VISIX V-Series All-in-One Cameras

User Manual

VIGIL v8.8 All-In-One Software

This manual applies to the following camera models:

Camera Type	Model
2 Megapixel Exterior Bullet Camera	VX-2A-B-IWD
2 Megapixel Exterior Bullet Camera w/Remote Focus	VX-2A-B-RIWD
2 Megapixel Exterior Dome Camera	VX-2AD3-IWD
2 Megapixel Interior Mini Dome Camera	VX-2A-IMD-X
VERA 36° Field-of-Vision Thermal Bullet Camera	VX-VT-36

Thank you for purchasing our product. If there are any questions, or requests, please do not hesitate to contact your sales representative or a 3xLOGIC support representative.

This manual may contain technical inaccuracies or printing errors. Examples are based on **VIGIL Software Version 8.80.0008** running over firmware **1.10.7.3**. The camera's UI appearance may appear differently depending on your current VIGIL software and camera firmware versions.

The content of this guide is subject to change without notice. The manual will be amended if there are any hardware updates or changes.

Regulatory Information

FCC Information

FCC compliance: This equipment has been tested and found to comply with the limits for a digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Conditions

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

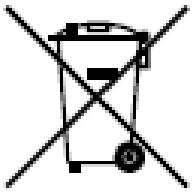
1). This device may not cause harmful interference.

2). This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the Low Voltage Directive 2006/95/EC, the EMC Directive 2004/108/EC, the RoHS Directive 2011/65/EU.

2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info.



2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info

Safety Instruction

These instructions are intended to ensure that the user can use the product correctly to avoid danger or property loss.

The precaution measure is divided into 'Warnings' and 'Cautions':

WARNING: Serious injury or death may be caused if any of these warnings are neglected.

CAUTION: Injury or equipment damage may be caused if any of these cautions are neglected.

WARNING:

- Please adopt a power adapter which can meet the safety extra low voltage (SELV) standard when possible, and source with 12 VDC or 24 VAC (depending on models) according to the IEC60950-1 and Limited Power Source standard. Before applying power to the camera, check the power source to ensure that it is within the specifications
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the camera yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)
- To reduce the risk of fire or electrical shock, do not expose this product to rain or moisture unless it is an exterior/weatherproof model. Please do not install the camera in a place exposed to direct sunlight. Do not operate the camera in environments beyond the specified temperature. Refer to the VISIX V-Series All-in-One Hardware and Installation manual for environmental conditions and limitations of your particular camera model.
- This installation should be made by a qualified service person and should conform to all the local codes.
- Please install blackout equipment into the power supply circuit to prevent footage and data loss.
- Please make sure that the ceiling can support more than 50(N) Newtons of gravity if the camera is fixed to the ceiling.

CAUTION:

- Make sure the power supply voltage is correct before using the camera.
- Do not drop the camera or subject it to physical shock.
- Do not touch sensor modules with fingers. If cleaning is necessary, use a clean cloth with a bit of ethanol and wipe it gently. If the camera will not be used for an extended period of time, put on the lens cap to protect the sensor from dirt.
- Do not aim the camera lens at the strong light such as sun or incandescent lamp. The strong light can cause fatal damage to the camera.
- The sensor may be burned out by a laser beam, so when any laser equipment is being used, make sure that the surface of the sensor not be exposed to the laser beam.
- Do not place the camera in extremely hot, cold temperatures (the operating temperature should be between -30°C ~ 60°C, or -40°C ~ 60°C if the camera model has an "H" in its suffix), dusty or damp environment, and do not expose it to high electromagnetic radiation.
- To avoid heat accumulation, good ventilation is required for a proper operating environment.

- Keep the camera away from water and any liquid.
- While shipping, the camera should be packed in its original packing.
- Improper use or replacement of the battery may result in hazard of explosion. Please use the manufacturer recommended battery type.

NOTE:

For cameras that support IR, you are required to pay attention to the following precautions to prevent IR reflection.

- Dust or grease on the dome cover will cause IR reflection. Please do not remove the dome cover film until the installation is finished. If there is dust or grease on the dome cover, clean the dome cover with clean soft cloth and isopropyl alcohol.
- Make certain the installation location does not have reflective surfaces of objects too close to the camera. The IR light from the camera may reflect back into the lens causing reflection.
- The foam ring around the lens must be seated flush against the inner surface of the bubble to isolate the lens from the IR LEDS. Fasten the dome cover to camera body so that the foam ring and the dome cover are attached seamlessly.

Table of Contents

1 VISIX V-Series All-in One Cameras

1.1 Introduction

VISIX V-Series All-in-One, edge-based IP cameras are powerful, full-featured, VMS and advanced analytic capable. VISIX V-Series cameras provide a complete surveillance solution for the small and medium sized businesses and for unique single-point applications.

These new cameras' embedded analytics use algorithms that automatically self-adjust, so the user can concentrate on the all-important detection rules. This feature greatly simplifies the analytical process, requiring only a few mouse clicks to configure a detection rule. Such advanced analytics enable object classification, direction determination, people counting, and dwell times meaning the camera's intelligence becomes valuable and can be leveraged across the organization, not just for security and loss-prevention.

When enabled, the embedded VIGIL Server software allows these cameras to be run as stand-alone devices, recording video to the onboard memory card. This makes these All-in-One cameras compatible with 3xLOGIC's existing software suite including VIGIL Client, VIGIL VCM, VIGIL View Lite II, and VIGIL Cloud applications. Simple plug-and-play installation enables camera access using a standard web browser (Microsoft IE/Edge required for ActiveX Control), VIGIL Client, or through a mobile device or tablet utilizing the easy-to-use QR code quick setup.

Several models exist to best suit any number of environments, however operation of the V-Series All-in-One software (web) interface remains uniform across all models. Details on identifying and connecting to a camera on your network, accessing a camera's web interface, settings, video and details regarding the camera's web interface itself are contained within this manual.

2 Identifying the Camera on your Network

2.1 Identifying Camera IP Address

To begin viewing video or configuring a camera's network settings from the camera's web/browser interface, the user must first identify the device's IP address. The default IP address of the camera is **192.168.XXX.XXX.** The default subnet mask is **255.255.0.0.**

On simple, private networks, a user can manually identify the IP address of the camera by converting the camera's MAC address hex values, however, the alternative method, which is recommended by 3xLOGIC, is to use the 3xLOGIC (VSX-IP) Camera Setup Utility. The utility makes detection and configuration of VISIX camera's in any network environment simple and easy, regardless of network complexity.

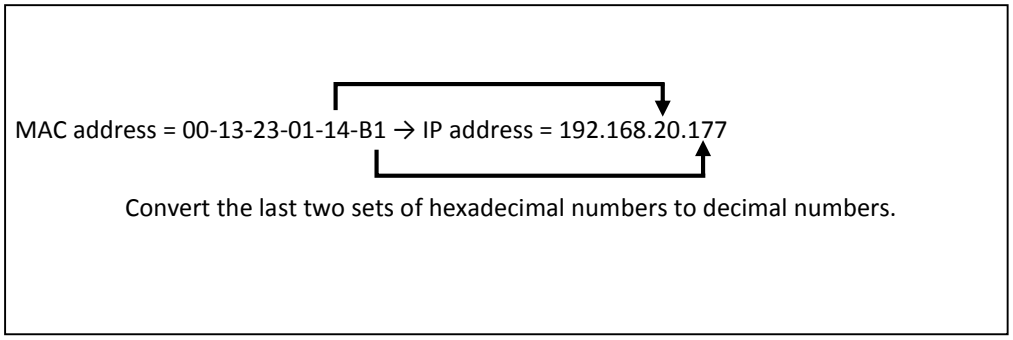
Please install the camera before continuing. Neither of the below methods require an external internet connection, however, the camera and the PC being used to communicate with it must reside on the same network.

MANUALLY IDENTIFY CAMERA IP ADDRESS (MAC ADDRESS HEX CONVERSION)

Users can access the camera's web interface and settings using a device's default IP address: In case of generic private network environment where IP address **192.168.XXX.XXX** are used, the following procedure can be used to identify a device's IP address.

Steps:

1). Convert the device's MAC address to the IP address. Refer to **Section 8:** Hexadecimal-Decimal Conversion Chart at the end of the manual (the MAC address of the device is written on the label affixed to the side or bottom of the device).



2). Start the Microsoft® Internet Explorer/Edge web browser and enter the address of the device.

3). Web streaming and device configurations are supported through ActiveX program. When the ActiveX installation window appears, authorize and install the ActiveX.

AUTOMATICALLY IDENTIFY CAMERA IP ADDRESS WITH 3XLOGIC CAMERA SETUP UTILITY

Using the 3xLOGIC Camera (VSX-IP) Setup Utility is recommended for any network environment as it will find all VISIX cameras across multiple subnet masks, utilizing mDNS search discovery. Camera information such as IP Address, Subnet Mask and Gateway Settings will be displayed and can be edited from this utility. To search for a device, launch the utility (VSXIPUtility.exe):

Steps:

1). Click on **Detect Online Devices/ Change IP Address** to proceed to the Online Devices window.

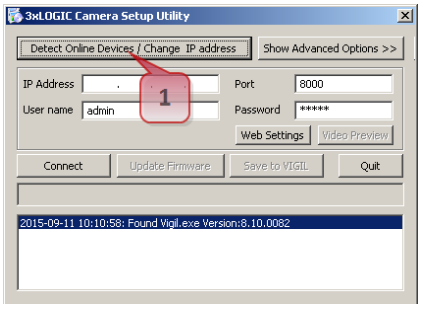


Figure 2-1: Detecting Online Devices

After clicking **Detect Online Devices/ Change IP Address** on the main page you will be taken to the Online Devices window. A list of all VISIX devices discovered on your network will be visible.

2). To select a device, click on the desired device in the generated menu under the **Select Online Devices** area.

3). To change an IP address for a selected VISIX camera in the **Detect Online Devices** window, select the desired camera, click on the **Change IP Address** button. The fields under the **Configure IP Address** area will un-grey to allow for manual editing of camera IP addresses as well as other settings.

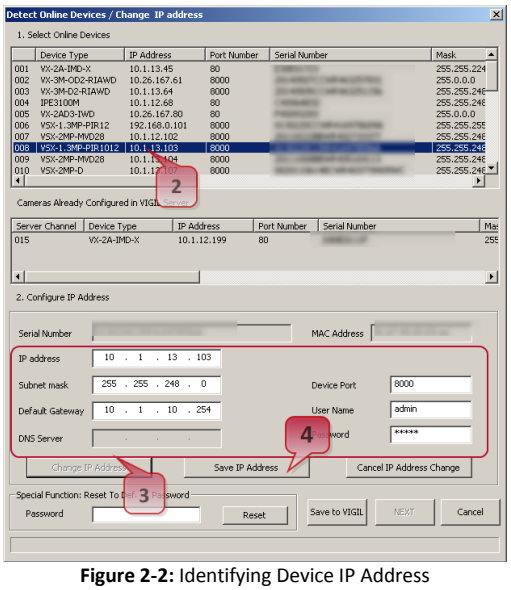


Figure 2-2: Identifying Device IP Address

4). When you have finished editing the settings, click **Save IP Address** to save new changes.

5). Start the Microsoft® Edge/Internet Explorer web browser and enter the address of the device.

6). Web streaming and device configurations are supported through ActiveX program. When the ActiveX installation window appears, authorize and install the ActiveX.

VIDEO PREVIEW USING THE 3XLOGIC CAMERA SETUP UTILITY

Amongst its many functions, the 3xLOGIC Camera Setup Utility can provide the user with a video preview from a currently selected device. This can be used to quickly confirm the correct camera has been located, and that it is successfully streaming/recording footage. To begin:

Steps:

1). Click **Detect Online Devices.**

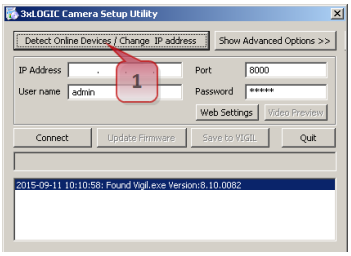


Figure 2-3: Video Preview - Detecting Online Devices

2). Double-click the camera you wish to video preview in the list of discovered devices.

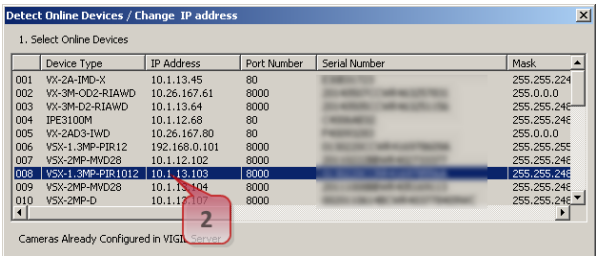


Figure 2-4: Video Preview – Selecting Device

3). The 3xLOGIC Camera Setup Utility main page will now load with the chosen device selected. Click **Video Preview.**

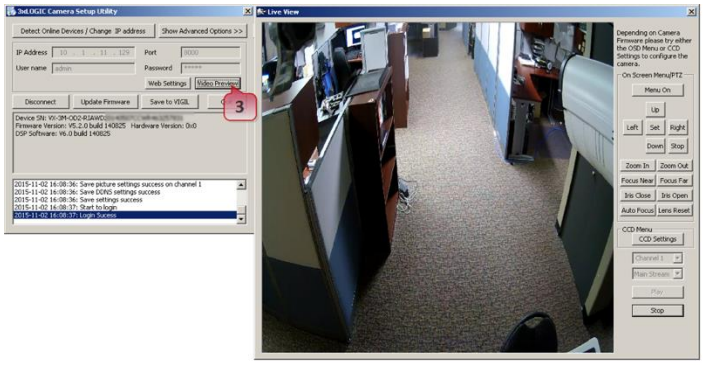


Figure 2-5: Video Preview

NOTE:
Whether directly accessing streaming video through the camera web interface or taking steps through 3xLOGIC Camera Setup Utility, ActiveX must be installed for Microsoft® Internet Explorer to have the complete configuration privileges.

3 Accessing the Camera Browser Interface

Once the device's proper IP address has been identified, type the IP into a web browser URL bar (Microsoft Internet Explorer/Edge required for ActiveX control) to view the camera's browser interface and video stream images, configure image settings, configure VCA rules, etc...

3.1 Logging In to the Camera

Upon entering the device IP address into your browser URL bar, a login prompt similar to the example below will deploy (appearance will vary depending on PC operating system, browser version, etc…). The default username and password is **admin/12345.**

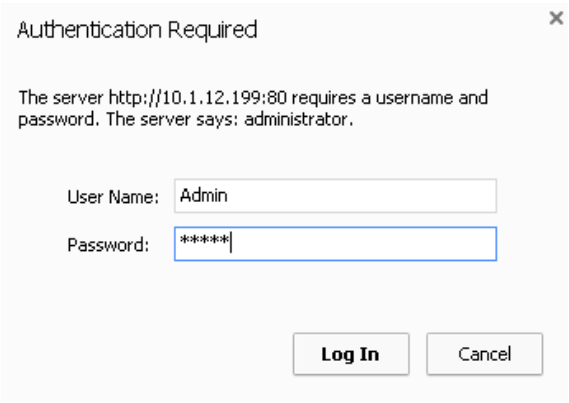


Figure 3-1: Camera Login

After successfully clearing the first login attempt, a connection will be made between your system and the camera. A second login sequence will be required to access the camera's VIGIL web interface. If this is the first time initializing access to the camera on your current PC system, an ActiveX control installation pop up may deploy. ActiveX is required for viewing video in the browser.

ACTIVEX INSTALLATION

Steps:

1). When the browser asks to install the AxUMF software, click **Install** to proceed.

2). When the setup installation pop-up window appears, click **Install** to proceed with rest of installation.

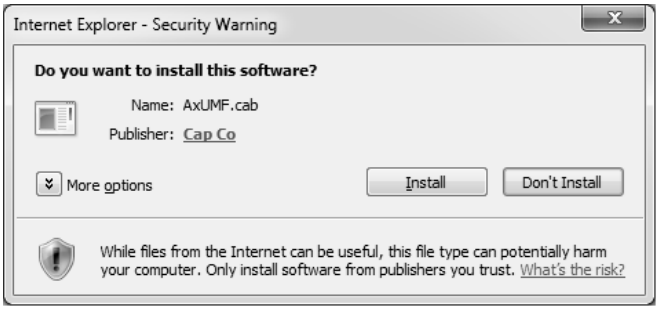


Figure 3-2: ActiveX (AxUMF.cab) Installation

NOTE:

Depending on system OS and Internet Explorer version, installation experience may differ from one another. Figures described above are from Windows 7, Internet Explorer 9 environment.

Upon completion, the camera's web/browser interface will be fully accessible for video viewing and settings configuration.

4 Quick Start

Contained within this section are quick start tips to help a user familiarize themselves with the basic operation of their VISIX V-Series All-in-One Camera. Please be sure to locate the camera on your network and access the camera's browser interface using the instruction in **Section 2:** Identifying the Camera on your Network and **Section 3:** Accessing the Camera Browser Interface before continuing through this section.

4.1 View Live and Playback (Recorded) Video

VIEWING LIVE VIDEO

After logging into the camera's browser interface, a user may view live video from the camera. To view live video:

Steps:

1). Select the **Live** tab at the top-left of the camera's browser interface.

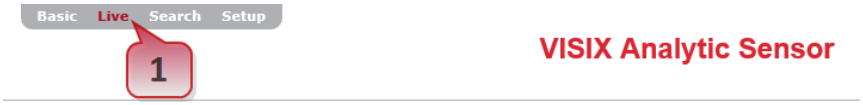


Figure 4-1: Opening the Live Tab

2). This will open the camera's **Live Viewer**.

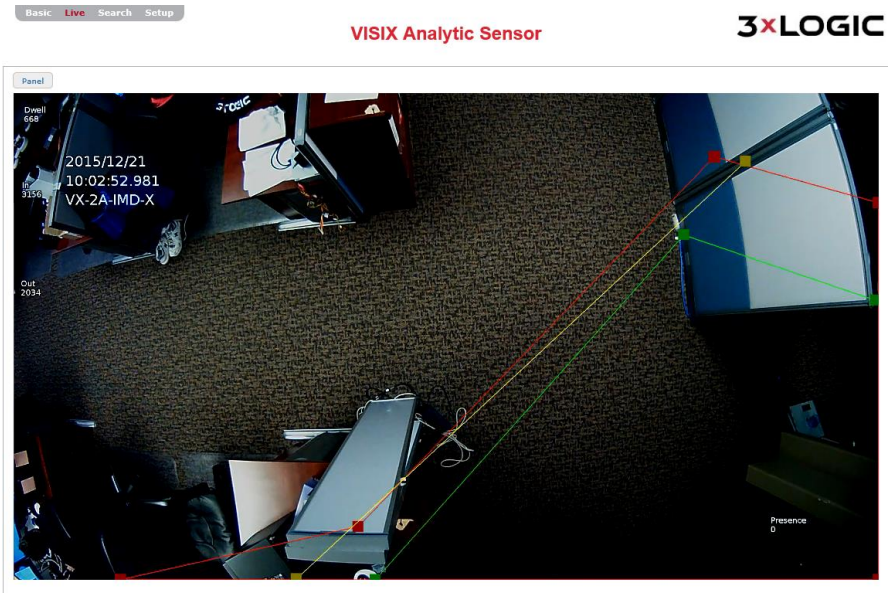


Figure 4-2: Live Tab

For more information on the Live tab user interface and options, see **Section 6.1: Live Tab.**

VIEWING PLAYBACK VIDEO

After logging into the camera's browser interface, a user may view playback video recorded by the camera.

Steps:

1). To view playback video, select the **Search** tab.

Figure 4-3: Opening the Search (Playback) Tab

2). This will open the camera's **Playback Search** window.

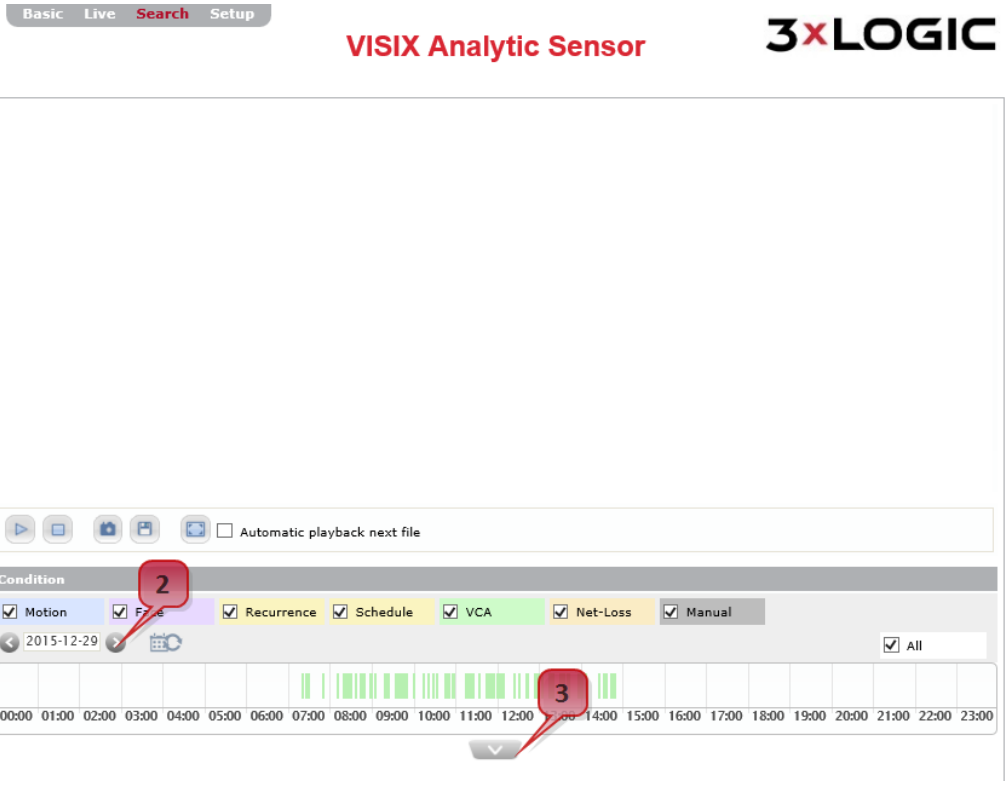


Figure 4-3: Search (Playback) Tab

3). Set the day (search time range is automatically set to the current day).

4). Click the context arrow to reveal all search results for the selected day. All search **Conditions** will be enabled by default. All available files, with an included thumbnail and file information, will be visible.

Figure 4-4: Search Result Thumbnails

5). Click the next to a file (thumbnail) to load and playback the video in the **Playback Viewer.**

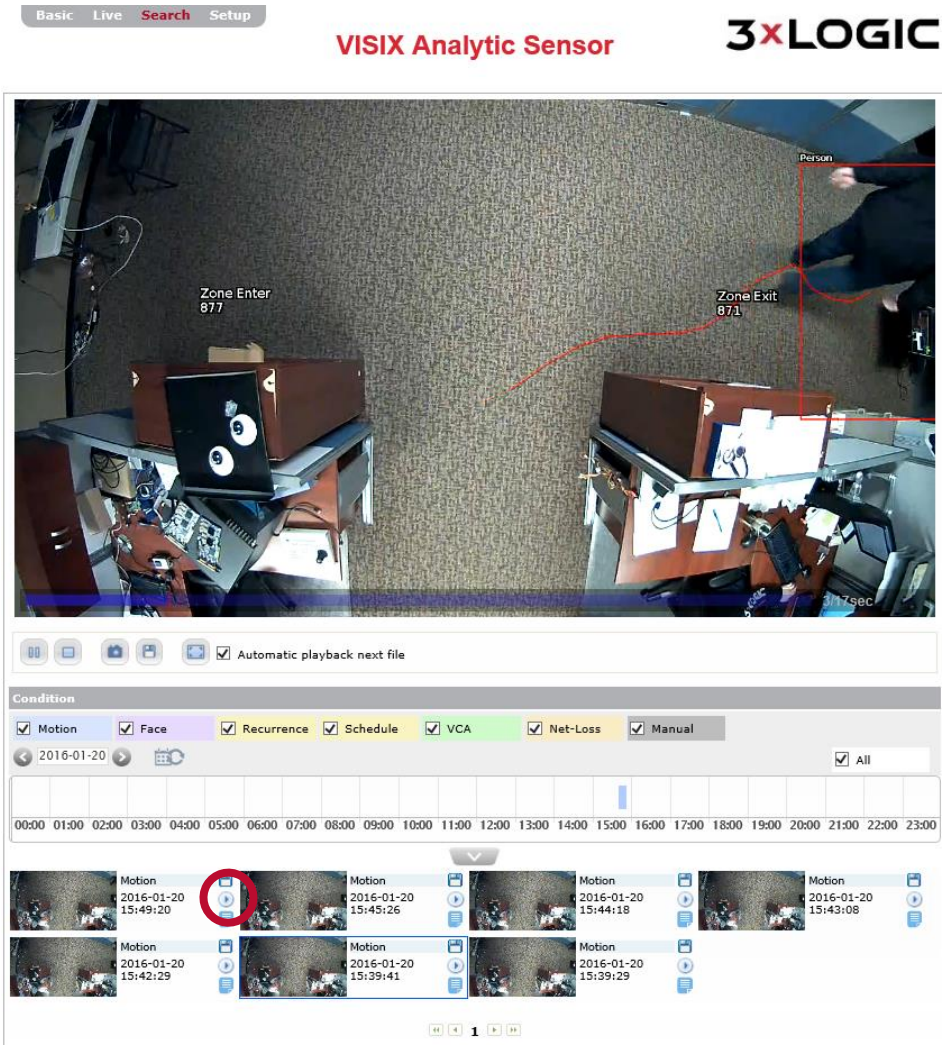


Figure 4-5: Video File Playback

When viewing playback, the followings tools may be utilized:

Playback Tools	Description
	Download a snapshot of the current frame to your local system.
	Download the clip to your current system
	View the video in full-screen mode
Automatic Playback Next File	Playback all available files sequentially in the order they were recorded.

6). Use the navigation controls at the bottom of the page to navigate multiple pages of search results.

For more information on the **Search (Playback) Tab** interface and functionality, see **Section 6.2:** **Search (Playback) Tab**.

4.2 Configure VIGIL Connect Alias

VIGIL Connect allows VIGIL VMS users to remotely connect to a VIGIL Server/V-Series All-in-One camera using the system serial number or a user defined VIGIL Connect **alias**, without the need for extensive changes to an existing network's settings. This allows for the device to be networked with other VIGIL suite utilities with little effort and minimal knowledge of the device's network connection values.

Steps:

1). To configure a VIGIL Connect alias, navigate to the camera's **Basic Tab>Camera Configuration Menu>Site Information Settings** page.

Figure 4-6: Configuring a VIGIL Connect Alias

2). Fill in the **VIGIL Connect Alias** field with an alias of your choosing.

3). Click **Apply** to save the new alias.

Your VISIX V-Series All-in-One camera can now be networked with other 3xLOGIC utilities and VIGIL suite applications (VIGIL Client, VIGIL VCM, View Lite II(Android and iOS), 3xCLOUD, etc…) using only the camera's VIGIL Connect Alias.

4.3 Configure a Video Analytics (VCA) Rule (Analytics License Required)

ENABLING VCA

Before configuring any analytics rules, VCA (video content analysis) must first be enabled on your All-in-One camera. An All-in-One Analytics license **is required** to configure and utilize VCA analytics rules on VISIX All-in-One cameras. To enable VCA:

Steps:

1). Navigate to the **Setup (Advanced) Tab > VCA > Enable/ Disable** settings page.

2). Check off **Enable** under the VCA Configuration section.

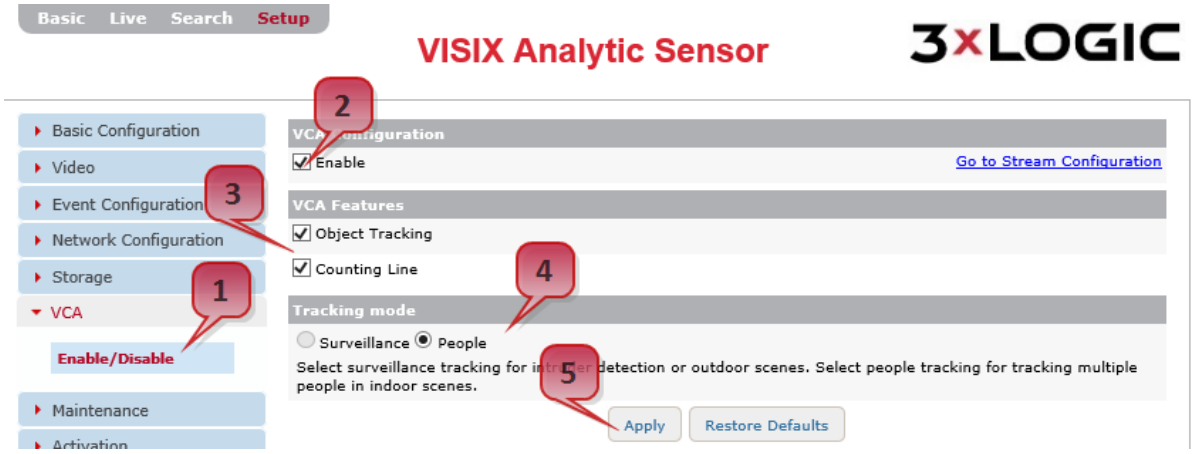


Figure 4-7: Enabling VCA Analytics

After enabling VCA, several other configuration options will be deployed.

3). Under the **VCA Features** section, select active analytics type. For the purposes of this example, both **Object Tracking** and **Counting Line** will be enabled.

4). Under the **Tracking Mode** section, select the analytics tracking mode. In this example, the **People** tracking mode is selected (People tracking requires an Advanced analytics license. If using **Surveillance** tracking mode, the steps in this example are still accurate.)

5). Click **Apply** to save the new settings.

VCA ANALYTICS CALIBRATION

Another preliminary step before configuring VCA analytics rules is the need to calibrate the cameras for accurate analytics object recognition and tracking.

The calibration process includes configuring the correct camera angle and field of view, as well as the delineation of anticipated object (people, car, etc…) size. Proper calibration of the camera is required to ensure accurate analytics counts and tracking. To begin calibration:

Steps:

1). Navigate to the **Setup (Advanced) Tab > VCA > Calibration** settings page.

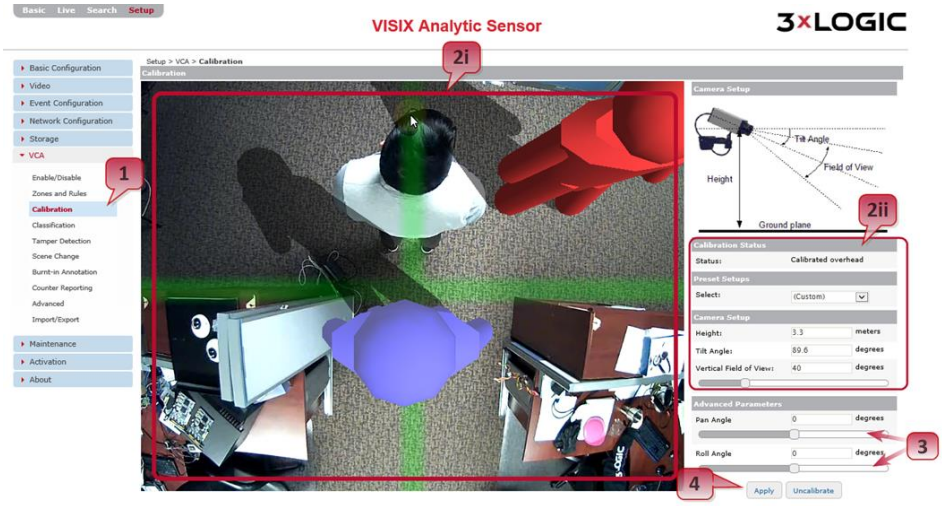


Figure 4-8: Calibrating Analytics

2). Adjust calibration settings as required. A user may perform basic calibration cameras via two separate methods:

   i. **Click-and-Drag**. - For this method, click and drag the green calibration grid to satisfactorily emulate the camera's height, tilt perspective, and field of view. The mimics may be moved around the image to help the user gauge perspective. The mouse scroll wheel is also utilized to adjust camera height, and consequentially the size of the calibration grid and mimics. Use resizing of these elements to anticipate average object size.

   ii. **Manual Configuration** - Manually enter/adjust calibration values under **Camera Setup**. As the user enters values, the calibration overlay on the live preview will react accordingly.

3). If required, adjust **Pan Angle and Roll Angle** under the **Advanced Parameters** section using the slider bars. As the sliders are moved, the calibration overlay over the preview image will react accordingly. Advanced Parameters must be entered and cannot be adjusted using Click-and-Drag.

Right-click within the video preview for the following calibration tools:

Right-Click Option	Description
Virtual Ruler	Select this tool to anchor a virtual ruler from the point-of the right click. Drag your mouse across the image to extend the ruler. Use this feature to ensure accurate perspective calibration settings.
Draw Horizon	Select this option to add a drawn horizon line to the calibration grid. This horizon line will be visible when the camera's tilt angle is twenty degrees or less.
Transparent Grid (enabled by default)	Select this option to make the green calibration grid transparent.
Add Mimic	Add another mimic to the live preview.
Pause	Pause the live preview image on the current frame.

4). When you have calibrated the camera to your satisfaction, click **Apply** to save the new calibration settings.

VCA ANALYTICS RULE CONFIGURATION

After enabling VCA and calibrating your All-in-One camera, a VCA rule may be configured. For the purpose of this example, two separate rules: a basic counting line (tripwire) and a dwell time zone, will be configured separately.

CONFIGURING A LINE (TRIPWIRE) WITH ON-SCREEN COUNTER

Steps:

1). To configure a VCA line, navigate to the **Setup (Advanced) Tab > VCA > Zones and Rules** settings page.

2). Right-click in the video preview area and select **Zone/Line>Create Line**.

3). Draw the line segment as desired by clicking to place both end points

4). Assign a **Name** and **Color** to the line.

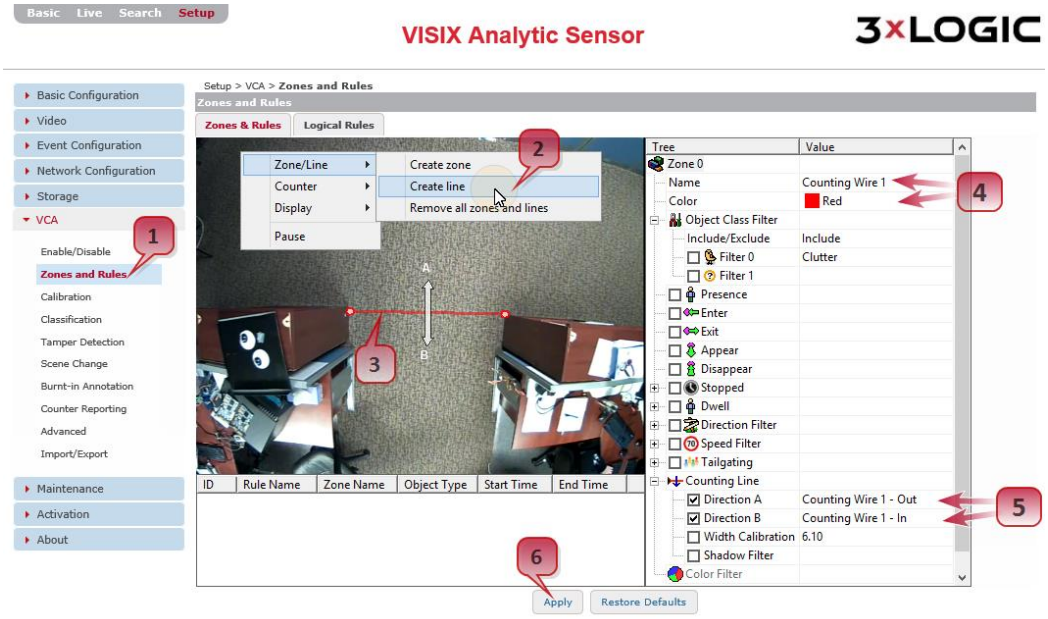


Figure 4-9: Configuring Analytics Rules

Now, the manner in which the line counts objects must be configured. The two most common counting methods using a line are:

i. **Presence** – Count will increase whenever an object makes contact with the line, regardless of direction.

ii. **Directional -** (located under **Counting Line**) – Count increases when the line is crossed toward a defined direction.

In the above example and for the purpose of this instructional, directional counting is used. To proceed:

5). Under the **Counting Line** section of the line settings, check-off both **Direction A** and **Direction B**. In the above example, **Direction A** was renamed “Counting Wire 1 - Out” and **Direction B** was renamed “Counting Wire 1 - In” for easy recognition.

6). Click **Apply** at the bottom of the window to save the newly configured counting line.

The tripwire will now tally separate counts for both configured directions. To display counts for each direction on-screen, a VCA counter must be configured. To configure a counter for use with your counting line/tripwire:

7). Right-click within the viewing area and select **Counter>Add Counter**

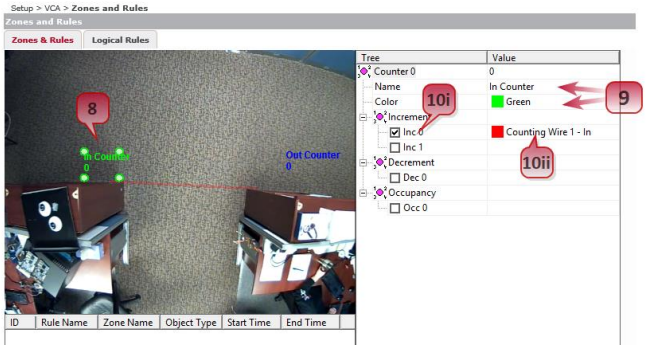


Figure 4-10: Configuring a VCA Counter

8). Place the counter overlay in the desired position.

9). Assign a **Name** and **Color** (**In Counter** and green used in the above example, respectively).

10). Configure the counter's **Increment** rule

i. Check off **Inc 0.**

ii. Set the **Inc 0** value to the desired trip wire/counting line. In the above example, **Inc 0** is set to increment whenever **Counting Wire 1 – In** is triggered.

11). Repeat Steps 7-12 to create a separate counter for **Counting Wire 1 – Out**

12). Click **Apply** to save the new counter settings.

The tripwire should now count both directions and display counts via the configured counters. For instructions on previewing your analytics overlay, see Previewing Analytics Overlay.

CONFIGURING A DWELL TIMER ZONE

Steps:

1). To configure a VCA Zone with Dwell Timer Alarm, navigate to the **Setup (Advanced) Tab > VCA > Zones and Rules** settings page.

