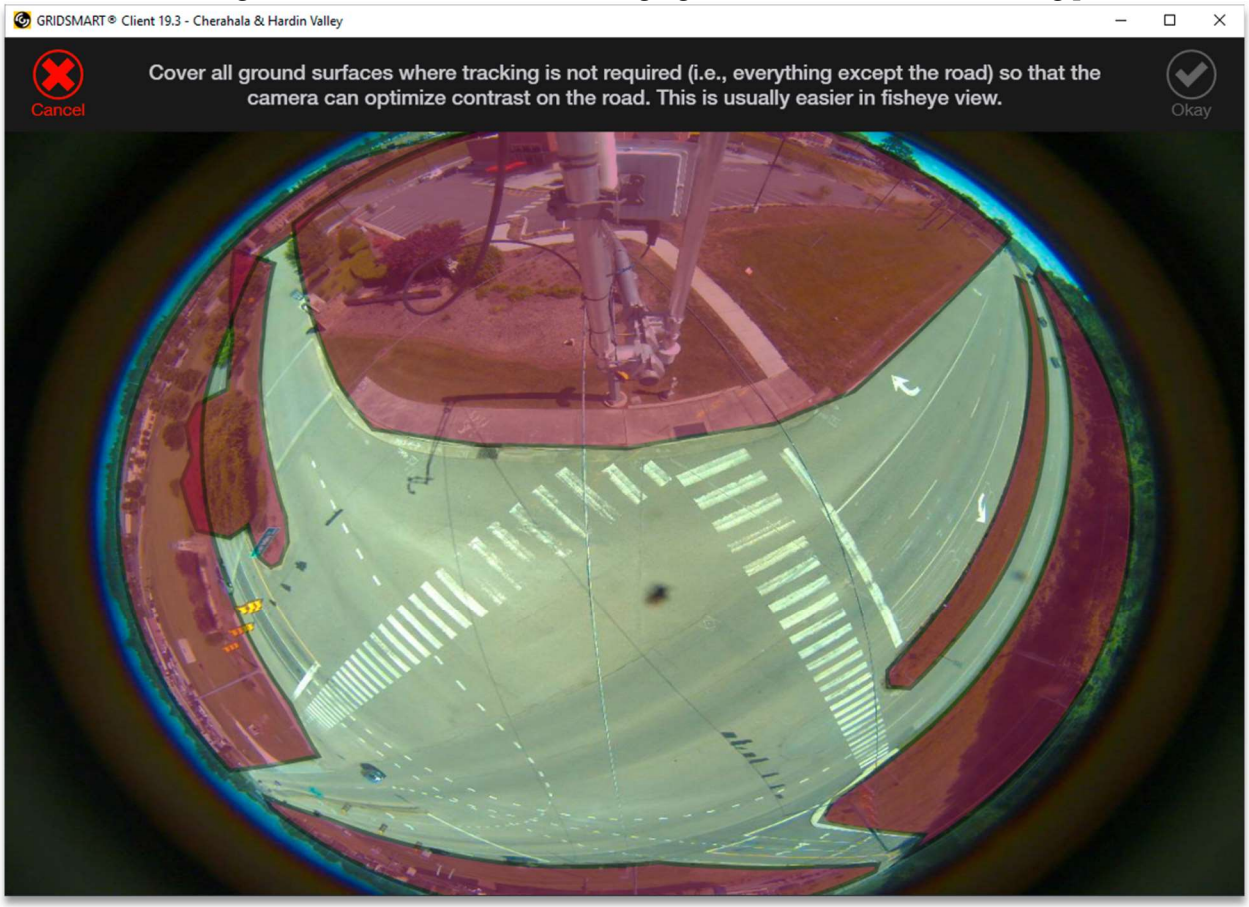
Click Okay.

4.0 Site Configuration

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

4.1 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.

4.2 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

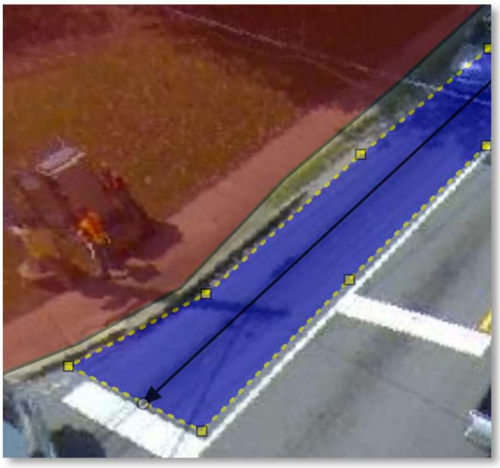
Mark the region for vehicle detection by clicking to add points.

Click back on the first point to complete the region.

Set the Flow Direction

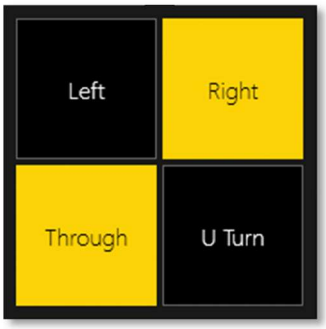
Left-click the front of the directional flow arrow.

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.

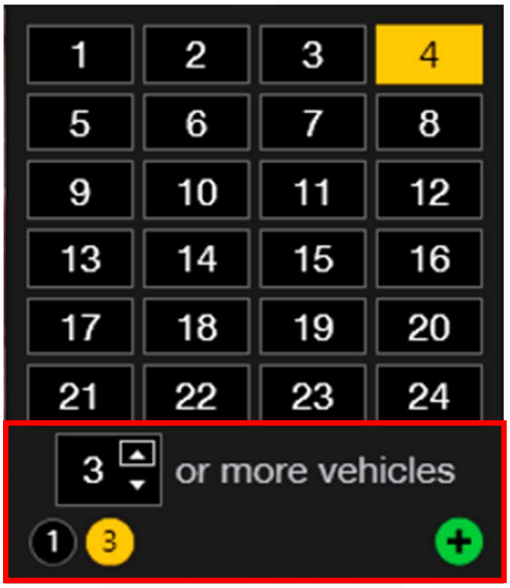
Output: TS1 / BIU / SIU

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.

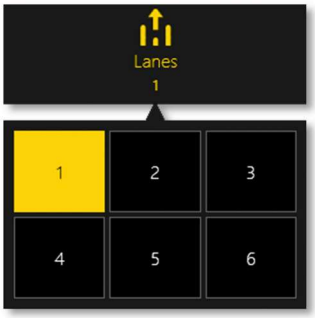
Occupancy Based Outputs can be configured while creating Zones. To Start, click the Green Plus icon under the output option for the zone. Select the number of cars desired (up to 6) for the new output. You can now add up to 6 different outputs for each zone.



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

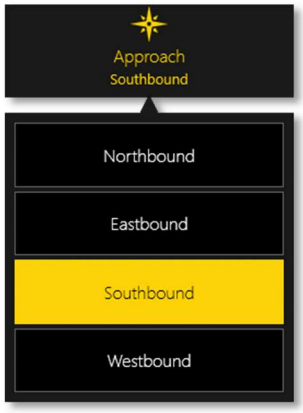
Lanes

Assign the number of lanes covered by the zone.



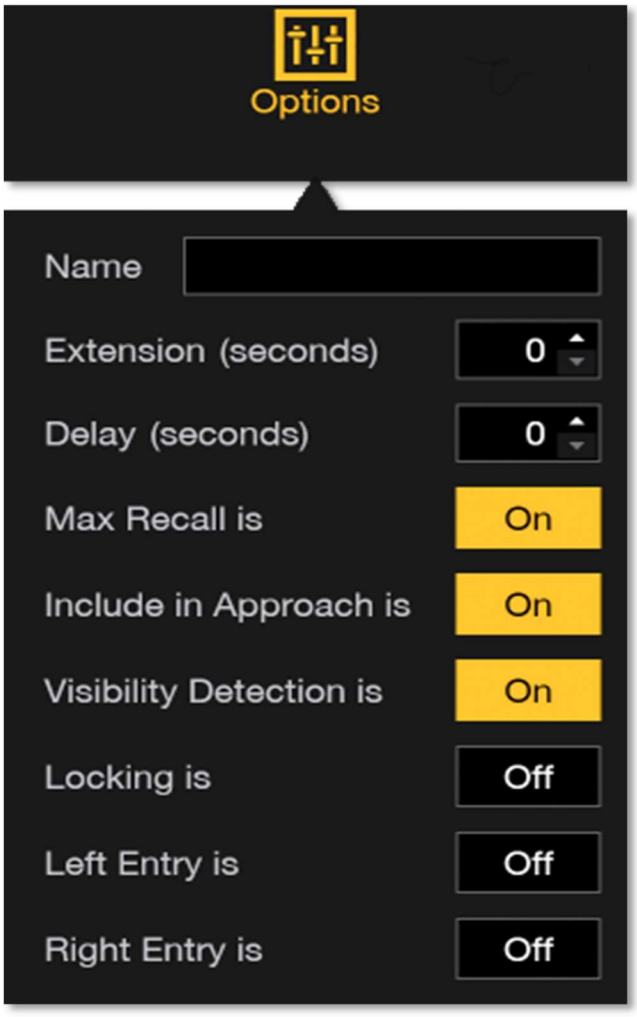
Approach

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.



4.3 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:

4.4 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.

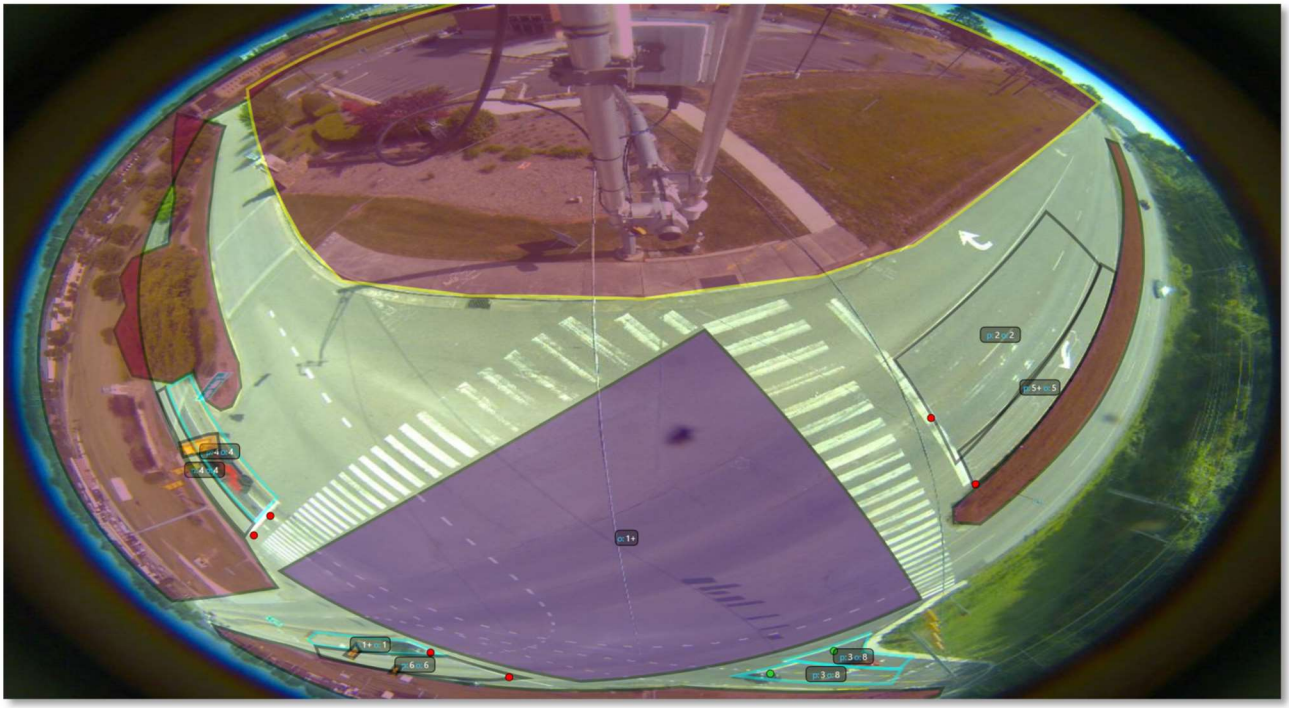
4. Select the Protected Pedestrian Phase and Output.

5. Select Alerts and Options as needed.

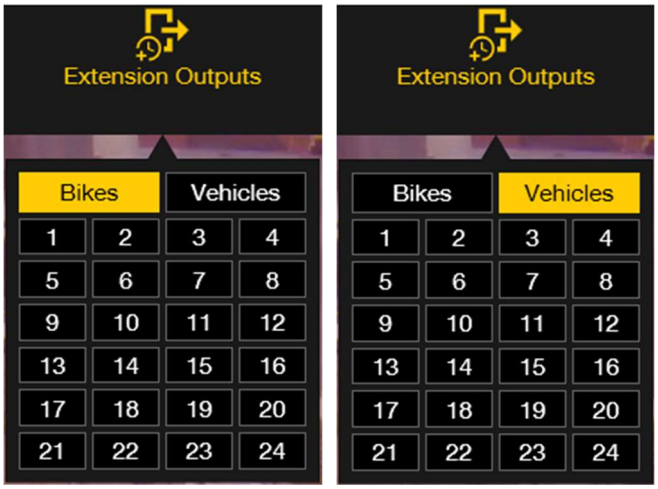
4.5 GRIDSMART Box

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.



4.5 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.

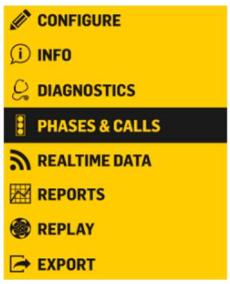
Reset to Factory does not remove the original Site Card from the Sites Homepage. If you no longer need the old Site Card, you can safely delete it by clicking the Yellow X in the upper right-hand corner of the card.

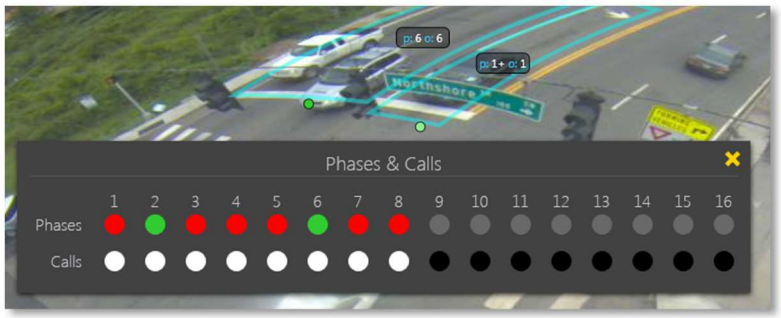
4.6 Quad View

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

4.7 Phases and Calls

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



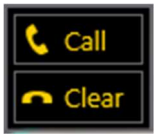


4.8 Make or Clear Calls on Operating Zones

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.

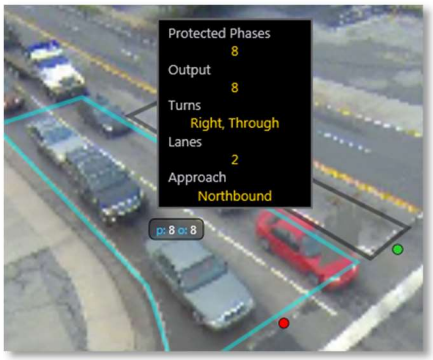
1. Click to select a Site Card from the Sites Homepage.
2. Move the mouse pointer into a zone and directly above the phase/output label. The phase/output label content changes to action/info icons represented by a gear and the letter "i" respectively.

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.