2). Right-click in the video preview area and select **Zone/Line>Create Zone**.

3). Draw the zone as desired by clicking and dragging each corner until a satisfactory shape and position is achieved.

4). Assign a **Name** and **Color** to the zone.

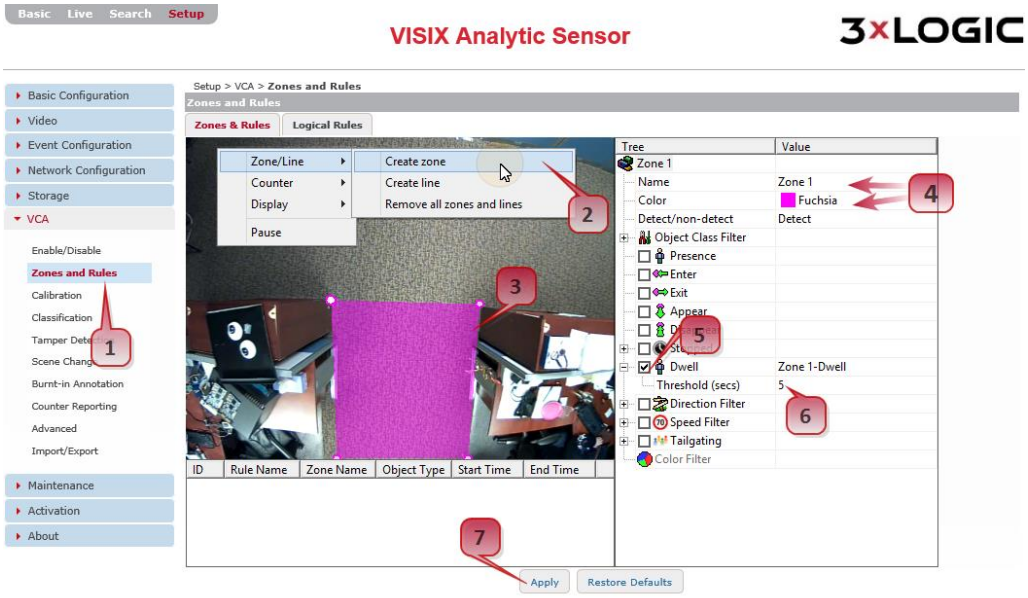


Figure 4-11: Configuring a VCA Dwell Timer Zone

5). Enable the **Dwell** rule.

6). Set an appropriate dwell **Threshold.** 5 seconds is used in the above example.

7). Click **Apply** to save the new zone settings.

An analytics dwell event(alarm) will now trigger whenever an object has spent more than 5 seconds in the defined zone. For instructions on previewing your analytics overlay, navigate to Previewing Analytics Overlay.

PREVIEWING ANALYTICS OVERLAY

Steps:

1). For a full live preview of your analytics overlay, select the **Live** tab.

2). In the Live viewer, right-click and select **Show Counter** and **Show Zones** to overlay counters and zones/lines.

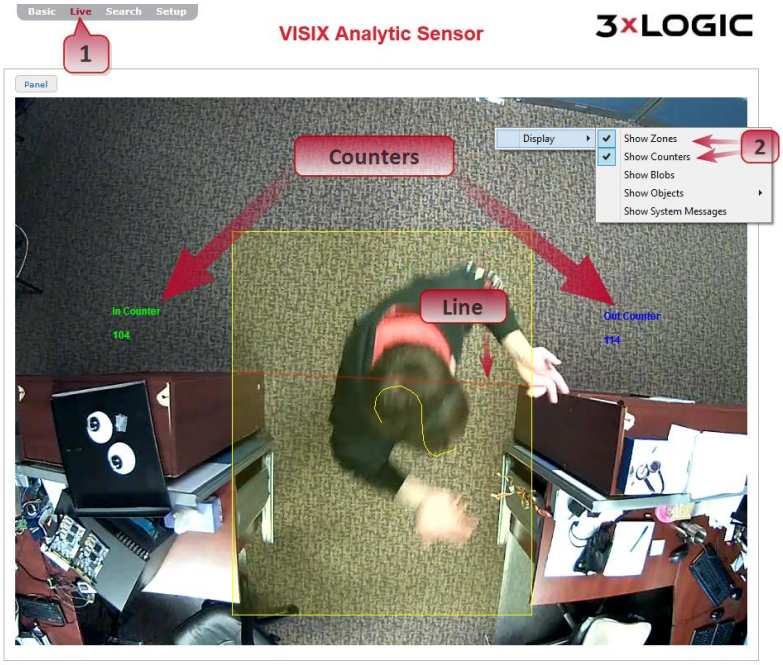


Figure 4-12: Example 1 Counting Line (Tripwire) Analytics Overlay

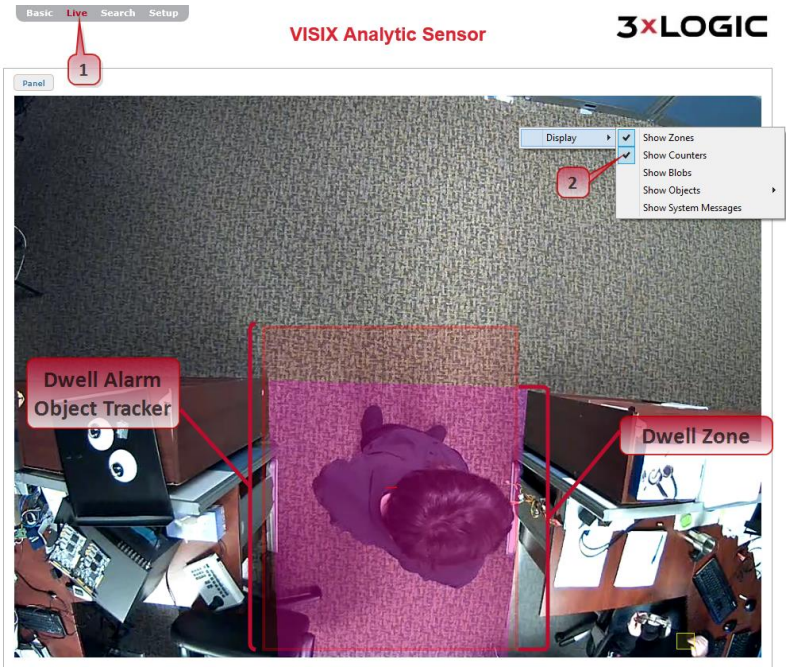


Figure 4-13: Example 2 - Dwell Timer Zone Analytics Overlay

4.4 Integrating All-in-One Camera with VIGIL Server Using VIGIL Analytics Bridge

VIGIL Analytics Bridge allows stand-alone VCA analytics rules found on a 3xLOGIC VISIX All-in-One Camera web settings to be used and processed by a VIGIL Server and other VIGIL business intelligence products. Quick configuration within VIGIL Server and VIGIL Analytics Bridge is all that is needed to obtain analytics data directly from a 3xLOGIC All-in-One camera.

INSTALLATION OF ANALYTICS BRIDGE

The utilization of a 3xLOGIC All-in-One camera in VIGIL Server requires the installation of the VIGIL Analytics Bridge program on the same system as VIGIL Server. The Analytics Bridge installer can be downloaded here from **www.3xlogic.com**. Once it is successfully downloaded to your computer:

Steps:

1). Double click on **VigilAnalyticsBridge.exe** to begin the installation.

2). You will be prompted to close all VIGIL Services. Click **Close All** and follow the on-screen instructions to continue the installation process.

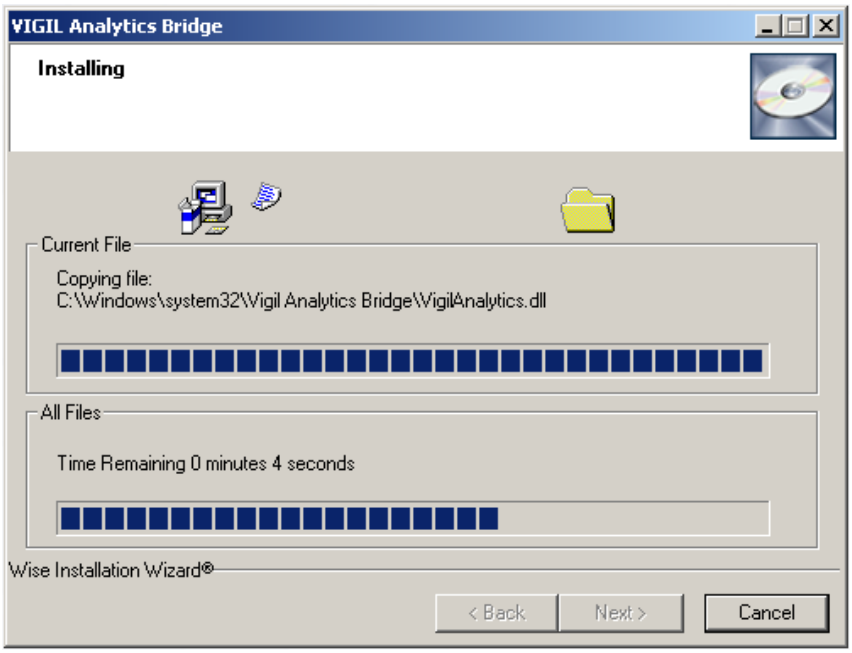


Figure 4-14: VIGIL Analytics Bridge Installation Progress

3). Once the installation has completed, you will be prompted to reboot your system.

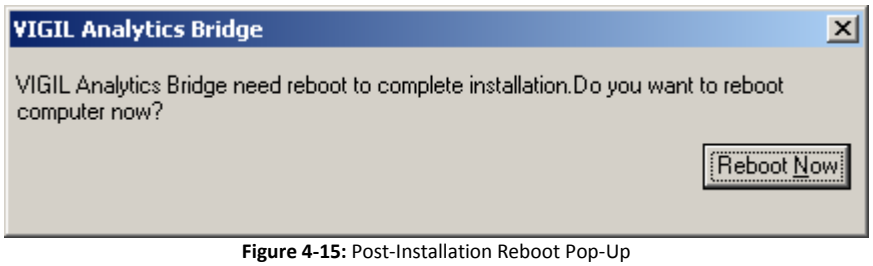


Figure 4-15: Post-Installation Reboot Pop-Up

4). Click **Reboot Now** to finalize the installation process.

VIGIL SERVER CONFIGURATION

To configure a network camera in VIGIL Server:

Steps:

1). Click on **Settings** in the icon menu toolbar on the VIGIL Server main screen. The **Settings** window will deploy.

2). Select the desired camera channel from the **Cameras** list.

3). Click the **Network Camera** checkbox.

4). Click the **Settings** button to launch the **Network Camera Settings** window. If **Network Camera** was not checked before the previous step, the **Network Camera Settings** window will have deployed automatically.

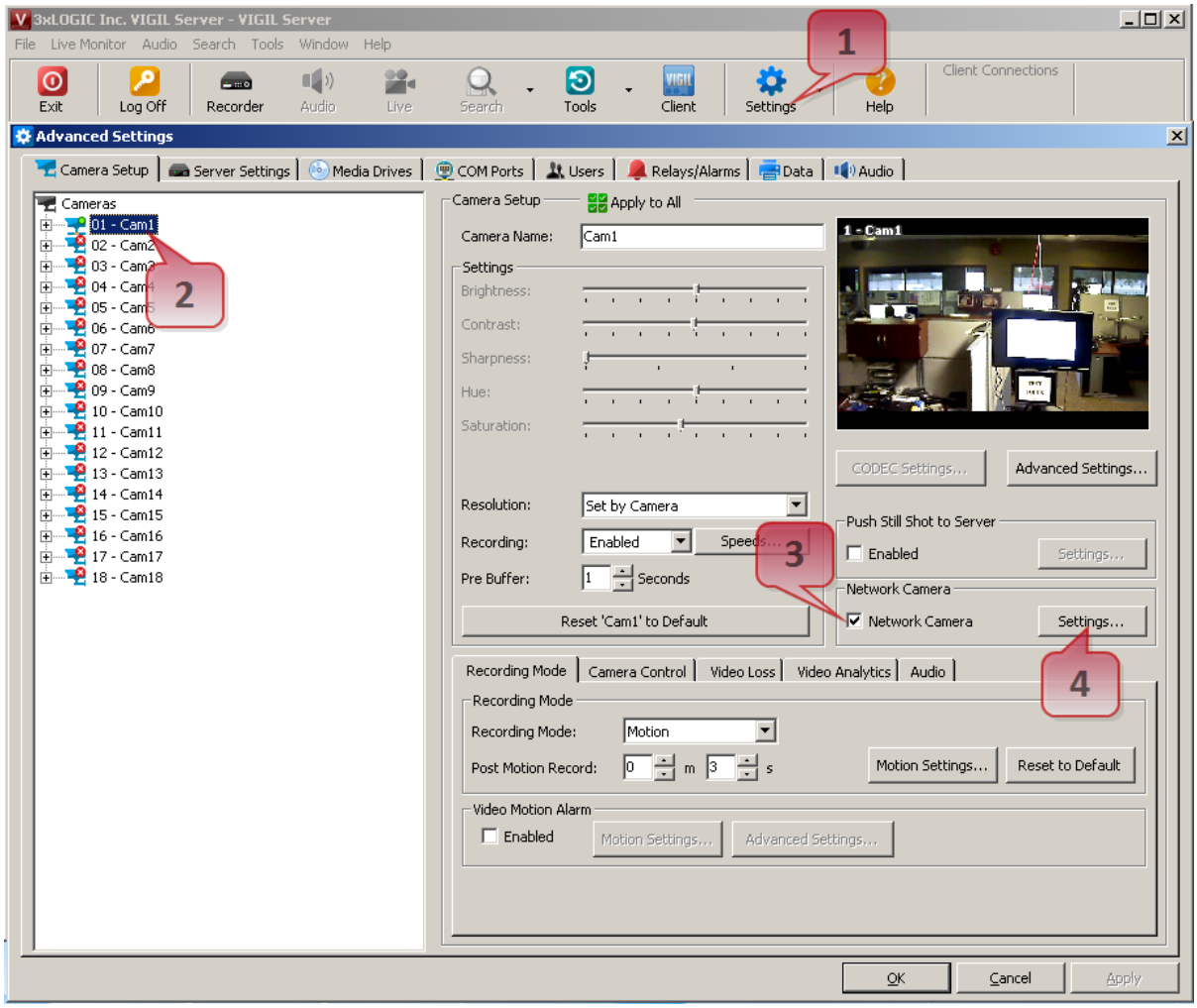


Figure 4-16: Configuring a Network Camera

VIGIL SERVER CONFIGURATION – NETWORK CAMERA SETTINGS

The **Network Camera Settings** window is where the direct configuration of the 3xLOGIC All-in-One camera will take place.

Steps:

1). Fill in all the required information and press **OK**.

2). After the **Network Camera Settings** window closes, click **OK** or **Apply** to save the settings in VIGIL Server.

VIGIL Server is able to receive video from one or many network cameras connected to the LAN or WAN. VIGIL Server currently supports several types of network cameras aside from 3xLOGIC All-in-One Cameras.

To edit a network camera at any time after initial configuration:

Steps:

1). Access **VIGIL Server Settings>Camera Setup Tab**, select the desired network camera and click the Network Camera **Settings** button. This will open the **Network Camera Settings** window.

NOTE:

The Network Camera feature disables the physical camera input on video capture cards for the selected camera channel.

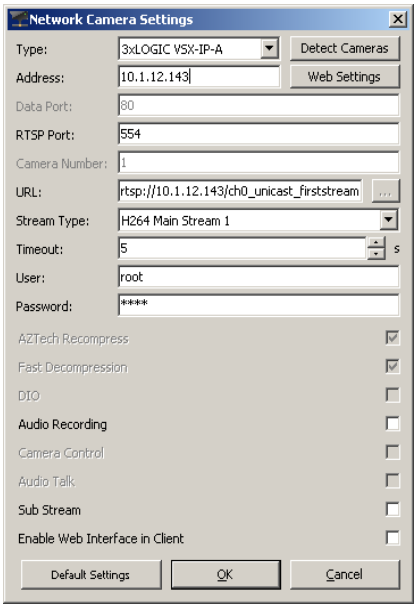


Figure 4-17: Network Camera Settings Window

Field	Description
Type	The type of network camera.
Address	The IP or HTTP address of the camera. It is not necessary to include http:// at the beginning of the HTTP address.
Web/Camera Settings	Connects to the camera's web interface to make changes to the camera's internal settings.
Data / RTSP Port	The network ports used to connect with the camera.
Camera Number	Some Network Camera types also support Encoders. Select the Camera number on the encoder to use for this network camera.
URL	Set this to the camera URL, if applicable. For 3xLOGIC All-in-One cameras, the url will be automatically set to **rtsp:// [ip address] /ch0_unicasy_firststream**
Stream Type	Select the video stream type for the camera: MPEG4, JPEG, or H264.
Timeout	The number of seconds to attempt to connect to the camera before timing out. If the timeout is reached, "Signal Loss" displays in the **Live Viewer** window.
User/Password	The user name and password to connect to the camera. The default values are automatically entered.

VIGIL ANALYTICS BRIDGE – LAUNCHING THE VIGIL ANALYTICS BRIDGE

Once the 3xLOGIC All-in-One camera has been configured in VIGIL Server, it must be configured in the VIGIL Analytics Bridge.

Steps:

1). To launch the Analytics Bridge, navigate to **Start > All Programs>VIGIL** and click **VIGIL Analytics Bridge**.

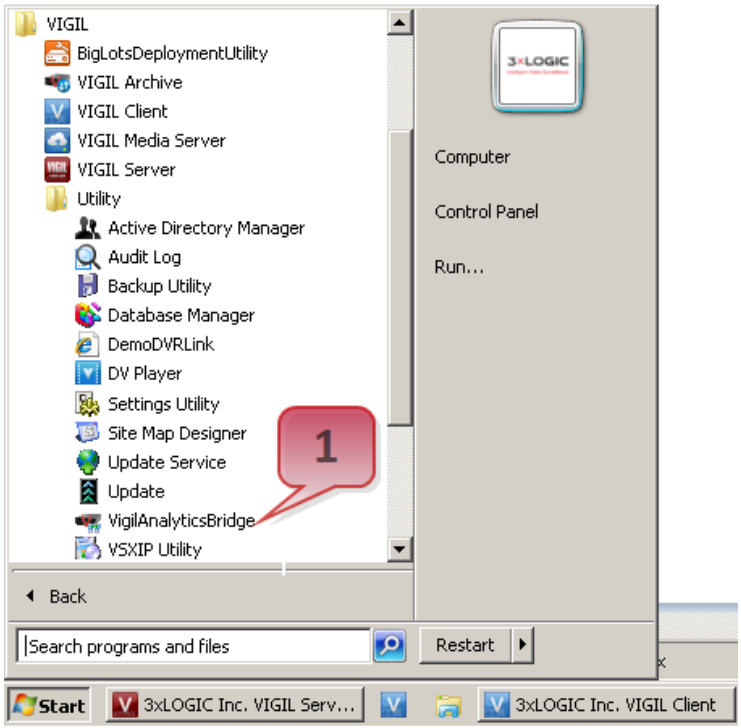


Figure 4-18: Launching VIGIL Analytics Bridge

2). If the Analytics Bridge UI does not deploy after launching from the Windows Start Menu, locate and double-click on the **Analytics Bridge** quick launch icon in the Windows Task Bar (pictured below).

Figure 4-19: VIGIL Analytics Bridge Quick Launch Icon

CONFIGURING A 3XLOGIC ALL-IN-ONE CAMERA IN THE VIGIL ANALYTICS BRIDGE

The Analytics Bridge main screen is pictured below. All configuration of the Analytics Bridge takes place from this screen.

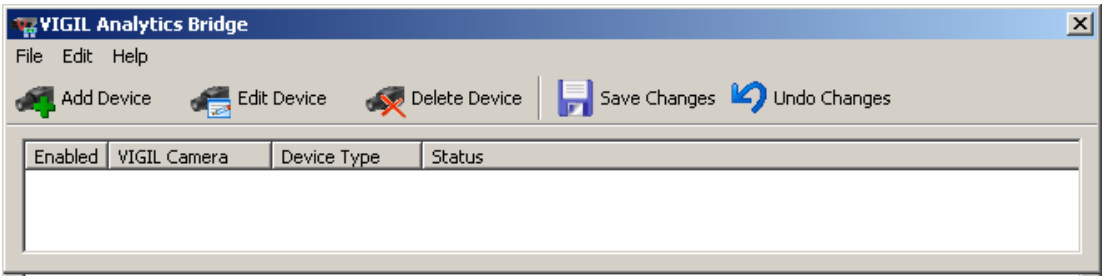


Figure 4-20: VIGIL Analytics Bridge Main UI

Field	Description
Add Camera	Add/Edit camera opens the Add/Edit window, pictured below.
Delete Camera	Deletes the currently selected camera.
Enable All	Enable/Disable All. Enables and disables all cameras configured in VIGIL Analytics Bridge. Disabling the cameras will stop VIGIL from perceiving the camera's analytics data.
Save Changes	Saves any changes done after a new camera is configured. Will only appear after a new camera has been configured or an existing one has been edited.
Undo Changes	Undoes any configuration changes. Will only appear after a new camera has been configured or an existing one has been edited.
Enabled	Enabled cameras will send analytics data to VIGIL Server. Disabled cameras will continue to record as normal, but will not retain any analytics data.
VIGIL Camera	The name of the camera as defined in VIGIL Server.
Type	The type of the camera: **3xLOGIC, SenTech Crosspoint, UDP or VideoIQ**. Select 3xLOGIC for 3xLOGIc All-in-One cameras.
Status	Will display either **Receiving events** or **Stopped.** Related to whether or not the camera is enabled or disabled.

Steps:

1). To begin configuration of the 3xLOGIC All-in-One camera within VIGIL Analytics Bridge, click **Add** Device.

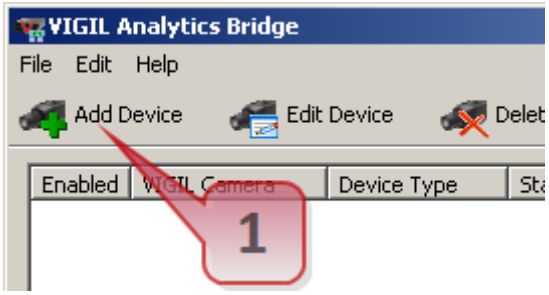


Figure 4-21: Adding a Device to VIGIL Analytics Bridge

2). The **Add/Edit Camera** window will appear, shown below. Fill in all the required information regarding the 3xLOGIC All-in-One camera and press **Load Device** for a video preview from the camera.

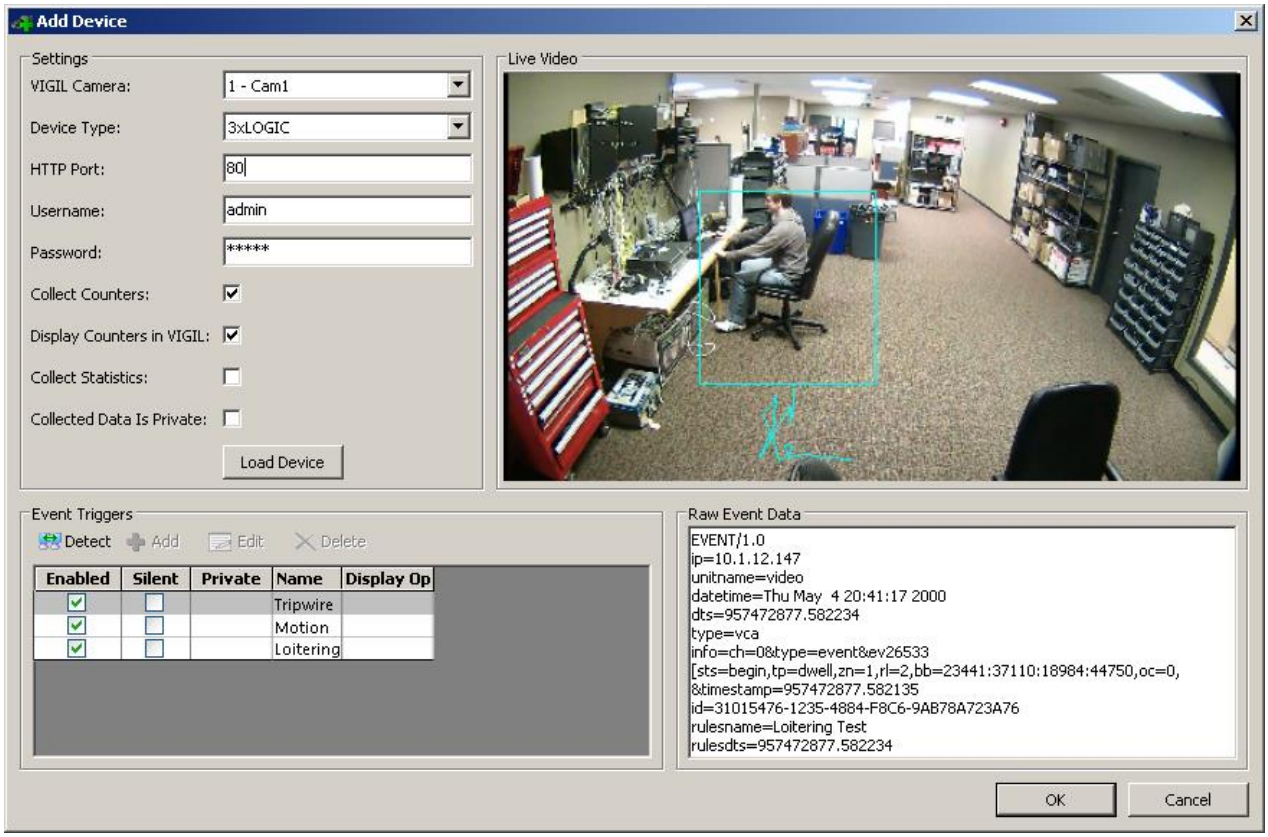


Figure 4-22: VIGIL Analytics Bridge - Add Device Window

Camera connection and configuration settings are described below:

Field	Description
VIGIL Camera	A dropdown list containing all of the cameras currently configured with VIGIL Server.
Device Type	The type of device/camera being edited or added. **3xLOGIC, SenTech Crosspoint, UDP or VideoIQ**. Select 3xLOGIC for 3xLOGIc All-in-One cameras.
HTTP Port	One of two ports used to connect to the camera's analytics data.
Username	Username required to sign in to the camera.
Password	Password required to sign in to the camera.
Collect Counters	Enables the collection of data counters
Collect Statistics	Enables the collection of analytics statistics
Collected Data is Private	This feature prevents VIGIL Central Management from acquiring analytics information collected by the camera.
Load Device	Click this button after the other device/camera settings have been correctly input. The device/camera's feed will be displayed in the **Live Video** window to the right,if available.
Raw Event Data	Contains a raw dump of analytics event data coming from the camera.

Event Triggers	Description
Detect	Detects any configured analytics rules located on the camera.
Add	Manually adds a rule. Adding a rule will tell VIGIL Analytics Bridge to search for a rule of that name. It will not add the rule to the camera.
Delete	Deletes a rule from VIGIL Analytics Bridge.
Enabled	Enabling a rule allows VIGIL Analytics Bridge to monitor the matching rule in the camera and place analytics data in VIGIL Server's database. The name of the rule in VIGIL Analytics Bridge is case sensitive and must be identical to a corresponding rule in a camera.
Silent	Enabling the **Silent** option will place analytics data for the associated rule into VIGIL Server's database, but will hide the rule from being seen by VIGIL Server.
Private	This field will indicate whether or not data from this camera is being collected by VIGIL Central Management (VCM).
Name	The name of the rule. The rule name must be identical to a rule located on the camera. The name is case sensitive.
Display Options	Lists any active display options.

3). Once you have configured camera connection information, click the **Detect** button to detect the analytics rules currently configured on the camera. Whenever new rules are configured on the camera, the **Detect** functionality must be used to update the rules in the Analytics Bridge.

4). Click **OK** after detecting. The **Add/Edit Device** window will close.

5). On the main screen, click **Save Changes**. **Save Changes** will only appear when a camera has been added or edited. All new rule settings will be pushed to VIGIL Server.

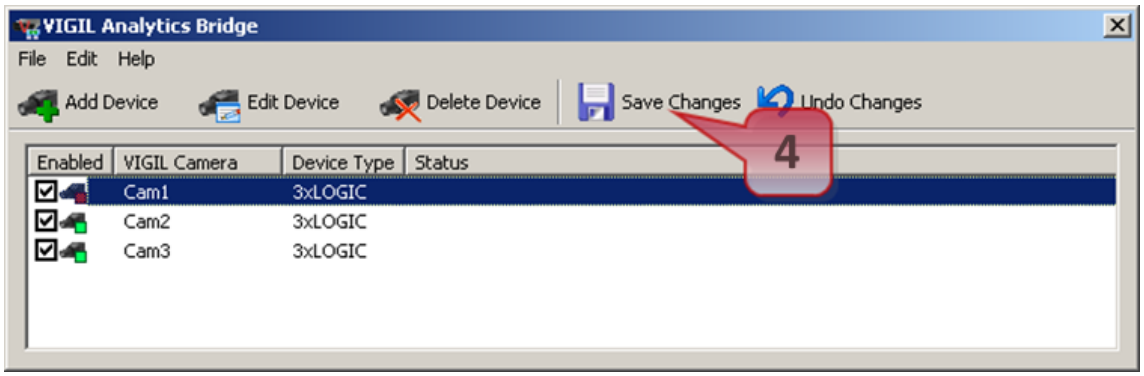


Figure 4-23: VIGIL Analytics Bridge - Saving Changes

Configuration is now complete. The VIGIL Server system will now record video and data based on the 3xLOGIC All-in-One camera's-detected analytics events.

4.5 Adding All-in-One Camera to VIGIL Suite Utilities

VIGIL CLIENT - ADDING A V-SERIES ALL-IN-ONE CAMERA

Steps:

1). To interface a VISIX All-in-One Camera with VIGIL Client Launch VIGIL Client (Local Mode only; VCM mode will only display Servers from a networked VCM Server) and select **Servers** from the **Servers** top menu. This will launch the Servers window. VISIX All-in-One devices are considered edge recording devices, and thus are recognized as their own VIGIL Server within the VIGIL suite.

2). Click **Add**. This will deploy the **Add/Edit VIGIL Server** window.

3). Enable the **Use VIGIL Connect** option. If connecting using traditional network connection criteria is desired, enter the cameras **IP Address/DNS Name** and confirm TCP/IP port status.

4). Enter in the VIGIL Connect alias of the desired VISIX All-in-One camera (**VIGILTest1** used in the below example). Skip this step if using traditional network connection criteria (IP/Port).

5). Click **Test VIGIL Connect** to confirm the camera can be communicated with through the Connect system using the provided alias. Skip this step if using traditional network connection criteria (IP/Port).

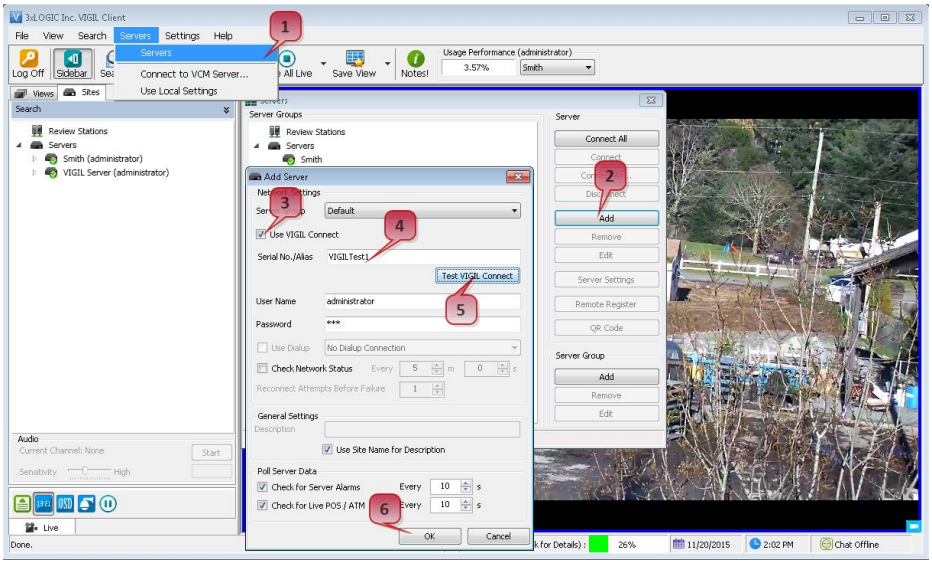


Figure 4-24: Adding All-in-One Camera to VIGIL Client

6). If the test is successful, then VIGIL Client can successfully communicate with the Server. Click **OK** at the bottom of the **Add Server** window after configuring all required fields to save the new Server to VIGIL Client. For more information on configuring VIGIL Servers, please see **Section 5.1** of the VIGIL Client Users Guide.

NOTE:

The camera will be visible in the Client treeview and will be represented by a icon. The camera video stream can be added to the VIGIL Client viewer in the same manner as VIGIL Server cameras; Simply extend the camera's drop-down menu and double click the icon to add it to the viewer. Alternatively, a user can drag-and-drop the camera stream icon into the desired frame of the VIGIL Client viewer.

For more information on configuring VIGIL Servers/V-Series All-in-One camera in VIGIL Client, please see **Section 5.1** of the VIGIL Client Users Guide.

VIGIL VCM - ADDING A V-SERIES ALL-IN-ONE CAMERA

Steps:

1). To add a VISIX All-in-One Camera to VCM for central management and health-monitoring purposes, launch a VCM Client.

2). Log into a VCM Server.

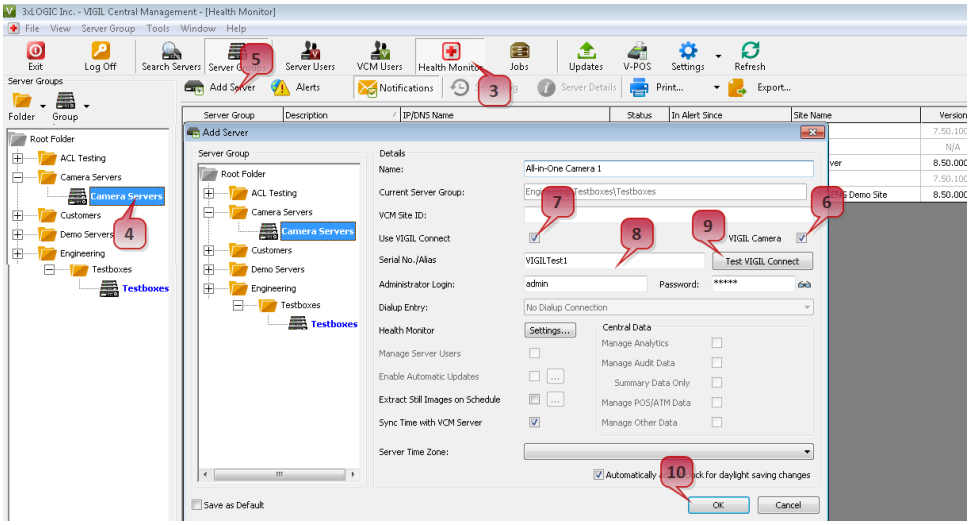


Figure 4-25: Adding an All-in-One Camera to VCM

3). Click the **Health Monitor** button.

4). Select (left-click) a **Server Group** from the **Server Groups** sidebar to. The **All-in-One** camera will be added to this group.

5). Click the **Add Server** button (only available after selecting an applicable **Server Group**). This will launch the **Add/Edit Server** form. VISIX All-in-One devices are considered edge recording devices, and thus are recognized as their own Server within the VIGIL suite, including VCM.

6). Check off **VIGIL Camera.** This will indicate to VCM that the device you are adding is a VISIX all-in-One camera.

7). Check-off **Use VIGIL Connect.** Alternatively, if you wish to use traditional network connection criteria, leave **Use VIGIL Connect** disabled and enter in **IP/DNS Name** and **Port** info (if using standard network connection values, also ignore step 8 of these instructions) for the device.

8). Enter the VIGIL Connect alias of the All-in-One camera in the **Serial No./Alias** field.

9). After entering an alias, click Test VIGIL Connect to ensure successful communication with the VIGIL Connect system.

10). Fill in all remaining required fields and click **OK** to add the camera to your list of centrally managed VIGIL Servers/VISIX All-in-One cameras.

If you experience issues connecting to the All-in-One camera in VCM, confirm the alias that has been entered is correct. If all settings appear to be correct, contact 3xLOGIC for further instruction or reference Tech Tip 140028 VIGIL Connect Troubleshoot Guide for troubleshooting tips.

3XLOGIC VIEW LITE II MOBILE (ANDROID AND IOS) – ADDING A V-SERIES ALL-IN-ONE CAMERA

Steps:

1). To interface a VISIX All-in-One camera with 3xLOGIC's View Lite II mobile app, launch the View Lite II app on your mobile device (Android OS is pictured in the below screenshot, however, the process is identical in the iOS version).

2). Tap the  icon to deploy the **Settings** menu.

3). Tap the **Servers** menu option.

4). Tap **Add VIGIL Server**. This will launch the **Add VIGIL Server** form. VISIX All-in-One devices are considered edge recording devices, and thus are recognized as their own VIGIL Server within the VIGIL suite, including View Lite.

Figure 4-26: Adding an All-in-One Camera to View Lite II

5). Enable **VIGIL Connect.** Alternatively, if you wish to use traditional network connection criteria, leave **VIGIL Connect** disabled and enter in an **IP/DNS Name** and **Port** info (if using standard network connection criteria, also ignore step 6 of these instructions) for the device.

6). Enter in the VIGIL Connect alias for the desired VISIX V-Series All-in-One camera (VIGILTest1 used in the above example).

7). Fill in the remaining required fields and tap **Save** to save the All-in-One camera to View Lite II. A user may now add the camera stream to the View Lite viewer using the same process as adding VIGIL Server or 3xCLOUD networked cameras.

3xCLOUD CROSS-PLATFORM WEB CLIENT – ADDING A V-SERIES ALL-IN-ONE CAMERA

Steps:

1). To interface a VISIX All-in-One camera with a 3xCLOUD web client account, login to your 3xCLOUD account (www.3xlogiccloud.com).

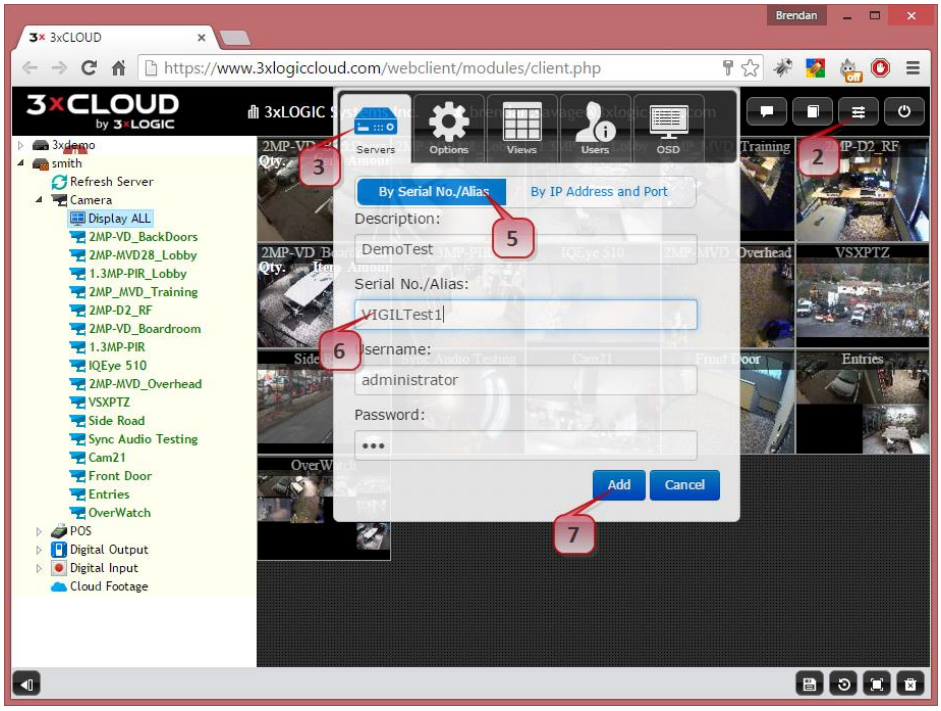


Figure 4-27: Adding an All-in-One Camera to a 3xCLOUD Account

2). Click the  button to open the Settings menu.

3). Select the **Servers** icon.

4). Click the 

button (not pictured above). This will deploy the **Add/Edit VIGIL Server** form. VISIX All-in-One devices are considered edge recording devices, and thus are recognized as their own VIGIL Server within the VIGIL suite, including 3xCLOUD.

5). Click the **By Serial No./Alias** tab to configure the Server with a VIGIL Connect alias. If using traditional network connection criteria is desired, click the **By IP Address and Port** button enter in an **IP** and **Port** info (if using standard network connection criteria, also ignore step 6 of these instructions) for the device.

6). Enter the VIGIL Connect alias of the desired All-in-One camera in the **Serial No./Alias** field (VIGILTest1 used in the above example).

7). Fill in all required fields and click **Add** to save the All-in-One camera to your 3xCLOUD VIGIL Server list.

The All-in-One camera should now be available to add to your 3xCLOUD layout. If you experience connection issues, confirm the connection info (IP Address and Port/VIGIL Connect Alias) you entered is correct. If all settings appear to be correct, contact 3xLOGIC for further instruction or reference Tech Tip 140028 VIGIL Connect Troubleshoot Guide for troubleshooting tips.

4.6 Reboot and Reset to Factory Default Procedures

REBOOTING THE CAMERA USING THE RESET BUTTON

Steps:

1). Press the reset button for **2 seconds** while the device is active. See the VISIX V-Series All-in-One Camera Hardware and Installation Manual for the location of your particular camera model's *Reset* button.

2). Wait for the system to reboot.

NOTE:

Please do not hold the reset button for more than 2 seconds. Otherwise, the camera may be switched to its Factory Default settings.

REBOOT THE CAMERA USING THE 3XLOGIC CAMERA SETUP UTILITY

Steps:

1). Open the 3xLOGIC Camera (VSX-IP) Setup Utility.

2). Select your device.

3). Open Advanced Settings.

4). Click Reboot.

REBOOT THE CAMERA VIA WEB BROWSER INTERFACE

Steps:

1). Login to the cameras web browser interface.

2). Navigate to **Basic Tab> Camera Configuration Menu > Maintenance**.

3). Click the **Reboot** button.

4). You will be prompted to confirm the reboot process. Click **OK** to proceed.

RESETTING CAMERA SETTINGS TO FACTORY DEFAULT

Resetting the device back to the factory default will reinitialize all parameters including the IP address back to the factory defaults. To reset back to the factory default:

Steps:

1). Press the reset button and hold it while the device is in use.

2). Release the button after 10 seconds.

3). Wait for the system to reboot.

Factory Default Connection Settings	
IP address	192.168.xx.yy
Network Mask	255.255.0.0
Gateway	192.168.0.1
Username	Admin
Password	12345

RESET TO FACTORY DEFAULT SETTINGS VIA CAMERA WEB INTERFACE

Steps:

1). Login to the camera's browser interface.

2). Navigate to **Basic Tab> Camera Configuration Menu > Maintenance** settings form.

3). Click the **Reset Camera Settings** button.

4). You will be prompted to confirm the factory reset process. Click **OK** to proceed.

5 Basic Tab

The initial landing page of the VISIX V-Series All-in-One Camera web interface is the **Basic Tab > Camera Status > Status** page.

NOTE:

Some UI components (logo, page title, location of minor settings within page hierarchy, etc…) may vary depending on firmware series version, VIGIL software version, and licensing. However, operation of all components and settings, regardless of their location within the UI remains unchanged.

5.1 Camera Status Menu

STATUS

Steps:

1). The **Basic Tab>Camera Status > Status** page is the initial landing page after logging into the camera. This page provides at-a-glance information regarding the camera's configuration and status, as well as storage status.

Figure 5-1: Basic Tab – Camera Stratus-Status Page

Status Indicator	Description
Camera Information	The **Camera Information** section provides at-a-glance information regarding: ■ Camera Model ■ Camera Firmware Version ■ VIGIL Software Version ■ Camera MAC Address ■ VIGIL Connect Alias ■ Company Name ■ Site Name ■ Camera Name
Camera Status	The **Camera Status** section provides at-a-glance information regarding: ■ Camera Current ■ Timezone ■ CPU Usage % ■ Memory Availability ■ UPnP Status ■ Internet Connection Status
Storage Status	The **Storage Status** section provides at-a-glance information regarding: ■ Storage Device Status ■ Total Capacity ■ Free Space ■ Recorded Footage Date/Time Range

5.2 Camera Configuration Menu

SITE INFORMATION

Steps:

1). Opening the **Basic Tab>Camera** Configuration drop-down menu and clicking the **Site Information** link will open the **Site Information** settings page.

Figure 5-2: Basic Tab – Camera Configuration – Site Information Form

2). From the **Site Information** page, a user may edit site information settings

Configuration settings including:

Field	Description
Company Name	The name of the company that owns the camera.
Site Name	The name of the field site in which the camera is deployed.
Camera Name	The name of the cameras. This will be used to identify the camera throughout the VIGIL software suite.
VIGIL Connect Alias	VIGIL Connect allows VIGIL VMS/VISIX V-Series All-in-One users to remotely connect to a VIGIL Server/V-Series All-in-One camera using the system serial number or a user defined VIGIL Connect **alias**, without the need for extensive changes to an existing network's settings.

3). After finishing configuration, click **Apply** to save the new settings.

TIME

Steps:

1). Opening the **Basic Tab>Camera Configuration** drop-down menu and clicking the **Time** link will open the **Time** settings page.

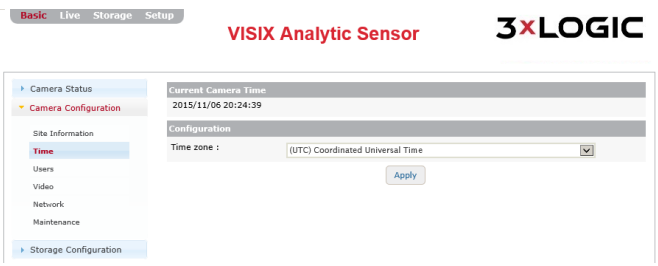


Figure 5-3: Basic Tab – Camera Configuration – Time Settings

2). From the **Time** page, a user may view the camera's current time or choose the camera's time zone. After finishing configuration, click **Apply** to save the new settings.

NOTE:

Advanced time settings (manual time configuration, time synchronization method, etc…) can be configured from the **Advanced Tab> Basic Configuration Menu>Time** page.

USERS

Steps:

1). Opening the **Basic Tab>Camera Configuration** drop-down menu and clicking the **Users** link will open the **Users** settings page.

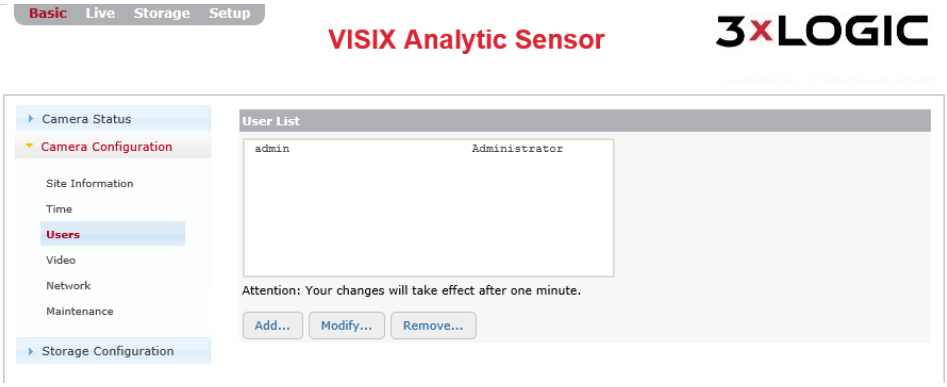


Figure 5-3: Basic Tab – Camera Configuration - Users Settings

2). From the **Users** page, a user may view the camera's list of user profiles. A user may also add, modify or remove a user profile. Details regarding each action are outlined in the proceeding sub-sections of this manual.

ADD A USER

Steps:

1). Click the **Add…** to add a new user profile. The **Add User** form (pictured right) will deploy.

Form Field	Description
Username and Password	Enter a username and password for the new user.
Confirm Password	Confirm the previously entered password.
User Group	Choose a User Group for the user.

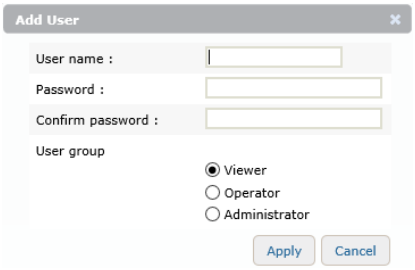


Figure 5-4: Add a User

2). After finishing configuration, click **Apply** to save the new settings.

MODIFY A USER

Steps:

1). Click the **Modify…**button to modify an existing user profile. The **Modify User** form (pictured right) will deploy.

Form Field	Description
Username and Password	Enter a username and password for the new user.
Confirm Password	Confirm the previously entered password.
User Group	Choose a User Group for the user.

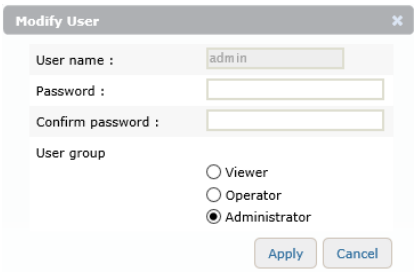


Figure 5-5: Modify a User

2). After finishing configuration, click **Apply** to save the new settings.

REMOVE A USER

Steps:

1). Click the **Remove** button to remove an existing user profile. This action is only available when a user profile is selected in the list.

2). You will be prompted for a confirmation before finalizing the removal.

VIDEO

Steps:

1). Opening the **Basic Tab>Camera Configuration** drop-down menu and clicking the **Video** link will open the **Video** settings page.

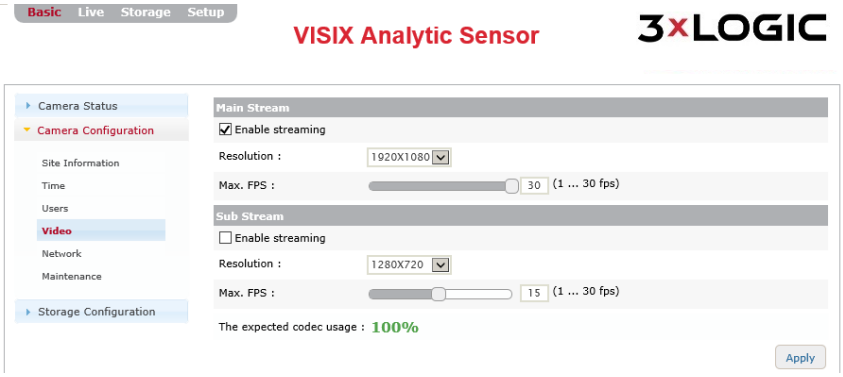


Figure 5-6: Basic Tab – Camera Configuration – Video Settings

From the **Video** page, a user may edit a camera's **Main Stream** and **Sub Stream** video settings.

Stream Settings	Description
Enable Streaming	Check this box to enable the chosen stream.
Resolution	Set the chosen stream's resolution. Full-resolution is generally reserved for main-stream. A smaller, less data-intensive resolution is generally reserved for sub stream.
Max FPS	Set the camera's maximum Frames-Per-Second value. A higher FPS is generally reserved for main stream, while a lower, less data-intensive value is generally reserved for sub stream.

NETWORK

Steps:

1). Opening the **Basic Tab>Camera Configuration** drop-down menu and clicking the **Network** link will open the **Network** settings page.

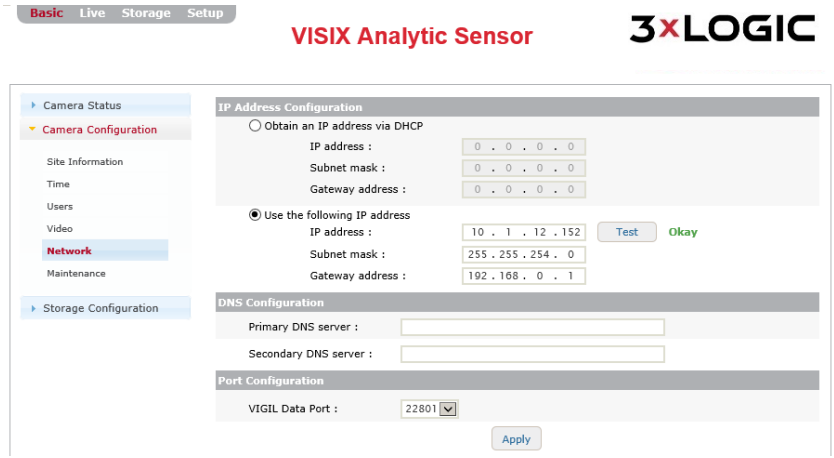


Figure 5-7: Basic Tab – Camera Configuration – Network Settings

2). From the Network settings page, a user may edit a camera's IP Address Configuration, DNS Configuration and Port Configuration.

Network Setting	Description
IP Address Configuration	Select the method by which the cameras will obtain an IP address: **Obtain an IP Address via DHCP** – Select this method to have your router's DHCP function automatically assign the camera's network connection settings. This method is enabled by default. The automatically-generated **IP, Subnet Mask and Gateway** addresses will be listed directly underneath. **Use the following IP Address (Manual Configuration**) – Select this option to manually enter network connection settings. **IP Address, Subnet Mask and Gateway Addresses** can be manually entered directly underneath this settings. Clicking the **Test** button will confirm the validity of the network connection values you have entered.
DNS Configuration	Enter in **Primary** and **Secondary DNS Server** connection information.
Port Configuration	Select the **VIGIL Data Port**. ***22801*** is the default and is the recommended port number by 3xLOGIC.

MAINTENANCE

Steps:

1). Opening the **Basic Tab>Camera Configuration** drop-down menu and clicking the **Maintenance** link will open the **Maintenance** settings page.

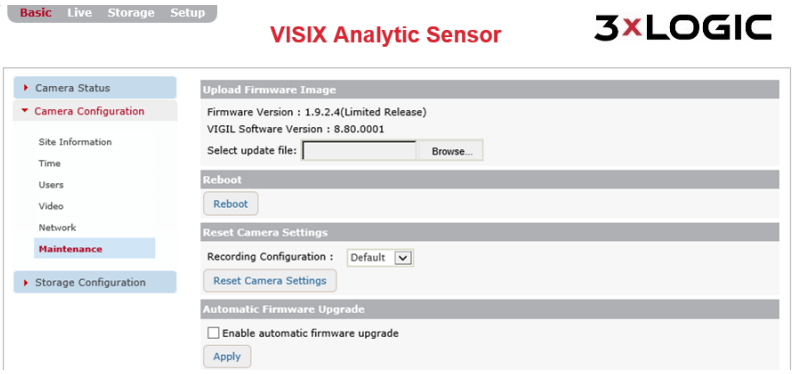


Figure 5-8: Basic Tab – Camera Configuration – Network Settings

2). From the **Maintenance** settings page, a user may perform basic maintenance functions such as pushing a firmware or VIGIL software update to the camera, reboot the camera or reset the camera to factory default settings.

Maintenance Setting	Description
Upload Firmware Image	The current firmware and VIGIL software version of the camera is listed: Click the **Browse** button to open a file browser and locate the firmware update file.
Reboot	Click the **Reboot** button to restart the device. You will be prompted to confirm the reboot process. Click **OK** to proceed.
Reset Camera Settings	Click the **Reset Camera Settings** button to reset all custom configured settings to factory default. You will be prompted to confirm the factory reset process. Click **OK** to proceed.
Automatic Firmware Upgrade	Enable automatic firmware upgrade. The camera will poll an update cloud server hosted by 3xLOGIC for new firmware and will apply an update when available.

5.3 Storage Configuration Menu

SD CARD

Steps:

1). Opening the **Basic Tab>Storage Configuration** drop-down menu and clicking the **SD Card** link will open the **SD Card** settings page.

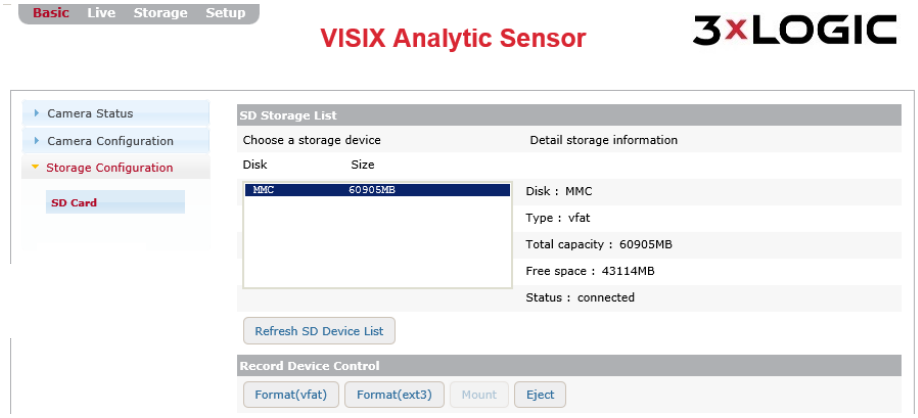


Figure 5-9: Basic Tab – Storage Configuration – SD Cards Settings

2). From the **SD Card** storage settings page, a user may choose their SD storage device, view information on the chosen device, change storage format or mount and eject storage devices.

SD STORAGE LIST

In the **SD Storage List** section, a user may select their desired storage device from the list. The following device details will be generated to the right of the device list after making a selection.

Storage Detail	Description
Disk	The storage device disk type of the selected device.
Type	The storage disk format of the selected device.
Total Capacity	The totally storage capacity of the selected device.
Free Space	Lists the remaining free space on the selected device.
Status	Current storage device status.

RECORDING DEVICE CONTROL

In the **Record Device Control** section, a user may select the desired storage format (vfat, ext3) and can also mount an inactive storage device or eject the currently active storage device.

Device Control	Description
Format (vfat)	Use *vfat* format for the selected device. Format progress will be displayed. **WARNING:** Re-formatting the storage device will wipe all stored footage. Download any footage you wish to retain before beginning the format process.
Format (ext3)	Use *ext3* format for the selected device. Format progress will be displayed. **WARNING:** Re-formatting the storage device will wipe all stored footage. Download any footage you wish to retain before beginning the format process.
Mount	Mount the currently selected device. This option is only available if the currently selected device is inactive.
Eject	Eject the currently selected device. This option is only available if the selected device is mounted.

6 Live and Search (Playback) Tabs

6.1 Live Tab

After logging into the camera's browser interface, a user may view live video from the camera. To view live video:

Steps:

1). Select the **Live** tab at the top-left of the camera's browser interface.

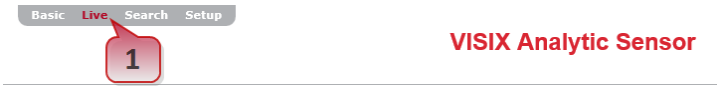


Figure 6-1: Opening the Live Tab

This will open the camera's **Live Viewer**.

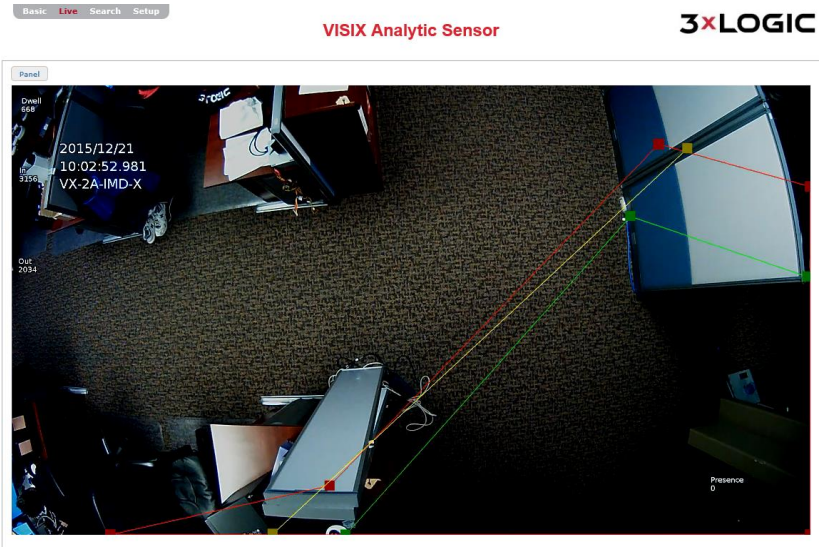


Figure 6-2: Live Tab

LIVE VIEWER – OPTIONS PANEL – OPTIONS TAB

Steps:

1). Clicking the **Panel** button and selecting the **Options** tab will open the **Options** panel.

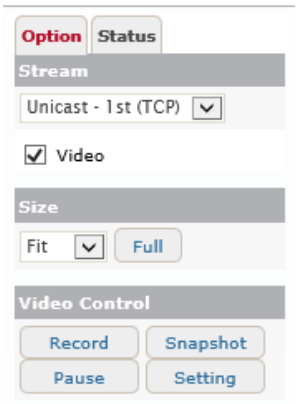


Figure 6-3: Live Tab Options

Live Viewer options are described below:

Option	Description
Stream	Select the stream and protocol type (UDP or TCP). **Unicast and Multicast** (UDP only) stream types can be selected can be applied to either the 1st (Main) or 2nd (Sub) streams. **EXAMPLE:** If a user selects **Unicast – 2nd (TCP)** the live stream will be unicast, using 2nd (sub) stream profile settings and UDP as its transmission layer protocol.
Size	Select the video size. Select **Fit** to stretch the image to fit your browser. Select a percentage to display the image at the selected percentage of its native resolution.
Video Control	Live view video controls are as follows: ■ **Record –** Click **Record** to begin recording a footage file separate of recording settings or the current recording mode. When you have recorded sufficient footage, click the **Stop** button. The recorded file will be automatically downloaded to your local system's **My Document/Documents** folder by default. This destination can be edited in the **Video Options Panel>Settings** interface. ■ **Pause –** Pause the live viewer on the current frame ■ **Snapshot -** Click **Snapshot** to capture a still image of the current live frame. The snapshot will be automatically downloaded to your local system's **My Document/Documents** folder by default. This destination can be edited in the **Video Options Panel>Settings** interface. ■ **Settings –**Click this button to open the live video settings window. From this window, **Local Recording** and **Snapshot** settings can be configured. a. **Local Recording –** Edit local recording settings including local recording destination (click **Browse** and select a destination on your local system), filename prefix, recording resources and maximum file size/duration. See Section 0 for more detailed information regarding recording settings. ■ **Snapshot –** Edit snapshot settings including snapshot export destination (click **Browse** and select a destination on your local system), and filename prefix.

LIVE VIEWER – OPTIONS PANEL – STATUS TAB

Steps:

1). Clicking the **Panel** button and selecting the **Status** tab will open the **Status** panel. From the **Status** panel, a user may view the below at-a-glance information related to the live video stream.

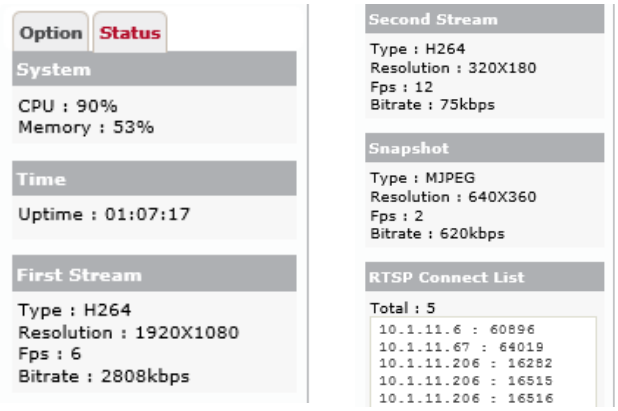


Figure 6-4: Live Tab Status

6.2 Search (Playback) Tab

After logging into the camera's browser interface, a user may search for and view playback (recorded) footage from the camera. To open the Search tab:

Steps:

1). Select the Search tab link at the top-left of the camera's browser interface.

Figure 6-5: Opening the Search (Playback) Tab

This will open the Playback Search form and viewing area.

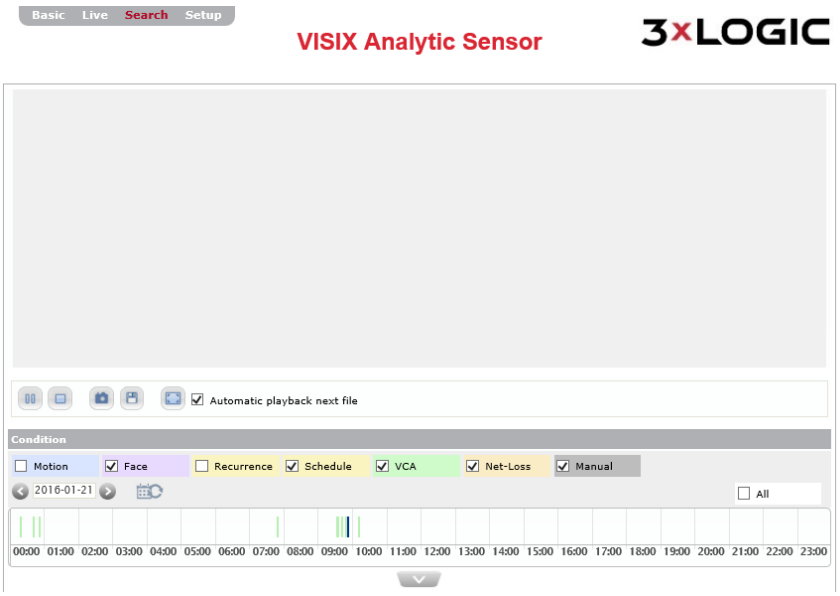


Figure 6-6: Search (Playback) Tab

When searching for playback, the following controls may be utilized:

Search Tools	Description
	Select the date (timerange) for your search. Footage will be searched from 00:00-24:00 on the selected day.
	Click this button to re-run the search using any new search parameters that have been changed.
Conditions	Conditions can be used similar to traditional search filters. Selecting specific conditions will filter out any footage files that do not meet the conditional requirements. (e.g. If **VCA** and **Motions** are selected, then only playback clips recorded due to **VCA** and/or **Motion** event triggers will be returned by the search. All search **Conditions** will be enabled by default.). The background color of each conditional check-box will also be used to identify clips of a specific condition within the visual search result timeline.

When the **Search** tab opens initially, a search using all **Conditions** will be performed by default.

To perform a custom search:

Steps:

1). Set the day (search time range is automatically set to the current day).

2). Select your desired conditions

3). Click the  button to run the search.

A **Visual Search Result Timeline** (see below example), color coded according to conditions, will be visible. Click within the timeline and use the mouse scroll-wheel to zoom in and out of the timeline to expand or narrow down the visible time range.

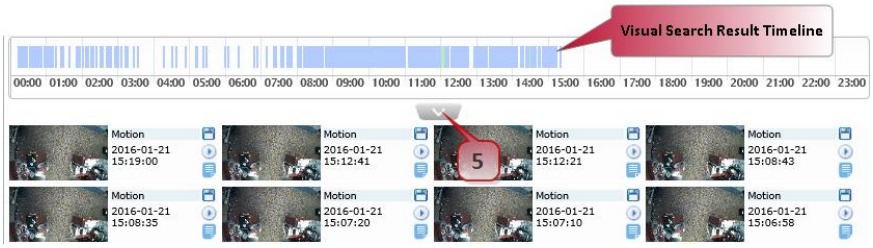


Figure 6-7: Visual Search Result Timeline and Search Result Thumbnails

4). Click the context arrow to reveal all search results as thumbnails.

Each search result thumbnail features the following file controls:

File Control	Description
- Download	Download the file to your browsers Downloads directory.
- Playback File	Playback the file in the viewer.
- Recording File Info	Mouse-over this icon to deploy a pop-up featuring metadata and duration info for the selected footage. **Recording File Information** Description(md): zone1, status=detect Duration: 00:00:13

5). To playback video, click the button next to the search result thumbnail for the desired file. The file will begin playback in the viewing area.

Figure 6-5: Video File Playback

When viewing playback, the followings tools may be utilized:

Playback Tools	Description
	Standard playback controls: **Play, Stop, Pause**.
	Click this button to download a snapshot of the current frame to your local system.
	Click this button to download the clip to your current system
	Click this button to view the video in full-screen mode
Automatic Playback Next File	Check-off this box to playback all available files sequentially in the order they were recorded. A file must be selected and manually started to begin the sequence.

6). Use the navigation controls at the bottom of the page to navigate multiple pages of search results.

7 Setup (Advanced) Tab

To configure advanced device settings, select the **Setup** (displayed as **Advanced** on some firmware versions) tab.

Figure 7-1: Opening the Setup (Advanced Settings) Tab

The left-side drop-down menu will now be populated with several new settings categories for advanced users wishing to customize advanced image/video, network, event, VCA and maintenance settings.

7.1 Basic Configuration Menu

USERS

Steps:

1). Opening the **Setup Tab>Basic Configuration** drop-down menu and clicking the **Users** link will open the **Users** settings page.

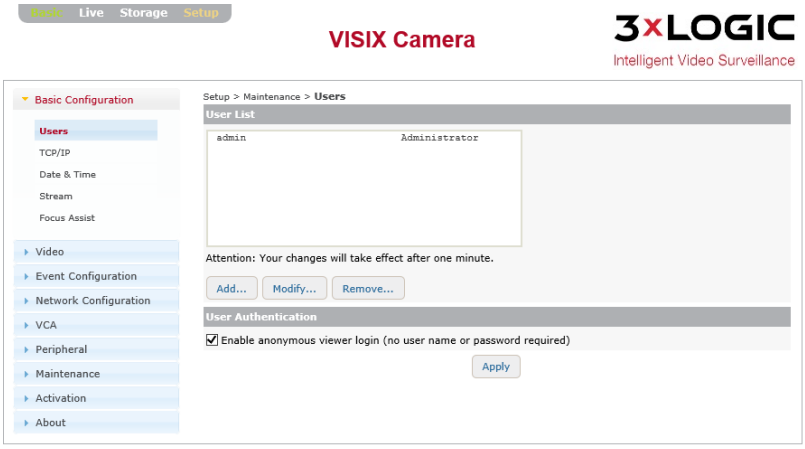


Figure 7-2: Setup Tab – Basic Configuration Menu – Users Settings

2). From the **Users** page, a user may view the camera's list of user profiles. A user may also add, modify or remove a user profile. Details regarding each action are outlined in the proceeding sub-sections of this manual. User settings can also be edited from the **Basic Tab>Camera Configuration>Users** settings page.

ADD A USER

Steps:

1). Click the **Add…** to add a new user profile. The Add User form (pictured right) will deploy.

Form Field	Description
Username and Password	Enter a username and password for the new user.
Confirm Password	Confirm the previously entered password.
User Group	Choose a User Group for the user.

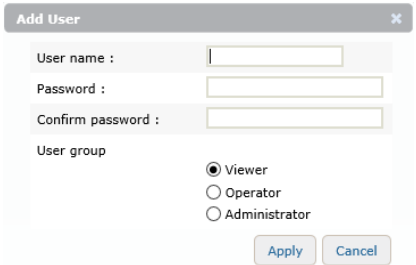


Figure 7-3: Add a User

2). After finishing configuration, click **Apply** to save the new settings.

MODIFY A USER

Steps:

1). Click the **Modify…**button to modify an existing user profile. The **Modify User** form (pictured right) will deploy.

Form Field	Description
Username and Password	Enter a username and password for the new user.
Confirm Password	Confirm the previously entered password.
User Group	Choose a User Group for the user.

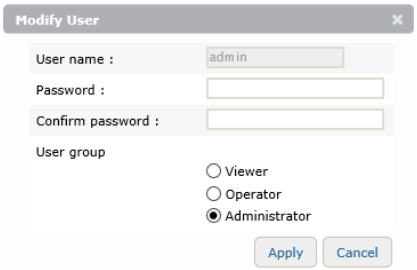


Figure 7-4: Modify a User

2). After finishing configuration, click **Apply** to save the new settings.

REMOVE A USER

Steps:

1). Click the **Remove** button to remove an existing user profile. This action is only available when a user profile is selected in the list.

2). You will be prompted for a confirmation before finalizing the removal.

USER AUTHENTICATION

Steps:

1). Check-off **Enable Anonymous Viewer Login** to enable anonymous viewing (no username or password required) of the camera's live view.

TCP/IP

Steps:

1). Opening the **Setup Tab>Basic Configuration** drop-down menu and clicking the **Users** link will open the Users settings page.

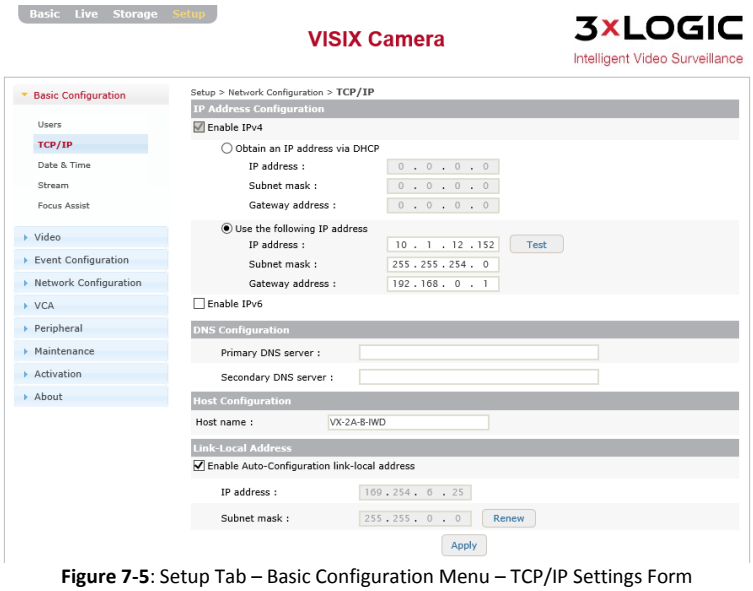


Figure 7-5: Setup Tab – Basic Configuration Menu – TCP/IP Settings Form

2). From the **TCP/IP** settings page, a user may edit a camera's **TCP/IP settings**. This includes all configurable settings from the **Basic Tab>Camera Configuration> Network** settings page (**IP Settings, DNS Server settings**) as well as the ability to enable IPv6 and configure host name and local link address details.

Network Setting	Description
IP Address Configuration	Select the method by which the cameras will obtain an IP address: **Obtain an IP Address via DHCP** – Select this method to have your router's DHCP function automatically assign the camera's network connection settings. This method is enabled by default. The automatically-generated **IP, Subnet Mask and Gateway** addresses will be listed directly underneath. **Use the following IP Address (Manual Configuration**) – Select this option to manually enter network connection settings. **IP Address, Subnet Mask and Gateway Addresses** can be manually entered directly underneath this setting. Clicking the **Test** button will confirm the validity of the network connection addresses you have entered. To enable IPv6 protocol, click **Enable IPv6**. For more information on IPv6 settings, see IPv6 Settings Configuration, below.
DNS Configuration	Enter in **Primary and Secondary DNS Server** connection information.
Host Configuration	Configure the device host name.
Link – Local Address	Checking-off **Enable Auto-configuration Link-Local Address** will generate an alternate internal IP address which can also be used to connect to the camera, access the UI via browser, etc... when on the same network as the camera.

BASIC CONFIGURATION MENU - TCP/IP SETTINGS - IPV6 SETTINGS CONFIGURATION

Steps:

a. When the enable IPv6 box is checked, IPv6 settings fields will deploy (pictured below).

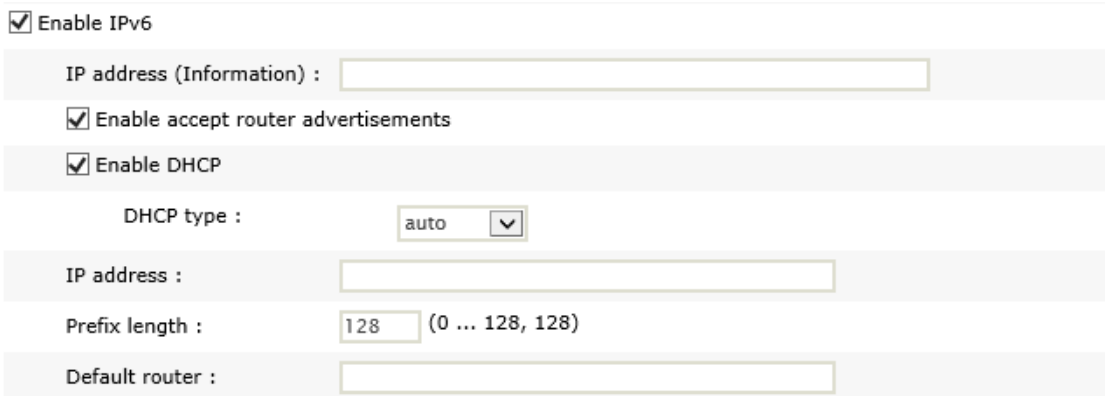


Figure 7-6: Setup Tab – Basic Configuration Menu – TCP/IP Settings – IPv6 Settings

IPv6 Setting	Description
Enable Accept Router Advertisements	**Enable Accept Router Advertisements** will allow the camera to accept router advertisements, signaling device availability and connectivity to the host router.
Enable DHCP	**Enable DHCP** for automatic IP address assignment. Select a **DHCP Type** from the drop-down menu.
IP Address	The device IP address. If DHCP is not enabled, the user may assign an address.
Prefix Length	Assign an address prefix length.
Default Router	Enter the default router address

DATE & TIME

Steps:

1). Opening the **Setup Tab>Basic Configuration** drop-down menu and clicking the **Date & Time** link will open the **Date & Time** settings page.