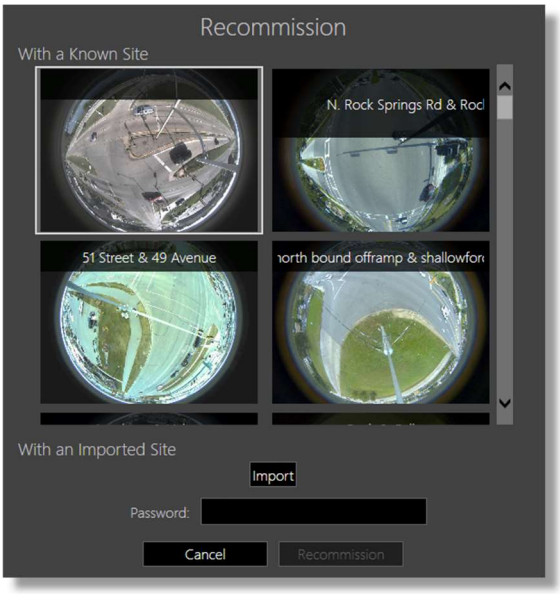
For zones with designated phases, calls will persist until the light receives a green. Without a designated phase, calls will persist for 10 seconds.
Calls are not placed for two seconds when cleared in this manner. The zone will not reactivate until a new vehicle enters the zone or a vehicle already in the zone moves.

Click to see zone phase information:



4.9 Recommission a Factory Default Processor

RECOMMISSION (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.

5.0 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 username and then "aldis#world9" for the password. We strongly encourage that the administrator of the Processor creates appropriate user credentials.

5.1 Security – Admin, Publish and Read-only

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

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

Permission Level	Username	Password	Capabilities using HTTP	Capabilities using HTTPS
Admin	admin	admin	Full access to GS2 Device Manager, Admin account disabled in client software.	Full access to GS2 Device Manager, Full access in client software.
Publish	publish	aldis#world9	Limited functionality in GS2 Device Manager, can publish to site from client	Limited functionality in GS2 Device Manager, can publish to site from client.
Read-only	aldis	aldis#world9	Limited functionality in GS2 Device Manager, cannot publish in client.	Limited functionality in GS2 Device Manager, cannot publish in client.

To change passwords, please refer to the Appendix - GS2 Networking & Security.

5.2 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.

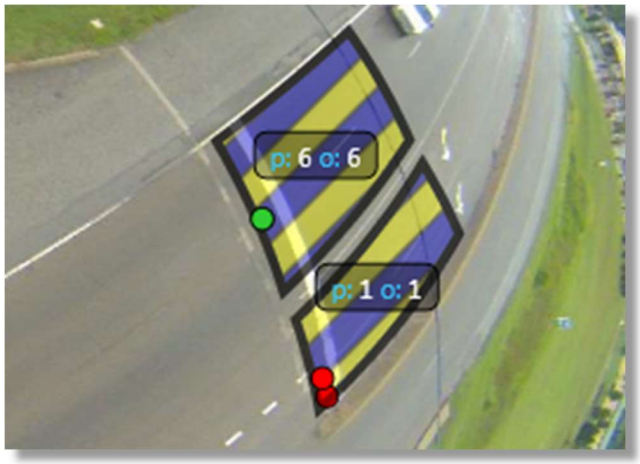
5.3 Make Changes to a Site Configuration

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.

5.4 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.

5.5 Publish History

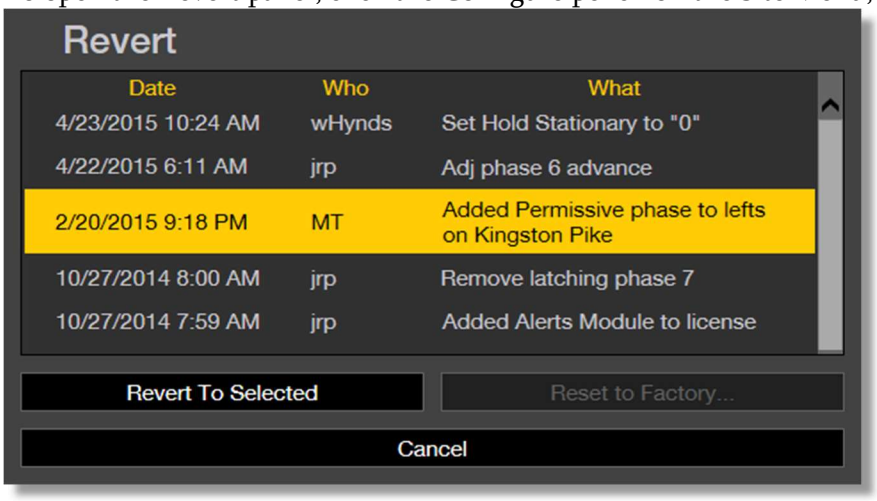
Publish History displays all previously published changes made to a site configuration. Click the Info icon on the Site Menu to see the date, time, username and description of the changes.

Publish History is also displayed in the Revert panel on the Site Configuration screen.

6.0 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.



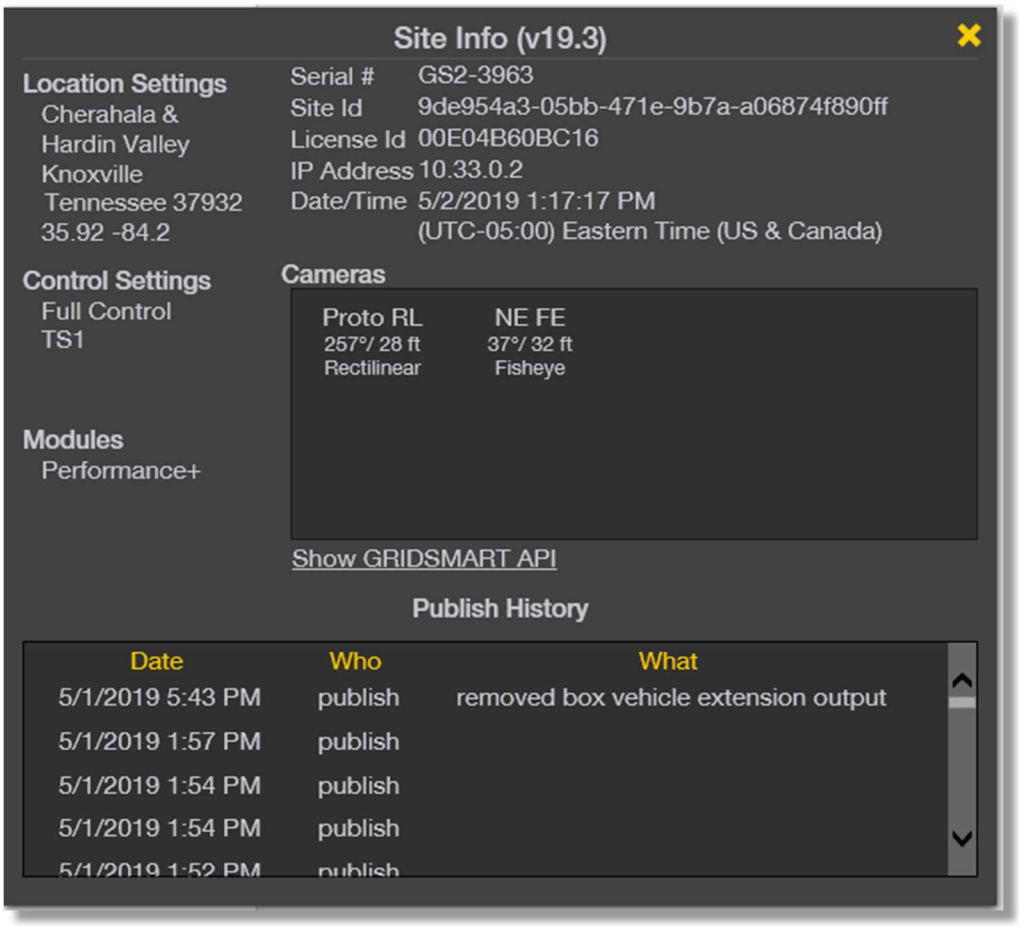
2. Select a previously published configuration, then click the Revert to Selected button.

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.

7.0 Site Info

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



8.0 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.

8.1 GRIDSMART Data Modules

FEATURE	Performance	Performance Plus
Client Reports		
Standard Reports		
Volume	X	X
Turning Movement Count	X	X
Vehicle Classification	X	X
Incident	X	X
Raw Export	X	X
Performance Reports		
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
Auto Reports	X[1]	X[3]
GRIDSMART.cloud Reports	X[1]	X[3]
Alerts[2]		
All System Events	X[1]	X[3]
Loss of Visibility		X[3]
Volume Exceeded		X[3]
Loss of Green (Flash)		X[3]
Zone Activated		X[3]
H.264 Streams		X[1,4]
Minute by Minute Display	X[1]	X[1]
Vulnerable Road Users		
Pedestrian Crosswalk Detection	With 19.10 VRU's are included with no Module needed. [4]	
Bicycle Clearance Extensions		

KEY

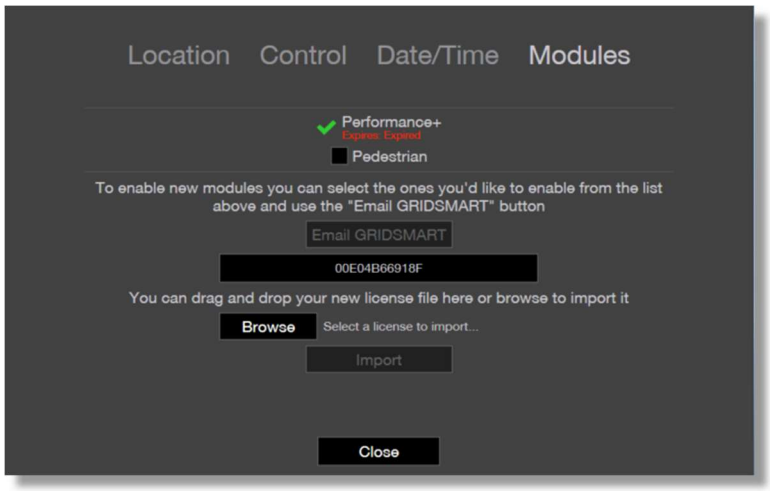
1 Requires WAN connectivity.
2 Alerts are delivered via email upon occurrence. Events shown in GRIDSMART Cloud are updated once daily, not upon occurrence.
3 Requires External Antenna or WAN connectivity.
4 Requires GS_2 Processor

8.2 Description 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.

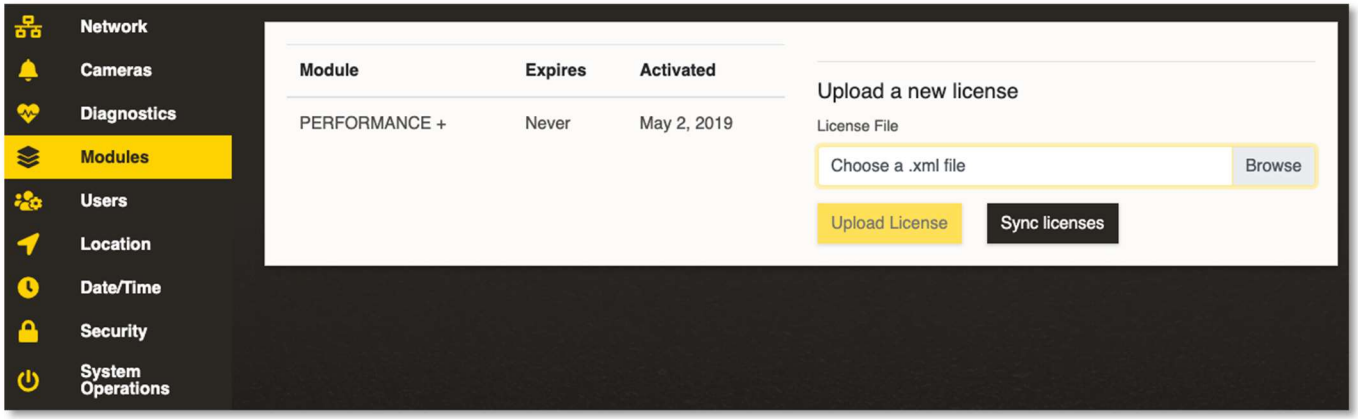
8.3 Adding a Module

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.

You can now manage Modules on the GS2 by opening the Device Manager.



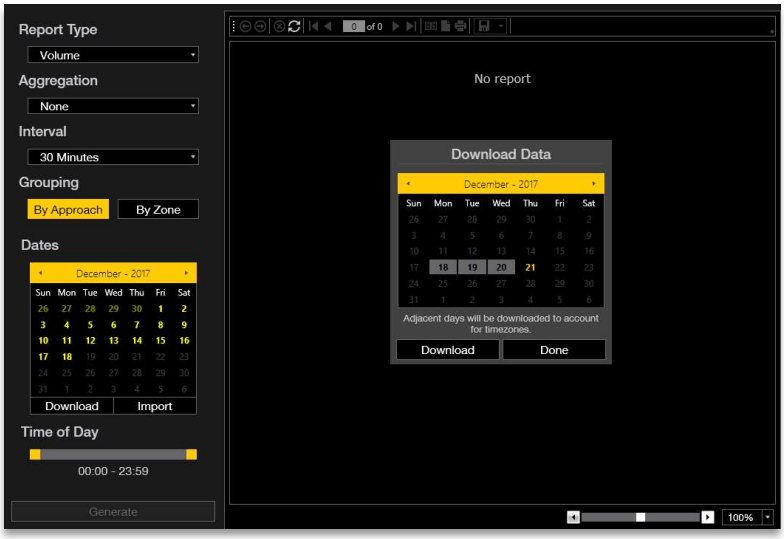
9.0 Reports

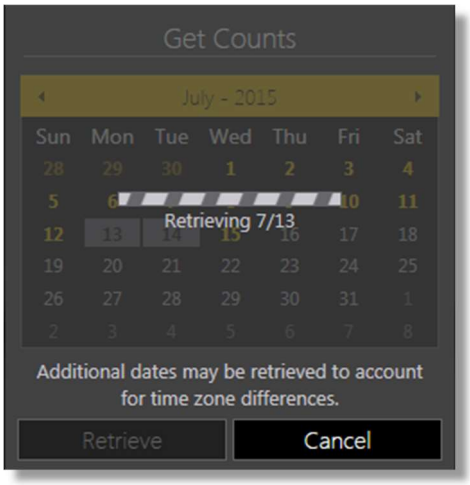
With the PERFORMANCE and PERFORMANCE PLUS Modules, GRIDSMART automatically logs vehicle counts for at least one year. Counts are stored on a first in, last out basis.

9.1 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.





9.2 Get PERFORMANCE DATA with a USB Storage Device

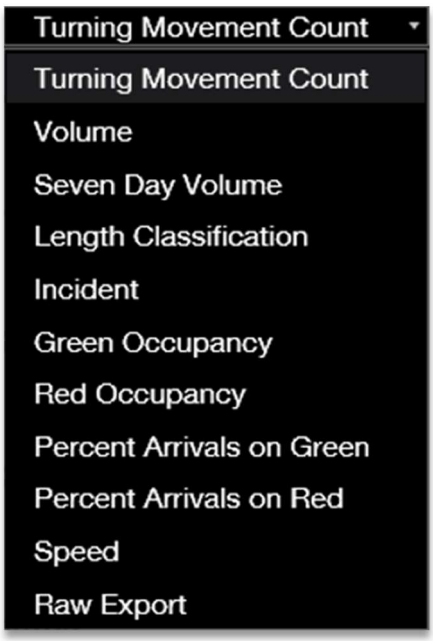
Note: This will only work if the USB sync is enabled in the Device Manager.

1. Begin with a freshly NTFS-formatted USB storage device or with a Data Stick or Drive that you have already used with GRIDSMART.
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.