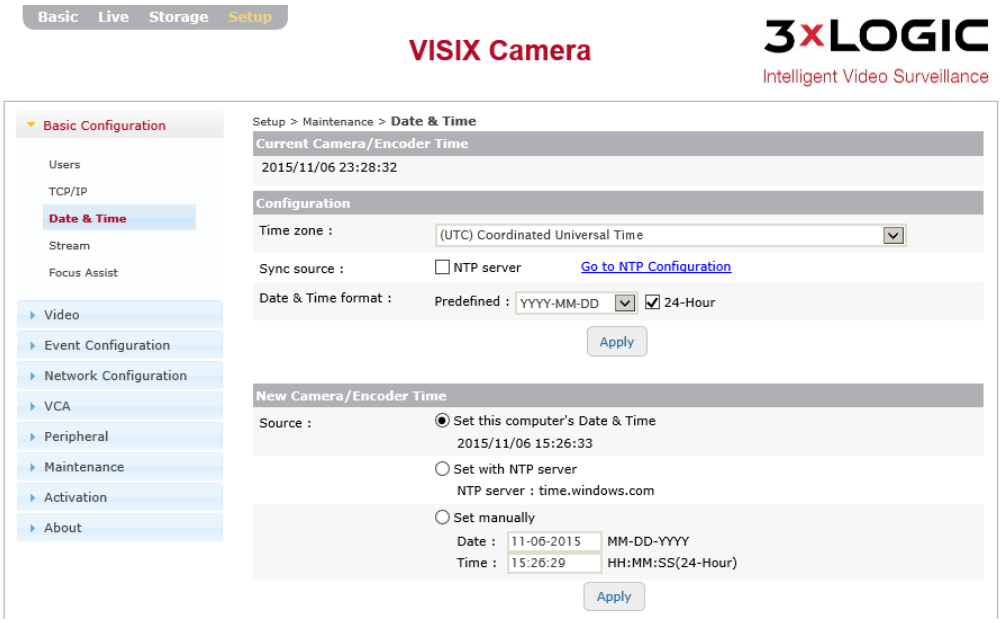


Figure 7-7: Setup Tab – Basic Configuration Menu – Date & Time Settings

2). From the **Date & Time** settings page, a user may edit a camera's time settings including time zone, time server, date and time format and time synchronization source.

Time Setting	Description
Current Camera Encoder Time	Displays the current camera time
Configuration	■ **Time Zone -** Select the camera time zone. ■ **Sync Source -** Set the active NTP server as your time sync source. Click the **Go to NTP Configuration** to be taken to the NTP Settings page. ■ **Date and Time Format –** Choose a predefined date-format. Enable **24-Hour** to use standard 24 hour time.
New Camera / Encoder Time	■ **Set this Computer's Date and Time –** Selecting this option will sync the camera's time with your current computer system. ■ **Set with NTP Server -** Selecting this option will sync the camera's time with the displayed NTP server (Default: time.windows.com) ■ **Set Manually –** Select this option to manually configure the camera's date and time.

3). Click **Apply** to save the new time settings.

STREAM

Steps:

1). Opening the **Setup Tab>Basic Configuration** drop-down menu and clicking the **Stream** link will open the **Stream** settings page.

NOTE:
Advanced stream settings can also be accessed from the **Setup Tab>Video Menu> Stream** link.

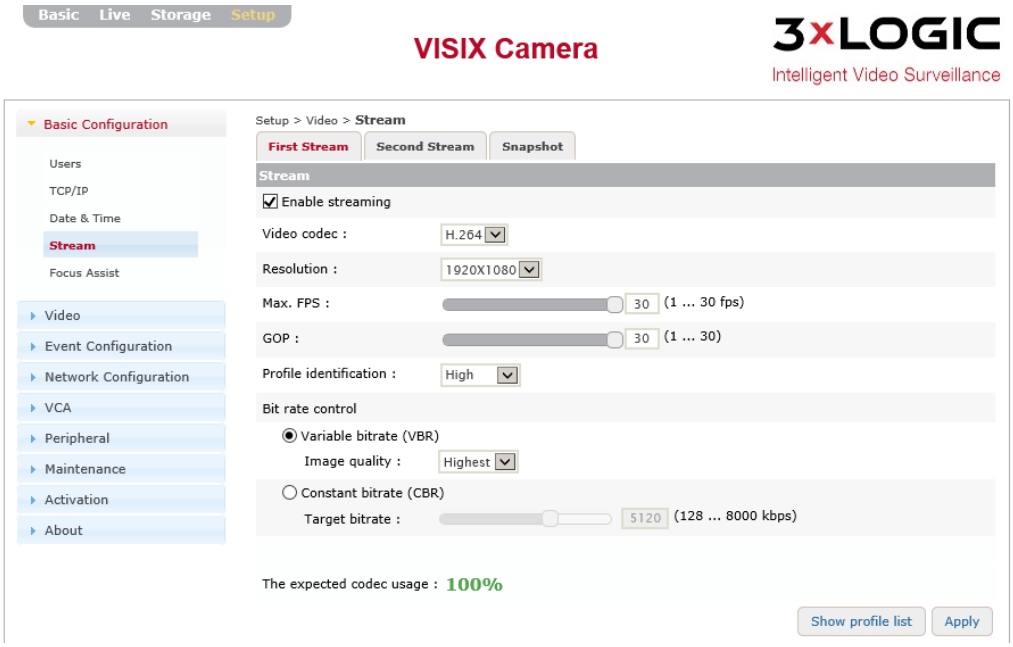


Figure 7-8: Setup Tab – Basic Configuration Menu – Stream Settings

STREAM SETTINGS

Select your desired stream profile tab (First/Main, Second/Sub) and check-off **Enable Streaming** to enable the chosen stream. In most cases, high quality image settings are reserved for the main/first stream, while lower quality, less bandwidth-intensive settings are reserved for the second/sub I stream.

The following settings can be configured for your chosen stream.

Stream Setting	Description
Video Codec	Select the stream's video codec from the options in the drop-down menu.
Resolution	Select the stream's video resolution from the options in the drop-down menu.
Max FPS	Set the maximum Frames per Second value for the selected stream.
GOP	Set the Group of Picture value (I-Frame interval) for the selected stream.
Profile Identification	
Bit Rate Control	Configure bit rate settings for the selected streams: ■ **Variable Bitrate (VBR) –** Have the camera adjust bitrate for the selected stream based on an image quality preference. Choose your preference from the drop-down. ■ **Constant Bitrate (CBR) –** Configure a target bitrate for the selected stream.

Steps:

1). Click the **Show Profile List** button for a list of preexisting encoder profiles. Existing profiles can be loaded by selecting them from the list and clicking **Load Profile Setting**s. Encoder profiles can be configured from the Encoder Profiles settings form (**Setup Tab>Video Menu>Encoder Profile**).

2). Click **Apply** to save new settings changes.

SNAPSHOT SETTINGS

Steps:

1). Click the Snapshot tab to open the **Snapshot** settings. Snapshot (still image) settings can be configured from this form.

Figure 7-9: Setup Tab – Basic Configuration Menu –Snapshot Stream Settings

2). Click the **Enable** button to enable camera still shots via the camera browser interface (VIGIL utilities interfaced with the device such as VIGIL Client can take snapshots regardless of the camera settings).

The following settings can be configured for camera snapshots:

Snapshot Setting	Description
Resolution	Select the snapshot image resolution from the options in the drop-down menu.
Max FPS	Set the maximum **Frames per Second** value for snapshot images using the slider. The smaller FPS range of 1-5 helps to prevent incorrect still shots from lag or delay. 1 is the default setting and is recommended for nearly all use-cases.
JPEG Quality	Set the JPEG quality value for snapshot images using the slider.

FOCUS ASSIST

Steps:

1). Opening the **Setup Tab>Basic Configuration** drop-down menu and clicking the **Stream** link will open the **Stream** settings page.

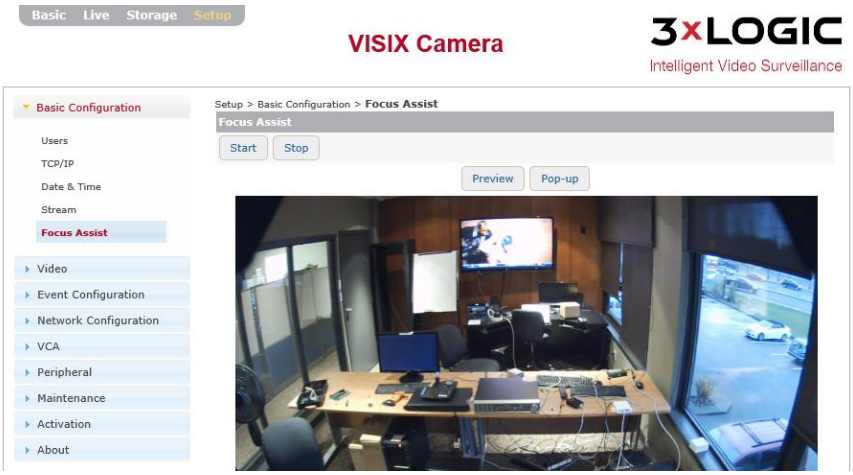


Figure 7-10: Setup Tab – Basic Configuration Menu – Focus Assist Settings

2). The **Focus Assist** tool is an auto-focus function intended to aid the user in achieving optimal lens focus to obtain the clearest image possible. Click **Start** to begin the focus assist process. When the image attains the desired focus level, click **Stop**.

3). Click **View** to close or open the video preview. Click **Pop-Up** to open the video preview in a separate browser window.

7.2 Video Menu

CAMERA

Steps:

1). Opening the **Setup Tab>Video** drop-down menu and clicking the **Camera** link will open the **Camera** settings page. A video preview is available at the bottom of the settings form. When configuring the settings described below, be sure to scroll-down and check the video preview as necessary.

2). Click the **Apply** button at the bottom of the settings form (above the video preview) to apply settings changes. Click the **Preview** button to toggle the video preview on/off. Click the **Pop-Up** button to open the preview in a separate browser window.

GENERAL SETTINGS

Steps:

a. Under the **General** section, a user may set the device name.

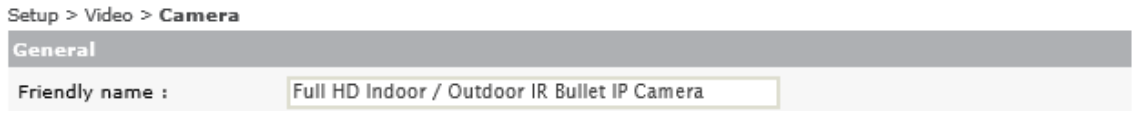


Figure 7-11: Setup Tab – Video Menu – Camera Settings – General

VIDEO APPEARANCE SETTINGS

Steps:

1). Under the **Video Appearance** sections, a user may adjust video image settings including **Brightness, Contrast, Saturation and Sharpness.**

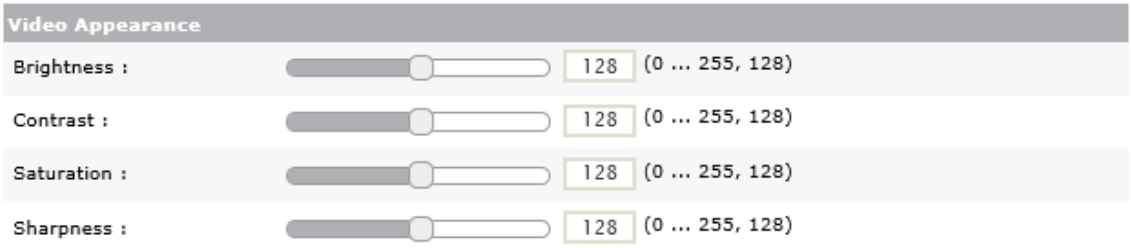


Figure 7-12: Setup Tab – Video Menu – Camera Settings – Video Appearance (Image) Settings

VIDEO TRANSFORM SETTINGS

Steps:

1). Under the **Video Transform** section, a user may vertical or horizontally flip their image by selecting the **Vertical Flip** or **Horizontal Mirror** option, respectively.

2). A digital image rotation (does not work with PTZ hardware) setting can also be chosen; **Left (-90 Degrees)** and **Right (+90 Degrees)**. This will digitally alter the image to give the appearance of a field-of-vision which has been rotated from the camera's actual fixed position.

Video Transformation settings may be automatically disabled depending on the presence of other camera settings. Conflicting settings will be listed (orange text, below).

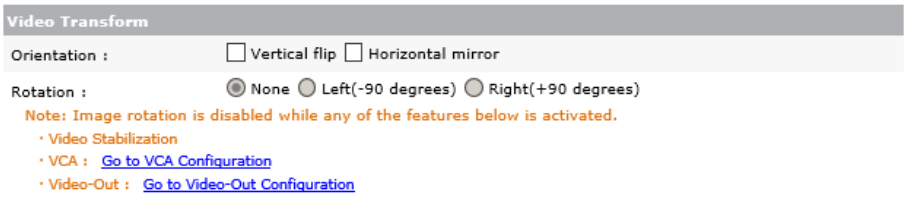


Figure 7-13: Setup Tab – Video Menu – Camera Settings – Video Transform

EXPOSURE SETTINGS

Steps:

1). Under the **Exposure** section, a user may configure the following settings:

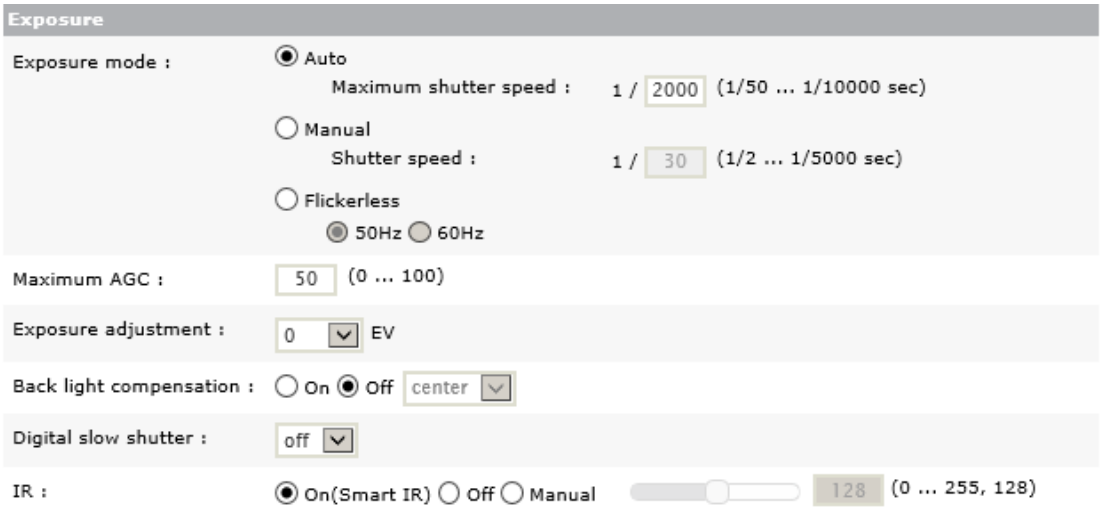


Figure 7-14: Setup Tab – Video Menu – Camera Settings – Exposure Settings

Exposure Setting	Description
Exposure Mode	▪ **Auto –** The camera will automatically adjust shutter speed based on environmental conditions and activity within the camera's field-of-vision. Configure a **Maximum Exposure Time** and **Minimum Exposure Time** to establish an operable range for automatic adjustments. ▪ **Manual –** Manually assign a static **Shutter Speed.** ▪ **Flickerless –** Enable **Flickerless** exposure mode. Set display system settings to either **PAL** (50Hz) or **NTSC** (60Hz). The optimal settings will depend on the monitor receiving the video output from the camera.
Maximum AGC	Configure the maximum **Automatic Gain Control** limit for the camera. Adjust this setting to improve image noise/snow distortion. The optimal setting will be dependent on the camera installation environment. The default setting is 50.
Exposure Adjustment	Configure the amount of exposure steps. One EV is to be considered one exposure step.
Backlight Compensation	Enable **Backlight Compensation**. Backlight compensation adjusts exposure to ensure a larger portion of the field-of-vision remains bright and visible when small areas of high illumination force the camera to decrease image brightness.
Digital Slow Shutter	Enable **Digital Slow Shutter**. The user may select the DSS speed from the drop-down menu. Increasing this setting will allow for a clearer picture in darker environment by allowing more than the normal amount of light into the camera lens.

Exposure Setting	Description
IR	Configure the Infrared settings for the camera. These settings are only available for camera models with IR capability. ■ **On (Smart IR) /Off –** Turn the cameras smart (auto) IR adjustment capability **On** or **Off.** ■ **Manual –** Manually configure the camera's IR sensor illumination level. Drag the slider to set the cameras IR illumination level. 128 is the default settings.

DIGITAL WIDE DYNAMIC RANGE SETTINGS

Steps:

1). Under the **Digital Wide Dynamic Range** section, a user may enable D-WDR and configure the dynamic range level between 1 and 16. 8 is the default setting.

Figure 7-15: Setup Tab – Video Menu – Camera Settings – D-WDR Settings

DAY & NIGHT SETTINGS

Steps:

1). Under the **Day and Night** section, a user may choose the cameras **Day/Night** mode setting.

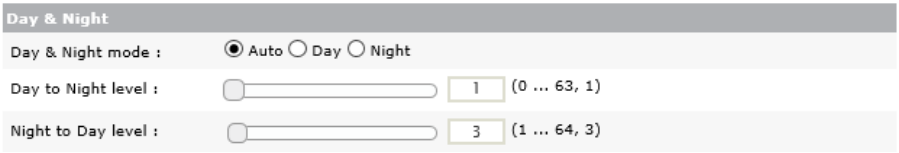


Figure 7-16: Setup Tab – Video Menu – Camera Settings – Day and Night Settings

Day and Night Setting	Description
Day and Night Mode	Place the camera in **Day** or **Night** mode. Select **Auto** to enable the camera to detect light conditions and auto-select the optimal mode accordingly.
Day to Night / Night to Day Level	Set the **Day to Night/Night to Day** light thresholds for the automatic day/night mode. Default values for **DtN** and **NtD** are 1 and 3, respectively.

WHITE BALANCE SETTINGS

Steps:

1). Under the **White Balance** section, a user may choose the cameras **White Balance Mode** setting from the drop-down. **Red** and **Blue** color temperature settings can also be adjusted using the slider bars.

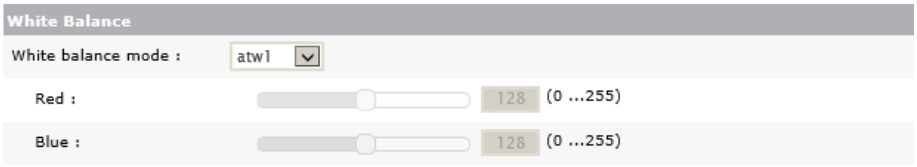


Figure 7-17: Setup Tab – Video Menu – Camera Settings – White Balance Settings

IMAGE SIGNAL PROCESSING SETTINGS

Steps:

1). Under the **Image Signal Processing** section, a user may configure the cameras **2D DNR (2 Dimension Dynamic Noise Reduction)** setting. Increasing this setting can reduce noise surrounding moving objects within the field-of-vision. Adversely, this can increase blurring and smudging around static objects.

2). If the camera is heated, **Defog** mode can also be enabled in this section. After enabling defog, the **Defog Level** can be selected in the drop-down menu.

Figure 7-18: Setup Tab – Video Menu – Camera Settings – Image Signal Processing Settings

3). The default setting is **3**.

VIDEO STABILIZATION SETTINGS

Steps:

1). Under the **Video Stabilization Settings** section, a user may enable Video Stabilization for any of the camera's stream profiles **(First/Main, Second/Sub, and Snapshot).** Check-off the box adjacent to each stream you wish to apply **Video Stabilization** too. The **Border Fill-In** setting can be chosen from the drop-down menu.

NOTE:

Video stabilization settings may be automatically disabled depending on the presence of other camera settings. Conflicting settings will be listed (orange text, below).

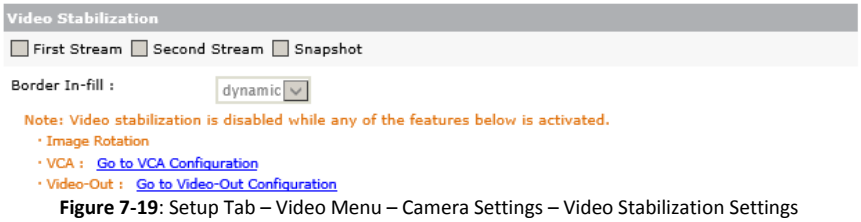


Figure 7-19: Setup Tab – Video Menu – Camera Settings – Video Stabilization Settings

BURNT-IN TEXT (OSD)

Steps:

1). Opening the **Setup Tab>Video** drop-down menu and clicking the **Burnt-In Text** link will open the **Burnt-In Text** (often referred to as On-Screen Display or OSD) settings page.

NOTE:

A video preview is available at the bottom of the settings form. When configuring the settings described below, be sure to scroll-down and check the video preview as necessary.

2). Click the **Apply** button at the bottom of the settings form (above the video preview) to apply settings changes. Click the **Preview** button to toggle the video preview on/off. Click the **Pop-Up** button to open the preview in a separate browser window.

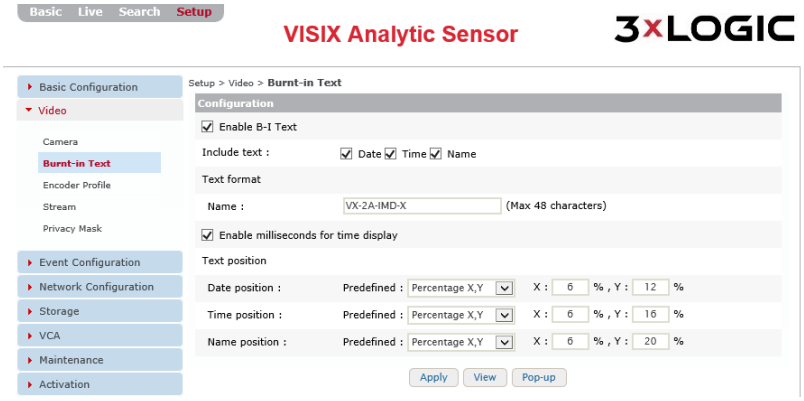


Figure 7-20: Setup Tab – Video Menu –Burnt-In Text Settings

3). From the **Burnt-In Text** settings page, a user can enable **B-I Text**.

The following related settings can be configured once BI-T has been enabled:

BI-T Setting	Description
Include Text	Designate info to be included in the on-screen text. Choose from **Date, Time and Name**.
Text Format	Configure the **Name text**. I.E Camera model name or description (Entrance 2)
Text Position	Configure the positions of the **Date, Time and Name** text. Select a preconfigured position from the drop-down or designate custom positions using standard X and Y screen coordinates.

ENCODER PROFILE

Steps:

1). Opening the **Setup Tab>Video** drop-down menu and clicking the **Encoder Profile** link will open the **Encoder Profile** settings page.

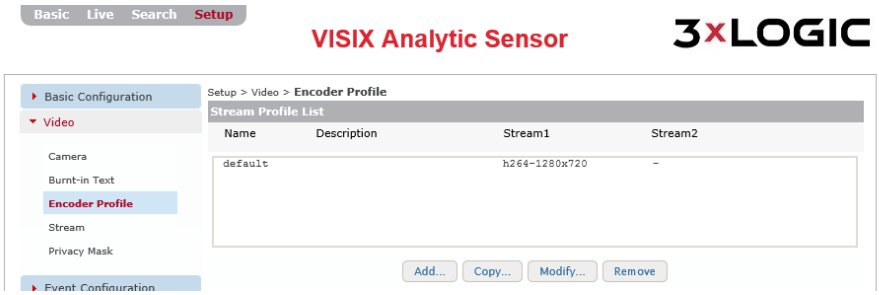


Figure 7-21: Setup Tab – Video Menu –Encoder Profile Settings

2). From the **Encoder Profile** settings page, a user may **Add**, **Copy**, **Modify** or **Remove** an **Encoder Profile.** An Encoder profile is a stream settings profile that delineates camera stream settings based on pre-configured customized settings.

3). To **Copy…** or **Remove….** an existing profile, select the profile from the list and click the corresponding button.

For information on adding or modifying a profile, proceed through the following section of this manual.

ADDING OR MODIFYING AN ENCODER PROFILE

Steps:

1). To create or modify a new encoder profile, click the **Add…** button (if modifying, select the desired profile from the list and click **Modify…**). This will deploy the below stream settings form.

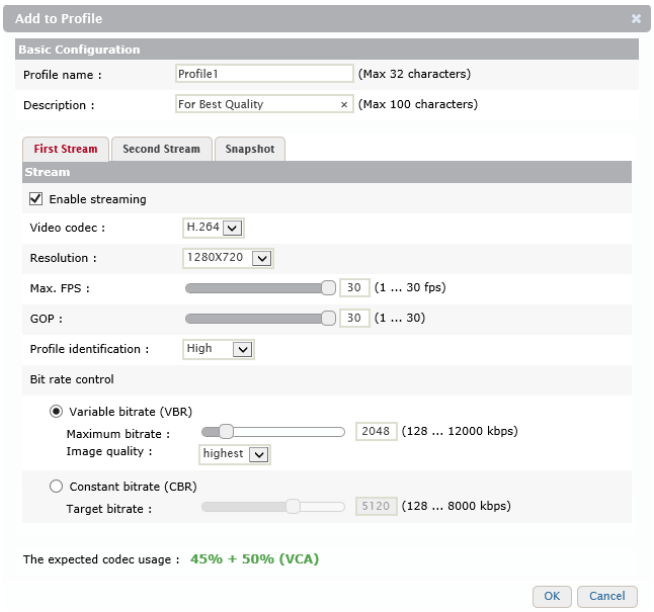


Figure 7-22: Setup Tab – Video Menu –Encoder Profile Settings – Adding/Modifying an Encoder Profile

2). Assign/edit **Profile Name** and **Description** at the top of the form and then configure stream settings. For more details on stream settings, please see the Setup Tab > Basic Configuration Menu> Stream Settings section.

3). Click **OK** to save the new **Encoder Profile**.

STREAM

Steps:

1). Opening the **Setup Tab>Video** drop-down menu and clicking the **Stream** link will open the **Stream** settings page.

NOTE:
The advanced stream settings form can also be accessed from the **Setup Tab> Basic Configuration Menu> Stream** link.

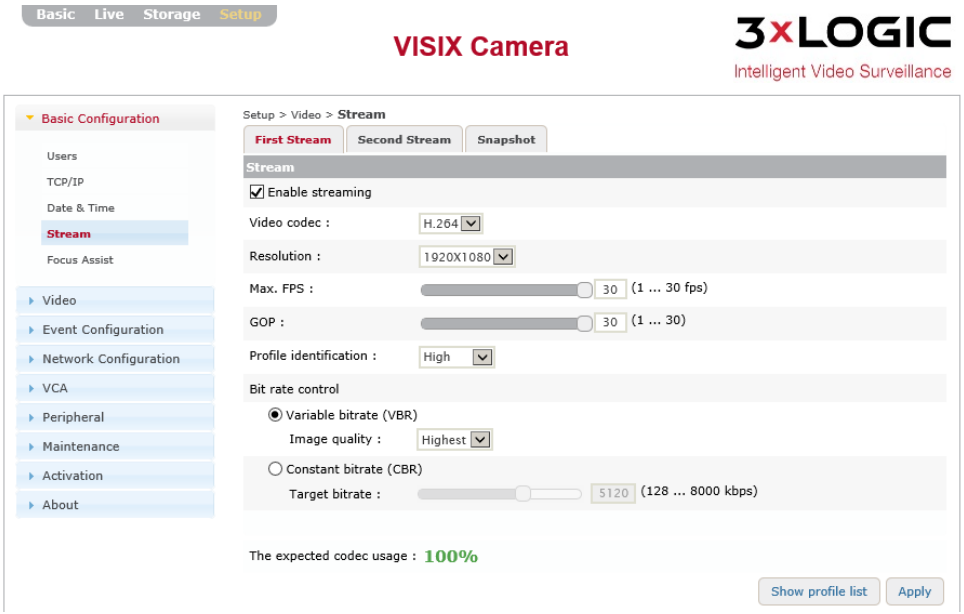


Figure 7-23: Setup Tab – Video Menu –Stream Settings

STREAM SETTINGS

Select your desired stream profile tab (First/Main, Second/Sub) and check-off **Enable Streaming** to enable the chosen stream. In most cases, high quality image settings are reserved for the main/first stream, while lower quality, less bandwidth-intensive settings are reserved for the second/sub stream.

The following settings can be configured for your chosen stream:

Stream Setting	Description
Video Codec	Select the stream's video codec from the options in the drop-down menu.
Resolution	Select the stream's video resolution from the options in the drop-down menu.
Max FPS	Set the maximum Frames per Second value for the selected stream.
GOP	Set the Group of Picture value (I-Frame interval) for the selected stream.
Profile Identification	
Bit Rate Control	Configure bit rate settings for the selected streams: ■ **Variable Bitrate (VBR) –** Have the camera adjust bitrate for the selected stream based on an image quality preference. Choose your preference from the drop-down. ■ **Constant Bitrate (CBR) –** Configure a target bitrate for the selected stream.

Steps:

1). Click the **Show Profile List** button for a list of preexisting encoder profiles. Existing profiles can be loaded by selecting them from the list and clicking **Load Profile Settings**. Encoder profiles can be configured from the Encoder Profiles settings form **(Setup Tab>Video Menu>Encoder Profile)**.

2). Click **Apply** to save new settings changes.

PRIVACY MASK

Steps:

1). Opening the **Setup Tab>Video** drop-down menu and clicking the **Privacy Mask** link will open the **Privacy Mask** settings page.

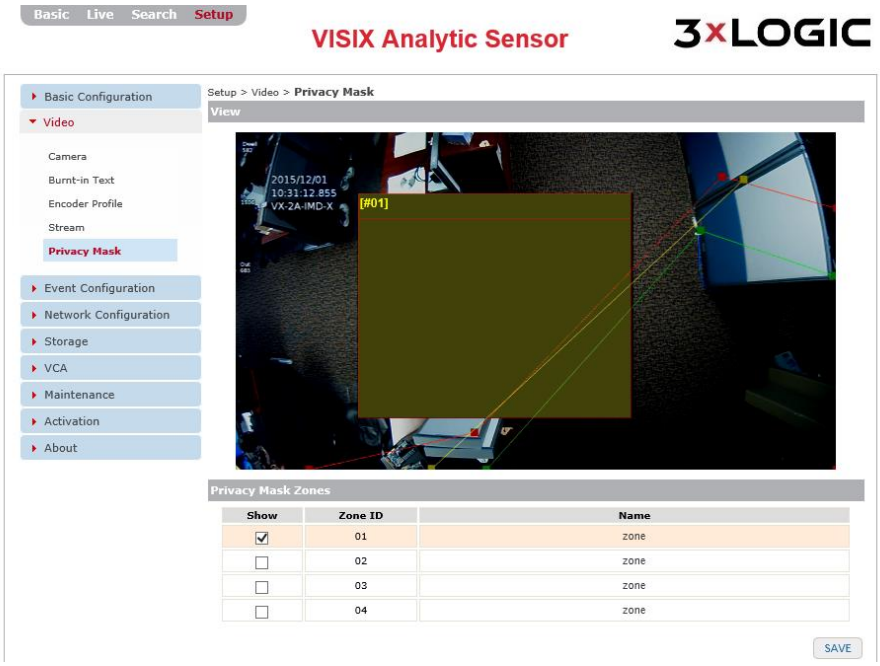


Figure 7-24: Setup Tab – Video Menu –Privacy Mask Settings

From the **Privacy Mask** settings, a user may draw up to four privacy masks within the camera image. A privacy mask obscures a portion of camera image in both live and recorded footage.

2). To enable a privacy mask, check-off the box in the **Show** column for the desired **Privacy Mask.** The privacy mask zone will deploy over the preview image.

3). Place and resize the zone as required.

4). Click the **Save** button at the bottom-right of the page to save the new privacy mask.

VIDEO OUT (BNC)

Steps:

1). Opening the **Setup Tab>Video** drop-down menu and clicking the **Video Out** link will open the **Video Out** settings page. **Video Out** settings will only be available on cameras with a BNC Video Out connection.

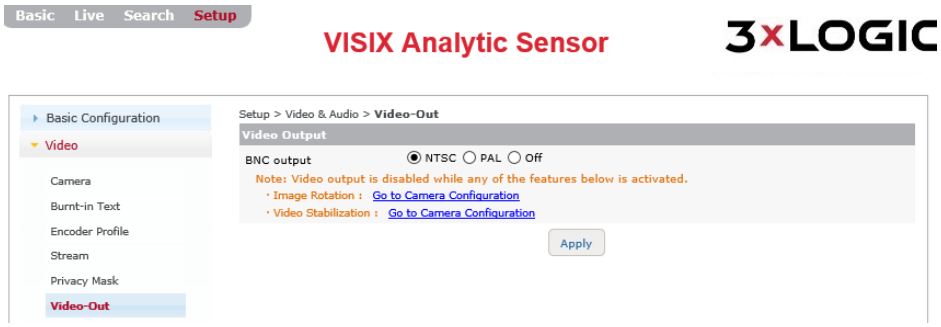


Figure 7-25: Setup Tab – Video Menu –Video Out (BNC) Settings

2). Select the BNC output mode. Choose between **NTSC (60Hz)** or **PAL (50Hz, auto color correction)**. The optimal setting is dependent on the monitor receiving the video output from the camera.

7.3 Event Configuration Menu

EVENT RULES

Steps:

1). Opening the **Setup Tab>Event Configuration** drop-down menu and clicking the **Event Rules** link will open the **Event Rules** settings page.

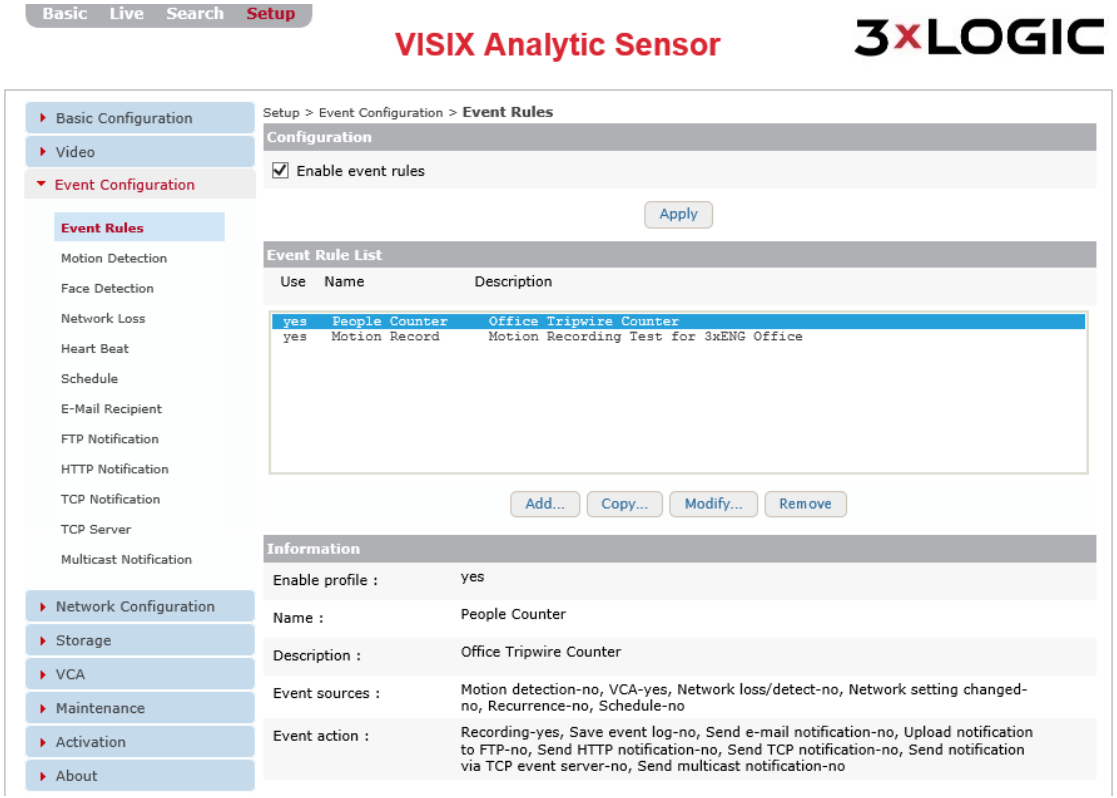


Figure 7-26: Setup Tab – Event Configuration – Event Rules Settings

2). From the **Event Rules** settings page, a user may enable and subsequently **Add** a new event rule. A user may also **Copy, Modify or Delete** and existing event rule.

3). To enable, check-off the **Enable Event Rules** box.

4). Select a rule from the list to display its **Event Source** and **Event Action** specifications under the **Information** section.

By default, VISIX V-Series All-in-One Camera's will have events enabled and with a single motion record rule configured, designed to trigger footage recording when motion is detected. This allows for recording directly out-of-the-box with no user interaction required.

5). To copy or delete an existing rule, select the desired rule from the list and click the **Copy…** or **Remove** button. You may be prompted to confirm the action. Click **OK** to confirm.

6). After adding, removing or modifying rules as desired, click the **Apply** button to save changes.

ADDING OR MODIFYING AN EVENT RULE

Steps:

1). To add an event rule, click the **Add…** button (if modifying, select the desired rule from the list and click **Modify…***).* The Add/Modify Event Rule window will deploy.