9.3 Generating Reports

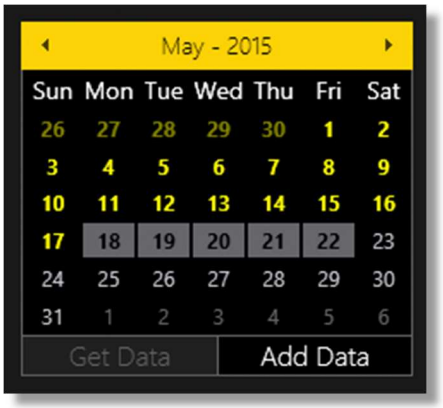
Once the Counts have been downloaded or synced to the Client, click the Reports icon and choose your options.

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.

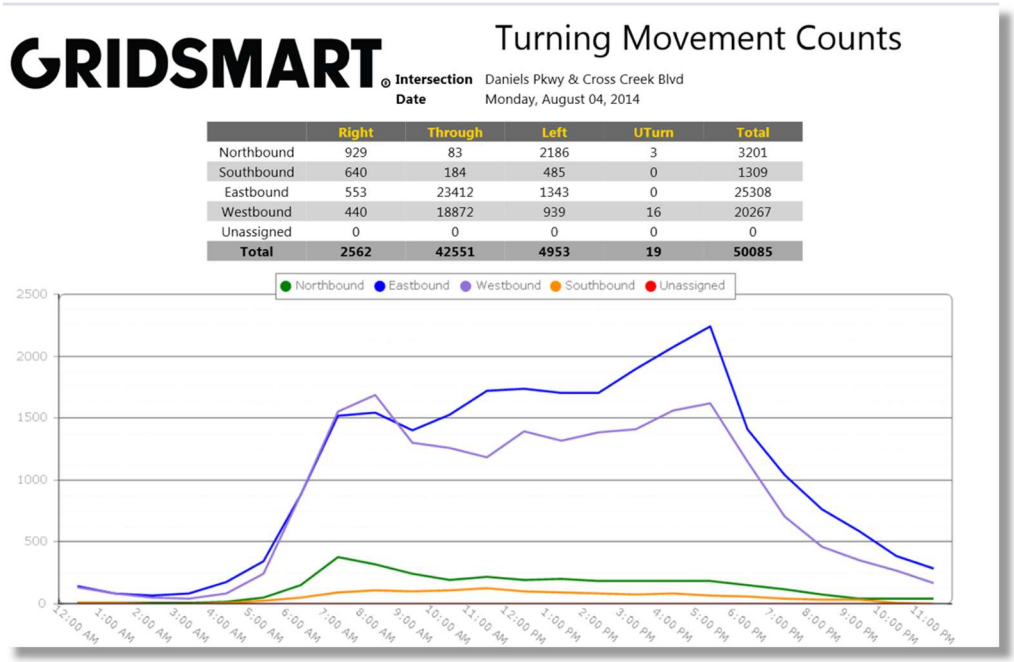
Click Generate.

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

Click the disk to save the report as:

1. PDF
2. Excel

9.3.1 Report – Turning Movement Counts

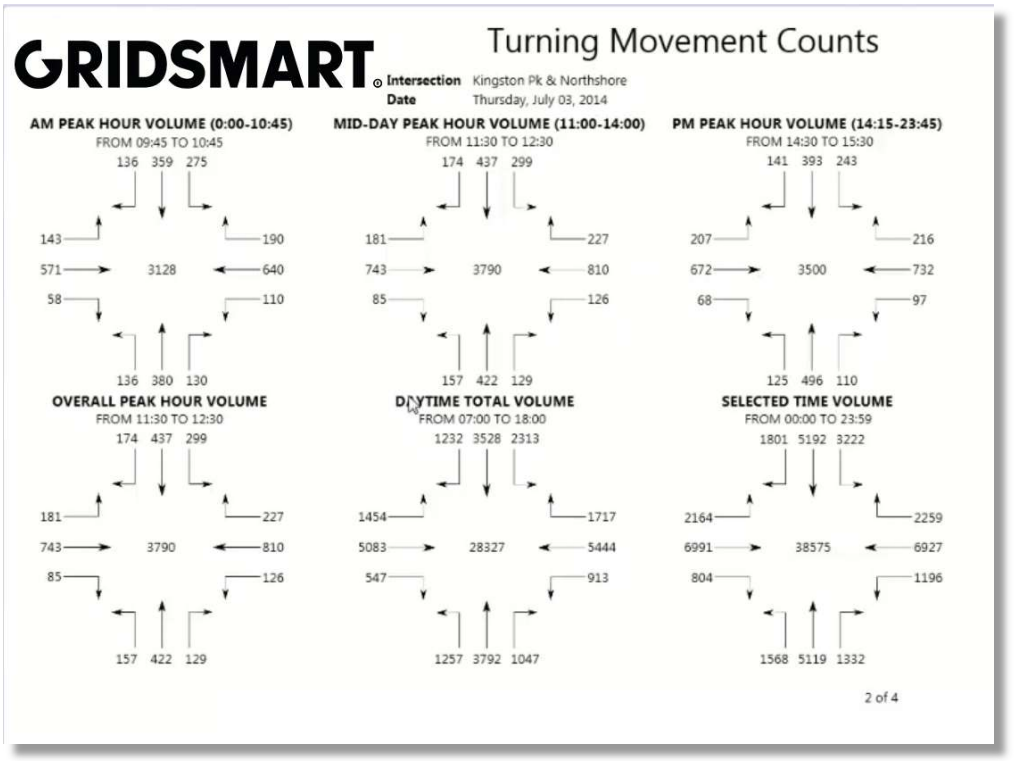


GRIDSMART

Turning Movement Counts

Intersection Daniels Pkwy & Cross Creek Blvd
Date Monday, August 04, 2014

	Right	Through	Left	UTurn	Total
Northbound	929	83	2186	3	3201
Southbound	640	184	485	0	1309
Eastbound	553	23412	1343	0	25308
Westbound	440	18872	939	16	20267
Unassigned	0	0	0	0	0
Total	**2562**	**42551**	**4953**	**19**	**50085**



GRIDSMART

Turning Movement Counts

Intersection Kingston Pk & Northshore
Date Thursday, July 03, 2014

AM PEAK HOUR VOLUME (0:00-10:45)
FROM 09:45 TO 10:45
136 359 275
143 190
571 3128 640
58 110
136 380 130

MID-DAY PEAK HOUR VOLUME (11:00-14:00)
FROM 11:30 TO 12:30
174 437 299
181 227
743 3790 810
85 126
157 422 129

PM PEAK HOUR VOLUME (14:15-23:45)
FROM 14:30 TO 15:30
141 393 243
207 216
672 3500 732
68 97
125 496 110

OVERALL PEAK HOUR VOLUME
FROM 11:30 TO 12:30
174 437 299
181 227
743 3790 810
85 126
157 422 129

DAYTIME TOTAL VOLUME
FROM 07:00 TO 18:00
1232 3528 2313
1454 1717
5083 28327 5444
547 913
1257 3792 1047

SELECTED TIME VOLUME
FROM 00:00 TO 23:59
1801 5192 3222
2164 2259
6991 38575 6927
804 1196
1568 5119 1332

2 of 4

9.3.2 Report – Vehicle Classification

Use the sliders under Edit Bins to define customized vehicle length bins. Bin names can be changed by clicking on the name of the bin.

GRIDSMART

Vehicle Classification Counts

Intersection Hardin Valley & Cherahala
Date Tuesday, June 02, 2015

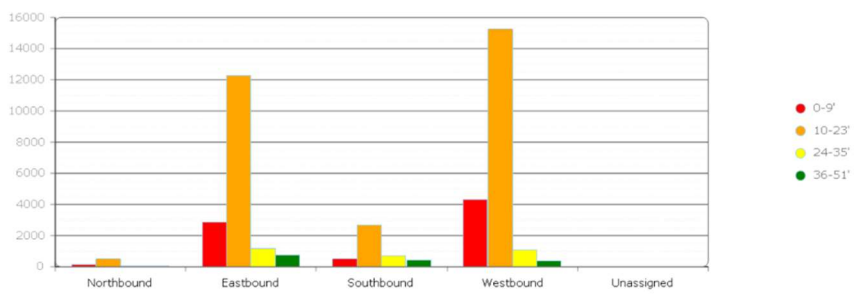
	Northbound				Southbound				
	0-9'	10-23'	24-35'	36-51'	0-9'	10-23'	24-35'	36-51'	0-9'
11:30 AM	4	20	2	2	6	54	11	6	26
11:45 AM	2	15	4	1	11	46	16	6	22
12:00 PM	6	26	1	0	12	63	13	8	28
12:15 PM	3	17	4	4	8	59	9	11	27
12:30 PM	4	16	3	1	7	36	5	5	29
12:45 PM	3	14	0	1	6	36	5	4	26
1:00 PM	1	16	3	1	5	43	7	5	20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

GRIDSMART

Vehicle Classification Counts

Intersection Hardin Valley & Cherahala
Date 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
Total	**712**	**4332**	**17071**	**20980**	**0**	**43095**



9.3.3 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
Total	**201**	**153**	**43**	**121**	**518**

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
Total	**0**	**14**	**0**	**0**	**2**	**4**	**0**	**13**	**0**	**0**	**16**	**3**

9.3.4 Report – Incidents Excel Output

A1 | 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											

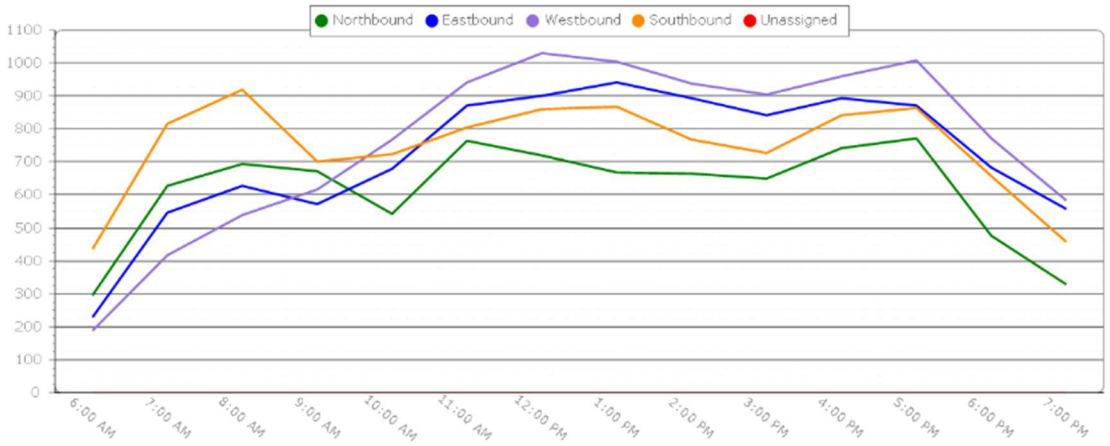
9.3.5 Report – Volume

GRIDSMART

Volume Report

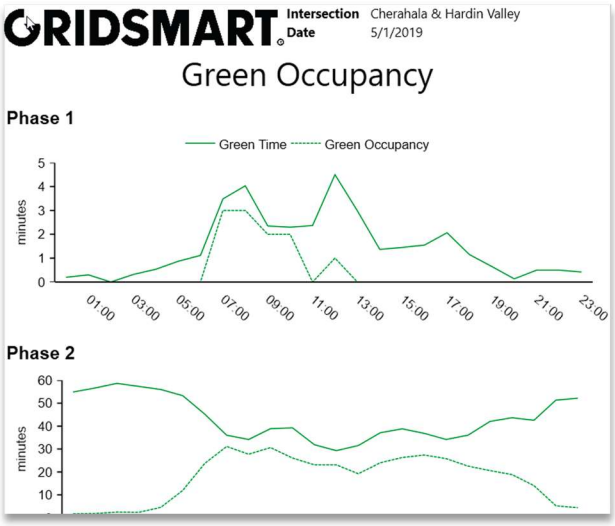
Intersection Kingston Pk & Northshore
Date Monday, July 13, 2015

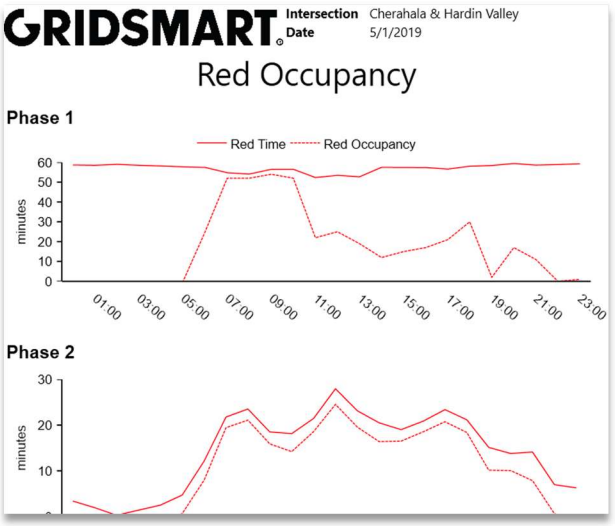
	Total
Northbound	8603
Southbound	10434
Eastbound	10106
Westbound	10663
Unassigned	0
Total	**39806**



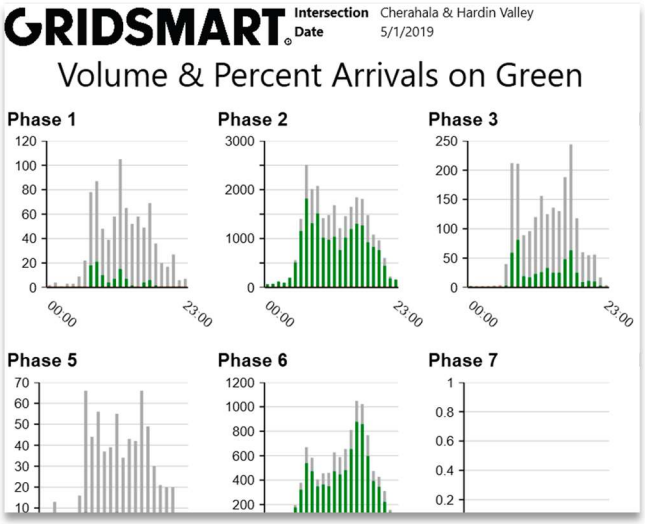
	Northbound	Southbound	Eastbound	Westbound	Total
6:00 AM	294	435	228	187	1144
7:00 AM	626	814	548	417	2405
8:00 AM	693	919	629	540	2781
9:00 AM	672	703	572	618	2565
10:00 AM	542	723	681	768	2714
11:00 AM	763	803	870	940	3376
12:00 PM	719	859	900	1029	3507
1:00 PM	667	866	942	1003	3478
2:00 PM	663	766	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
Total	**8603**	**10434**	**10106**	**10663**	**39806**

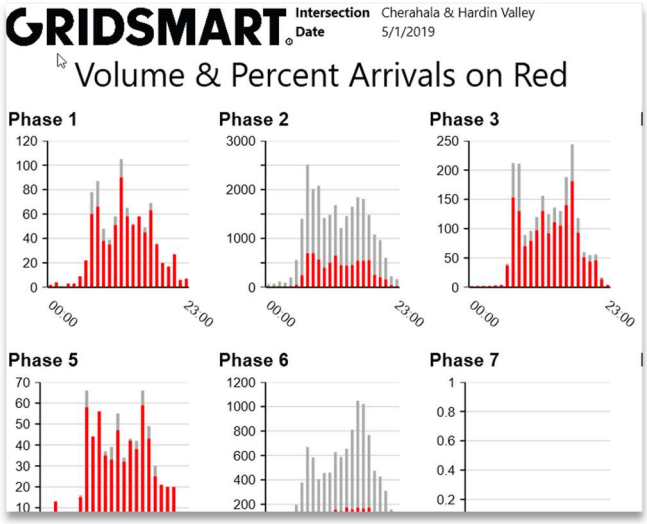
9.3.6 Report – Green/Red Occupancy



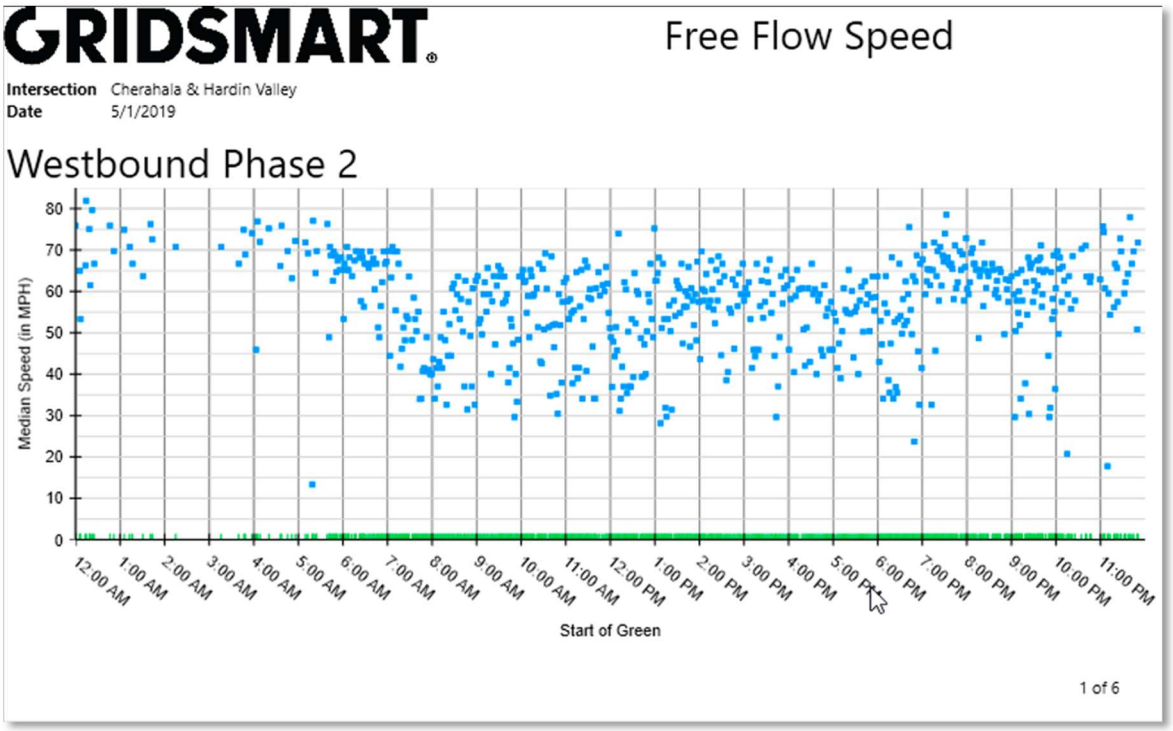


9.3.7 Report – Percent Arrivals On Green/Red





9.3.8 Report – Speed



9.3.9 Report – Raw Data Export

Creates a CSV file with raw count data.

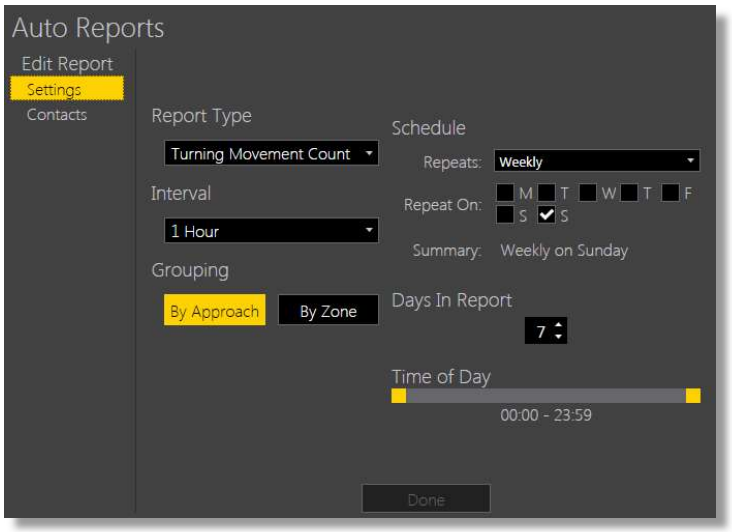
A1 | Date-UTC

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Date-UTC	ApproachType	Name	SecondsSinceLastExit	SecondsInZone	SecondsSinceLastGreen	TurnType	SpeedOnExit	DayMode	CarLength	LightState	QueueLength	AllowableTurnType
2	2015-07-14T11:30:01.0625000-04:00	Eastbound		84.48439789	3.799999952	0	Straight	4	D	10	Green	4	Right, Straight
3	2015-07-14T11:30:02.5625000-04:00	Eastbound		1.5	5.300000191	0	Straight	5	D	11	Green	4	Right, Straight
4	2015-07-14T11:30:03.8750000-04:00	Eastbound		1.3125	6.699999809	0	Straight	14	D	14	Green	4	Right, Straight
5	2015-07-14T11:30:05.5625000-04:00	Eastbound		1.6875	1.100000024	0	Straight	15	D	5	Green	4	Right, Straight
6	2015-07-14T11:30:05.9687500-04:00	Eastbound		0.40625	3.900000095	0	Straight	17	D	17	Green	3	Right, Straight
7	2015-07-14T11:30:06.7656250-04:00	Westbound		5.5	3.900000095	0	Straight	11	D	22	Green	5	Right, Straight
8	2015-07-14T11:30:06.7656250-04:00	Westbound		19.2031002	0.100000001	15.3593998	Left	0	D	11	None	3	Left
9	2015-07-14T11:30:06.9687500-04:00	Westbound		0.203125	4	0	Straight	11	D	10	Green	3	Right, Straight
10	2015-07-14T11:30:07.7656250-04:00	Eastbound		1.796880007	10.5	0	Straight	13	D	5	Green	2	Right, Straight
11	2015-07-14T11:30:08.5625000-04:00	Eastbound		0.796875	5.099999905	0	Straight	18	D	4	Green	1	Right, Straight
12	2015-07-14T11:30:10.0625000-04:00	Westbound		0.796875	7.099989891	0	Straight	18	D	21	Green	4	Right, Straight
13	2015-07-14T11:30:10.5625000-04:00	Eastbound		2	3.5	0	Straight	14	D	10	Green	2	Right, Straight
14	2015-07-14T11:30:10.9687500-04:00	Westbound		0.6875	0.5	0	Right	26	D	14	Green	3	Right, Straight
15	2015-07-14T11:30:11.5625000-04:00	Eastbound		0.203125	2.799999952	0	Straight	26	D	5	Green	2	Right, Straight
16	2015-07-14T11:30:13.1718750-04:00	Westbound		0.703125	5	0	Straight	26	D	30	Green	3	Right, Straight
17	2015-07-14T11:30:13.6718750-04:00	Eastbound		2.109380007	2.5	0	Straight	16	D	4	Green	3	Right, Straight
18	2015-07-14T11:30:14.8750000-04:00	Westbound		1.203130007	4.099999905	0	Straight	21	D	12	Green	2	Right, Straight
19	2015-07-14T11:30:15.4687500-04:00	Eastbound		1.796880007	3.200000048	0	Straight	26	D	5	Green	4	Right, Straight
20	2015-07-14T11:30:15.6718750-04:00	Eastbound		0.203125	4.099999905	0	Straight	16	D	6	Green	3	Right, Straight
21	2015-07-14T11:30:16.5625000-04:00	Westbound		2.890630007	3.400019884	0	Straight	24	D	20	Green	6	Right, Straight
22	2015-07-14T11:30:16.7656250-04:00	Westbound		0.203125	3.100029945	0	Straight	28	D	26	Green	4	Right, Straight
23	2015-07-14T11:30:17.2656250-04:00	Eastbound		0.203125	2.400029898	0	Straight	28	D	11	Green	6	Right, Straight
24	2015-07-14T11:30:18.5625000-04:00	Westbound		0.203125	0.400000006	0	Straight	23	D	18	Green	2	Right, Straight
25	2015-07-14T11:30:18.8750000-04:00	Eastbound		1.609380007	3.800019979	0	Right	12	D	13	Green	2	Right, Straight

9.4 Auto Reports

Automatically email reports to a group of contacts on a schedule. This functionality is included as part of the Performance+ 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.



10.0 Alerts

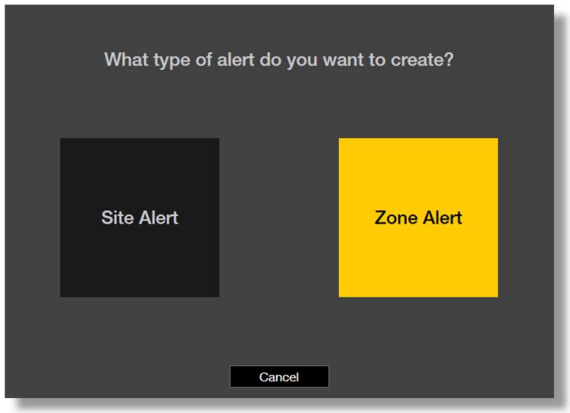
The Performance+ Module sends emails to a user-defined set of contacts when the GRIDSMART Processor detects certain events.

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.

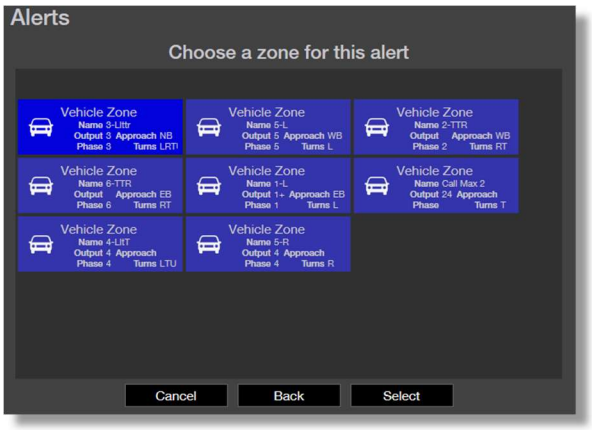
To create an Alert, click the Configure pencil on the Site Menu, then click Alerts in the upper right-hand corner.

Click New.

Click Site Alert or Zone Alert.

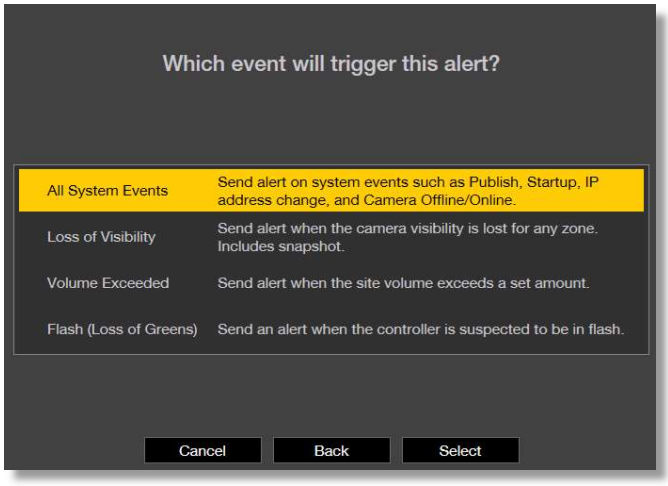


If you are creating a Zone Alert, choose a vehicle zone, then click Select.



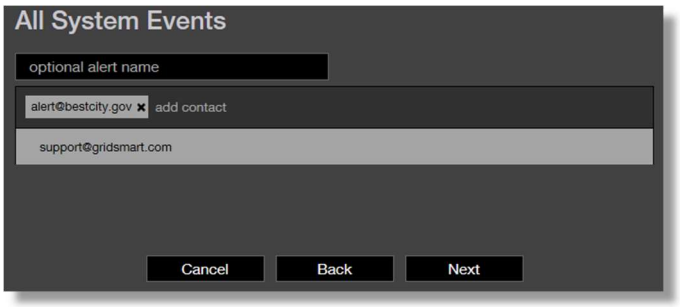
Choose an event to trigger the alert, then click Select.

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.

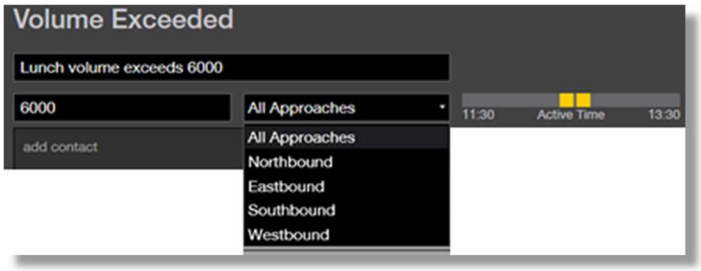
Optionally add an alert name. The name defaults to the event type.



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.

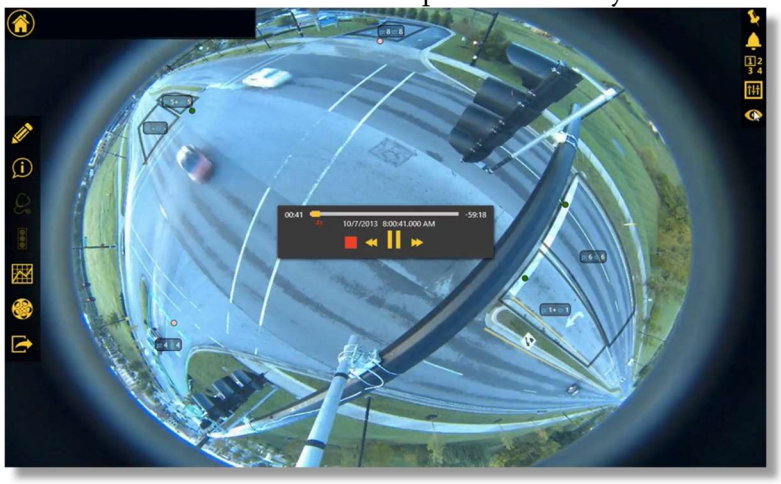
Publish your changes.

11.0 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 images 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

11.1 Record and Review Images and/or Performance Data

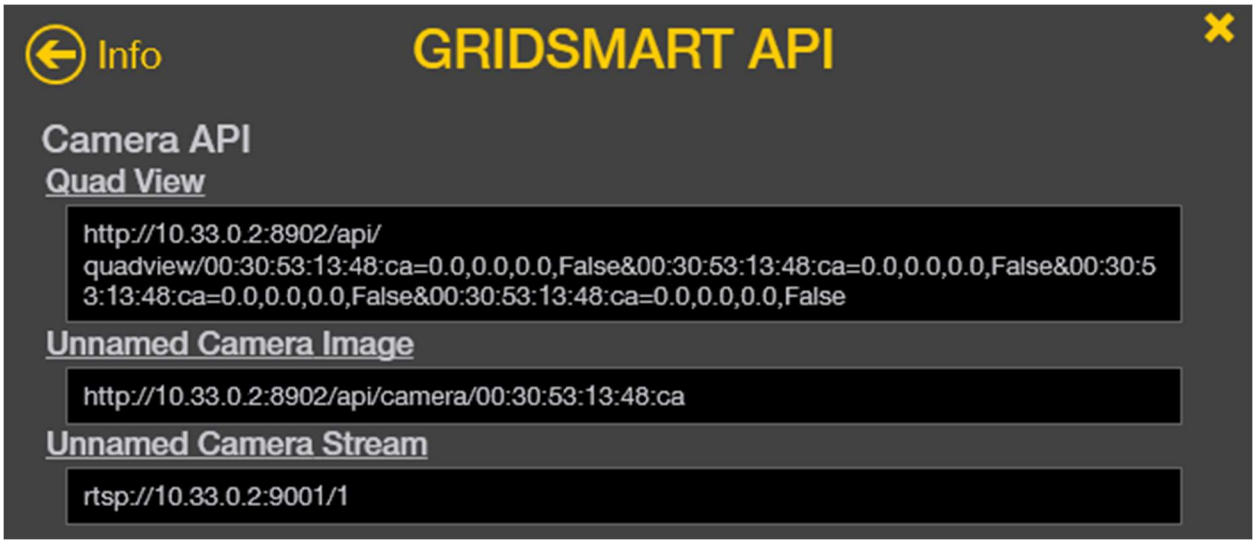
Note: This will only work if the USB sync is enabled in the Device Manager.