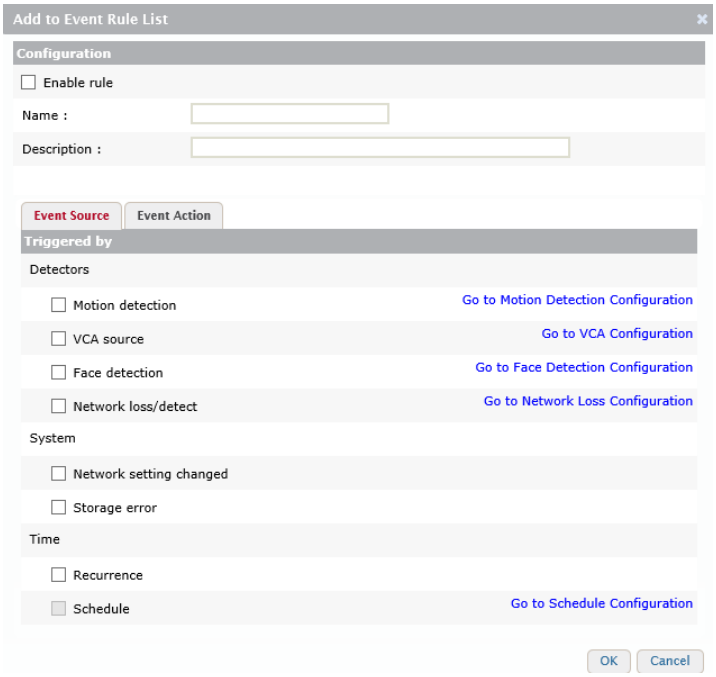


Figure 7-27: Setup Tab – Event Configuration Menu – Event Rules Settings – Adding/Modifying a Rule - Event Source Tab

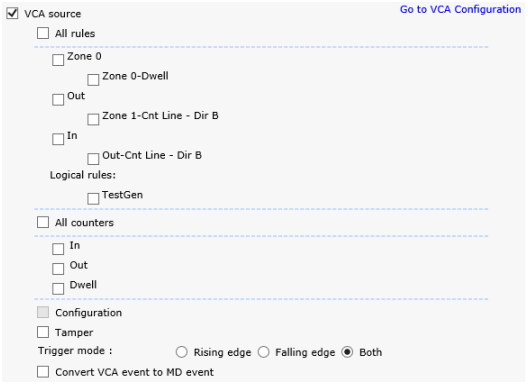
2). Check-off the **Enable** box.

3). Enter a **Name** and **Description** for the rule. This name will be used to reference this specific rule throughout the camera's browser interface.

EVENT SOURCE (TRIGGERS) TAB – ADDING/MODIFYING EVENT RULE

Steps:

1). Under the **Event Source** tab of the **Add/Modify Event Rule** form, the following event trigger settings can be configured:

Event Source (Trigger) Setting	Description
Motion Detection	Enable the rule to trigger based off of Motion Detection. Click the **Go to Motion Detection Configuration** to edit motion detection settings.
VCA Source	Enable to rule to trigger based off of a VCA (video analytics) source. (i.e. tripwire, customer not present, etc…) When this box is checked, an additional form will deploy allowing the user to pick specific VCA elements as trigger criteria (pictured below).  **Figure 7-28**: Setup Tab – Event Configuration Menu – Event Rules Settings – Event Source Tab - VCA Source Settings Available criteria will vary based on active VCA rules. A trigger mode can also be chosen. Select **Rising Edge** to trigger an event at the onset of a VCA rule being triggered. Select **Falling Edge** to trigger an event at the conclusion of an event being triggered (latched). Select **Both** to trigger an event rule regardless of the state of a VCA event. Click **Go to VCA Configuration** to edit video analytics rule settings.
Face Detection	Enable the rule to trigger based off of facial recognition of a specific person. Click **Go to Face Detection Configuration** to edit facial recognition settings.
Network Loss/Detect	Enable the rule to trigger whenever network signal loss is detected. Click **Go to Network Loss Configuration** to edit network loss settings.
Network Setting Changed	Enable this rule to trigger whenever a network setting change is detected.
Storage Error	Enable the rule to trigger whenever a storage error is detected.
Recurrence	Enable the rule to trigger on a reoccurring basis. When selected, the user will be able to assign a time interval for the reoccurring trigger.
Schedule	Enable the rule to trigger based on a schedule. The event rule will remain active only during the scheduled times. Click the **Go to Schedule Configuration** link to open the **Schedule** settings and configure a schedule as needed. The **Schedule** event source option will not be available until schedule settings have been properly configured.

EVENT ACTION TAB – ADDING/MODIFYING EVENT RULE

Steps:

1). Under the **Event Action** tab of the **Add/Modify Event Rule** form, the following event action settings can be configured:

Figure 7-29: Setup Tab – Event Configuration Menu – Event Rules Settings – Event Action Tab

Event Action Setting	Description
Recording	Enable this option to start recording footage when the rule is triggered. Recording options (**Prebuffer** and **Postbuffer** values, **Attach Thumbnail/Face Image** option) will be displayed when this rule is selected. Click **Go to Recording Configurations** to edit recording settings.
Save Event Log	Enable this option to save an event log when the rule is triggered. Navigate to **Setup Tab>Maintenance Menu> System Log** settings page for access to system event logs.
Send E -Mail Notification	Enable this option to have the camera send an email notification to a recipient of your choosing whenever the rule is triggered. Email notification options (**To** and **Subject** fields, **Attach Thumbnail/Face Image, Attach Snapshot options**) will be displayed when the rule is selected. An email recipient must be configured to enable this option. Click the **Go to E-Mail Recipient Configuration** link to edit recipient settings.
Upload Notification to FTP	Enable this option to have the camera upload a notification (JPEG image with timestamp) to an FTP whenever the rule is triggered. Click the **Go to FTP Notification Configuration** link to edit FTP connection settings.
Send HTTP Notification	Enable this option to have the camera send a push notification across an HTTP service whenever the rule is triggered. Click the **Go to HTTP Notification Configuration** link to edit HTTP connection settings.
Send TCP Notification	Enable this option to have the camera send a notification via TCP whenever the rule is triggered. Click the **Go to TCP Notification Configuration** link to edit TCP Notification settings.
Send Notification via TCP Event Server	Enable this option to have the camera send a notification via TCP Event Server whenever the rule is triggered. Click the **Go to TCP Server Configuration** link to edit TCP Server connection settings.
Send Multicast (UDO) Notification	Enable this option to have the camera broadcast a UDP Multicast notification whenever the rule is triggered. Click the **Go to Multicast Notification Configuration** link to edit Multicast Notification settings.

MOTION DETECTION

Steps:

1). Opening the **Setup Tab>Event Configuration** drop-down menu and clicking the **Motion Detection** link will open the **Motion Detection** settings page.

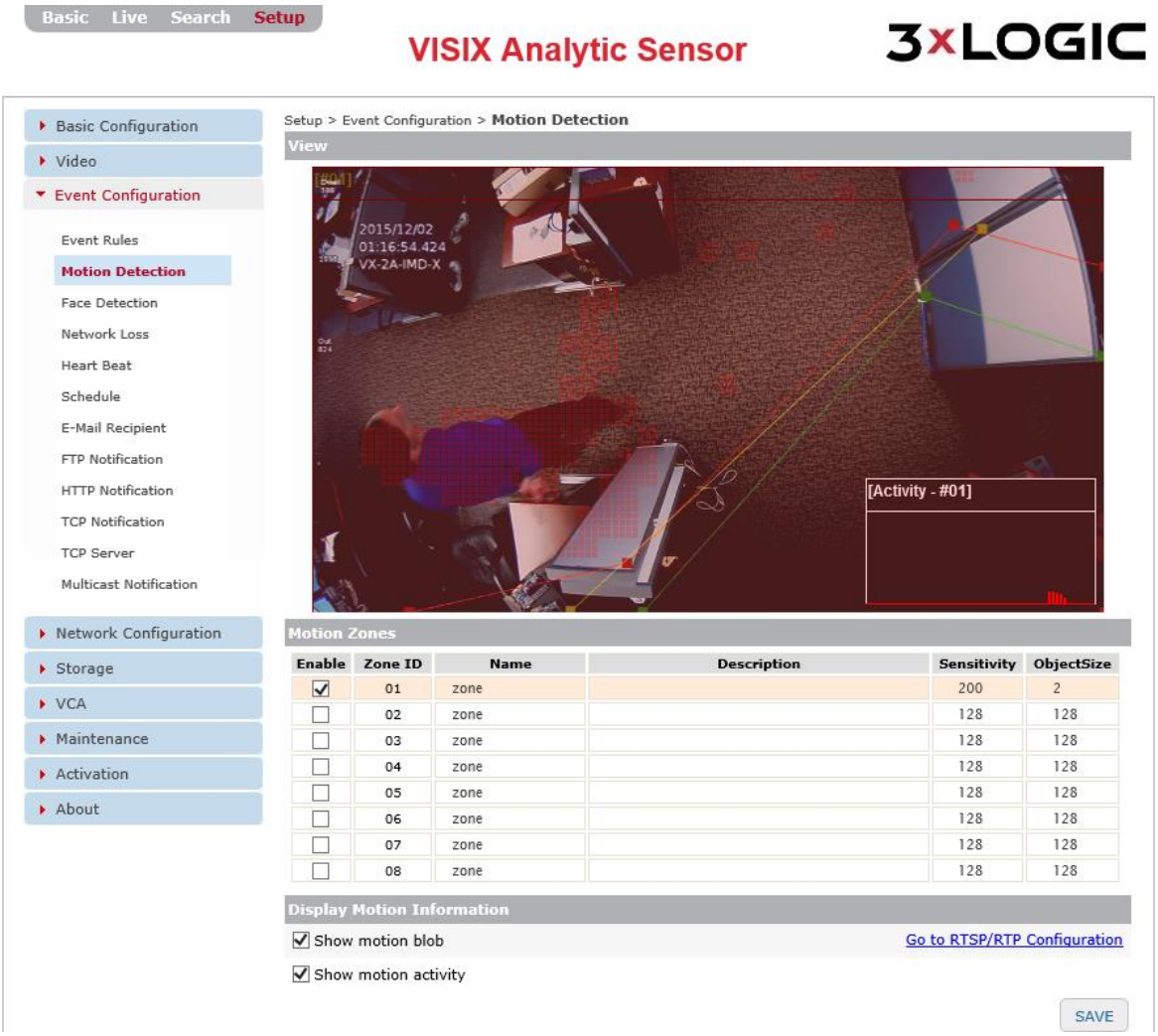


Figure 7-30: Setup Tab – Event Configuration Menu – Motion Detection Settings

2). From the **Motion Detection** settings page, a user may draw up to eight motion detection zones, and activate each as necessary.

3). Check off the **Enable** column box for the desired zone. This will deploy the zone over the image. Resize the zone as desired.

4). A Name, Description, Sensitivity and Object Size value can be assigned to each zone.

5). Enable **Show Motion Blob** to overlay a visualization of detected motion activity on the image (the red squares in the above example).

6). Enable **Show Motion Activity** to deploy a motion activity graph as a video overlay (bottom-right of the video preview in the above example). Motion activity will only be graphed when a motion detection zone is actively selected within the image.

7). Click the **Save** button to save changes to motion detection settings.

FACE DETECTION

Steps:

1). Opening the **Setup Tab>Event Configuration** drop-down menu and clicking the **Face Detection** link will open the **Face Detection** settings page.

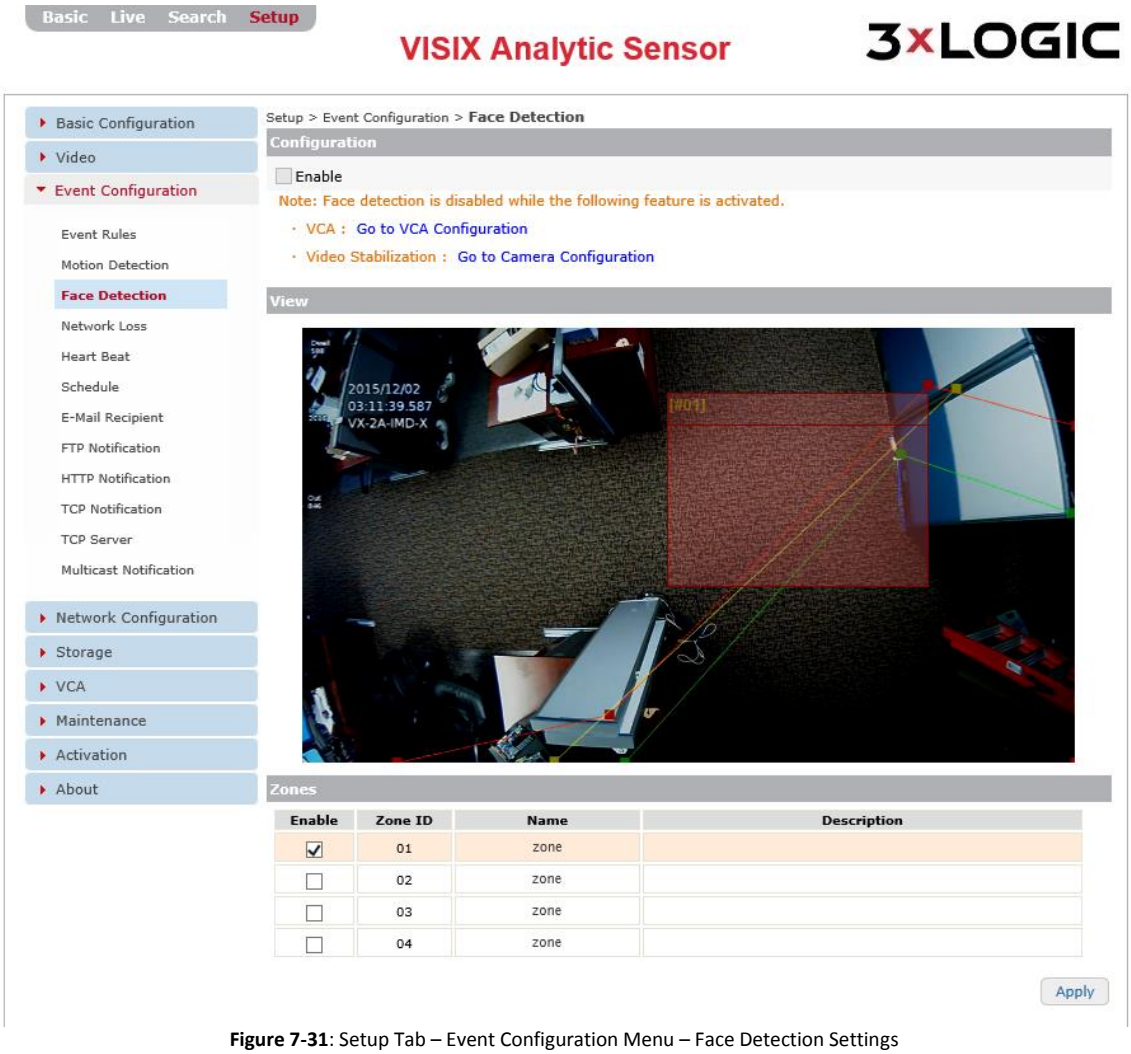


Figure 7-31: Setup Tab – Event Configuration Menu – Face Detection Settings

2). From the **Face Detection** settings page, a user may draw up to four facial detection zones, and activate each as necessary.

NOTE:

Do not confuse **Facial Detection** with **Facial Recognition**. Face detection merely detects the presence of a human face. There is no Facial Recognition algorithm. The camera cannot be configured to recognize specific faces.

3). Check off the **Enable** column box for the desired zone. This will deploy the zone over the image. Resize the zone as desired.

4). A **Name** and **Description** value can be assigned to each zone.

5). Click **Apply** to save any settings changes.

NETWORK LOSS

Steps:

1). Opening the **Setup Tab>Event Configuration** drop-down menu and clicking the **Network Loss** link will open the **Network Loss** settings page.

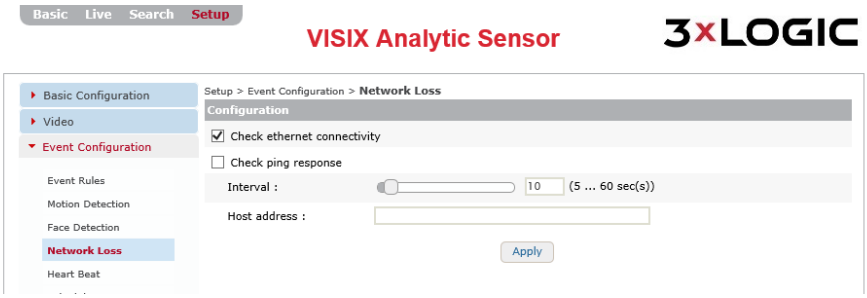


Figure 7-32: Setup Tab – Event Configuration Menu – Network Loss Settings

2). From the **Network Loss** settings page, a user may configure the following network signal loss settings:

Stream Setting	Description
Check Ethernet Connectivity	Enable the camera to check for Ethernet (physical) connectivity.
Check Ping Response	Enable the camera to check for network connectivity, via network ping.
Interval	Configure the time interval in between checks/pings.
Host Address	Enter the address of the device you would like the camera to ping. When this device cannot be reached/ a ping response is not received, the camera will fall into a network loss state.

3). Click **Apply** to save changes to network loss settings.

HEART BEAT

Steps:

1). Opening the **Setup Tab>Event Configuration** drop-down menu and clicking the **Heart Beat** link will open the **Heart Beat** settings page.

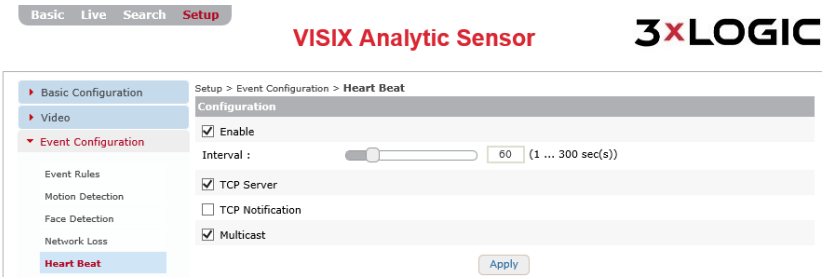


Figure 7-33: Setup Tab – Event Configuration Menu – Heart Beat Settings

2). In network and computer science, a **Heart Beat** is a periodic signal generated by hardware (or software) to indicate normal operation.

3). Check off **Enable** to activate a heartbeat signal from the camera.

After enabling, a user may configure the following options:

Stream Setting	Description
Interval	Configure the time interval between heart beat signal broadcasts.
TCP Server	Enable a heartbeat signal broadcast via TCP Event Server.
TCP Notification	Enable a heartbeat signal broadcast via TCP Notification.
Multicast	Enable a heartbeat signal broadcast via UDP Multicast.

4). Click **Apply** to save **Heart Beat** settings changes.

SCHEDULE

Steps:

1). Opening the **Setup Tab>Event Configuration** drop-down menu and clicking the **Schedule** link will open the **Schedule** settings page.

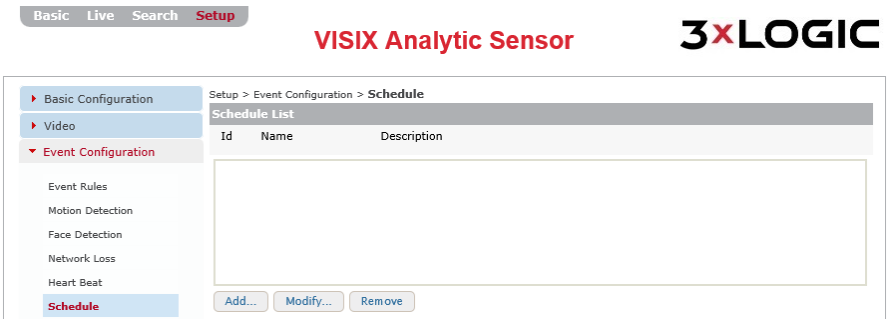


Figure 7-34: Setup Tab – Event Configuration Menu – Schedule Settings

2). From the **Schedule** settings page, a user may **Add**, **Modify** or **Remov***e* an event schedule. When associated with a schedule, an event will trigger only during the specified time range.

3). Select a schedule from the list to display Schedule information.

4). To remove a schedule, select the desired schedule from the list and click **Remove**.

ADDING/MODIFYING A SCHEDULE

Steps:

1). To add a schedule, click the **Add…** button (if modifying, select the desired schedule from the list and click **Modify…***).* The **Add to Schedule List** form will deploy.

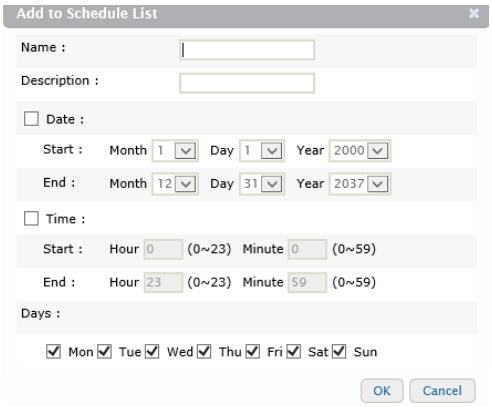


Figure 7-35: Setup Tab – Event Configuration Menu – Schedule Settings – Adding/Modifying Schedule

Schedule Setting	Description
Name	Name the schedule. This name will be used to identify this particular schedule when assigning it to an event.
Description	Provide a brief description of the schedule (intended use, etc…). This description will be displayed when the schedule is selected on the schedule settings page. .
Date	Check-off the **Date** box to enable. If enabled, a user may configure a **Start** and **End** date range for the schedule.
Time	Check-off the **Time** box to enable. If enabled, a user may configure a Start and End time range for the schedule.
Days	Select which days of the week to apply the schedule to.

2). After configuring the desired time range, click **OK** to save the new schedule.

E-MAIL RECIPIENTS

Steps:

1). Opening the **Setup Tab>Event Configuration** drop-down menu and clicking the **E-Mail Recipient** link will open the **E-Mail Recipient** settings page.

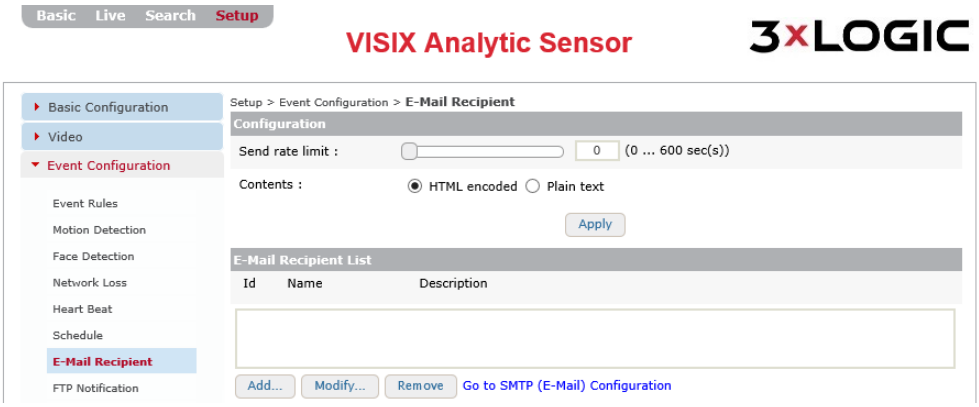


Figure 7-36: Setup Tab – Event Configuration Menu – E-Mail Recipients Settings

2). From the **E-Mail Recipients** settings page, a user may **Add, Modify or Remove** an e-mail notification recipient. General recipient settings may also be edited, including **Send Rate Limit** (minimum e-mail notification time interval) and content delivery modes (**HTML Encoded or Plain Text**).

3). Select a recipient from the list to display recipient information. To remove a recipient, select the desired recipient from the list and click **Remove.**

4). **SMTP (E-mail Server) Settings** must be configured in order for e-mail notifications to function. Click the **Go to SMTP (E-Mail) Settings** link to open the SMTP settings form and configure settings as necessary. See SMTP (E-Mail Server) Settings for more info.

ADD/MODIFY AN E-MAIL RECIPIENT

Steps:

1). To add a recipient, click the **Add…** button (if modifying, select the desired recipient from the list and click **Modify…**). The **Add/Modify E-Mail Recipient** form will deploy.

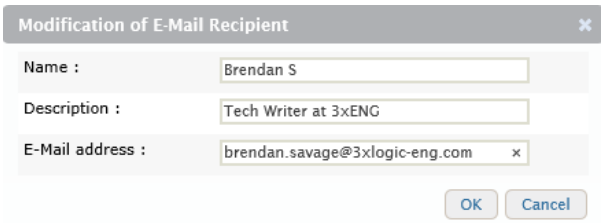


Figure 7-37: Setup Tab – Event Configuration Menu – E-Mail Recipients Settings - Add/Modify a Recipient

2). Fill in the **Name, Description and E-mail Address** fields for the desired recipient.

E-Mail Recipient Setting	Description
Name	Name the recipient. This name will be used to identify this particular recipient when assigning it to an e-mail notification.
Description	Provide a brief description of the recipient (intended use, etc…) This description will be displayed when the schedule is selected on the schedule settings page.
E-Mail Address	Enter the e-mail address of the recipient.

3). When you have filled in all the fields, click **OK** to save the new recipient.

FTP NOTIFICATION

Steps:

1). Opening the **Setup Tab>Event Configuration** drop-down menu and clicking the **FTP Notification** link will open the **FTP Notification** settings page.

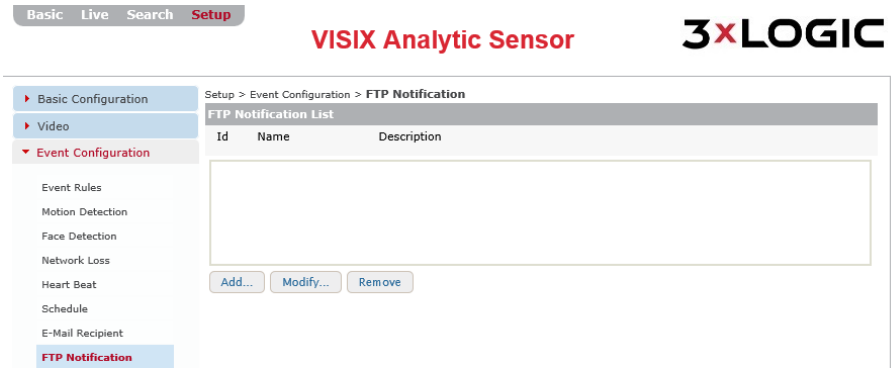


Figure 7-38: Setup Tab – Event Configuration Menu – FTP Notification Settings

2). From the **FTP Notifications** settings page, a user may **Add, Modify or Remove** an FTP Server. Notifications will be sent in the form of a .jpg image containing an image of the event and corresponding data (time stamp, camera name, rule, etc…)

3). To remove an existing FTP server, select it from the list and click **Remove**. You will be prompted to confirm. Click **OK** to confirm the removal.

ADD/MODIFY AN FTP SERVER

Steps:

1). To add an FTP Server, click the **Add…** button (if modifying, select the desired schedule FTP server from the list and click **Modify…***).* The **Add to/Modify FTP Notification List** form will deploy.

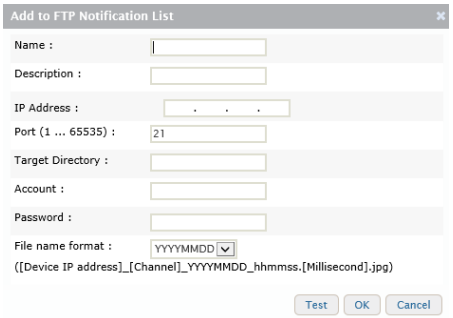


Figure 7-39: Setup Tab – Event Configuration Menu – FTP Notification Settings – Add/Modify an FTP

FTP Notification Setting	Description
Name	Name the FTP server. This name will be used to identify this particular FTP when assigning it to an e-mail notification.
Description	Enter a description for the FTP. This information will be displayed when the FTP is selected on the FTP Notification settings window.
IP Address/Port	Enter network connection values for the desired FTP Server.
Target Directory	Enter the target destination directory on the FTP for the FTP notifications.
Account / Password	Enter the user login credentials for the FTP. 3xLOGIC recommends using an administrative level account when possible to avoid permissions conflicts.
Filename Format	Assign the filename format for the .jpg notifications.

2). Click **Test** to test FTP connectivity. If the test fails, confirm the correct settings have been entered for the selected FTP server.

3). Click **OK** to save the new FTP server settings.

HTTP NOTIFICATIONS

Steps:

1). Opening the **Setup Tab>Event Configuration** drop-down menu and clicking the **HTTP Notification** link will open the **HTTP Notification** settings page.

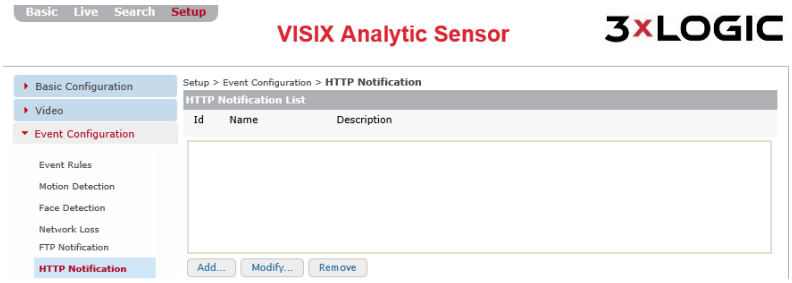


Figure 7-40: Setup Tab – Event Configuration Menu – HTTP Notification Settings

2). From the **HTTP Notifications** settings page, a user may **Add, Modify or Remove** an HTTP web server for receiving event notifications.

3). To remove an existing HTTP server, select the server from the list and click **Remove.** You will be prompted to confirm.

4). Click **OK** to confirm the removal.

ADD/MODIFY AN HTTP SERVER

Steps:

1). To add an HTTP web server, click the **Add…** button (if modifying, select the desired schedule HTTP server from the list and click **Modify…**). The **Add to/Modify HTTP Notification List** form will deploy.

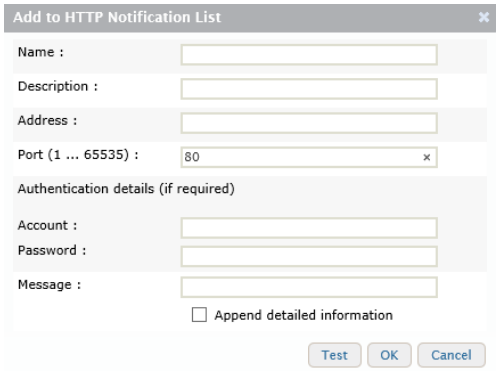


Figure 7-41: Setup Tab – Event Configuration Menu – HTTP Notifications – Adding/Modifying an HTTP Server

HTTP Notification Setting	Description
Name	Name the HTTP server. This name will be used to identify this particular HTTP server when assigning it to an e-mail notification.
Description	Enter a description for the HTTP server. This will be displayed when the HTTP server is selected on the HTTP Notification settings window.
IP Address/Port	Enter network connection values for the desired HTTP Server.
Account / Password	Enter the user login credentials for the HTTP server. 3xLOGIC recommends using an administrative level account when possible to avoid permissions conflicts.
Message	Enter a customized message to include with the notification.
Append Detailed Information	Enable this checkbox to append detailed information including event details, the custom **Message** field, etc…

2). Click **Test t**o test for a successful connection with the defined HTTP web server. Once you have configured your desired settings.

3). Click **OK** to save the newly configured HTTP web server.

TCP NOTIFICATIONS

Steps:

1). Opening the **Setup Tab>Event Configuration** drop-down menu and clicking the **TCP Notification** link will open the **TCP Notification** settings page.

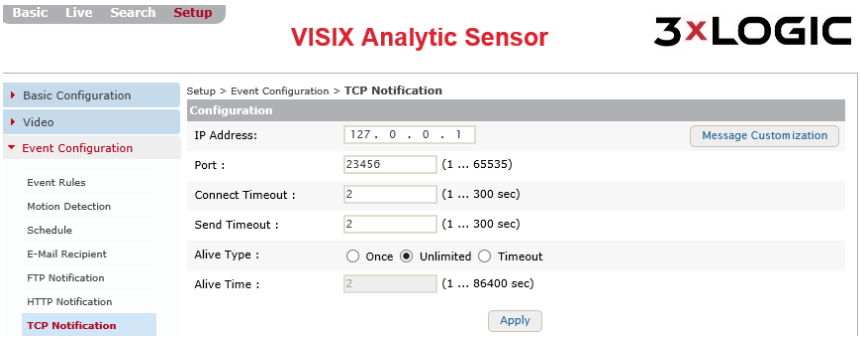


Figure 7-42: Setup Tab-Event Configuration Menu – TCP Notification Settings

2). From the **TCP Notifications** settings form, a user may configure the following settings:

TCP Notification Setting	Description
IP Address / Port	Enter TCP notification's destination network connection info.
Connect Timeout	Configure the connection timeout value.
Send Timeout	Configure the Send Timeout value.
Alive Type	Configure the TCP keep-alive packet mode.
Alive Time	Configure the time interval between keep-alive retransmissions.

3). Click **Apply** to save changes to the TCP Notification settings.

TCP SERVER

Steps:

1). Opening the **Setup Tab>Event Configuration** drop-down menu and clicking the **TCP Server** link will open the **TCP Server** settings page.

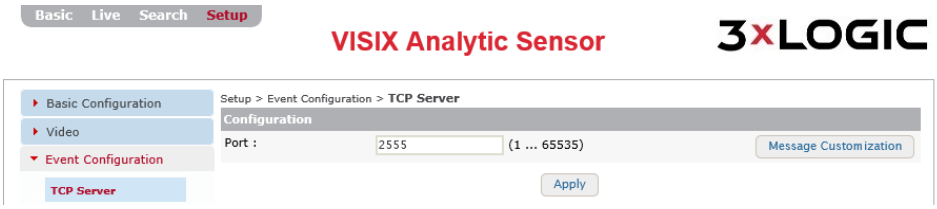


Figure 7-43: Setup Tab – Event Configuration Menu - TCP Server Settings

2). From the TCP Server setting pages, a user may enter a **Port** value for the TCP Event Server. Click the **Message Customization** button to deploy the event message settings for TCP Event servers.

TCP Message Settings	Description
Message Header Tab	Enable and customize a custom message header.
VCA Tab	Select a default message or configure a custom message for **VCA Config, VCA Alarm and VCA Counter** events.
MD Tab	Select a default message or custom message for motion detection events.
Network Tab	Select a default message or configure a custom message for **Network** events.
DI/DO Tab	Select a default message or configure a custom message for **DI/DO** events.

3). Click **Apply** to save changes to the TCP Server settings.

MULTICAST NOTIFICATION

Steps:

1). Opening the **Setup Tab>Event Configuration** drop-down menu and clicking the **Multicast Notification** link will open the **Multicast Notification** settings page.

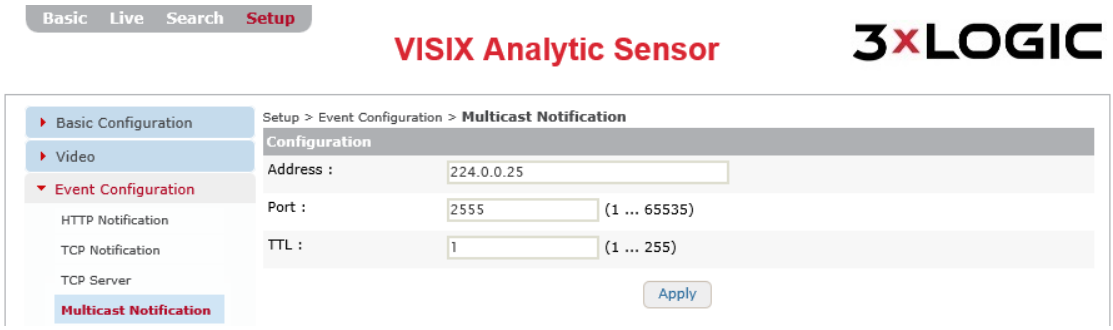


Figure 7-44: Setup Tab –Event Configuration Menu – Multicast Notification Settings

2). From the **Multicast Notification** setting pages, a user may configure the following UDP multicast settings:

Multicast Notification Settings	Description
Address	Enter the UDP multicast notification destination's IP address.
Port	Enter the UDP multicast notification destination's enter the Port.
TTL	Set the TTL threshold. The TTL threshold is a time value which delineates how long a data packet can exist across an information network (local intranet, internet, etc…) before being invalidated. Approximation of TTL threshold value effects are listed below: ■ **0** - Restricted to the same host. Won't be output by any interface. ■ **1** - Restricted to the same subnet. Won't be forwarded by a router. ■ **<32 -** Restricted to the same site, organization or department. ■ **<64** - Restricted to the same region. ■ **<128** - Restricted to the same continent. ■ **<255** - Unrestricted in scope; Global.

7.4 Network Configuration Menu

TCP/IP SETTING

Steps:

1). Opening the **Setup Tab>Network Configuration** drop-down menu and clicking the **TCP/IP** link will open the network **TCP/IP** settings page.

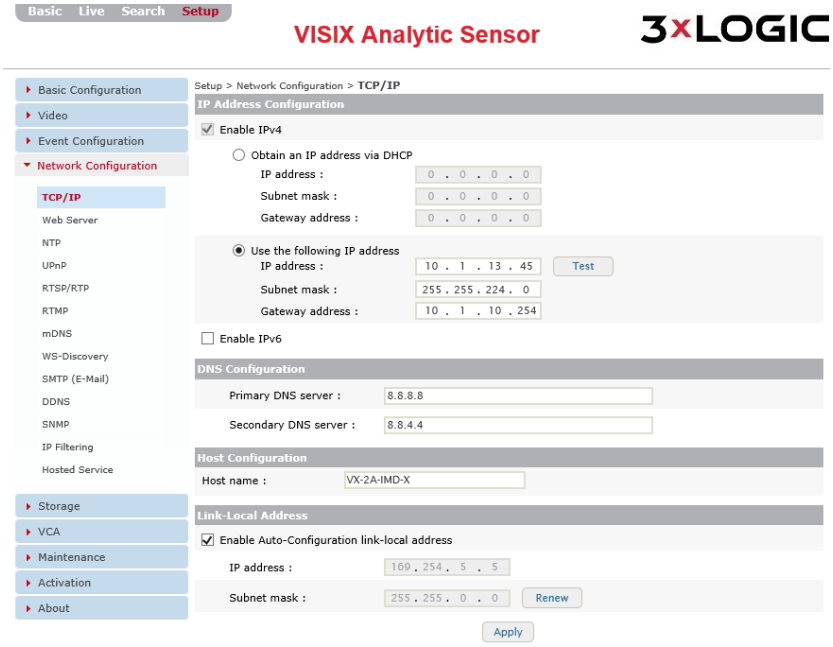


Figure 7-45: Setup Tab –Network Configuration Menu – TCP/IP Settings

2). From the **TCP/IP** settings page, a user may edit a camera's **TCP/IP settings**. This includes all configurable settings from the **Basic Tab>Camera Configuration> Network settings (IP Settings, DNS Server settings** pages as well as the ability to enable IPv6 and configure host name and local link address details). These settings can also be accessed via the **Advanced Tab>Basic Configuration Menu>Network Settings.**

Network Setting	Description
IP Address Configuration	Select the method by which the cameras will obtain an IP address: ■ **Obtain an IP Address via DHCP** – Select this method to have your router's DHCP function automatically assign the camera's network connection settings. This method is enabled by default. The automatically-generated **IP, Subnet Mask and Gateway** addresses will be listed directly underneath. i. **Use the following IP Address (Manual Configuration**) – Select this option to manually enter network connection settings. **IP Address, Subnet Mask and Gateway Addresses** can be manually entered directly underneath this setting. Clicking the **Test** button will confirm the validity of the network connection addresses you have entered. ii. To enable IPv6 protocol, click **Enable IPv6**. For more information on IPv6 settings, see IPv6 Settings Configuration, below.