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.

12.0 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 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.

13.0 Streaming H.264 streams via RTSP

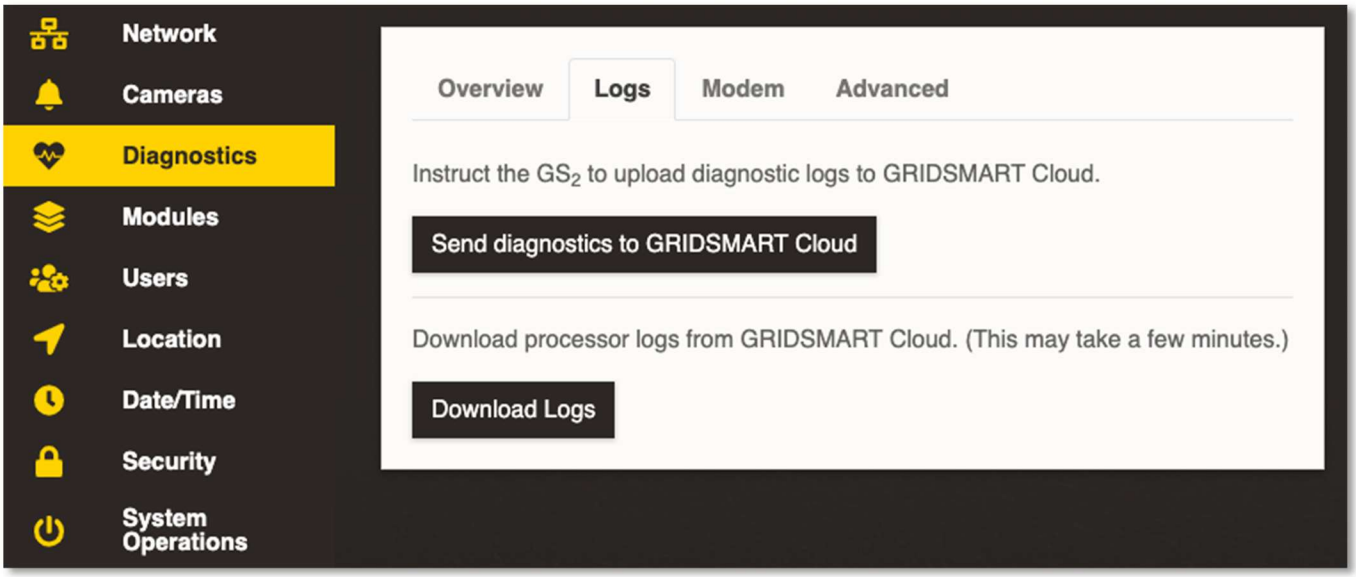
Streaming is now possible with the purchase of a Performance Plus module and with a high-speed connection to the GS2 processor and video management or network video system software and/or hardware. The customer and/or customer's vendor are responsible for de-warping the images, if desired, as well as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

14.0 Support

Before contacting GRIDSMART Support, please prepare the following:

1. Diagnostic logs collected through the Device manager.
   Sent to GRIDSMART through the cloud or downloaded to your local machine by clicking the corresponding button in the Device Manger.



2. Export your site configuration AGS file and Client Logs.

There are several ways to get support -

1. Go to support.gridsmart.com, log in and click create ticket
2. Email GRIDSMART Support
3. Email your regional GRIDSMART Field Application Engineer.

Three ways to contact GRIDSMART Support:

Email: support@gridsmart.com
Web: support.gridsmart.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.

14.2 External hard Drive

A USB 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.

Please make sure to include timestamps for when the issue is occurring.

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.

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.

NOTICE: VNC will be removed in the next release. Remote desktop access, if enabled, will use RDP.
Remote Desktop Protocol (RDP) enables you to remotely access the GRIDSMART Client resident on the Processor as well as the Processor's Windows operating system. Contact Support for details on the captive user.

14.5 Upgrade a GRIDSMART Processor with an Update Stick

Note: This will only work if the USB sync is enabled in the Device Manager.

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.

GS2 Processor

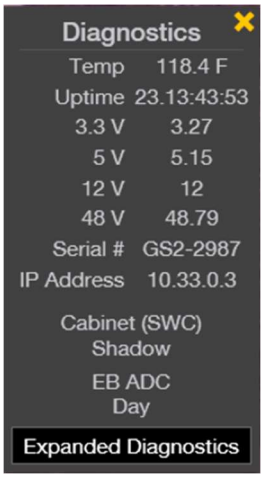
The front panel of the GS2 processor will display stages of the update via the Call Lights and the Phase lights. Once the Call Lights are all on and Phase Lights are solid green, the update is complete, and the USB stick can be removed.

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

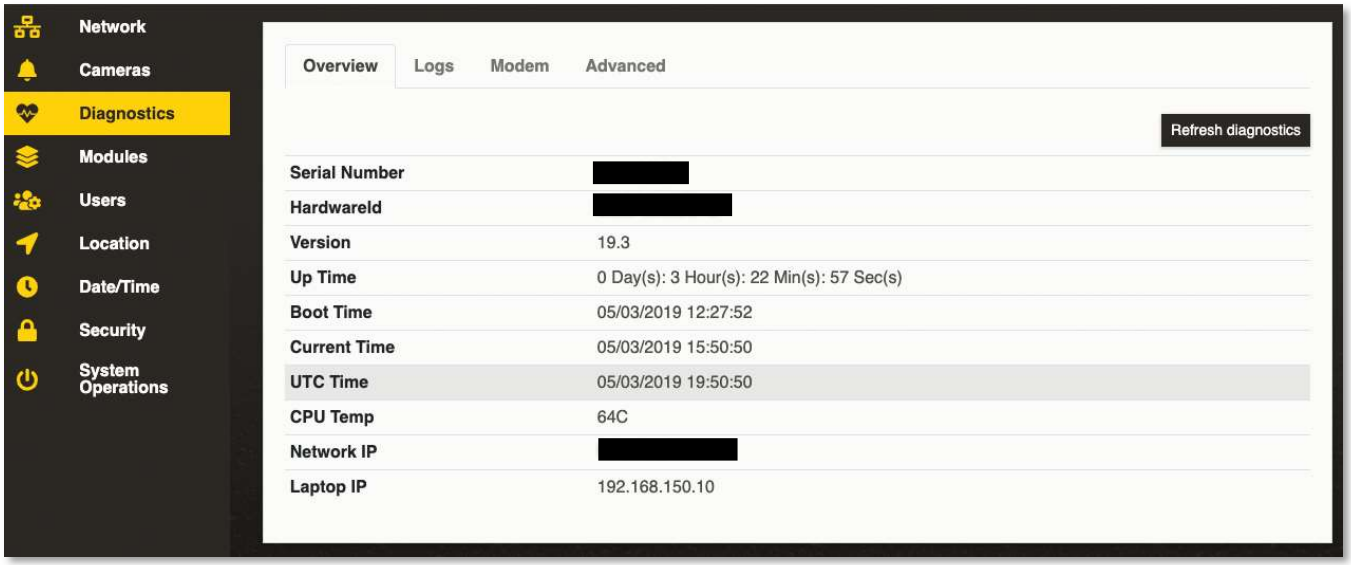
Click the Diagnostics icon on the Site Menu to see data for the current site.



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

Device manager 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. The software will flag any areas of concern with warning icons.



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/UC6Cyj0ORFNOAl3rno2u6_xQ

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

Support: https://support.gridsmart.com

Copyright © 2019 GRIDSMART, A Cubic Company.
10545 Hardin Valley Road, Knoxville, Tennessee 37932 USA
gridsmart.com

All rights reserved. GRIDSMART is a registered trademark of GRIDSMART , A Cubic Company. All other marks are property of their respective owners.

MADE IN THE USA

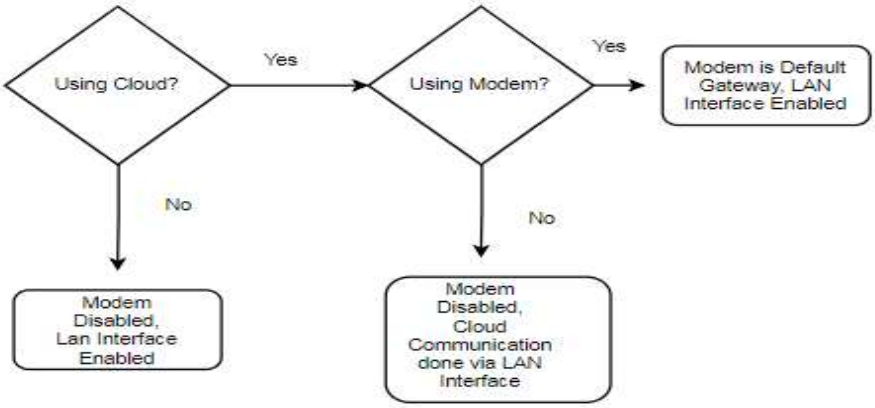
GS_2 Networking and Security

Introduction

The GRIDSMART GS_2 Processor is an enterprise appliance that has the flexibility to operate in a variety of network configurations. Starting in 19.3, the GRIDSMART Device Manager utility has been added to allow configuration of and management of the GS_2 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_2 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 100Mbs 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_2 processor on a private LAN that is optimized specifically for transmission of video to the GS_2 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_2 Processor with software release 19.3 or higher contains a feature rich set of security features including:

- **The GS_2 Device Manager is a new application for easy configuration of network and security settings, user 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_2 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.**

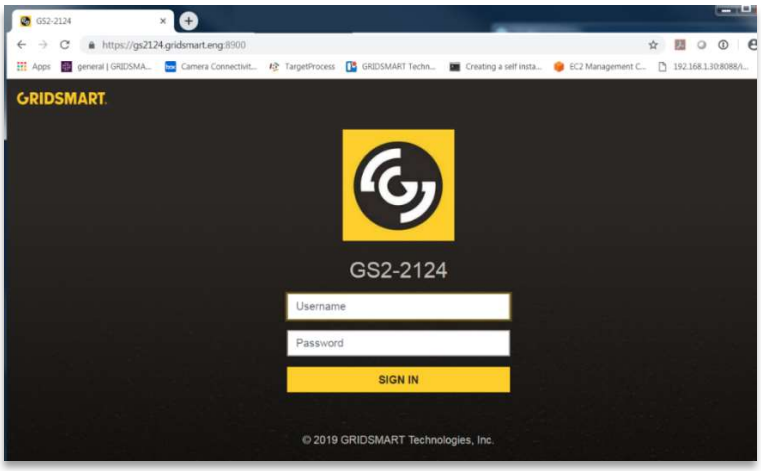
In addition to these features, the GS_2 process undergoes intense penetration testing during each software cycle to ensure vulnerabilities are minimized as much as possible.

2.0 GS$_2$ Device Manager

2.0.1 Connecting to Device Manager

The GS$_2$ 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$_2$ Device Manager open a browser and enter.

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$_2$ 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$_2$ Device Manager by clicking on the following icon.

2.0.2 Default Credentials

The following default accounts will be configured as defaults in 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.

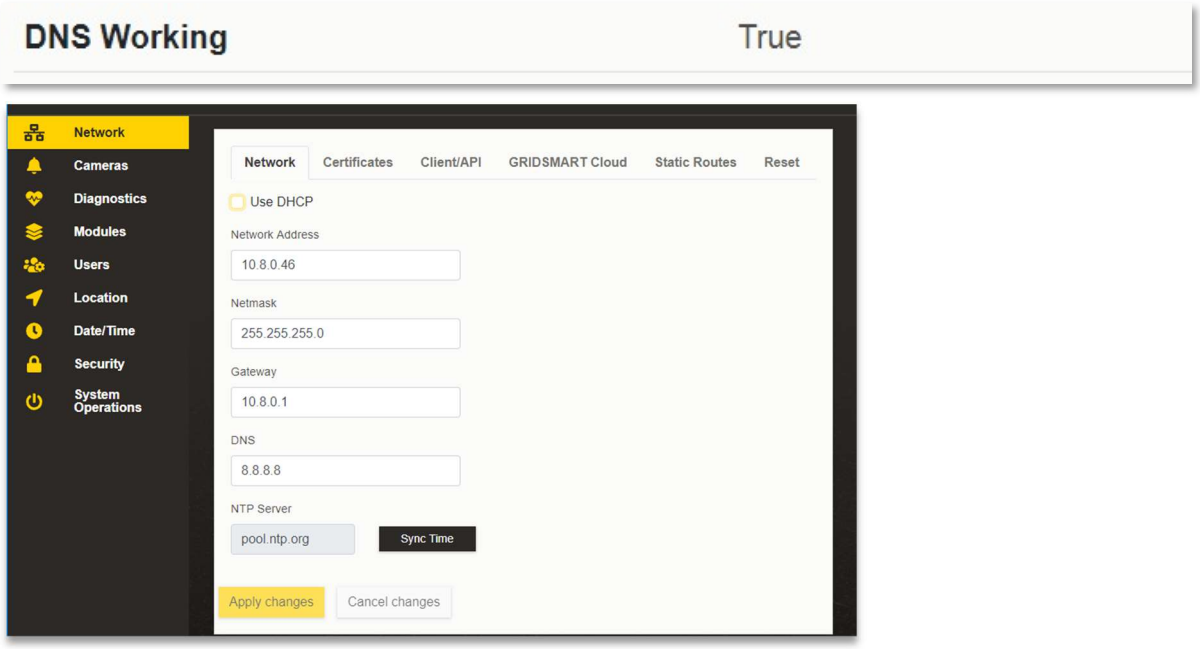
Permission Level	Username	Password	Capabilities using HTTP	Capabilities using HTTPS
Admin	admin	admin	Full access to GS2 Device Manager, Admin account disabled in client software.	Full access to GS2 Device Manager, Full access in client software.
Publish	publish	aldis#world9	Limited functionality in GS2 Device Manager, can publish to site from client	Limited functionality in GS2 Device Manager, can publish to site from client.
Read-only	aldis	aldis#world9	Limited functionality in GS2 Device Manager, cannot publish in client.	Limited functionality in GS2 Device Manager, cannot publish in client.

It is highly recommended that default credentials be changed immediately.
To comply with California legislation (California SB-327 Information privacy: connected devices) restricting the use of default passwords, the ability to access the GRIDSMART Client from the device desktop has been disabled by default. If this type of access is required, then this may be enabled using the Device Manager.

2.0.3 Network Settings

The GS2 processor supports a variety of network configurations including DHCP, static IPV4 addressing, and static routes. The GS2 processor does not support IPV6.
All Network settings for the processor **must be done in the GS2 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.