Network Setting	Description
DNS Configuration	Enter in **Primary and Secondary DNS Server** connection information.
Host Configuration	Configure the device host name.
Link – Local Address	Checking-off **Enable Auto-Configuration Link-Local Address** will generate an alternate internal IP address which can also be used to connect to the camera, access the UI via browser, etc…. when on the same network as the camera.

NETWORK CONFIGURATION MENU - TCP/IP SETTINGS - IPV6 SETTINGS CONFIGURATION

Steps:

1). When the enable IPv6 box is checked, IPv6 settings fields will deploy (pictured below).

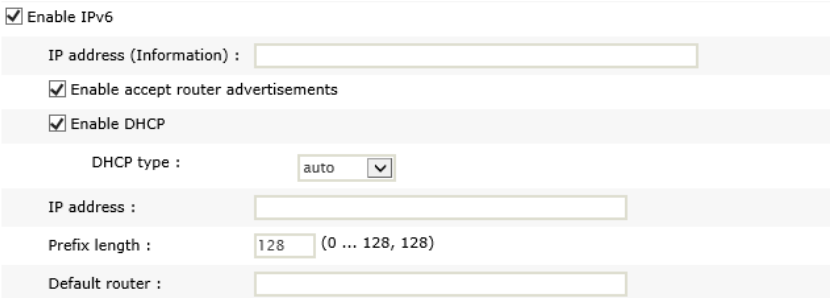


Figure 7-46: Setup Tab –Network Configuration Menu – TCP/IP Settings – IPv6 Settings

IPv6 Setting	Description
Enable Accept Router Advertisements	**Enable Accept Router Advertisements** will allow the camera to accept router advertisements, signaling device availability and connectivity to the host router.
Enable DHCP	**Enable DHCP** for automatic IP address assignment. Select a **DHCP Type** from the drop-down menu.
IP Address	The device IP address. If DHCP is not enabled, the user may assign an address.
Prefix Length	Assign an address prefix length.
Default Router	Enter the default router address.

WEB SERVER SETTINGS

Steps:

1). Opening the **Setup Tab>Network Configuration** drop-down menu and clicking the **TCP/IP** link will open the network **TCP/IP** settings page.

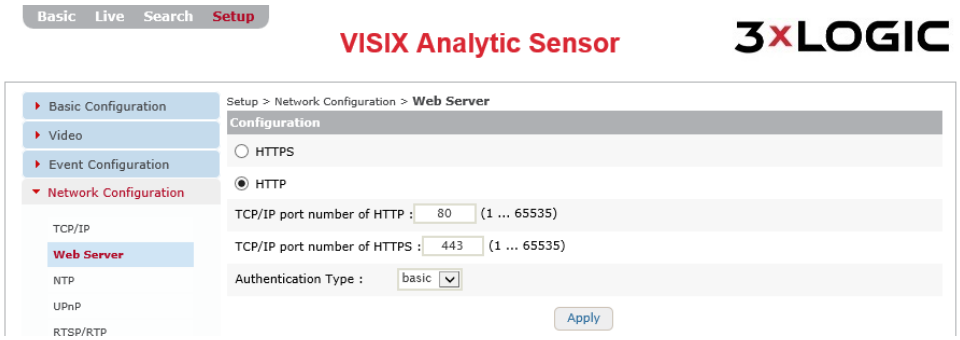


Figure 7-47: Setup Tab –Network Configuration Menu – Web Server Settings

2). From the **Web Server** settings form, a user may configure the camera's web server connection settings. Configurable settings include choosing the hypertext protocol **(HTTP or HTTPS)**, assigning separate port numbers for each protocol and choosing the **Authentication Type (basic or digest)** for the active protocol.

3). Click **Apply** to save any new changes to the **Web Server** settings.

NTP SETTINGS

Steps:

1). Opening the **Setup Tab>Network Configuration** drop-down menu and clicking the **NTP** link will open the network **NTP** settings page.

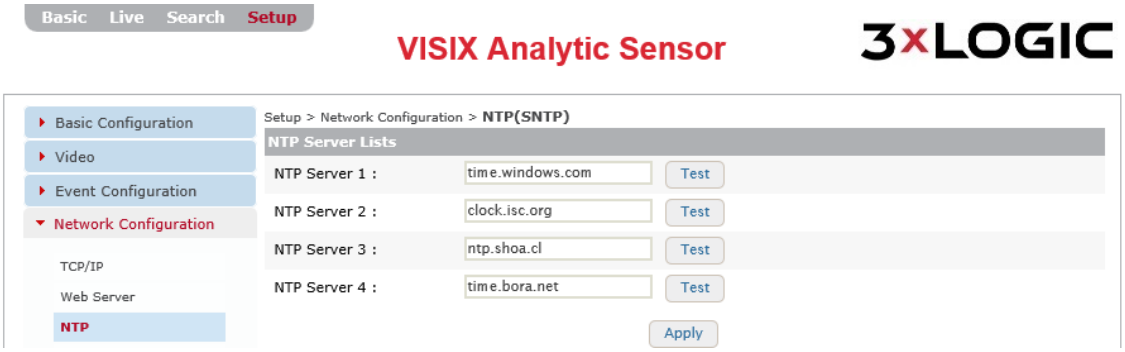


Figure 7-48: Setup Tab –Network Configuration Menu – NTP Settings

2). From the **NTP** settings page, a user may enter NTP server connection info for time synchronization purposes. Up to four NTP servers can be added.

3). After entering a time server address, click the **Test** button to confirm a connection between the camera and the selected NTP Server. If the test fails, confirm you have entered in the correct address for the NTP Server.

4). Click **Apply** to save settings changes.

UPNP SETTINGS

Steps:

1). Opening the **Setup Tab>Network Configuration** drop-down menu and clicking the **UPnP** link will open the network **UPnP** settings page.

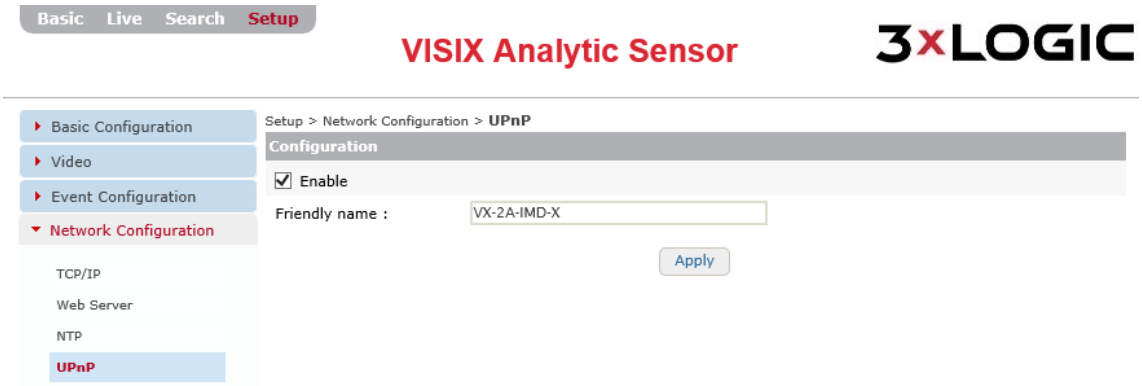


Figure 7-49: Setup Tab –Network Configuration Menu – UPnP Settings

2). From the **UPnP settings** page a user may enable UPnP. UPnP (Universal Plug and Play) is a set of networking protocols that permits networked devices mobile devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing, communications, and entertainment. UPnP is intended primarily for residential networks without enterprise-class devices.

3). Check-off the **Enable** box to enable UPnP. A user may also enter a device name. The camera model number will be used as the default name.

4). Click **Apply** to save changes to UPnP settings.

RTSP/RTP SETTINGS

Steps:

1). Opening the **Setup Tab>Network Configuration** drop-down menu and clicking the **RTSP** link will open the network **RTSP** settings page.

RTSP CONFIGURATION

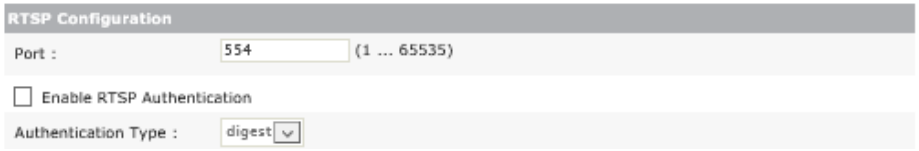


Figure 7-50: Setup Tab –Network Configuration Menu – RTSP/RTP Settings – RTSP Configuration

Steps:

1). Under the **RTSP Configuration** section of the **RTSP** settings page, a user may configure an RTSP port (default is 554). The user may also enable and choose the **RTSP Authentication Type (digest or basic).**

SRTP

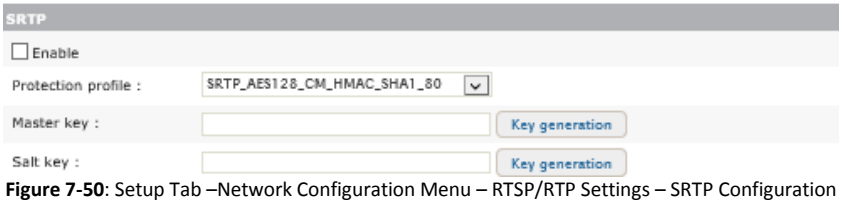


Figure 7-50: Setup Tab –Network Configuration Menu – RTSP/RTP Settings – SRTP Configuration

Steps:

1). Under the **SRTP (Secure RTP) Configuration** section of the **RTSP** settings page, a user may enable **SRTP**, a **Protection Profile** type may be chosen and **Maste*r*** and **Salt** keys may be generated.

UNICAST

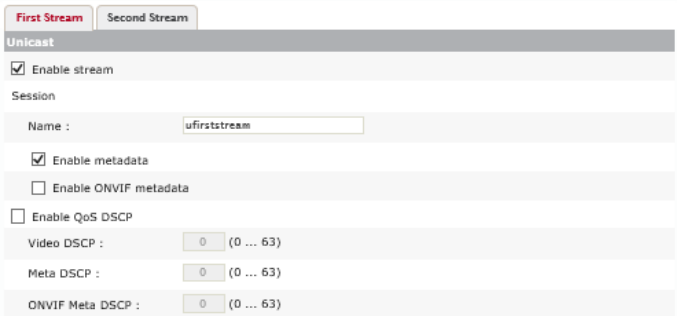


Figure 7-51: Setup Tab –Network Configuration Menu – RTSP/RTP Settings –Unicast Configuration

Steps:

1). Under the **Unicast** section of the **RTSP** settings page, a user may enable and configure Unicast settings for the camera's First (Main) and Second (Sub) streams. Before configuring, make sure the desired stream tab has been selected (above the **Unicast** section header).

Unicast Setting	Description
Name	Name the unicast stream.
Enable Metadata	Check-off this box to include metadata with the stream transmission.
Enable ONVIF Metadata	Check-off this box to include ONVIF metadata with the stream transmission.
Enable QoS DSCP	Enable Quality of Service differentiated services.
Video / Meta / ONVIF Meta DSCP	Assign DSCP levels for **Video, Meta and ONVIF** Meta. Low-latency services will be dedicated starting with components featuring the highest DSCP value.

MULTICAST

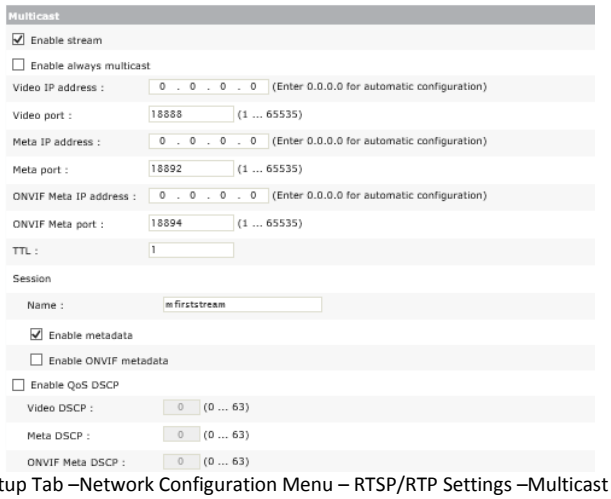


Figure 7-52: Setup Tab –Network Configuration Menu – RTSP/RTP Settings –Multicast Configuration

Steps:

1). Under the **Multicast** section of the **RTSP** settings page, a user may enable and configure **Multicast** settings for the camera's **First** (Main) and **Second** (Sub) streams. Before configuring, make sure the desired stream tab has been selected (above the **Unicast** section header). Configurable settings include:

Multicast Setting	Description
Enable Always Multicast	Enabling this option will have the selected stream use UDP multicast indefinitely for RTSP streaming.
Video IP Address/Port	Enter a static address (or leave blank for auto configuration) for broadcast of UDP Multicast video.
Meta IP Address/Port	Enter a static address (or leave blank for auto configuration) for broadcast of UDP Multicast meta data.
ONVIF Meta IP Address/Port	Enter a static address (or leave blank for auto configuration) for broadcast of UDP Multicast ONVIF meta data.
TTL	Set the TTL threshold. The TTL threshold is a time value which delineates how long a data packet can exist across an information network (local intranet, internet, etc…) before becoming invalidated. Approximation of TTL threshold value effects are listed below: **0** - Restricted to the same host. Won't be output by any interface. **1** - Restricted to the same subnet. Won't be forwarded by a router. **<32** - Restricted to the same site, organization or department. **<64** - Restricted to the same region. **<128** - Restricted to the same continent. **<255** - Unrestricted in scope; Global.
Name	Name the multicast stream.
Enable QoS DSCP	Enable Quality of Service differentiated services.
Video / Meta / ONVIF Meta DSCP	Assign DSCP levels for **Video, Meta and ONVIF** Meta. Low-latency services will be dedicated starting with components featuring the highest DSCP value.

RTMP SETTINGS

Steps:

1). Opening the **Setup Tab>Network Configuration** drop-down menu and clicking the **RTMP** link will open the network **RTMP** settings page.

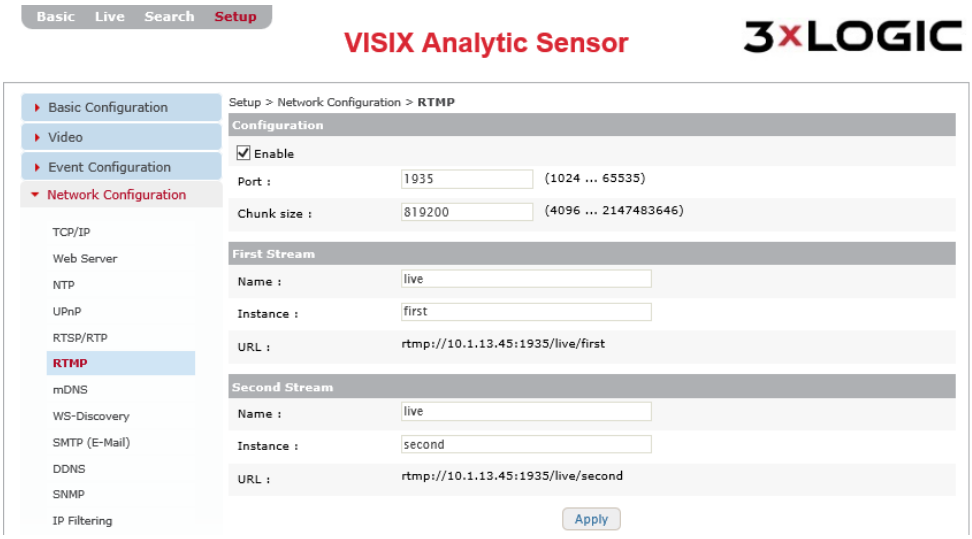


Figure 7-53: Setup Tab –Network Configuration Menu – RTMP Settings

2). From the **RTMP Settings** page, a user may enable RTMP. Real Time Messaging Protocol (RTMP) was initially a proprietary protocol developed by Macromedia for streaming audio, video and data over the Internet, between a Flash player and a server. V-Series All-in-One cameras can broadcast either of their stream profiles using RTMP.

3). Check-off the **Enable** box to initiate RTMP streaming. The user may name the RTMP **Name and Instance** for both first and second streams. RTMP streaming URL for both stream profiles will be displayed.

4). Click **Apply** to save RTMP settings changes.

MDNS SETTINGS

Steps:

1). Opening the **Setup Tab>Network Configuration** drop-down menu and clicking the **mDNS** link will open the network **mDNS** settings page.

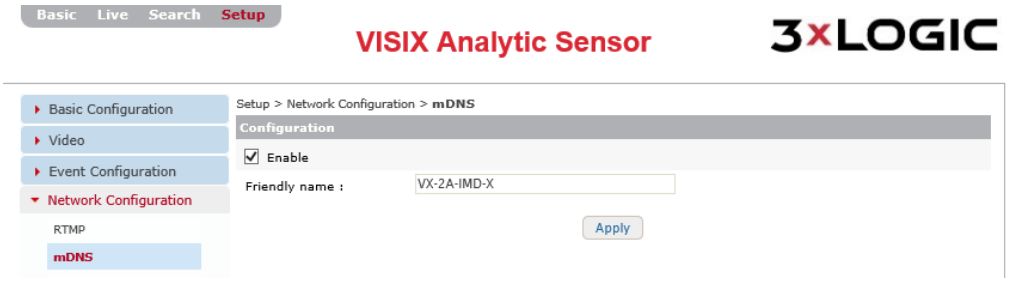


Figure 7-54: Setup Tab –Network Configuration Menu – mDNS Settings

NOTE:

The **multicast Domain Name System (mDNS)** resolves host names to IP addresses within small networks that do not include a local name server. It is a zero-configuration service, using essentially the same programming interfaces, packet formats and operating semantics as the unicast Domain Name System (DNS).

2). From the mDNS settings page, a user may check-off **Enable** to enable mDNS for this camera and assign a device **Name.** Click **Apply** to save settings changes.

WS-DISCOVERY SETTINGS

Steps:

1). Opening the **Setup Tab>Network Configuration** drop-down menu and clicking the **WS Discovery** link will open the network **WS Discover** settings page.

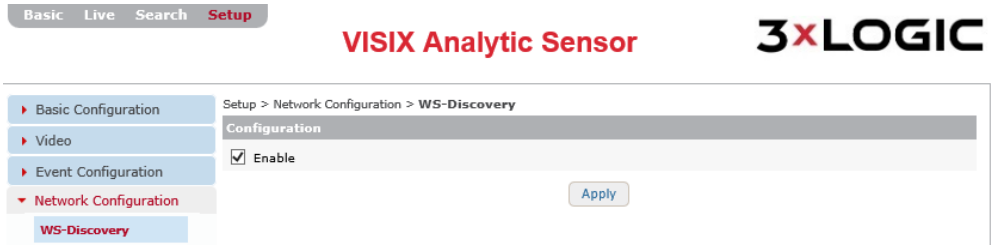


Figure 7-55: Setup Tab –Network Configuration Menu – WS-Discovery Settings

2). Check-off the **Enable** box to enable WS Discovery (Web Services Dynamic Discovery).

3). Click **Apply** to save settings changes.

SMTP (E-MAIL SERVER) SETTINGS

Steps:

1). Opening the **Setup Tab>Network Configuration** drop-down menu and clicking the **SMTP** link will open the network **SMTP** settings page.

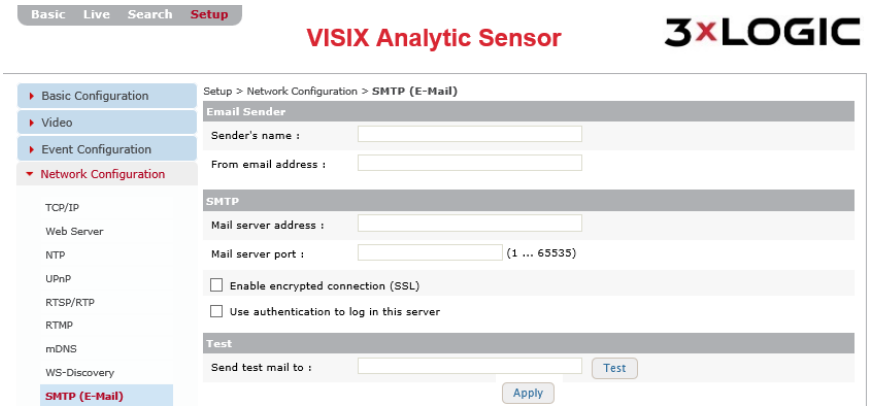


Figure 7-56: Setup Tab –Network Configuration Menu – SMTP Settings

2). From the **SMTP** settings page, a user may configure e-mail server settings. SMTP settings must be configured correctly to allow for the successful transmission of event e-mail notifications. Configurable settings include:

SMTP Setting Category	Description
E-Mail Sender	Configure a **Sender Name** (to be displayed in the **From** email field) and **From Email Address.**
SMTP	Configure the SMTP **Mail Server Address and Port.** Check-off **Enable Encrypted Connection (SSL)** to enable SSL encryption of e-mails sent through the configured SMTP Server. Check-off **Use Authentication to Log In This Server** to require login when
Test	Configure a test email. Enter the test recipient address and click the **Test** button to confirm successful SMTP configuration.

3). Click **Apply** to save changes to SMTP settings.

DDNS SETTINGS

Steps:

1). Opening the **Setup Tab>Network Configuration** drop-down menu and clicking the **DDNS** link will open the network **DDNS** settings page.

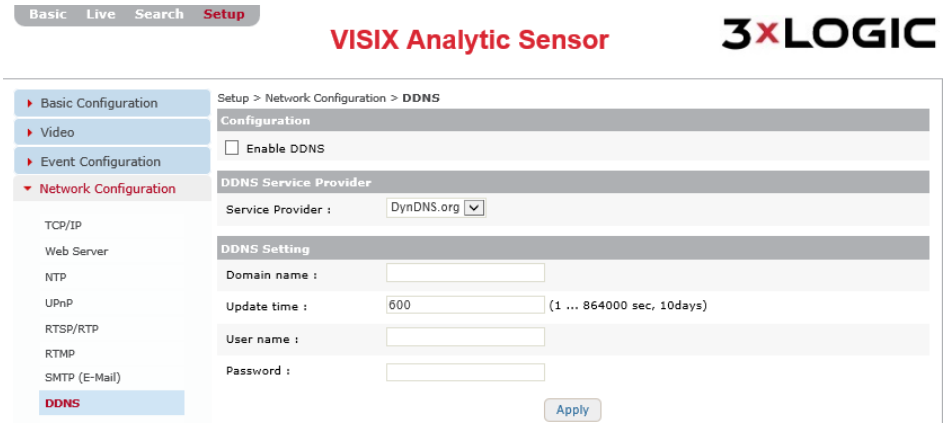


Figure 7-57: Setup Tab –Network Configuration Menu – DDNS Settings

2). From the **DDNS (Dynamic Domain Name System)** settings page, a user may enable DDNS and configure related settings. Available configurable settings include:

DDNS Setting	Description
Service Provider	Choose the DDNS service provider **(DynDNS.org, FreeDNS.org, NO-IP.com)**
Domain Name	Configure a domain name for use with the DDNS service.
Update Time	Configure a DDNS update interval (in seconds).
Username and Password	Configure login credentials if required. Field availability is dependent on chosen DDNS service provider.

3). Click **Apply** to save DDNS settings changes.

SNMP SETTINGS

Steps:

1). Opening the **Setup Tab>Network Configuration** drop-down menu and clicking the **SNMP** link will open the network **SNMP** settings page.

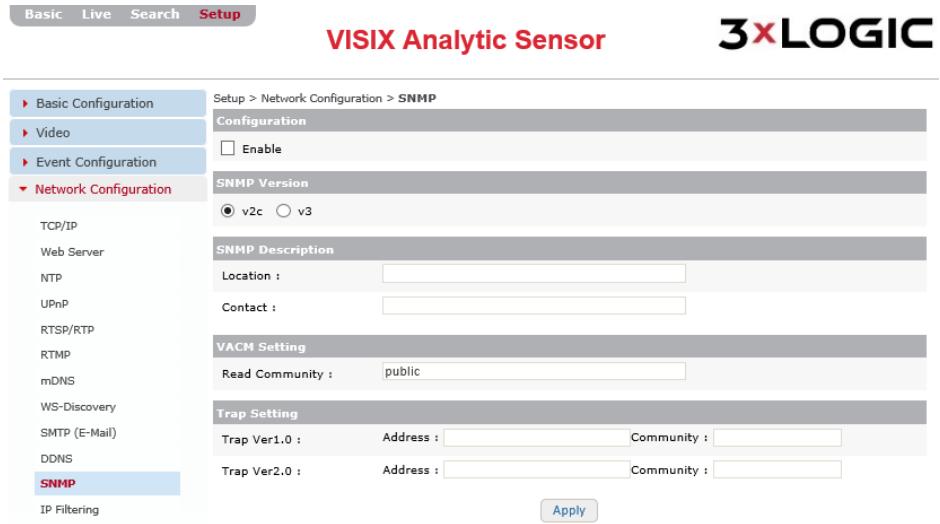


Figure 7-58: Setup Tab –Network Configuration Menu – SNMP Settings

NOTE:

SNMP (Simple Network Management Protocol) is an Internet-standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.

2). From the SNMP settings page, a user may **Enable** SNMP and configure the following related settings:

SNMP Setting Category	Description
SMNP Version	Select the SMNP version to use with the camera.
SMNP Description	Configure SMNP **Location** and **Contact** description information.
VACM Setting	Configure the **View-based Access Control Model Read Community**. The camera default settings is **public (read-only). Private (read-write)** can also be used.
Trap Setting	Define an **Address** and **Community** for Trap Ver 1.0 and 2.0.

3). Click **Apply** to save SNMP settings changes.

IP FILTERING SETTINGS

Steps:

1). Opening the **Setup Tab>Network Configuration** drop-down menu and clicking the **IP Filtering** link will open the network **IP Filtering** settings page.

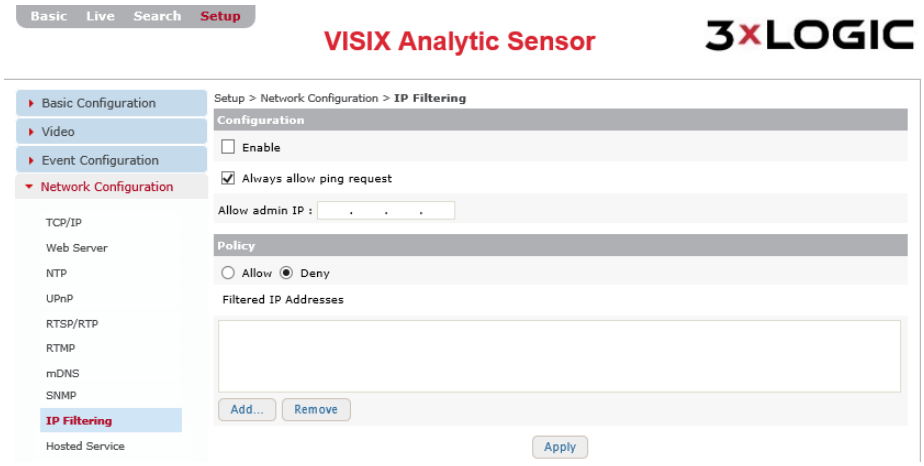


Figure 7-59: Setup Tab –Network Configuration Menu – IP Filtering Settings

NOTE:

IP Filtering is a simple process which essentially decides which types of IP datagrams will be processed using normal procedures and which will be discarded/ignored.

2). From the **IP Filtering** settings page, a user may enable IP filtering and configure the following related settings.

IP Filtering Setting	Description
Always Allow Ping Request	If enabled, the camera will accept pings, regardless if the incoming ping is sent from a device with a filtered IP address.
Allow/Deny	Set the IP Filtering Mode to **Allow** or **Deny.** Based on your choice, addresses in the **Filtered IP Addresses** list will be denied or allowed.
Add…/Remove	Select the **Add…** button to add an IP address for filtering. Enter an IP Address and click **OK** to save the new address. To remove an existing address from the filtered list, select the address in the list and click **Remove.** You will be prompted to confirm the removal. Click **OK** to confirm.

3). Click **Apply** to save changes to **IP Filtering** settings.

HOSTED SERVICE SETTINGS

Steps:

1). Opening the **Setup Tab>Network Configuration** drop-down menu and clicking the **Hosted Service** link will open the **Hosted Service** settings page.

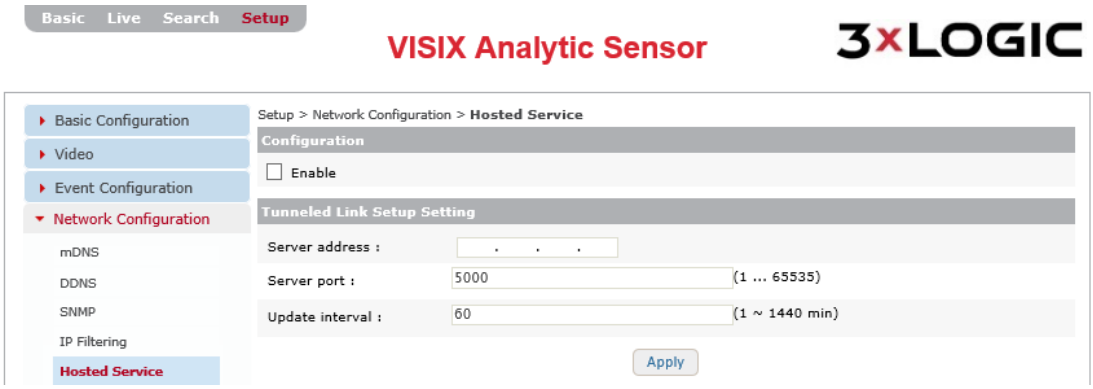


Figure 7-60: Setup Tab –Network Configuration Menu – Hosted Service Settings

2). From the **Hosted Service** settings page, a user may enable configure connection settings for camera integration with a hosted service. Available configurable settings include:

Hosted Service Settings	Description
Server Address and Port	Enter the hosted service IP Address and Port.
Update Interval	Enter an update interval (in minutes)

3). Click **Apply** to save hosted service settings.

7.5 Storage Menu

SD SETTINGS

Steps:

1). Opening the **Setup Tab>Storage** drop-down menu and clicking the **SD** link will open the **SD** settings page.

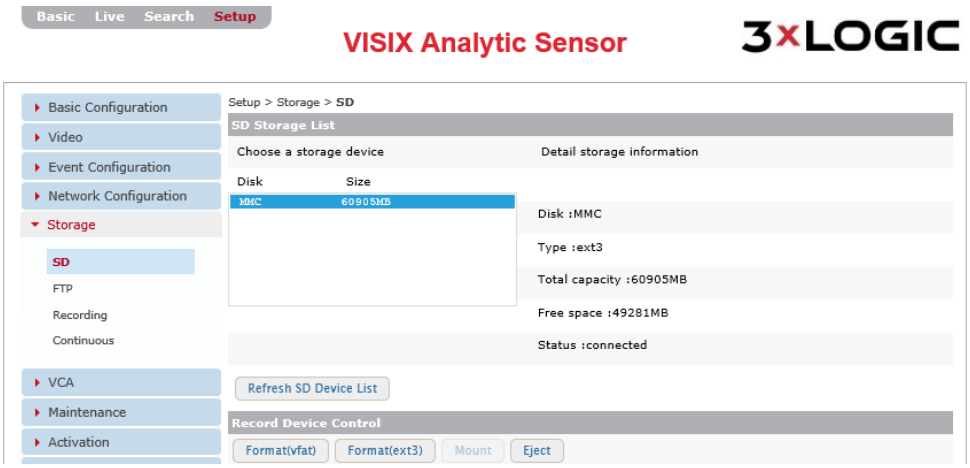


Figure 7-61: Setup Tab –Storage Menu – SD Settings

2). From the **SD Card** storage settings page, a user may choose their SD storage device, view information on the chosen device, change storage format or mount and eject storage devices. These settings can also be accessed from Basic Tab>Storage Configuration Menu>SD.

SD STORAGE LIST

In the SD Storage List section, a user may select their desired storage device from the list. The following device details will be generated to the right of the device list after making a selection:

Storage Detail	Description
Disk	The storage device disk type of the selected device.
Type	The storage disk format of the selected device.
Total Capacity	The totally storage capacity of the selected device.
Free Space	Lists the remaining free space on the selected device.
Status	Current storage device status.

RECORDING DEVICE CONTROL

In the Record Device Control section, a user may select the desired storage format (vfat, ext3) and can also mount an inactive storage device or eject the currently active storage device:

Device Control	Description
Format (vfat)	Use **vfat** format for the selected device. Format progress will be displayed. **WARNING:** Re-formatting the storage device will wipe all stored footage. Download any footage you wish to retain before beginning the format process.
Format (ext3)	Use **ext3** format for the selected device. Format progress will be displayed. **WARNING:** Re-formatting the storage device will wipe all stored footage. Download any footage you wish to retain before beginning the format process.
Mount	Mount the currently selected device. This option is only available if the currently selected device is inactive.
Eject	Eject the currently selected device. This option is only available if the selected device is mounted.

FTP SETTINGS

Steps:

1). Opening the **Setup Tab>Storage** drop-down menu and clicking the **FTP** link will open the **FTP** storage settings page.

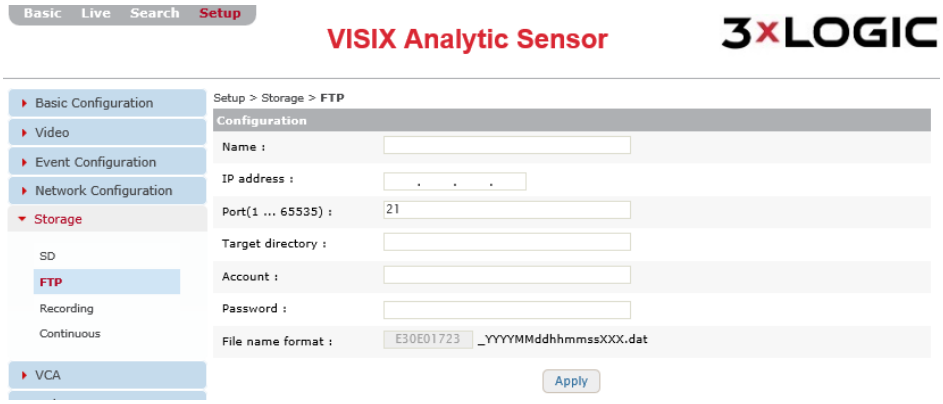


Figure 7-62: Setup Tab –Storage Menu –FTP Settings

2). If uploading footage data to an FTP destination is desired, a user may configure connection settings from for their desired FTP service on the **FTP Settings page.**

FTP Setting	Description
Name	Name the FTP server. This name will be used to identify this particular FTP when selecting it for storage purposes.
IP Address/Port	Enter network connection values for the desired FTP Server.
Target Directory	Enter the target destination directory on the FTP for storing uploaded files.
Account / Password	Enter the user login credentials for the FTP. 3xLOGIC recommends using an administrative level account when possible to avoid permissions conflicts.
Filename Format	Assign the filename format for the files uploaded to the FTP.

3). Click **Apply** to save changes to FTP storage settings.

RECORDING

Steps:

1). Opening the **Setup Tab>Storage** drop-down menu and clicking the **Recording** link will open the **Recording** storage settings page.

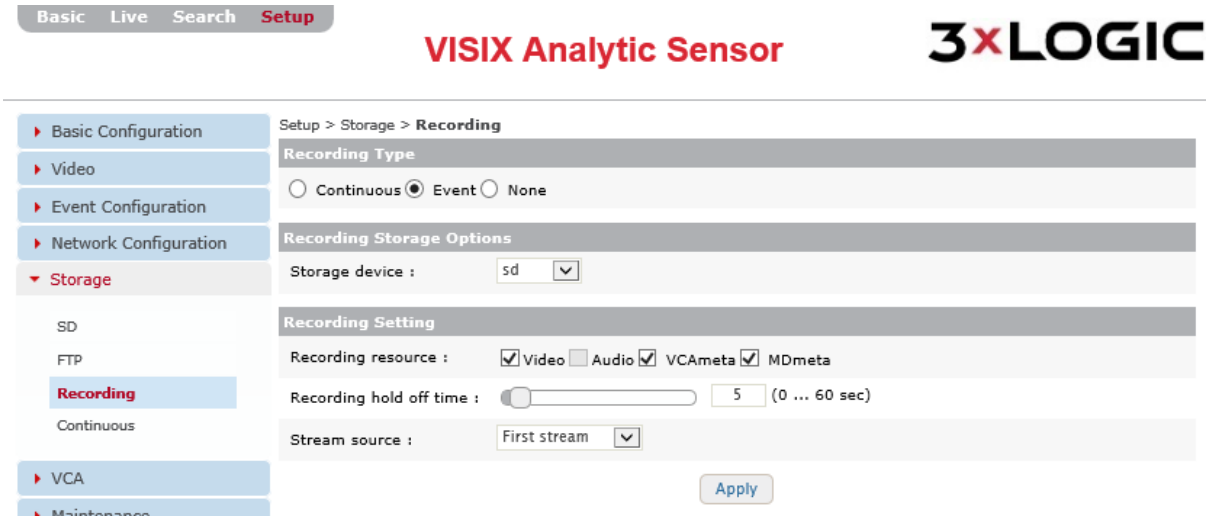


Figure 7-63: Setup Tab –Storage Menu –Recording Settings

2). From the **Recording** settings page, a user may configure settings related to the cameras recording functionality.