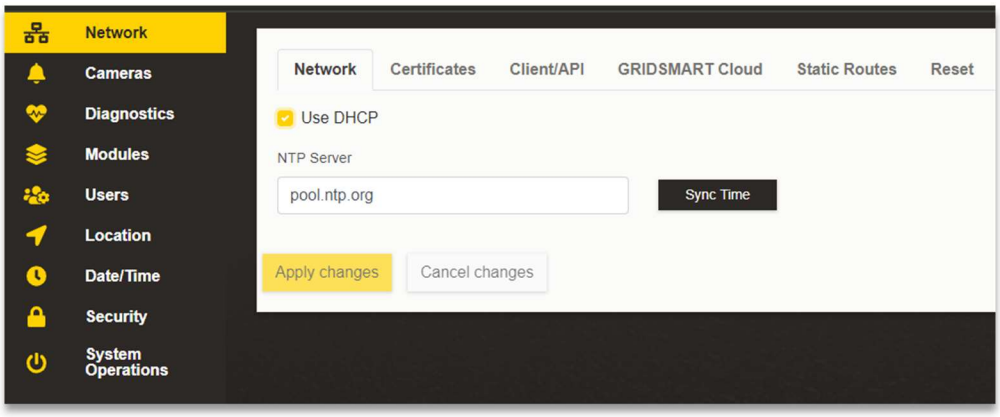
By default, the public interface is set to DHCP. In the GS2 Device Manager, go to 'Network' → 'Network' and deselect 'Use DHCP' to enter a static address. If you select a static address, you must make sure the DNS server is working. Once you have applied changes, you can verify DNS is working by checking the DNS status on the "Advanced Diagnostic Page".



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 GS2 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 GS2 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 GS2 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.



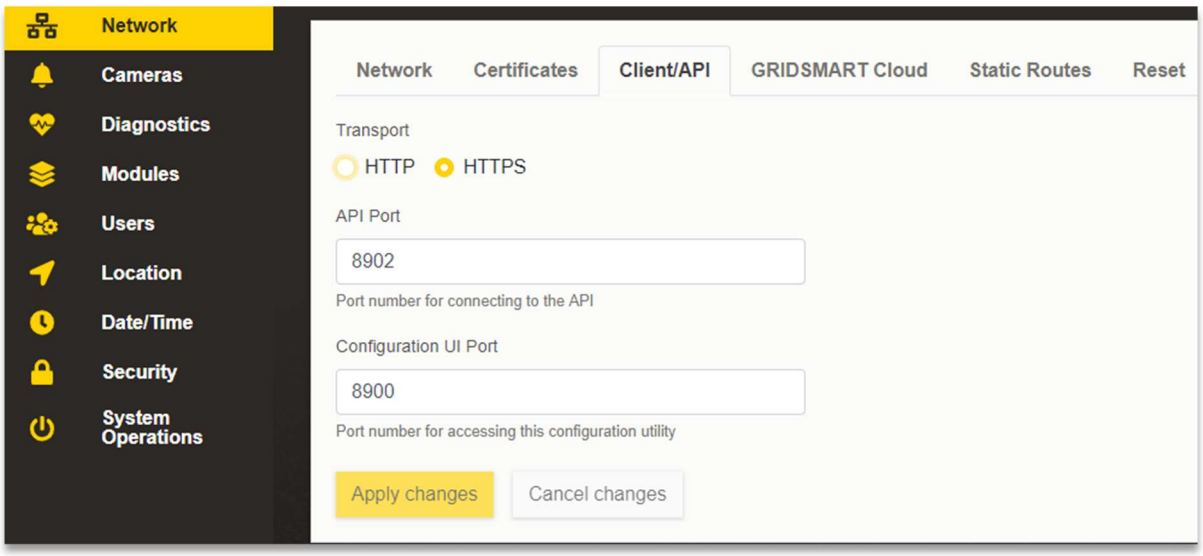
2.1 Upgrading from HTTP to HTTPS

It is highly recommended to upgrade any GS2 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.

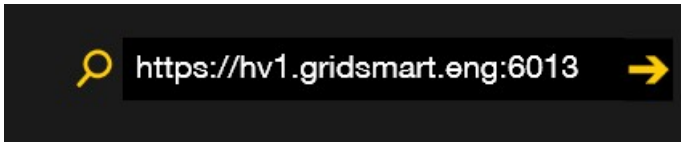
If you choose to enable HTTPS transport for the client traffic, a password is required for ALL processor operations. It is highly recommended you enable HTTPS transport for all production systems.

2.2 Client/API Settings

In the GS2 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 GS2 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.

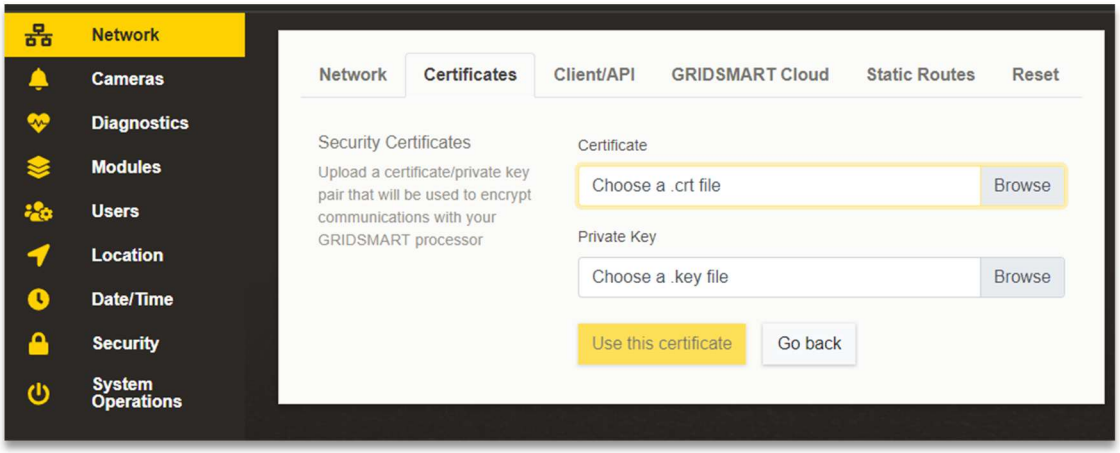
2.3 Importing a signed SSL Certificate

The GS2 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 GS2 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 GS2 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)

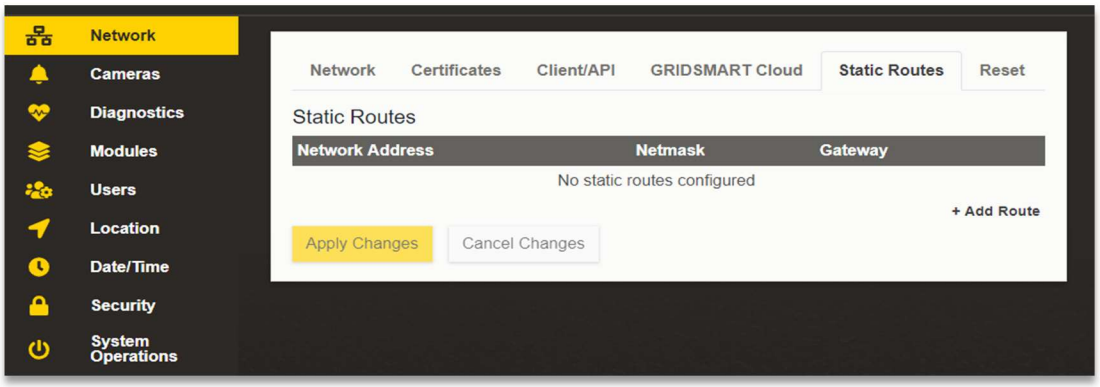
Standalone devices with no external connectivity can be setup with modem only access. In this mode, all traffic will be routed to the Cloud except for DNS, and NTP traffic.

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 GS2 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 GS2 Processor. Setting up static routes should be done by a qualified networking professional who has knowledge of the local network setup.

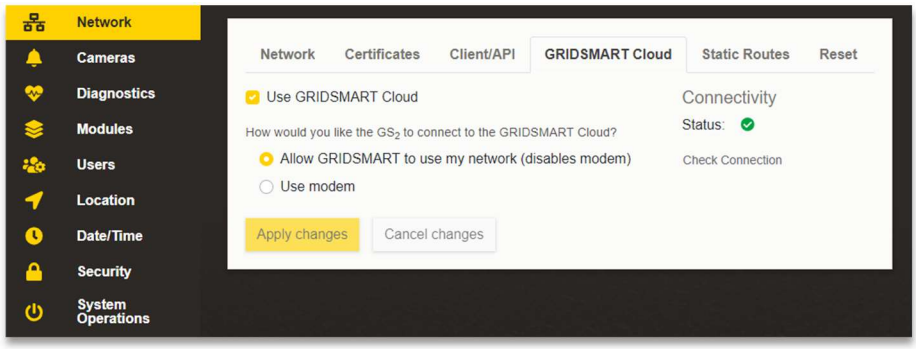


2.6 GRIDSMART Cloud

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_2 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.

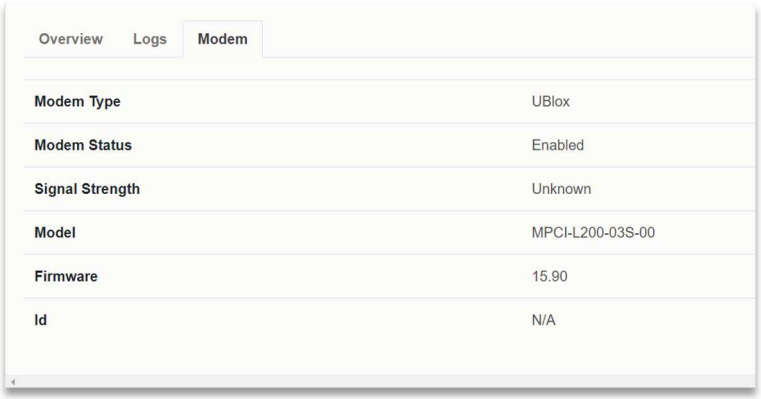
2.6.1 Using your network to connect to GRIDSMART Cloud

In the GRIDSMART Device Manager, go to 'Network' → 'GRISDMART Cloud' and select 'Allow GRIDSMART to use my network (disables modem)'

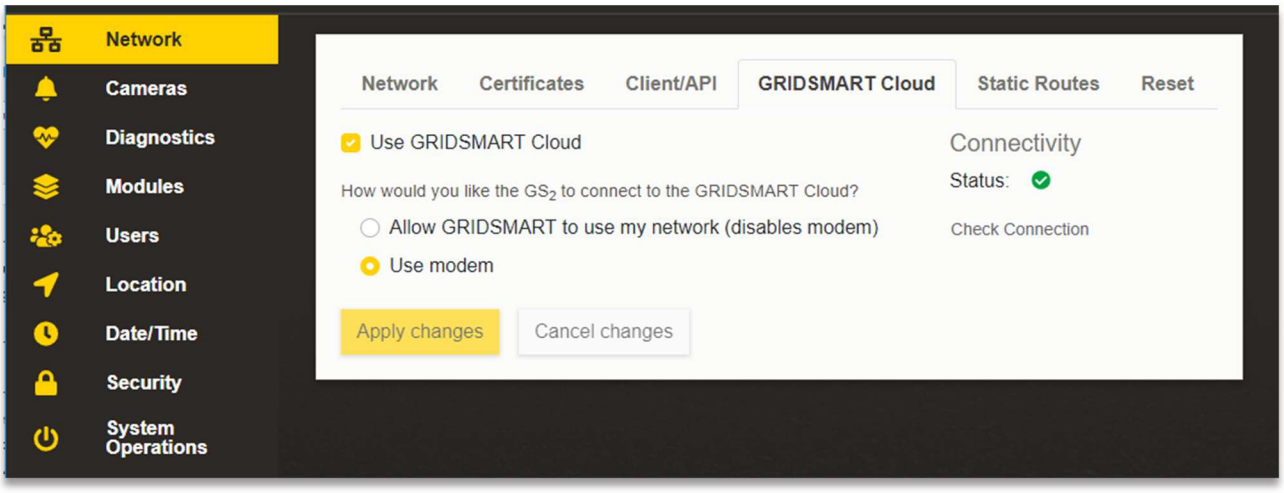


2.6.2 Using the modem to connect to GRIDSMART Cloud

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.



In the GRIDSMART Device Manager, go to 'Network' → 'GRISDMART 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.

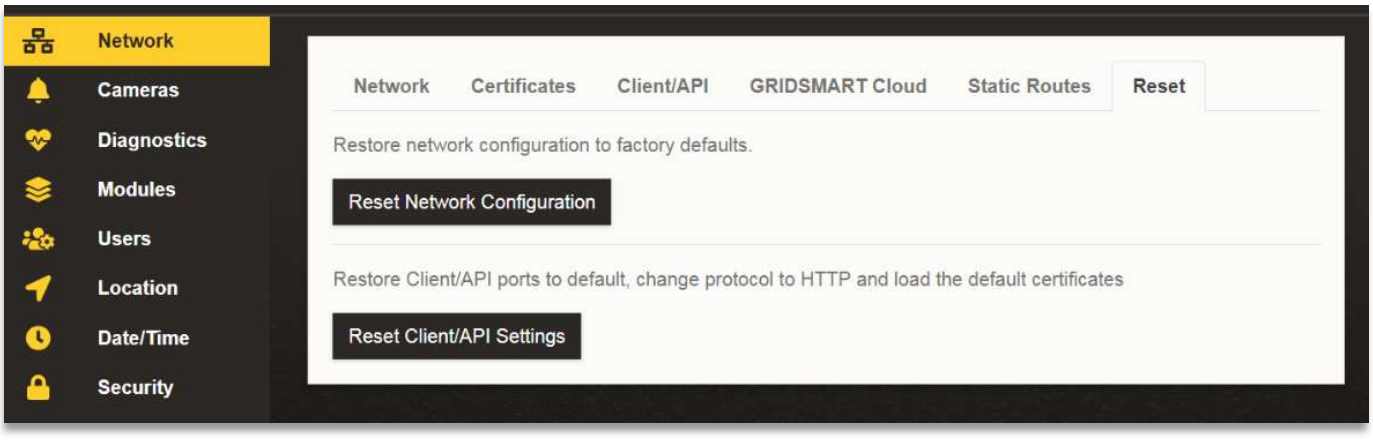


If you do not get a green check mark, check the following:

- 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 "DIAGNOSTICS OVERVIEW" page.
- More Advanced Diagnostics can be done on the "ADVANCED DIAGNOSTIC PAGE"

2.7 Restoring to Factory Default Network Settings:

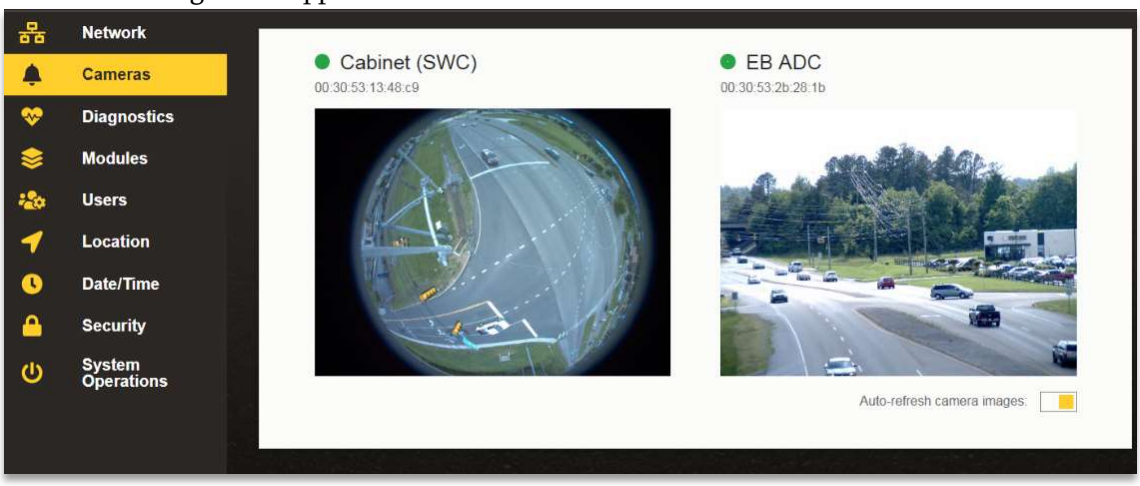
In the GRIDSMART Device Manager, go to 'Network' → Reset and select the appropriate option.



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.

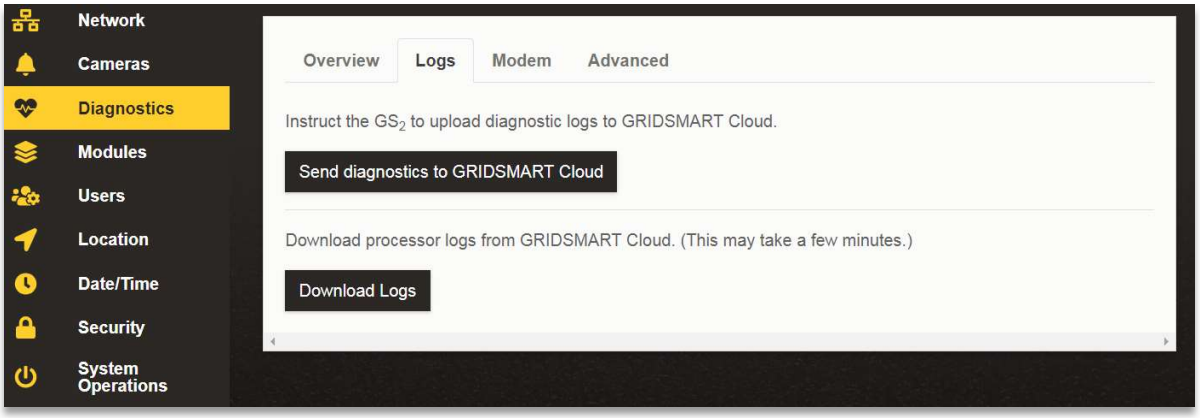
The camera images will appear as shown below when the cameras are online.



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

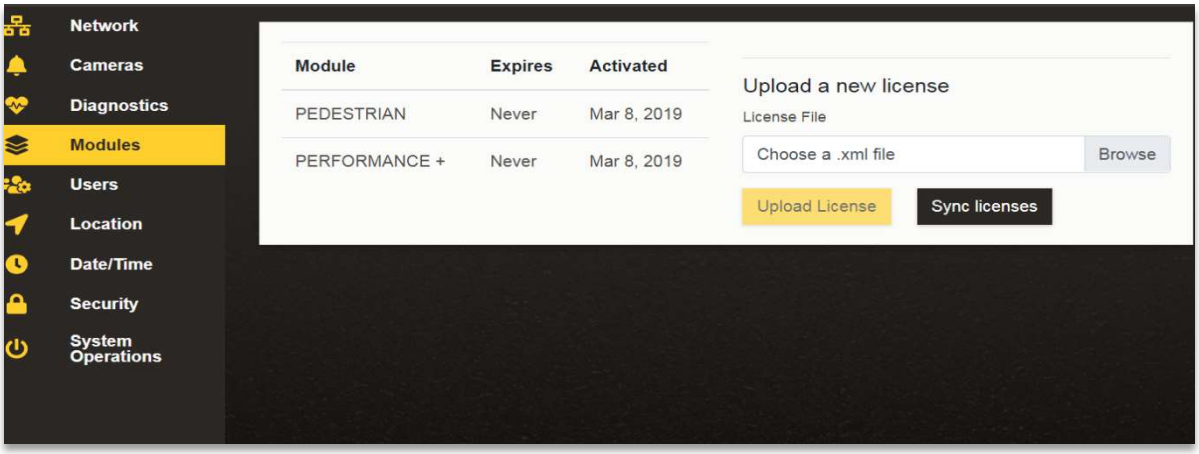
2.9 Diagnostics

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.



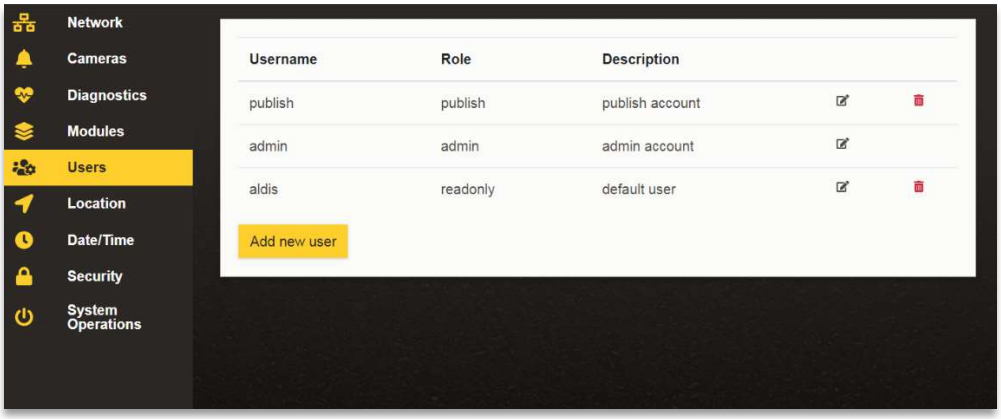
2.10 Modules

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



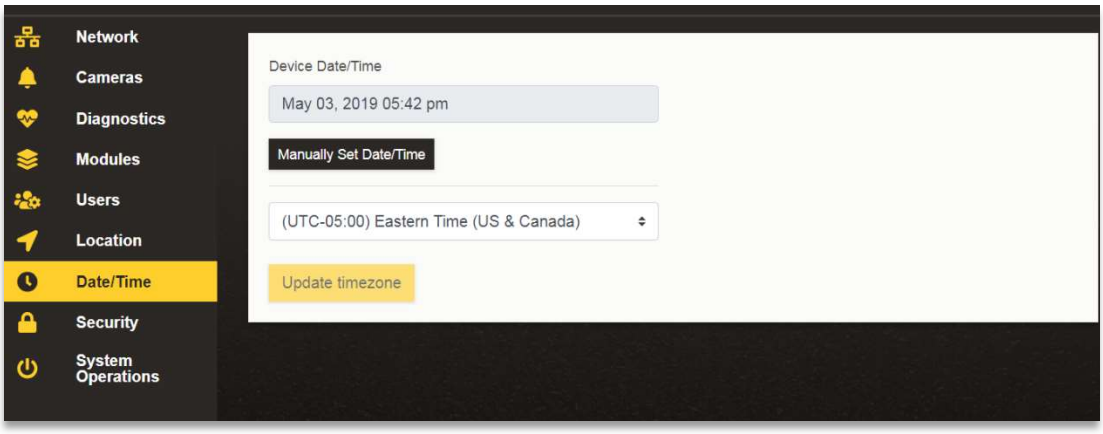
2.11 User Management

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. Starting in 19.10 users will be prompted to change the default passwords.

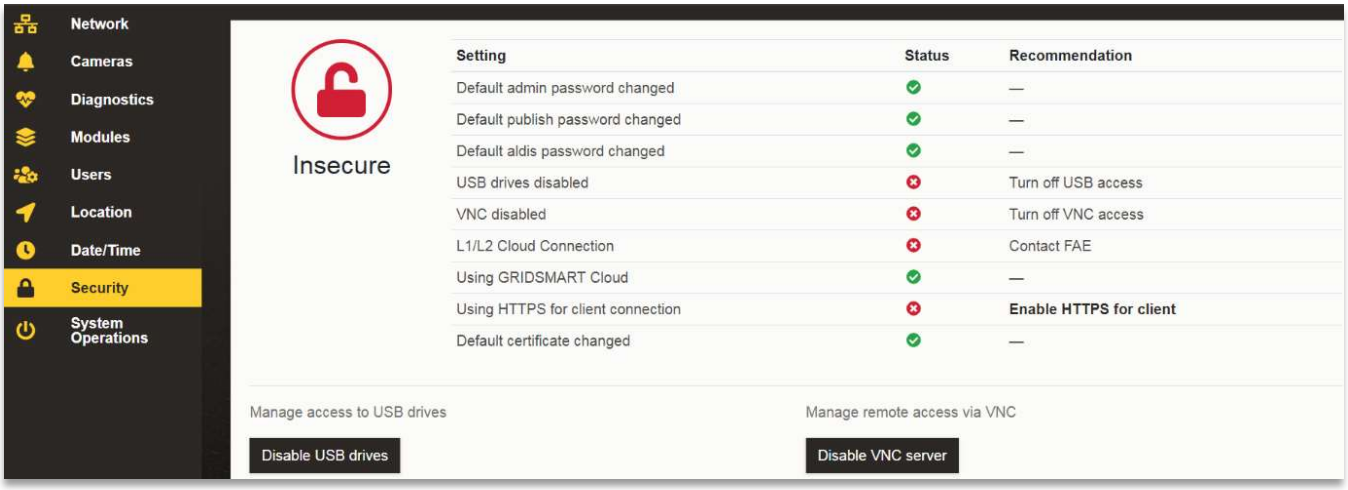
2.12 Manually setting the clock and Time Zone.



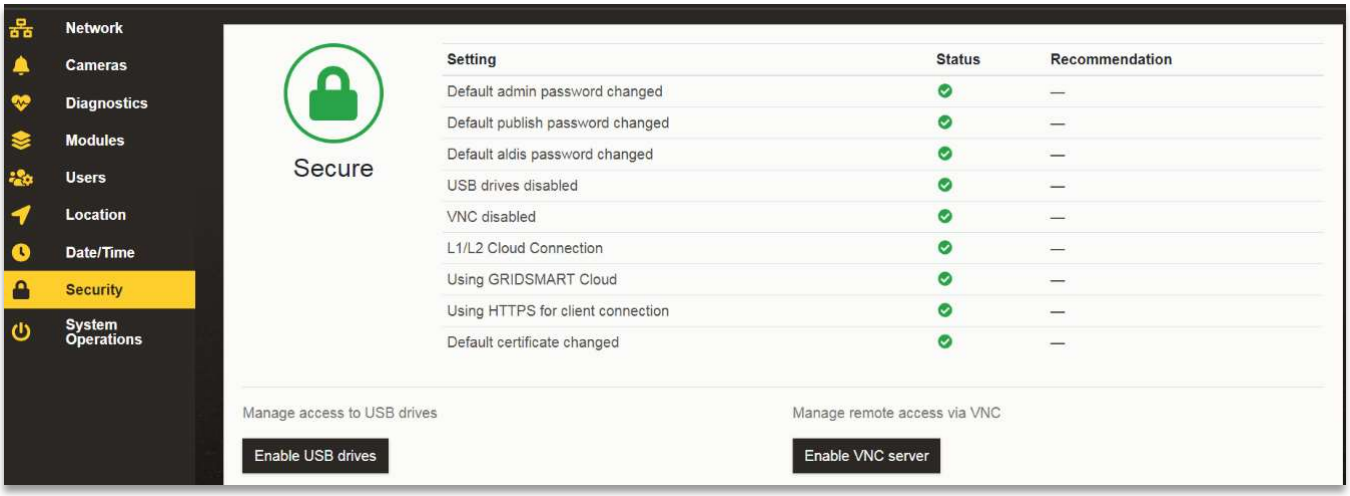
2.13 Security Self Audit

As a best practice each GS2 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.

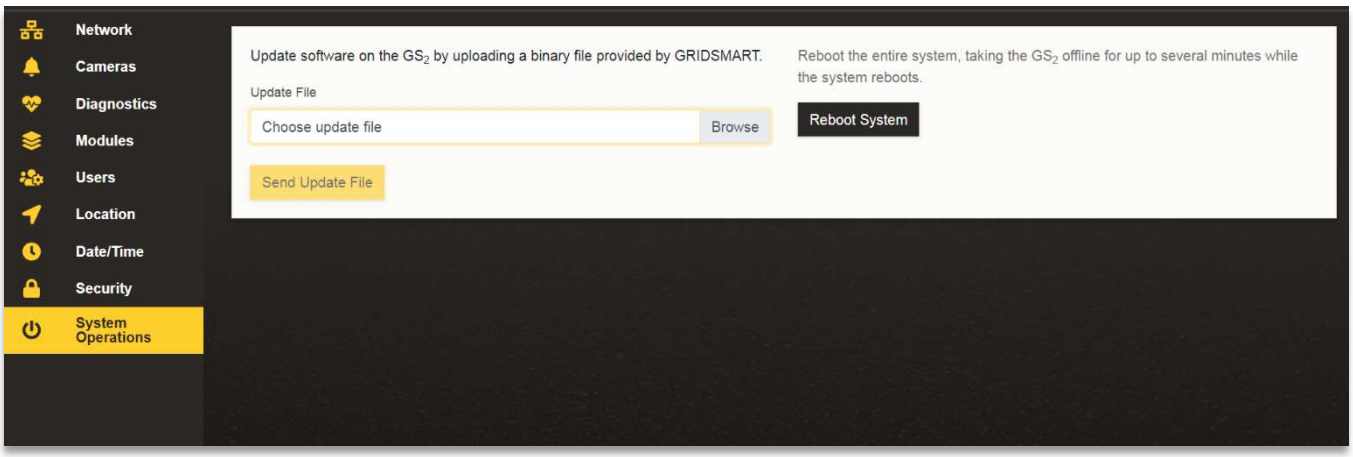


After these conditions were corrected the system indicates it has been hardened.



2.14 Remote Updates

Starting in 19.3 remote updates could be applied from the GS2 Device Manager. 19.10 will introduce a more user friendly remote update that will provide feedback to the user as the update progresses.