Configurable recording settings include:

Recording Setting Category	Description
Recording Type	Select a recording mode for the cameras. The following modes are: ■ **Continuous –** Select **Continuous** recording mode to have the camera constantly record. ■ **Event** - Select **Event** recording mode to have the camera begin recording based on an events (i.e. motion detection, VCA tripwire, DIO etc…). ■ **None** – Select the **None** mode to use the camera as a live-view only device.
Recording Storage Options	Select a storage device from the drop-down menu. If **Continuous** is selected as the **Recording Type**, the user must select the storage **Recycling** mode. Choose **Stop Recording** to halt recording when storage is at full capacity. Choose **Delete Files and Recycle (Oldest First)** to continue recording and overwrite the oldest files on the storage device when storage has reached full capacity.

Recording Setting Category	Description
Recording Settings (With *Event* Recording Type)	**Recording Resource** - Select recording resources. Choose from **Video, Audio** (for audio-capable camera models only), **VCA Meta Data** and **Motion Detection (MD) Meta Data**. Chosen resources will be captured when recording. Specify the length of time the camera will continue to record after a trigger has been deactivated by setting a **Recording Hold Off Time** value (seconds). A maximum of one minute (60 seconds) can be configured. Select the recording **Stream Source** (First/Main Stream, Second/Substream).from the available drop-down menu.
Recording Settings (With *Continuous* Recording Type)	**Filename Prefix –** Designate a filename prefix for continuous recording files. **Recording Resource** - Select recording resources. **Video Only** is the recommended (and default) setting to maximize storage utilization. Select the maximum continuous **Recording File size/Duration** by selecting and adjusting the **Size** or **Time** slider accordingly. When the maximum limit is reached, a new file will begin recording and the current file will be available for download from the **Continuous** storage page. Select the recording **Stream Source** (First/Main Stream, Second/Substream).from the available drop-down menu.
Instant Recording (*Continuous* Recording Type Only)	Configure an **Instant Recording** time interval (in seconds). Use this feature to quickly create a footage file without waiting until the configured **Maximum Filesize/Duration** is reached. Click **Start** to end the current file and begin recording a new file for the length you have configured.

3). Click **Apply** to save **Recording** settings changes.

CONTINUOUS (RECORDING) SETTINGS

Steps:

1). Opening the **Setup Tab>Storage** drop-down menu and clicking the **Continuous** link will open the **Continuous** storage settings page.

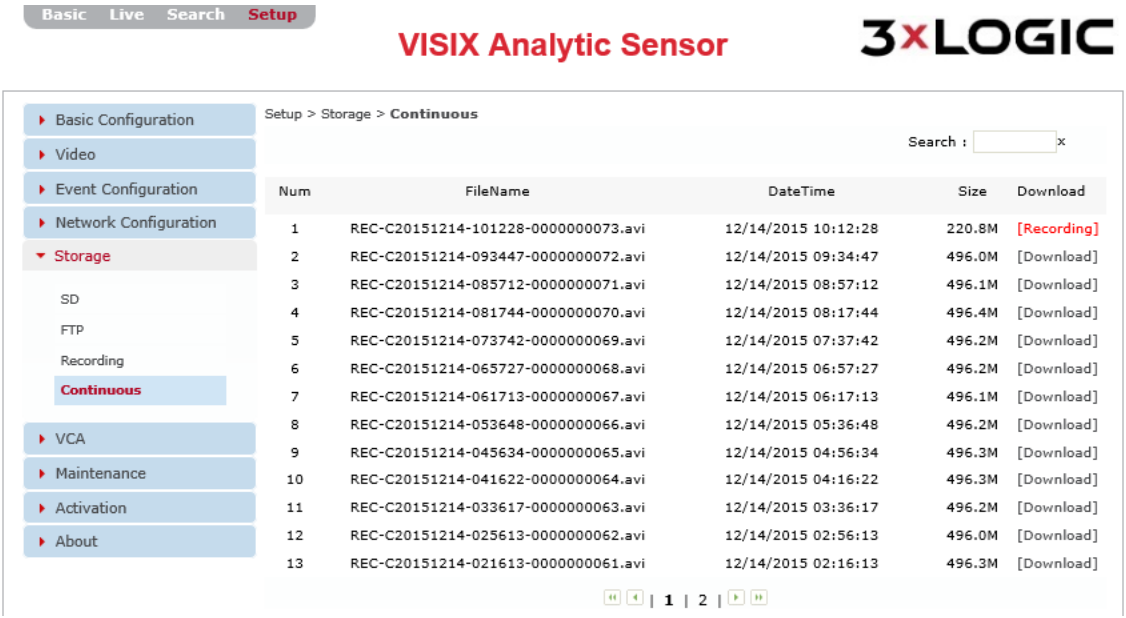


Figure 7-64: Setup Tab –Storage Menu –Continuous (Recording) Settings

2). From the **Continuous** storage settings page, a user may access any files recorded using **Continuous** recording type. File info including **File Name, Date/Time** range, and **Size (in MB)** will be displayed for each available file. If a file is currently being recorded, it will display as **Recording** under the **Download** column.

3). To download an available file, simply click the corresponding **Download** link.

4). Use the navigation controls at the bottom of the file list to navigate multiple pages of files.

NOTE:

Continuous footage files can only be accessed (downloaded) from this page and cannot be viewed via the Search (Playback tab).

7.6 VCA Menu

ENABLE/DISABLE

Steps:

1). Opening the **Setup Tab>VCA** drop-down menu and clicking the **Enable/Disable** link will open the VCA **Enable/Disable** settings page.

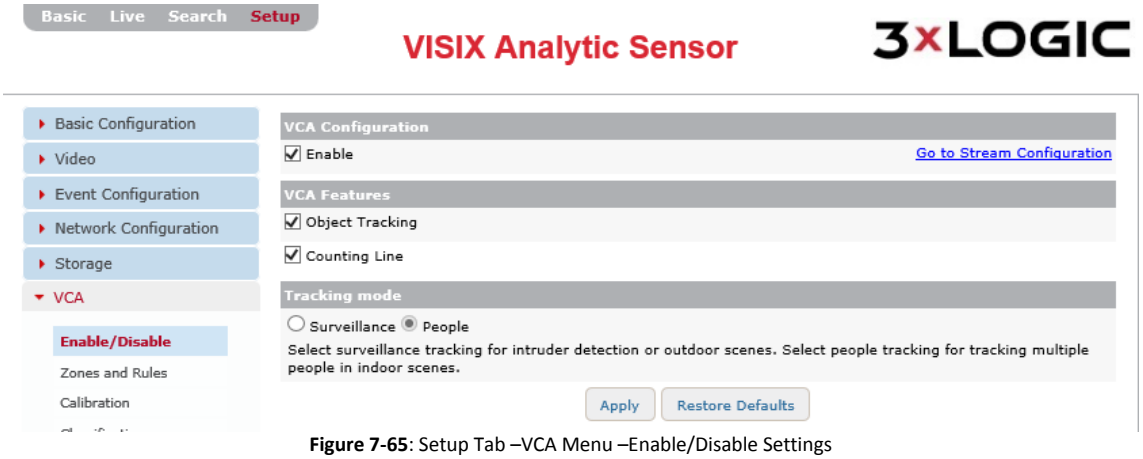


Figure 7-65: Setup Tab –VCA Menu –Enable/Disable Settings

2). From the VCA **Enable/Disable** settings page, a user may enable VCA and configure the following settings:

VCA Setting	Description
VCA Features	Enable desired VCA features: **Object Tracking** - Enable this function to use the Object Tracking analytic. Object tracking analytics are generally utilized to count queue times, trigger no-customer present exceptions, etc… **Counting Line** - Enable this function to use the Counting Line analytic. Counting Line/Tripwire analytics are generally used to count objects entering/exiting a space.
Tracking Mode	Choose the VCA tracking mode. **Surveillance –** Surveillance tracking mode should be used for intruder detection or outdoor surveillance. **People –** People tracking mode is most suitable for tracking multiple people in indoor, high traffic environments. People tracking requires an advanced All-in-One Analytics license.

3). To restore VCA **Enable/Disable** settings to their factory default state, click **Restore Defaults**

4). Click **Apply** to save settings changes.

ZONES AND RULES SETTINGS

Steps:

1). Opening the **Setup Tab>VCA** drop-down menu and clicking the **Zones and Rules** link will open the VCA **Zones and Rules** settings page.

2). From the VCA **Zones and Rules** page, a user may perform the majority of VCA analytics configurations. The **Zones and Rules** settings page consists of two separate tabs. The **Zones & Rules** tab and the **Logical Rules** tab. By default, the page will open with the **Zones & Rules** tab deployed.

ZONES AND RULES SETTINGS – ZONES & RULES TAB

Steps:

1). On the **Zones and Rules** tab, **Zones, Lines** and **Counters** *(*and the analytics **Rules** pertaining to each) can all be constructed or placed within the live preview image.

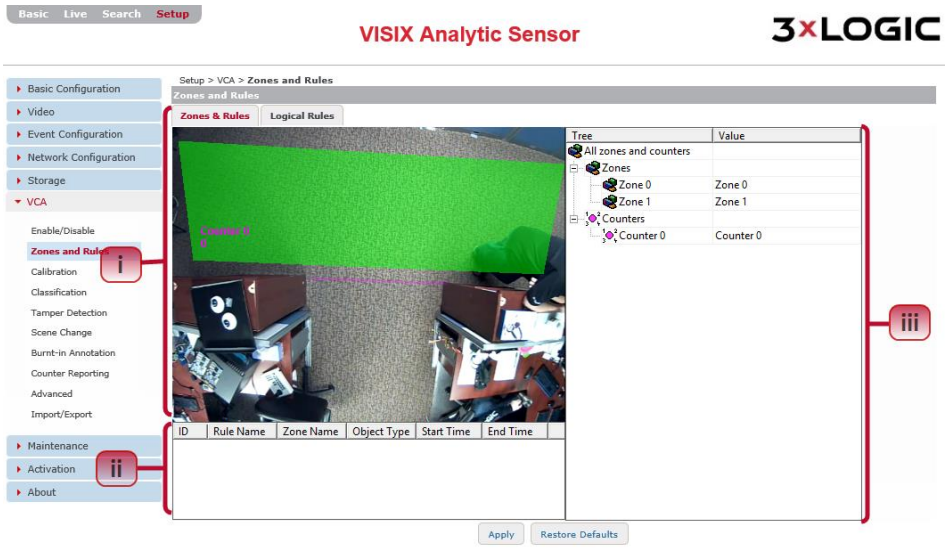


Figure 7-66: Setup Tab –VCA Menu –Zones and Rules Settings – Zones & Rules Tab

2). The **Zones & Rules** tab consists of three segments:

i. **Preview Area** – A live preview of the camera's image. In the preview area, user may overlay analytics Zones, Lines and Counters for use with the analytics engine.

ii. **Zone and Rule List** – Recent object interaction with zones/lines will be listed in this area with the following information provided for each entry: **ID, Rule Name, Zone Name, Object Type, Start Time, and End Time**.

iii. **Rule Configuration Menu** - When a zone, line or counter is selected, rule options pertaining to the selected elements functionality will be available for configuration in this menu. When no item is actively selected, this section will display all zones/lines and counters currently configured on the device (as pictured in the above example).

3). To create analytics rules or zones, right-click within the preview area.

The following menu options will be available:

Right-Click Option	Description
Zone/Line	**Create Zone** – Create an analytics zone. Zones are often used for queue wait and dwell timers. **Create Line** – Create an analytics line/tripwire. Lines are generally used for people counting. **Remove All Zones and Lines** – Remove all active zones and line.
Counter	**Add Counter** – Create a counter. Counters can be used to tally present objects in a dwell zone. **Reset All Counters** – Reset all active counters to zero. **Remove All Counters** – Remove all counters from the overlay.
Display	**Display Blobs –** Display motion blob. This option is generally used for visual diagnostics and is only available when Blob has been **Displays Objects –** From this men, the user may enable several object display options. Options include: ■ **Display Objects –**Track objects on-screen. ■ **Display Objects in Multiple Colors –** Use differing colors for object trackers when multiple objects are present. ■ **Display Non-Alarmed Objects –** Display objects which are not currently triggering an alarm/event (Object detected in field of visions but does not enter dwell zone/ cross counting line). ■ **Display Object Speed –** Display the object speed value. ■ **Display Object Height –** Display the object height value. ■ **Display Object Area –** Displays object area size value (in square meters) alongside object tracker. ■ **Display Object Classification –** List the object class alongside object tracker. **Display System Messages –** Display analytics system messages generated by the camera on-screen.
Pause	Pause the live video preview on the current frame.

CREATE ZONE

Steps:

1). To create a zone, right-click within the preview area and select **Zone/Line>Create Zone.**

2). Draw the zone within the preview area as desired by clicking and dragging each corner until a satisfactory shape and position is achieved.

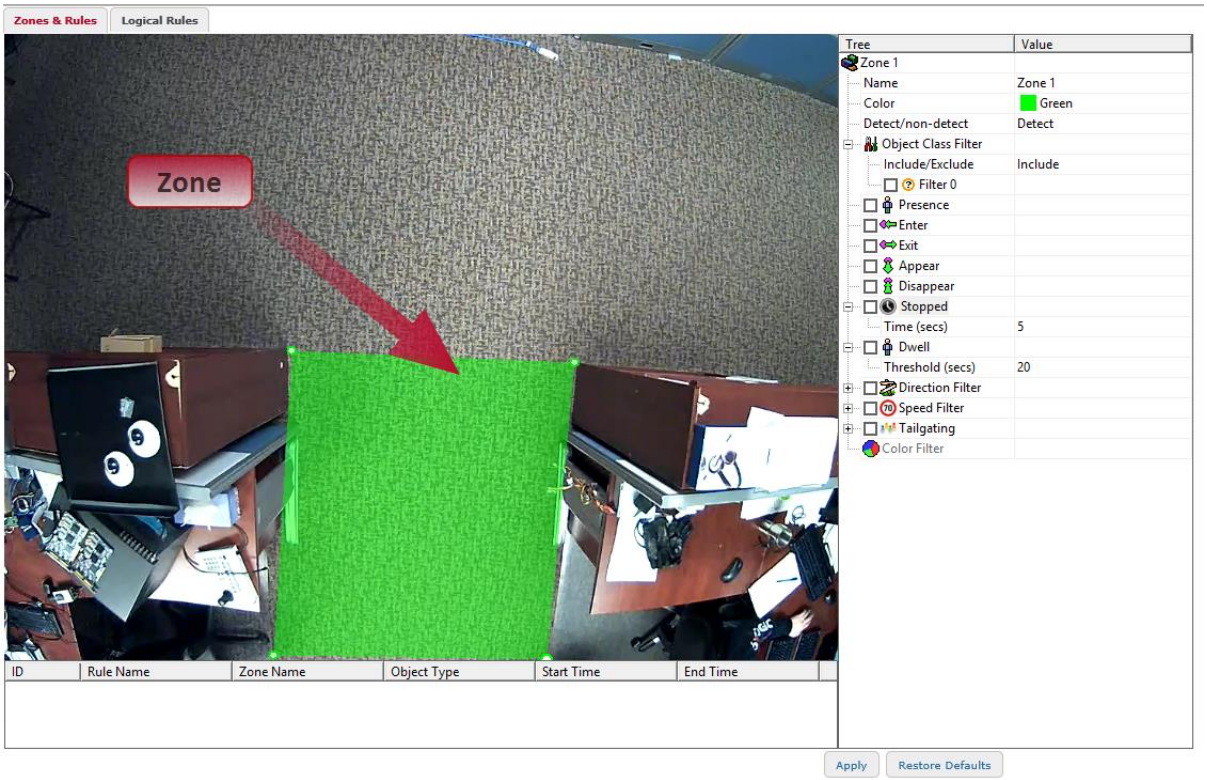
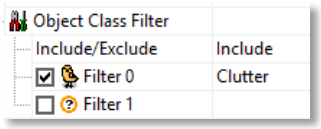


Figure 7-67: Setup Tab –VCA Menu –Zones and Rules Settings – Creating a Zone

3). When a zone is selected, the following options will be available in the **Rule Configuration Menu**:

VCA Zone – Rule Config.	Description
Name	Name the zone. This name will be used to refer to this particular zone throughout the cameras browser interface.
Color	Assign a color to the zone. This will allow for fast visual recognition when multiple zones are present.
Detect/Non-Detect	Select the zone's detection mode. ▪ **Detect**- Detect object motion within the analytics zone. ▪ **Non-Detect** -Cease detecting objects within the camera's field of vision when they enter the analytics zone. Non-Detect zones are often utilized as a mask.

VCA Zone – Rule Config.	Description
Object Class Filter	Create an **Object Filter**. Object filters can be used to filter predefined objects from triggering an analytics event. Filters can also be configured to trigger an event ONLY when a specific object class is detected within a zone. **Include/Exclude –** Select **Include** to apply analytics only to objects of the selected classification. Select **Exclude** to exclude objects of the selected classification from triggering analytics events. To create an **Object Class Filter**, check off a filter and choose the object class in the **Value** field drop-down (**Filter 0** is actively filtering the **Clutter** object class in the below example).  For information on configuring object classes, see Classification Settings.
Presence	Enable this rule to trigger an analytics event whenever an object comes into contact with any portion of the zone. The zone will remain triggered so long is presence is detected.
Enter	Enable this rule to trigger an analytics event whenever an object enters the zone.
Exit	Enable this rule to trigger tan analytics event whenever an object exits the zone.
Appear	Enable this rule to trigger an analytics event whenever an object appears within the zone.
Disappear	Enable this rule to trigger an analytics event whenever an object disappears from the zone.
Stopped	Enable this rule to trigger an analytics event whenever an object has stopped moving within the analytics zone for equal to or longer than the defined **Time (Seconds).**
Dwell	Enable this rule to trigger an analytics event whenever an object has dwelled within the zone longer than the defined **Threshold (Seconds).**
Direction Filter	Enable this rule to trigger analytic events based on directional movement through the zone. A directional indicator will be overlaid over the zone. Adjust the **Direction** and **Acceptance** angle to configure a direction spectrum. Only objects travelling through the zone within this directional spectrum will trigger an analytics event.
Speed Filter	Enable this rule to trigger an analytics events whenever an object travels through the zone within the defined speed range Configure a **Lower Bound (km/h)** and **Upper Bound (km/h)** speed value to define your speed range.

VCA Zone – Rule Config.	Description
Tailgating	Enable this rule to trigger an analytics event whenever an object enters the zone within the defined **Time (Seconds)** period after another object has entered. If the **Time (Seconds)** value is set to 5, then anytime an object enters a zone within 5 seconds of another object, the camera will consider this tailgating and an analytics event will be triggered.
Color Filter	Enable this rule to trigger an analytics event whenever an object of a specified color is detected within the zone. Set a **Threshold (%)** to designate how much of an object must feature the specified color to trigger the alarm. If the Color is set to Blue, and the **Threshold** is set to 25%, than an object which is 25% blue or more will trigger an analytics event.

4). Right-clicking a zone within the preview area will deploy a menu with the following options:

VCA Zone – Right-Click Option	Description
Remove Zone	Remove the zone from the live preview. All rules associated with the zone will be deleted.
Insert/Remove Node	**Insert/Remove** a node to the zone border. Adding nodes will allow the user to further customize the shape of the zone.
Rules	Enable a rule. If a secondary setting for a rule exists **(Dwell, Directional Filter, etc…)** default values for the secondary settings will be used.
Pause	Pause the live video preview on the current frame.

5). Click the **Apply** button to save your new VCA Zone settings.

CREATE LINE (TRIPWIRE)

Steps:

1). To create a line, right-click within the preview area and select **Zone/Line>Create Line.**

2). Draw the line within the preview area as desired by clicking and dragging to place both line endpoints.

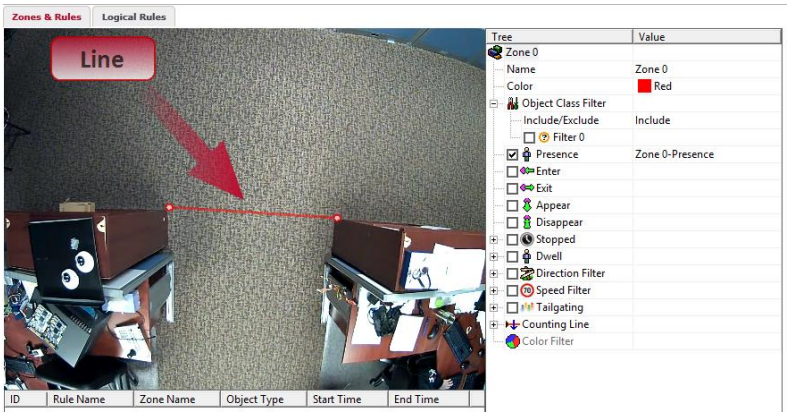
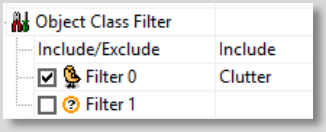


Figure 7-68: Setup Tab –VCA Menu –Zones and Rules Settings – Creating a Line

3). When a line is selected, the following options will be available in the **Rule Configuration Menu**:

VCA Line – Rule Config.	Description
Name	Name the line. This name will be used to refer to this particular line throughout the cameras browser interface.
Color	Assign a color to the line. This will allow for fast visual recognition when multiple zones/lines are present.
Object Class Filter	Create an **Object Filter**. Object filters can be used to filter predefined objects from triggering an analytics event. Filters can also be configured to trigger an event ONLY when a specific object class has contacted the line. **Include/Exclude –** Select **Include** to trigger an event with only objects of the selected classification. Select **Exclude** to exclude objects of the selected classification from triggering analytics events. To create an **Object Class Filter**, check off a filter and choose the object class in the **Value** field drop-down (**Filter 0** is actively filtering the **Clutter** object class in the below example).  For information on configuring object classes, see Classification Settings.
Presence	Enable this rule to trigger an analytics event whenever an object comes into contact with any portion of the line. The line will remain triggered so long as contact is maintained between the line and the object.
Enter	Enable this rule to trigger an analytics event whenever an object contacts the line.
Exit	Enable this rule to trigger tan analytics event whenever an object ceases contact with the line.
Appear	Enable this rule to trigger an analytics event whenever an object is detected and is already in contact with the line. This rule is generally reserved for use with zones and is not recommended for lines.
Disappear	Enable this rule to trigger an analytics event whenever the camera ceases tracking an object which was in contact with the line before tracking ceased. This rule is generally reserved for use with zones and is not recommended for use with lines (tripwires).
Stopped	Enable this rule to trigger an analytics event whenever an object has stopped moving on the line for equal or greater than the defined amount of **Time (Seconds)**.

VCA Line – Rule Config.	Description
Dwell	Enable this rule to trigger an analytics event whenever an object has dwelled on the line longer than the defined **Threshold (Seconds)**. This rule is generally reserved for zones and functions similarly to the **Stopped** rule when used with a line.
Direction Filter	Enable this rule to trigger analytic events based on directional movement across the line. A directional indicator will be overlaid over the line. Adjust the **Direction** and **Acceptance** angle to configure a direction spectrum. Only objects travelling across the line within this directional spectrum will trigger an analytics event.This rule is generally reserved for use with zones, and functions similarly to the **Counting Line** rule (outlined below) when used with a Line (tripwire).
Speed Filter	Enable this rule to trigger an analytics events whenever an object travels through the zone within the defined speed range Configure a **Lower Bound (km/h)** and **Upper Bound (km/h)** speed value to define your speed range.
Tailgating	Enable this rule to trigger an analytics event whenever an object enters the zone within the defined **Time (Seconds)** period after another object has entered. If the **Time (Seconds)** value is set to 5, then anytime an object enters a zone within 5 seconds of another object, the camera will consider this tailgating and an analytics event will be triggered.
Counting Line	Enable this rule to trigger an analytics event whenever an object crosses the line in a chosen direction. **Directions** - Configure which directions to monitor by selecting **Direction A, Direction B,** or both. An on-screen overlay will be visible to demonstrate which directions correspond to A and B. **Width Calibration** - Enable **Width Calibration** to indicate the anticipated width of counted objects. An overlay will appear in the live preview, over the line. Small lines on either side show the minimum and maximum object widths. Use your mouse-wheel or click-and-drag the marker to change the width. **Shadow Filter** - Enable **Shadow Filter** to help mitigate the possibility of shadows causing a false trigger. This technology utilizes light and color sensitivity to avoid detection of shadows but **does not** guarantee false trigger prevention.
Color Filter	Enable this rule to trigger an analytics event whenever an object of a specified color contacts the line. Set a **Threshold (%)** to designate how much of an object must feature the specified color to trigger the alarm. If the Color is set to Blue, and the **Threshold** is set to 25%, than an object which is 25% blue or more will trigger an analytics event.

4). Right-clicking a line within the preview area will deploy a menu.

The options are as followed:

VCA Line– Right-Click Option	Description
Remove Line	Remove the line from the live preview. All rules associated with the zone will be deleted.
Insert/Remove Node	**Insert/Remove** a node to the line to create another line segment.
Rules	Enable a rule. If a secondary setting for a rule exists **(Dwell, Directional Filter, etc…)** default values for the secondary settings will be used.
Pause	Pause the live video preview on the current frame.

5). Click the **Apply** button to save your new VCA Zone/Line settings.

CREATE COUNTER

Steps:

1). To create a **Counter**, right-click within the preview area at the location you wish to overlay the counter and select **Counter>Add Counter.**

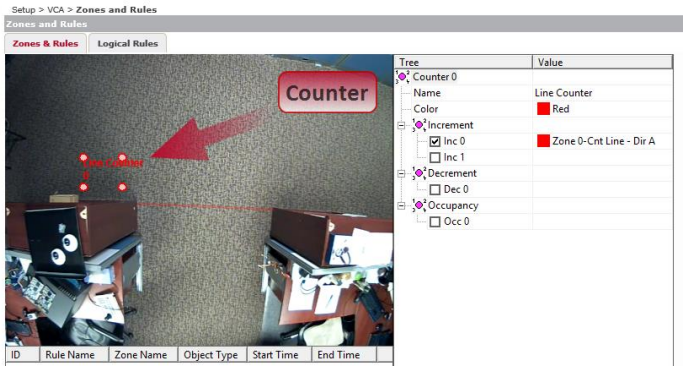
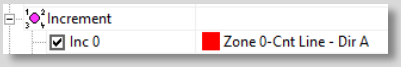
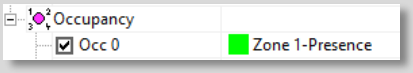


Figure 7-69: Setup Tab –VCA Menu –Zones and Rules Settings – Creating a Counter

2). When a counter is selected, the following options will be available in the **Rule Configuration Menu**:

VCA Counter– Rule Config	Description
Name	Name the counter. This name will be used to refer to this particular line throughout the cameras browser interface and on the counter overlay itself.
Color	Assign a color to the counter. This will allow for fast visual recognition when multiple zones/lines/counters are present.
Increment	Enable **Increment** to increment the counter anytime a chosen analytics event occurs.  Activate the desired increment rule (**Inc 0** used in the above example) and assign a rule trigger under the **Value** column (A counting line rule named **Zone 0 –Cnt Line – Dir A** is used in the above example).

VCA Counter – Rule Config.	Description
Decrement	Enable **Decrement** to decrement the counter anytime a chosen analytics event occurs.  Activate the desired increment rule (**Dec 0** used in the above example) and assign a rule trigger under the **Value** column (A counting line rule named **Zone 0 –Cnt Line – Dir A** is used in the above example).
Occupancy	Enable **Occupancy** to count occupants of a specified zone.  Activate the desired occupancy rule (**Occ 0** used in the above example) and assign a rule trigger under the **Value** column (A zone presence rule named **Zone 1 – Presence** is used in the above example).

3). Click the **Apply** button to save your new VCA Counter settings.

ZONES AND RULES SETTINGS – LOGICAL RULES TAB

From the **Logical Rules** tab, a user may set up further rules governed by a set of custom logical operators. Logical rules can be written in such a manner that they can run on a schedule; while other rules or events are active (or not active); when a digital input is received, etc. These **Logical Rules** can also be used to trigger the generation of events (alarms/DO); incrementing of custom counters, etc…

Steps:

1). To open the **Logical Rules** settings tab, click the Logical Rules tab on the **Setup (Advanced Tab)>VCA>Zones and Rules** settings page.

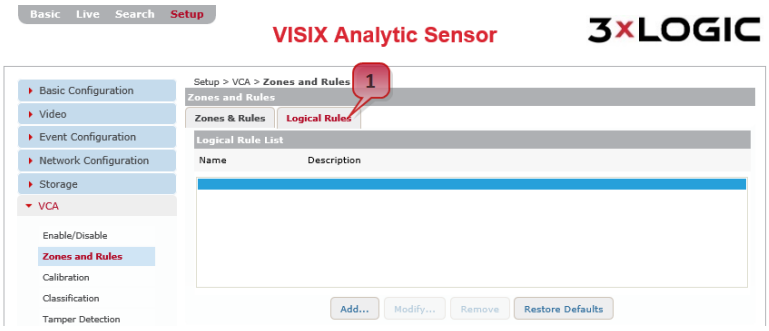


Figure 7-70: Setup Tab –VCA Menu –Zones and Rules Settings – Opening the Logical Rules Tab

2). From the **Logical Rules** settings tab, a user may **Add, Modify, or Remove** a logical rule.

3). For instructions on adding/modifying a logical rule, see Adding/Modifying a Logical Rule. To remove an existing logical rule, select the rule from the list and click **Remove.** You will be prompted to confirm the removal. Click **OK** to confirm.

ADDING/MODIFYING A LOGICAL RULE

Steps:

1). To add a logical rule, click the **Add…** button. If modifying an existing rule, select the rule from the list and click **Modify…** Both actions will cause the **Add/Modify New Rule** window to deploy.

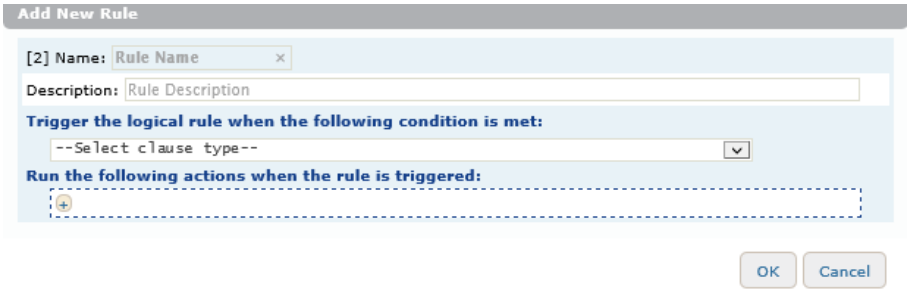


Figure 7-71: Setup Tab –VCA Menu –Zones and Rules Settings – Logical Rules Form

2). Assign a **Name** and **Description** to the rule by filling in the respective fields.

3). Under the **Trigger the Logical Rule when the Following Condition is Met** text, a user may select a condition clause. Some of these clauses will require secondary conditional clauses to be chosen as well **([and], [or], etc…)** Descriptions of the available condition clauses are listed below:

Logical Rule - Clause	Description
[rule]	Select this conditional clause to trigger the logical rule whenever a VCA rule is true/active. Select the conditional trigger rule from the available drop-down.
[and]	Select this conditional clause to trigger the logical rule whenever multiple clauses are simultaneously true/active. Select the conditional clause from the available drop-down. All chosen conditional clauses must be true to trigger the logical rule.
[or]	Select this conditional clause to trigger the logical rule whenever one of multiple clauses rules is true. Select each conditional trigger rule from the drop-downs as necessary. Only one of the multiple configured rules must be triggered/active to trigger the logical rule.
[not]	Select this conditional clause to trigger when a specified clause is not true.
[continuously]	Select this conditional clause to trigger the logical rule whenever a clause has been continuously true/false for a specified period of time.
[previous]	Select this conditional clause to trigger the logical rule when a clause was previously true/false for a specified period of time.
[was]	Select this conditional clause to trigger the logical rule when a clause was true/false a specified period of time ago.
[time]	Select this conditional clause to trigger the logical rule during a specified daily time range.

Logical Rule – Clause	Description
[day]	Select this conditional clause to trigger the logical rule on a specified day of the week.
[date]	Select this conditional clause to trigger the logical rule on a specified date of the year.
[value]	Select this conditional clause to trigger the logical rule whenever a VCA counter reaches a specified value. Select the desired **Counter, operator (<, >, =)** and specify a counter value in the available text field.
[input]	Select this conditional clause to trigger the logical rule whenever a digital input of your choosing is in a state (open, closed) of your choosing. Select the desired input and state from the available drop-down menus.
[before]	Select this conditional clause to trigger the logical rule whenever a specified **[and]** conditional clause occurs before another. **NOTE:** This clause is only available as a secondary conditional clause within an **[and]** clause.
[identity]	Select this conditional clause to trigger the logical rule whenever two specified clauses are each triggered by the same (or different; user specified) objects. **NOTE:** This clause is only available as a secondary conditional clause within an **[and]** clause.
[within]	Select this conditional clause to trigger the logical rule whenever two specified **[and]** conditional clauses are each triggered within a specified amount of time of one another. **NOTE:** This clause is only available as a secondary conditional clause within an **[and]** clause.
[classification]	Select this conditional clause to trigger the logical rule whenever a specified **[and]** conditional clause is triggered by an object of a specified class. **NOTE:** This clause is only available as a secondary conditional clause within an **[and]** clause.
[between]	Select this conditional clause to trigger the logical rule whenever a specified **[and]** conditional clause is triggered between two specified times. Select the desired clause and configure the two times using the available drop-down menus. **NOTE:** This clause is only available as a secondary conditional clause within an **[and]** clause.
[tamper]	Select this conditional clause to trigger the logical rule whenever tampering detected. See Tamper Detection Settings for more info on configuring tamper detection.
[learning]	Select this conditional clause to trigger the logical rule whenever a scene is being learned.

4). Configure your conditional trigger clause as desired. When you have configured the clause, the trigger actions must also be selected. The trigger action is simply the resulting action of the logical rule being triggered.

A list of available trigger actions is described below:

Logical Rule - Action	Description
[generateevents]	Select this action to generate an event whenever the logical rule is triggered.
[incrementcounter]	Select this action to increment a specified VCA counter whenever the logical rule is triggered.
[learnscene]	Select this action to have the camera perform scene learning whenever the logical rule is triggered.
[resetcounter]	Select this action to reset a specified VCA counter whenever the logical rule is triggered.

5). Once you have configured both a conditional clause and a trigger action, click **OK** to save the new logical rule.

CALIBRATION SETTINGS

Steps:

1). Opening the **Setup Tab>VCA** drop-down menu and clicking the **Calibration** link will open the network **DDNS** settings page.

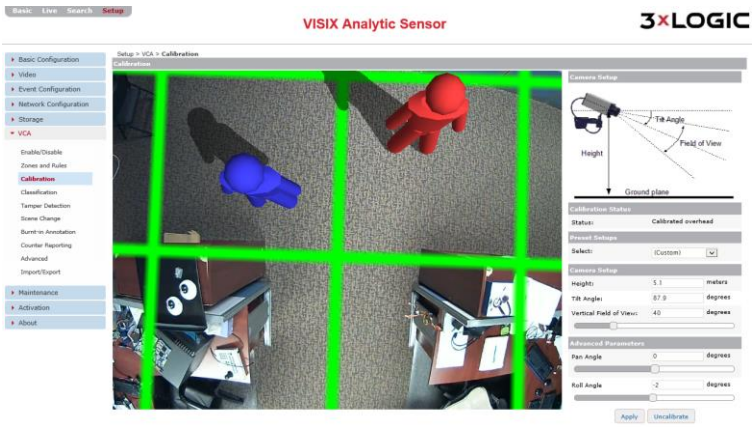


Figure 7-72: Setup Tab –VCA Menu –Calibration Settings

2). The VCA calibration process includes configuring the correct camera angle and field of view, as well as the delineation of anticipated object **(people, car, etc…)** size. Proper calibration of the camera is required to ensure accurate analytics counts and tracking.

The following calibration specifications are available for configuration:

VCA Calibration Spec	Description
Preset Select	Select a preconfigured preset. Presets include: **Overhead, 60 Degree Lookdown, 30 Degree Lookdown**.
Height	Adjust calibration height. Use this to best emulate the height of the camera from the ground. Note the mimic size in comparison with an actual person to gain the best results.
Tilt Angle	Adjust calibration tilt angle. Use this to best emulate the camera's tilt angle.
Vertical Field of View	Adjust the calibration vertical field-of-view. Use this to best emulate the camera's vertical perspective.
Pan Angle	Adjust the calibration roll angle. Use this to best emulate the camera's pan perspective.
Roll Angle	Adjust the calibration roll angle. Use this to best emulate the camera's pan perspective.

Steps:

1). To begin calibration, adjust calibration settings as required. A user may perform basic calibration cameras via two separate methods:

1). **Click-and-Drag**. - For this method, click and drag the green calibration grid to satisfactorily emulate the camera's height, tilt perspective, and field of view. The mimics may be moved around the image to help the user gauge perspective. The mouse scroll wheel is also utilized to adjust camera height, and consequentially the size of the calibration grid and mimics. Use resizing of these elements to anticipate average object size.

2). **Manual Configuration** - Manually enter/adjust calibration values under the **Camera Setup** section. As the user enters values, the calibration overlay on the live preview will react accordingly.

3). If required, adjust **Pan Angle** and **Roll Angle** under the **Advanced Parameters** section using the slider bars. As the sliders are moved, the calibration overlay over the preview image will react accordingly. Advanced Parameters must be manually entered and cannot be adjusted using the Click-and-Drag technique.

4). Right-click within the video preview area for the following calibration tools:

Right-Click Option	Description
Virtual Ruler	Select this tool to anchor a virtual ruler from the point-of the right click. Drag your mouse across the image to extend the ruler. Use this feature to ensure accurate perspective calibration settings.
Draw Horizon	Select this option to add a drawn horizon line to the calibration grid. This horizon line will be visible when the camera's tilt angle is twenty degrees or less.
Transparent Grid (enabled by default)	Select this option to make the green calibration grid transparent.

Right-Click Option	Description
Add Mimic	Add another mimic to the live preview.
Pause	Pause the live preview image on the current frame.

5). When you have calibrated the camera to your satisfaction, click **Apply** to save the new calibration settings.

6). If desired, click **Uncalibrate** to reset all calibration specifications to their default value.

CLASSIFICATION SETTINGS

Steps:

1). Opening the **Setup Tab>VCA** drop-down menu and clicking the **Classification** link will open the VCA object **Classification** settings page.