3.0 Other Considerations

3.1 Monitoring the GS2

The GS2 will not respond to ICMP echo requests, i.e. ping. Enabling this feature on the GS2 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 GS2 processor

3.2 Firewall Ports

The following ports should be reachable within the network for each GS2 processor:

Inbound Ports

5900 (Cannot be changed)
8900 (default) – GS2 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

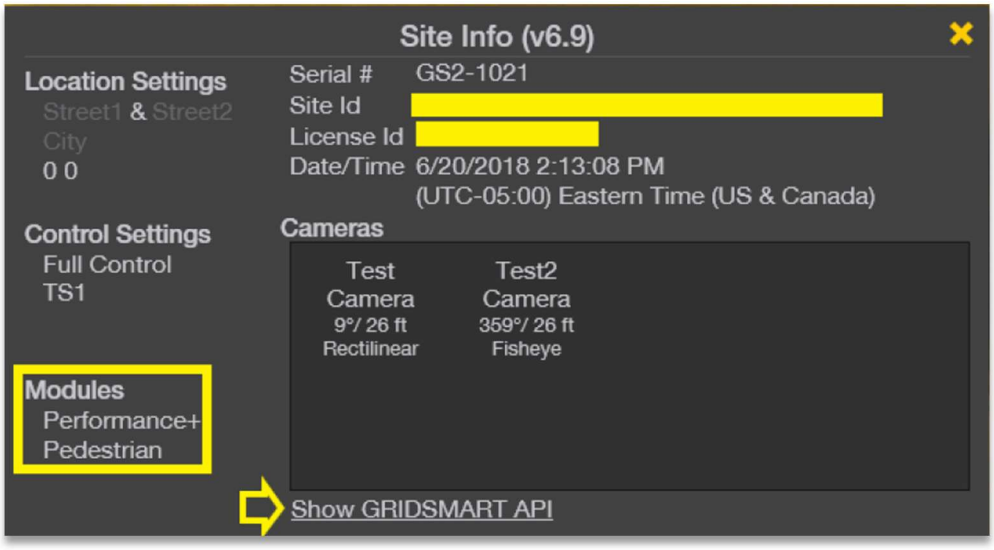
GRIDSMART supports RTSP streams from the GRIDSMART cameras using the STREAMS module included in the *Performance+ module*. Any other method used to stream video from the cameras other than using the GRIDSMART client or STREAMS module voids the system warranty and WILL BE DETECTED and Disabled in a future 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

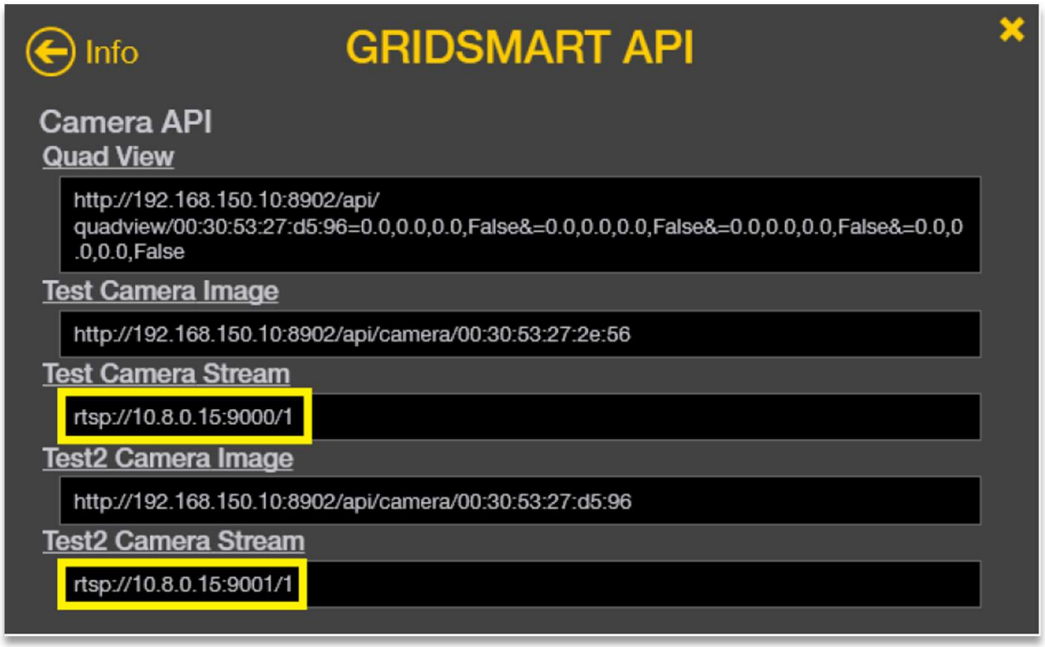
To setup STREAMS you must setup a static IP on the GS2 processor. As a Best Practice it is recommend to setup a static IP on the processor with a DHCP reservation. See section 2.0.3 on how to configure a static IP address. Additionally, any client connecting to the video stream must be able to reach the GS2 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.

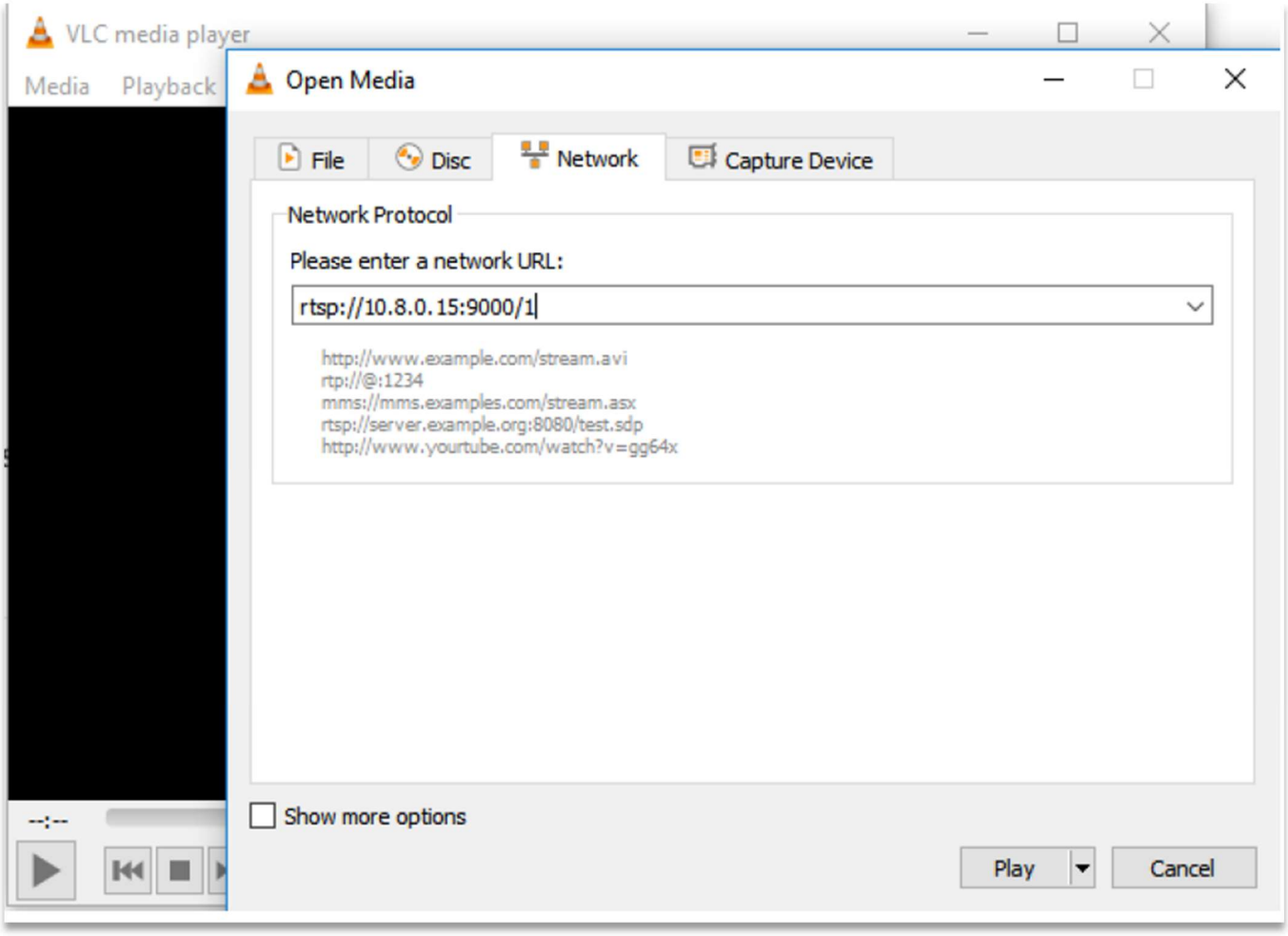


Click on **Show GRIDSMART API** to bring up API endpoints. Your screen should look similar to the following screenshot, but the IP address should reflect what you set as your static IP.



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).



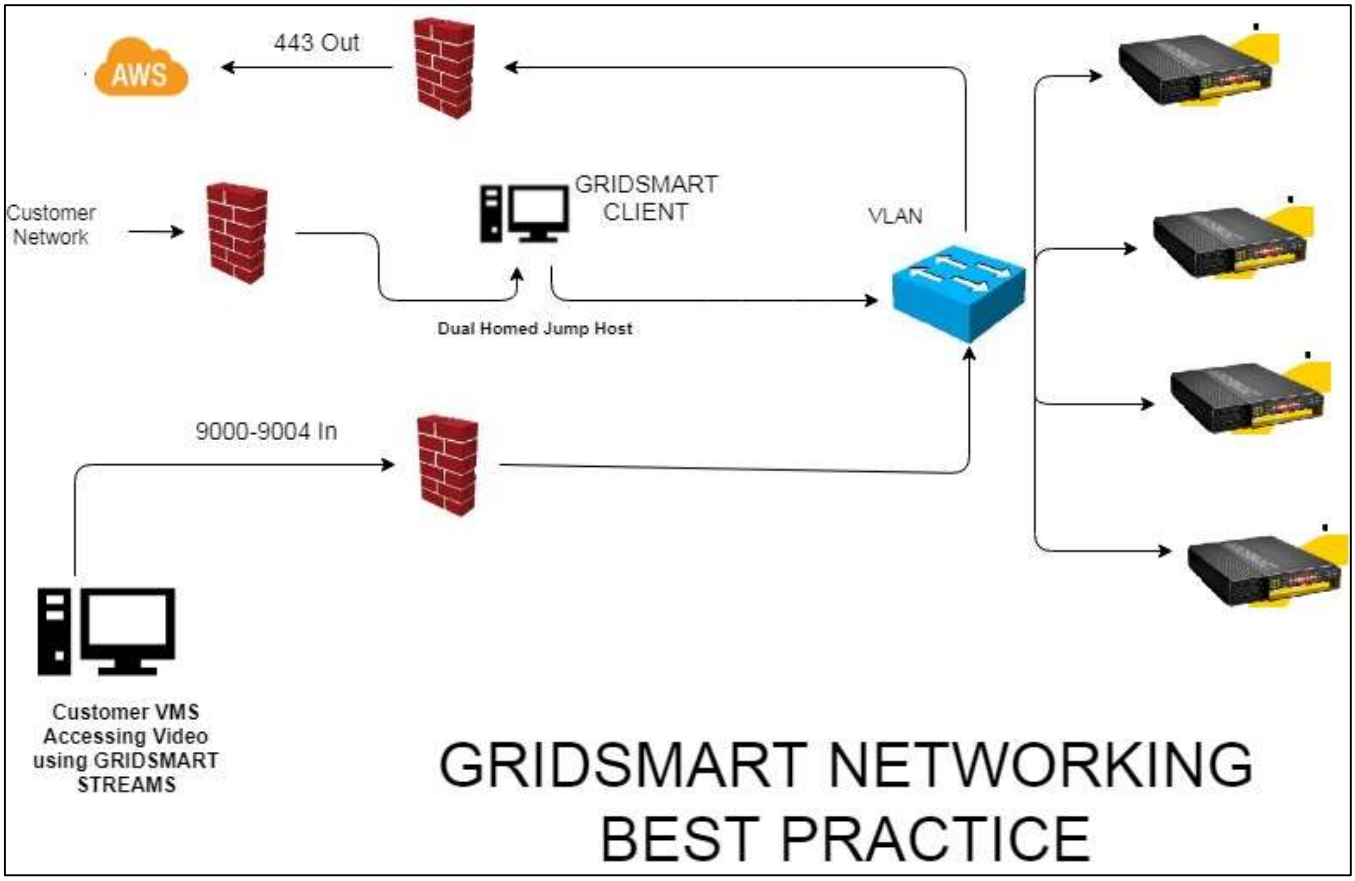
3.7 Private LAN connection (Laptop Port)

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 GS2 processors on a separate VLAN with a jump host client used to directly access the GS2 processors. It is not recommended to use the GRIDSMART client for monitoring video. For video streaming and monitoring use the Streams Module.

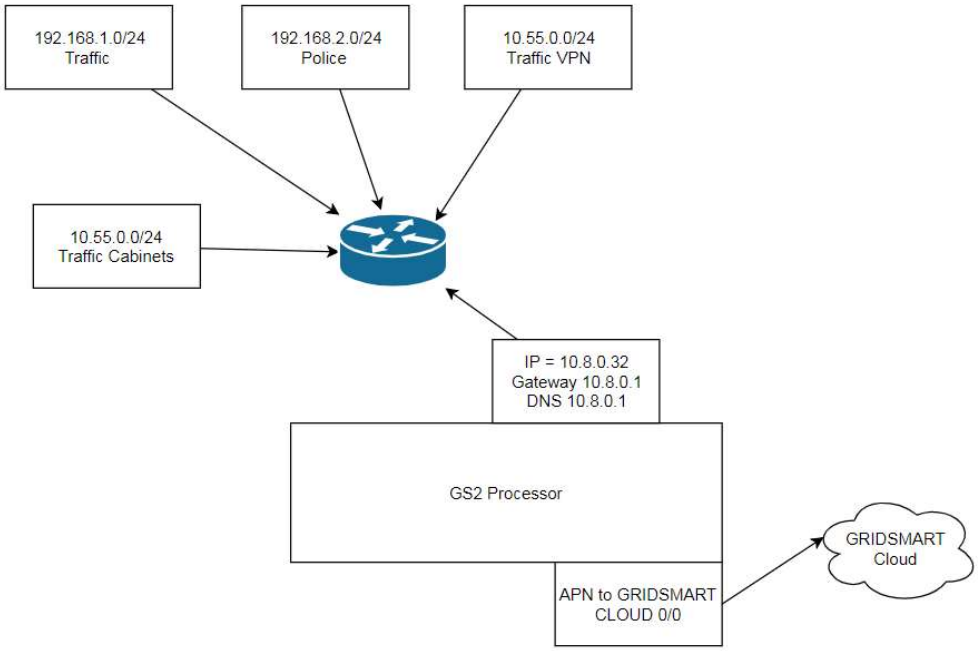
DO NOT CONNECT a GS2 Processor directly to the Internet on a public facing IP address.



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: 10.8.0.0/24 (Router Address 10.8.0.1)

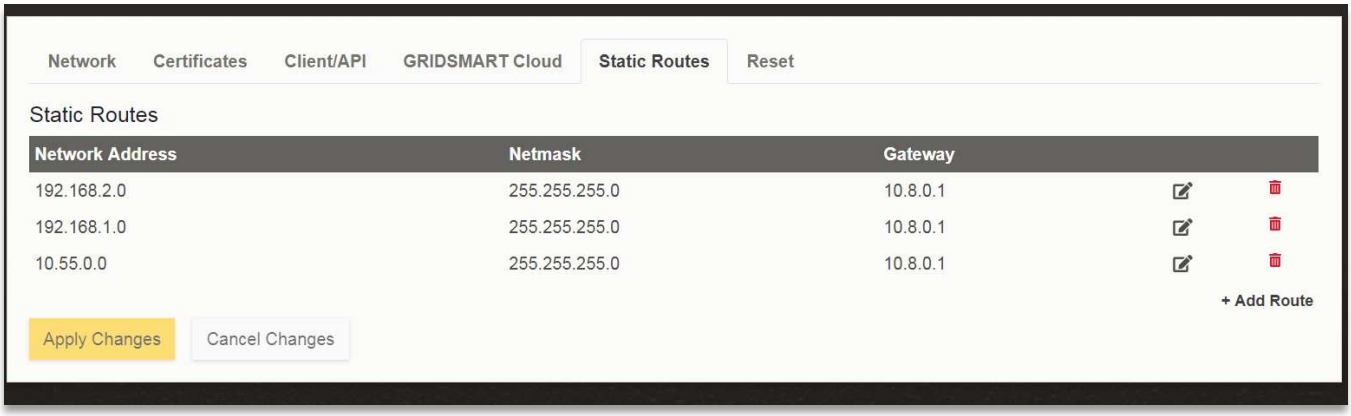


The connection to the traffic cabinet is done via 900 MHz radios running at 10Mbps.
The police department wishes to stream video to their operations center. The traffic department would like to upload configuration changes and send alerts using the GRIDSMART cloud. They have decided the modem can be used for cloud communications to save bandwidth instead of using the limited bandwidth of the radio. Additionally, the traffic department wants to access the GS2 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 GS2 and the default route will be the modem, two static routes are needed on the GS2 processor to allow traffic to the police and traffic department's network.

The Cloud configuration would be set as follows:

The static Routes would be setup as follows:



With this configuration, cloud traffic will be routed via the modem and all the stakeholders involved will have connectivity to the GS2 processor.

FAQs

Q: Can antivirus/firewall software be installed on the GS2 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 GS2 is an embedded appliance. We cannot guarantee the GS2 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 19.3, use the GRIDSMART Device Manager to push updates to a networked GS2 Processor. **Note, the GS2 MUST be running 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.
Note- VNC will be replaced by Remote Desktop Protocol (RDP) in a future release.

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 you 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 GS2 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.