Figure 7-72: Setup Tab –VCA Menu –Classification Settings

2). From the **Classification** settings page, a user may **Add, Remove** or modify an object classification. Four default classifications exists: **Clutter, Person, Group of People, and Vehicle**.

3). To create a new classification, click the **Add** button and configure the required classifier information. To modify an existing classification, select it from the list and edit the classifier information as required. Classifier information is described below:

Classifier Info	Description
Name	Name the classification.
Enable	Enable the classification to have the camera actively classify objects that meet the classification's parameters. If disabled, the camera will not classify objects with this class.
Min Area	The minimum area (in square meters) taken up by an object of this classification.
Max Area	The maximum area (in square meters) of an object of this classification.
Min. Speed	The minimum travelling speed (in km/h) of an object of this classification.
Max. Speed	The maximum travelling speed (in km/h) of an object of this classification.

4). Click **Apply** to save the new classification settings.

5). Click **Restore Defaults** to reset the classifications to their default settings. This will delete any custom classification.

TAMPER DETECTION SETTINGS

Steps:

1). Opening the **Setup Tab>VCA** drop-down menu and clicking the **Tamper Detection** link will open the VCA object **Tamper Detection** settings page.

Figure 7-72: Setup Tab –VCA Menu –Tamper Detection Settings

2). From the **Tamper Detection** settings window, a user may enable **Tamper Detect**, and configure related settings. **Tamper Detection** safeguards the camera against vandalism or view obscuration by generating an alarm whenever tampering is detected.

3). To activate tamper detection, check-off **Enable**.

The following tamper detection settings can be configured:

Classifier Info	Description
Tamper Duration Until Alarm	The amount of time allowed to transpire during tampering until the tamper alarm is triggered.
Tamper Image Area	The amount of the image to use for the tamper detection algorithm.
Suppress Alarm on Lights On/Off	Select this option to suppress alarms accidentally generated by lights within the image turning on/off.

4). Click **Apply** to save changes to tamper detection settings. Click **Restore Defaults** to restore tamper detection settings to their default state.

SCENE CHANGE SETTINGS

Steps:

1). Opening the **Setup Tab>VCA** drop-down menu and clicking the **Scene Change** link will open the **Scene Change** settings page.

Figure 7-73: Setup Tab –VCA Menu –Scene Change Settings

2). From the **Scene Change** settings page, a user may configure scene changes settings and enable day/night mode detection.

Descriptions of configurable settings are listed below:

Scene Change Setting	Description
Mode	■ **Automatic –** Automatically detect scene changes. ■ **Manual -** Manually trigger ■ **Disabled –** Disable **Scene Change** detection.
Advanced Settings	■ **Changed Time –** The amount of time that must transpire after a detected scene change to trigger event. ■ **Changed Image Area –** The amount of the image area that will be utilized to detect scene changing.
Day/Night Mode Change Detection	Select **Enable** to detect the transition between day and night. This process works by looking for color from/to the grayscale transition between two successive frames.

BURNT-IN ANNOTATION SETTINGS

Steps:

1). Opening the **Setup Tab>VCA** drop-down menu and clicking the **Burnt-In Annotation** link will open the **Burnt-In Annotation** settings page.

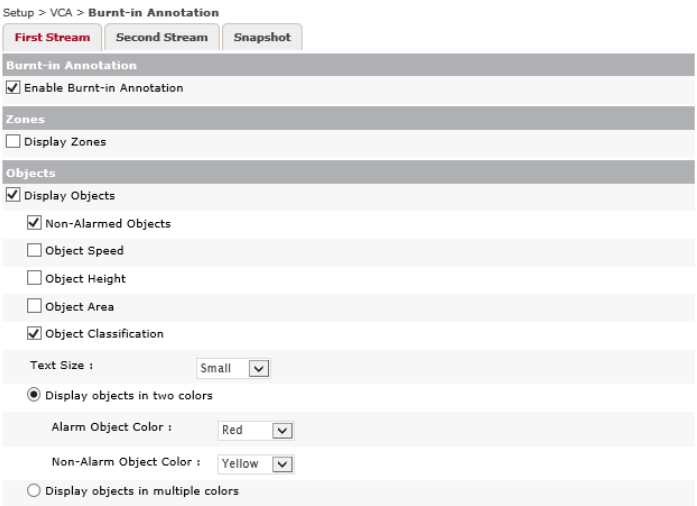


Figure 7-74: Setup Tab –VCA Menu –Burnt-In Annotation Settings 1(screenshot cont'd on next page)

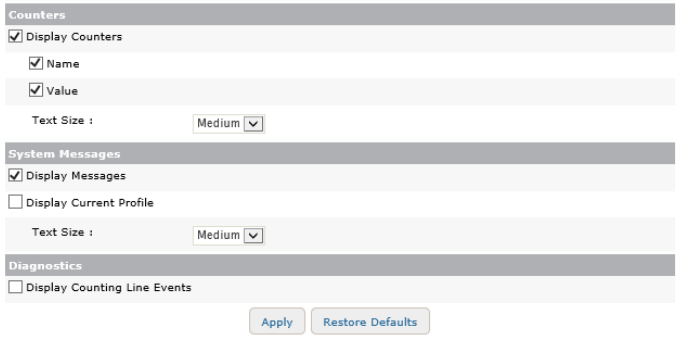


Figure 7-75: Setup Tab –VCA Menu –Burnt-In Annotation Settings 2

2). From the **Burnt-In Annotation** settings, a user may configure settings related to the on-screen display of VCA components in live and recorded footage. Settings may be configured for each individual stream profile by selecting the desired profile tab near the top of the settings form.

NOTE:
VCA components are visible in the VCA Rules and Zones settings page video preview as well as on the Live tab (if chosen to be displayed in the Live tab right-click menu). These are for reference during configuration only and are not burnt-in to recorded video. Enable burnt-in annotation for desired VCA components to ensure they are visible on recorded video.

3). Click **Enable Burnt-In Annotation** to enable burnt-in annotations and reveal related options and settings.

Burnt-In Settings	Description
Zones	**Display Zones** – Select this option to burn any VCA zones into the camera image.
Objects	**Display Objects –** Select this option to burn in VCA object trackers. The following options may be enabled for burnt-in object tracking: ▪ **Non Alarmed Objects –** Burn-in object tracking for objects not triggering an alarm/event. ▪ **Object Speed –** Burn-in the object's speed value (km/h). ▪ **Object Height –** Burn in the objects height measurement value. ▪ **Object Area –** Burn in the object area measurement value (m^2). ▪ **Object Classification –** Burn in the objects classifications ▪ **Text Size –** Select a preconfigured size (small, medium, large) for the burnt-in text. ▪ **Display Objects in Two Colors –** Display burnt-in colors for **Alarmed and Non-Alarmed** (Objects not currently triggering an alarm/event) objects differently. Select the color for each object type from the available drop-down menu. ▪ **Displays Objects in Multiple Colors –** Enable multiple burnt-in object tracking colors when multiple objects are present.
Counters	**Display Counters –** Select this option to burn in any VCA counters into the camera image. A user may choose to burn-in the counter's *Value*, *Name* or both by checking off the corresponding box.
System Messages	**Display System Messages** – Select this option to burn system messages into the camera image. **Display Current Profile –** Select this option to burn the current stream profile's information into the camera image. ▪ **Text Size –** Select a preconfigured size (small, medium, large) for the burnt-in text.
Diagnostics	**Display Counting Line Events –** Select this option to burn counting line event information into the camera image.

4). Click **Apply** to save settings changes. Click **Restore Defaults** to restore settings to their default state.

COUNTER REPORTING SETTINGS

Steps:

1). Opening the **Setup Tab>VCA** drop-down menu and clicking the **Counter Reporting** link will open the **Counter Reporting** settings page.

2). The Counter Reporting settings page is split across three tabs: The Reporting Service, Database Service and E-mail Notifications tabs.

Each is outlined in the below sections.

REPORTING SERVICE TAB – COUNTER REPORTING SETTINGS

Steps:

1). From the **Reporting Service** tab, a user may configure settings related to the reporting of VCA counter data.

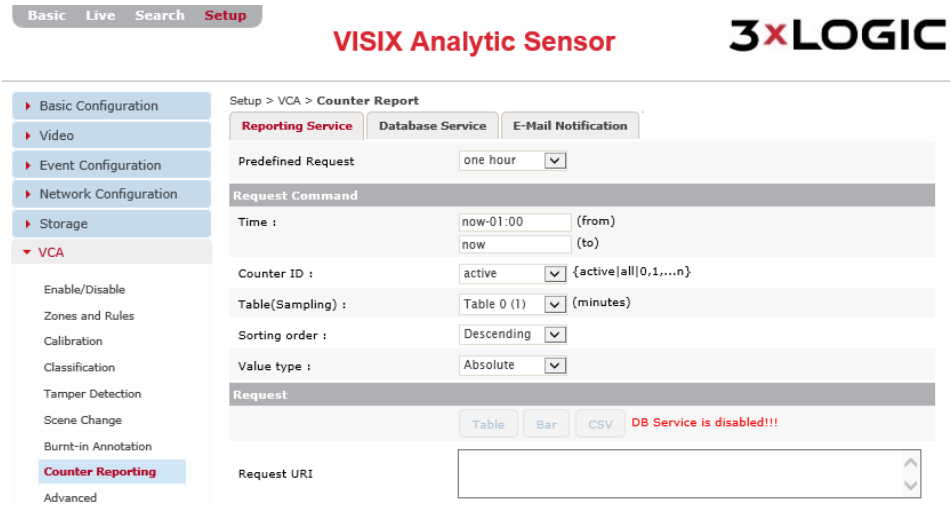


Figure 7-76: Setup Tab –VCA Menu –Counter Reporting Settings – Reporting Service Tab

2). If desired, select a **Predefined Request** from the drop-down menu to autofill the **Request Command** information. Available options include **One Hour, Today, Yesterday, One Day** (the last 24 hours), **This Week** (first day of the current week until present), **Last Week, One Week, This Month** (first day of the current month until present) and **Last Month.**

3). If a custom counter report is desired, fill out the required fields in the **Request Command** section manually.

Available settings include:

Request Command	Description
Time	Fill out the **To** and **From** fields to designate a time range for the counter report.
Counter ID	Select the counter to report data on. An individual counter may be chosen by selecting its corresponding ID (1-19). Select **Active** to report on only active counters. Select **All** to report on all counters.
Table (Sampling)	Select the table to use in the report. Each table features a separate **Sampling Interval and Roll-Over Count**. See Database Service Tab for more information on configuring counter report tables.
Sorting Order	Select whether the results should be displayed in **Ascending** or **Descending** order.
Value Type	Select whether the displayed results should be **Absolute** value of each counter, or the **Difference** between counters.

4). Under the **Request** section, select the report style. Available styles include: **Table, Bar** and **CSV**. Please note, a **Counter Report** cannot be generated without enabling **Database Service** on the Database Service tab. Please enable **Database Service** to enable counter report generation.

5). After selecting a style, a pop-up will open with your report and a URL link to the report will also be available in the **Request URL** field.

DATABASE SERVICE TAB – COUNTER REPORTING SETTINGS

Steps:

1). From the **Database Service** tab, a user may enable **Database Service** (required for counter reporting and counter report email notifications) and configure related settings.

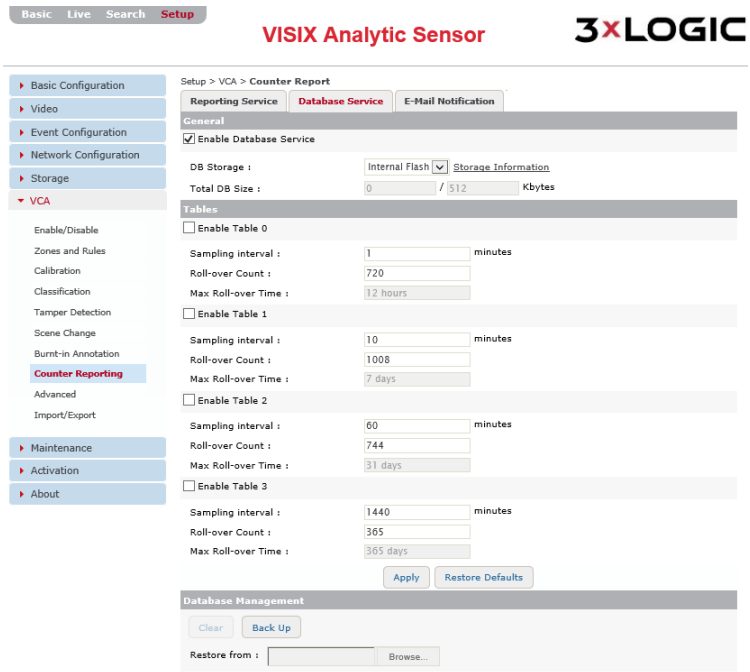


Figure 7-77: Setup Tab –VCA Menu –Counter Reporting Settings– Database Service Tab

2). Enabling **Database Service** will create a database to store counter reporting data.

3). Select the **DB Storage** medium by choosing either **Flash** (internal) or **SD** (removable storage) from the drop-down menu. After selecting your storage medium, designate a **Total DB Size** (in kilobytes). The maximum available amount of storage will vary depending on your chosen storage medium.

4). Under the **Tables** section, a user may enable up to four DB tables by checking off the corresponding **Enable Table x** box.

The following table settings can be configured:

Table Settings	Description
Sampling Interval	Set the table's sampling interval (in minutes).
Roll-Over Count	Set the table's **Roll-Over** count. New entries will begin to replace the oldest existing entries when the count has reached this value.
Max Roll-Over Time	The maximum amount of time that can be allowed to transpire before overwriting of the oldest existing entries will begin based on the defined **Sampling Interval** and **Roll-Over Count** values. This setting is not directly configurable.

5). Click **Apply** to save settings changes. Click **Restore Defaults** to restore all settings to their default state.

6). Under the **Database Management** section, a user may select **Clear** to clear the current database. Select **Back-Up** to make a back-up copy of the database and its current structure and content. The backup will be automatically downloaded to your browser's **Downloads** folder.

7). If the database requires restoration, select the **Browse** button next to the **Restore From** field and select a DB backup file to restore DB structure and contents.

E-MAIL NOTIFICATION TAB – COUNTER REPORTING SETTINGS

Steps:

1). From the **E-Mail Notification** tab, a user may configure VCA counter report e-mail notifications and their related settings.

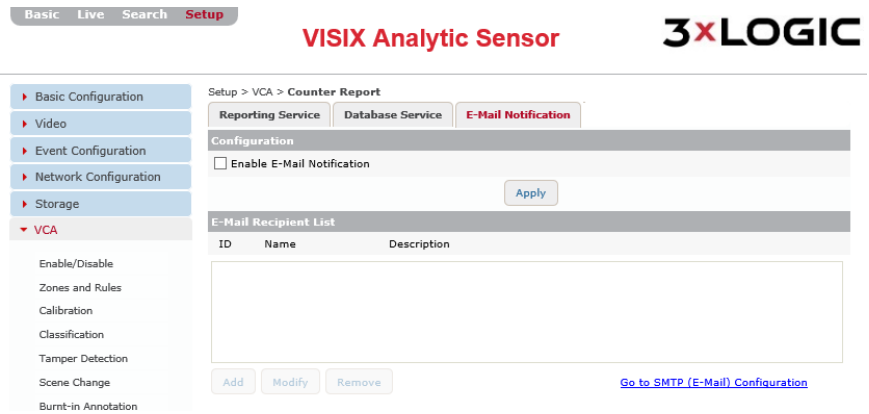


Figure 7-78: Setup Tab –VCA Menu - Counter Reporting Settings–E-Mail Notifications Tab

2). To enable VCA counter reporting e-mail notifications, check-off **Enable E-Mail Notification**.

3). Once notifications are enabled, a user may **Add, Modify or Remove** a counter reporting e-mail notification recipient. When adding/modifying a recipient, recipient and report settings may also be edited.

4). Select a recipient from the list to display recipient information. To remove a recipient, select the desired recipient from the list and click **Remove.**

5). **SMTP (E-mail Server) Settings** must be configured in order for e-mail notifications to function. Click the **Go to SMTP (E-Mail) Settings** link to open the SMTP settings form and configure settings as necessary. See SMTP (E-Mail Server) Settings for more info.

ADD/MODIFY A COUNTER REPORT E-MAIL NOTIFICATION RECIPIENT

Steps:

1). To add a recipient, click the **Add…** button (if modifying, select the desired recipient from the list and click **Modify…**). The **Add/Modify E-Mail Recipient** form will deploy.

E-MAIL CONFIGURATION

Steps:

1). In the **E-Mail Configuration** section of the form, a user may enter basic recipient info.

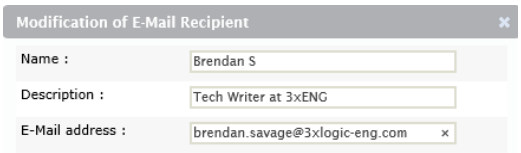


Figure 7-79: Setup Tab –VCA Menu - Counter Reporting Settings–E-Mail Notifications Tab – Add/Modify E-Mail Recipient

2). Fill in the **Name, Description** and **E-mail Address** fields for the desired recipient.

E-Mail Recipient Setting	Description
Name	Name the recipient. This name will be used to identify this particular recipient when assigning it to an e-mail notification.
Description	Provide a brief description of the recipient (intended use, etc…). This description will be displayed when the schedule is selected on the schedule settings page.
E-Mail Address	Enter the e-mail address of the recipient.

SCHEDULE CONFIGURATION

Steps:

1). In the **Schedule Configuration** section of the **Add/Modify Recipient** window, a user may configure a notification schedule for the recipient.

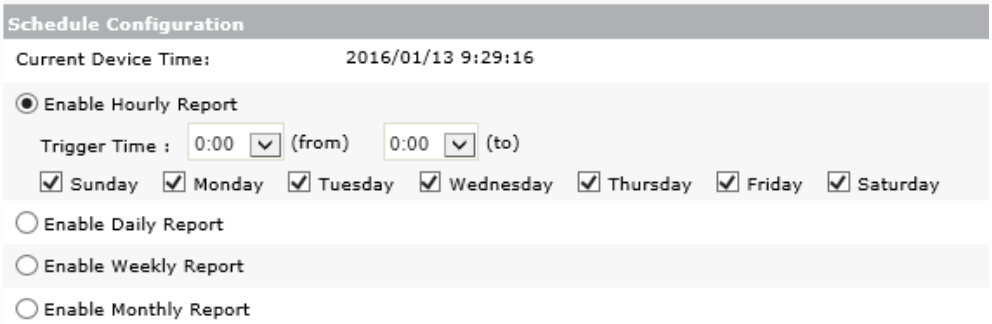


Figure 7-80: Setup Tab –VCA Menu - Counter Reporting Settings–E-Mail Notifications Tab – Schedule Configuration

2). Enable an **Hourly, Daily, Weekly** or **Monthly** report. When the desired report is selected, related settings will be deployed and can be customized.

Schedule Settings	Description
Hourly	Enable hourly reporting to send a report on a customized hourly basis. Select **From** and **To** trigger times from the available drop-down menus to choose which hours in a day the hourly report will be sent. If 1:00 and 8:00 are selected as **From** and **To** respectively, then a report will be e-mailed on the hour from 01: 00 to 08:00. Select the days of week the report will be emailed on. The report will be sent on the chosen days, during the designated trigger hour range.
Daily	Enable daily reporting to send reports on a customized daily basis. Select a **Trigger Time** from the drop-down menu. The report will be e-mailed at the selected time. Select days of week the report will be emailed on. The report will be sent on the chosen days, at the designated trigger hour.
Weekly	Enable weekly reporting to send reports on a customized weekly basis. Select a **Trigger Day** and **Trigger Time** from the available drop-down menus. The report will be emailed to the recipient on the chosen day, at the chosen time.
Monthly	Enable monthly reporting to send reports on a customized monthly basis. Select a **Trigger Day** (1-31) and **Trigger Time** from the available drop-down menus. Reports will be emailed to the recipient on the chosen day of the month, at the chosen time.

REPORT CONFIGURATION

Steps:

1). In the **Report Configuration** section of the **Add/Modify Recipient** window, a user may configure an email counter report settings.

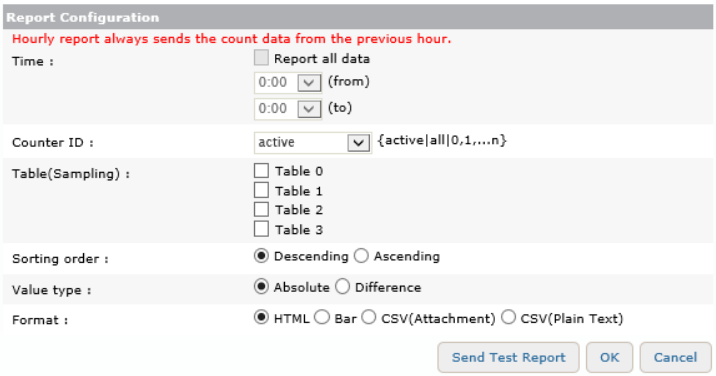


Figure 7-81: Setup Tab –VCA Menu - Counter Reporting Settings–E-Mail Notifications Tab – Report Configuration

Report Setting	Description
Time	Select **Report All Data** to report all counter data within the schedule range. If a custom range is desired, fill out the **To** and **From** fields to designate a time range for the counter report.
Counter ID	Select the counter to report data on. An individual counter may be chosen by selecting its corresponding ID (1-19). Select **Active** to report on only active counters. Select **All** to report on all counters.
Table (Sampling)	Select the table(s) to use in the report. Each table features a separate **Sampling Interval and Roll-Over Count**. See Database Service Tab for more information on configuring counter report tables.
Sorting Order	Select whether the results should be displayed in **Ascending** or **Descending** order.
Value Type	Select whether the displayed results should be **Absolute** value of each counter, or the **Difference** between counters.
Format	Select the report format for the email counter report.

2). Click **Send Test Report** to send a test report using the currently configured settings to the e-mail entered in the **E-mail Configuration** section**.**

3). Click **OK** to save the new recipient. Click **Cancel** to close the window without saving the recipient.

ADVANCED VCA SETTINGS

Steps:

1). Opening the **Setup Tab>VCA** drop-down menu and clicking the **Advanced** link will open the **Advanced** VCA settings page.

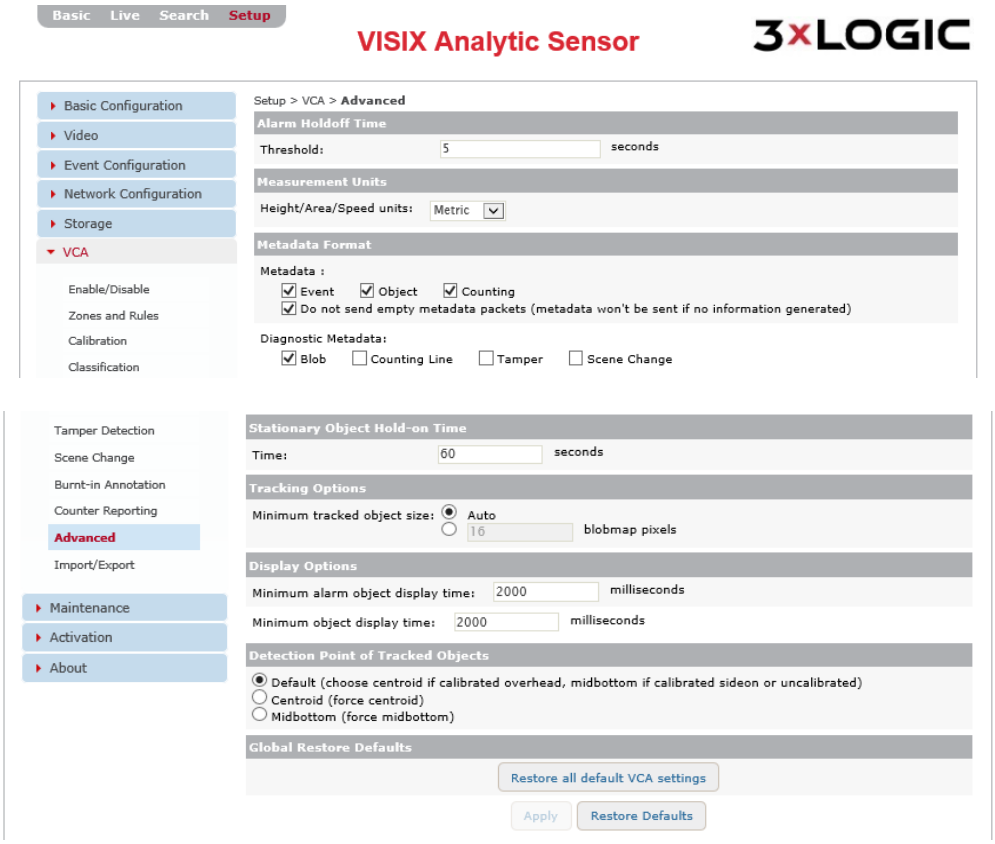


Figure 7-82: Setup Tab –VCA Menu –Advanced VCA Settings

2). From the **Advanced** VCA settings page, a user may configure settings related to advanced operation of VCA video analytics.

Configurable settings include:

Advanced Setting	Description
Alarm Hold-Off Time	Configure the amount of time (in seconds) allowed to transpire between a VCA event/alarm creation and the action which triggered the event/alarm.
Measurement Units	Select a desired measurement system from the available drop-down. These units will be used for approximating VCA object height/area/speed. Metric is the camera default.
Metadata Format	**Metadata** - Select your desired metadata categories: **Event, Object**, and **Counting**. Select **Do Not Send Empty Metadata Packets** to avoid sending packets when there is no data available. **Diagnostic Metadata** - Select your desired diagnostic metadata categories: **Blob (Motion), Counting Line, Tamper** and **Scene Change**.
Stationary Object Hold-On Time	Configure the amount of time the camera will track a stationary VCA object before it ceases tracking.

Advanced Settings	Description
Tracking Options	Configure the **Minimum Tracked Object Size**. Select *Auto* to only track objects equal to or larger than the smallest object classification. To configure a custom size, select the **Blobmap Pixels** option and enter the desired value.
Display Options	Configure a **Minimum Alarm Object Display Time**. Objects which have triggered an event/alarm will display an alarm tracker (red object tracker) for, at a minimum, the designated amount of time.
Detection Point of Tracked Items	Configure a detection point for tracked objects: 1). **Default** - Default mode will use **Centroid** if calibrated as overhead or **Midbottom** if calibrated as sideview or if the camera is uncalibrated. 2). **Centroid** – Detection point for objects is at centroid. Recommended for overhead camera 3). **Midbottom** – Detection point for objects is the Midbottom region. Recommended for sideview or uncalibrated cameras.
Global Restore Defaults	Select **Restore All Default VCA Settings** to restore all VCA settings to their factory default state.

3). Click **Apply** to save settings. Click **Restore Defaults** to restore all VCA advanced settings to their default state.

IMPORT/EXPORT SETTINGS

Steps:

1). Opening the **Setup Tab>VCA** drop-down menu and clicking the **Import/Export** link will open the **Import/Export VCA Settings** page.

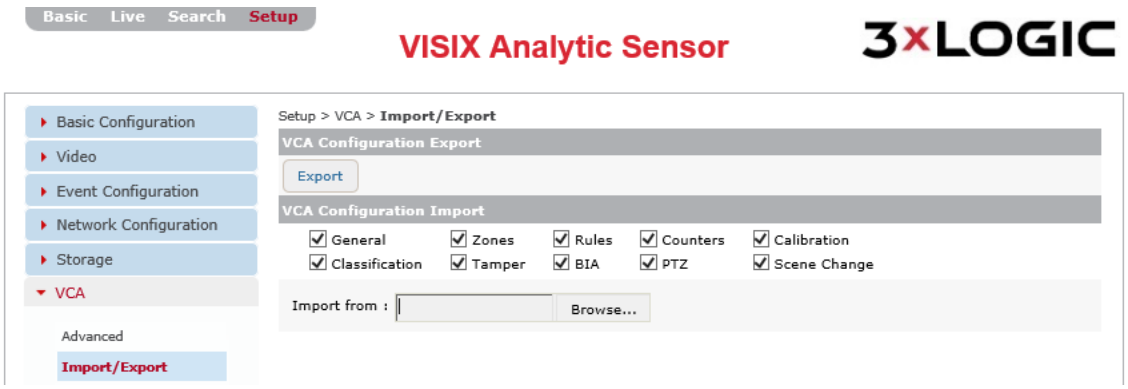


Figure 7-83: Setup Tab –VCA Menu –Import/Export Settings

2). From the **Import/Export VCA Settings** page, a user may export or import an .xml containing VCA configuration settings.

3). Click the **Export** button to download an xml file **(vca_config.xml)** to your browsers downloads destination. This file can be imported to other cameras to assign them the same VCA configurations as the device from which is was exported.

4). Under the **VCA Configuration Import** section, a user may select which VCA settings configuration to import from the file.

5). To import a VCA settings file, click the **Browse** button, navigate to and select the desired xml file and click **Open.** Only VCA settings configurations which have been checked-off in the **VCA Configuration** Import section will be imported to the device.

7.7 Maintenance Menu

USERS

Steps:

1). Opening the **Setup Tab>Maintenance** drop-down menu and clicking the **Users** link will open the **Users** settings page.

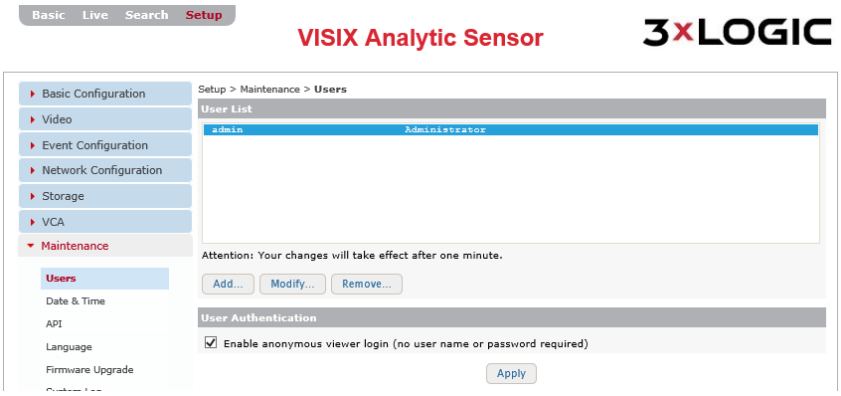


Figure 7-84: Setup Tab –Maintenance Menu – Users

2). From the **Users page**, a user may view the camera's list of user profiles. A user may also add, modify or remove a user profile. Details regarding each action are outlined in the proceeding sub-sections of this manual. User settings can also be edited from both the **Basic Tab>Camera Configuration>Users** and the **Setup (Advanced) Tab>Basic Configuration>Users** settings pages.

ADD A USER

Steps:

1). Click the **Add…** to add a new user profile. The **Add User** form (pictured right) will deploy.

Form Field	Description
Username and Password	Enter a username and password for the new user.
Confirm Password	Confirm the previously entered password.
User Group	Choose a User Group for the user.

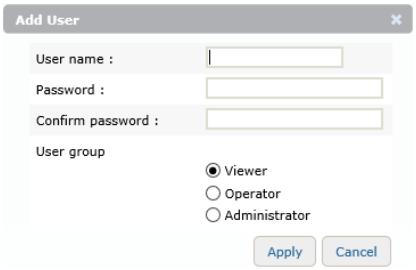


Figure 7-85: Setup Tab –Maintenance Menu – Users – Add User

2). After finishing configuration, click **Apply** to save the new settings.

MODIFY A USER

Steps:

1). Click the **Modify…**button to modify an existing user profile. The **Modify User** form (pictured right) will deploy.

Form Field	Description
Username and Password	Enter a username and password for the new user.
Confirm Password	Confirm the previously entered password.
User Group	Choose a User Group for the user.

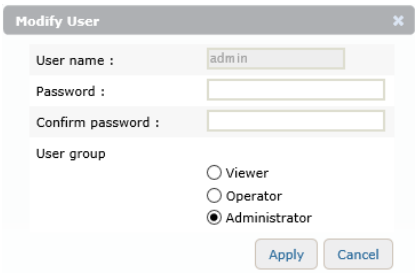


Figure 7-86: Setup Tab –Maintenance Menu – Users – Modify User

2). After finishing configuration, click **Apply** to save the new settings.

REMOVE A USER

Steps:

1). Click the **Remove** button to remove an existing user profile. This action is only available when a user profile is selected in the list. You will be prompted for a confirmation before finalizing the removal.

USER AUTHENTICATION

Steps:

1). Check-off **Enable Anonymous Viewer Login** to enable anonymous viewing (no username or password required) of the camera's live view

DATE & TIME SETTINGS

Steps:

1). Opening the **Setup Tab>Maintenance** drop-down menu and clicking the **Date & Time** link will open the **Date & Time** settings page.

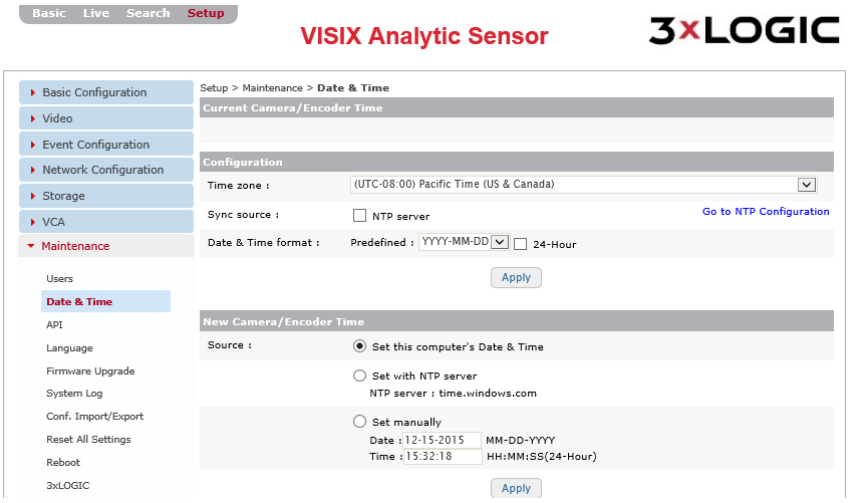


Figure 7-87 Setup Tab –Maintenance Menu – Date and Time Settings

2). From the **Date & Time** settings page, a user may edit a camera's time settings including time zone, time server, date and time format and time synchronization source.

Time Setting	Description
Current Camera Encoder Time	Displays the current camera time
Configuration	■ **Time Zone -** Select the camera time zone. ■ **Sync Source -** Set the active NTP server as your time sync source. Click the **Go to NTP Configuration** to be taken to the NTP Settings page. ■ **Date and Time Format –** Choose a predefined date-format. Enable **24-Hour** to use standard 24 hour time.
New Camera / Encoder Time	■ **Set this Computer's Date and Time –** Selecting this option will sync the camera's time with your current computer system. ■ **Set with NTP Server -** Selecting this option will sync the camera's time with the displayed NTP server (Default: time.windows.com) ■ **Set Manually –** Select this option to manually configure the camera's date and time.

3). Click **Apply** to save the new time settings.

API SETTINGS

Steps:

1). Opening the **Setup Tab>Maintenance** drop-down menu and clicking the **API** link will open the **API** settings page.

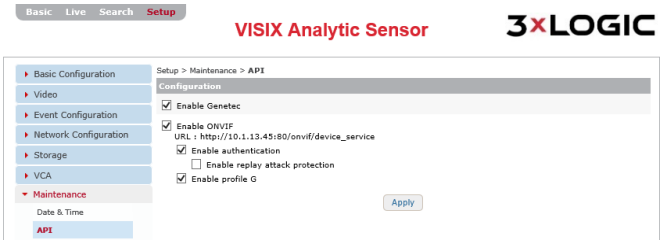


Figure 7-88 Setup Tab –Maintenance Menu –API Settings

2). From the API settings page, a user may activate settings related to the camera's application programming interface.

Configurable settings include:

Storage Detail	Description
Enable Genetec	Enable integration with Genetec security center.
Enable ONVIF	Enable ONVIF on the camera: **Enable Authentication -** Enable ONVIF Authentication. The user may also enable **Replay Attack Protection** to protect the camera against malicious/ fraudulent activity. **Enable Profile G** – Enable ONVIF Profile G.

3). Click **Apply** to save settings changes.

LANGUAGE SETTINGS

Steps:

1). Opening the **Setup Tab>Maintenance** drop-down menu and clicking the **Language l**ink will open the **Language s**ettings page.

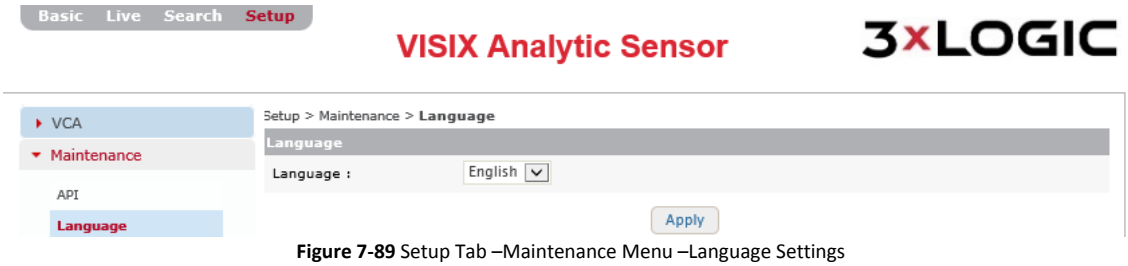


Figure 7-89 Setup Tab –Maintenance Menu –Language Settings

2). From the **Language** settings page, a user may select the camera interface language. Select a desired language from the available drop-down menu. Languages include: **English, Chinese** and **Korean**.

3). Click **Apply** to save settings changes.

FIRMWARE UPGRADE

Steps:

1). Opening the **Setup Tab>Maintenance** drop-down menu and clicking the **Firmware Upgrade** link will open the **Firmware Upgrade** page.

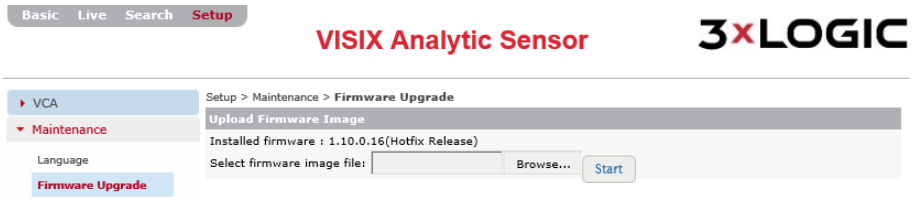


Figure 7-90 Setup Tab –Maintenance Menu –Firmware Upgrade Settings

2). From the **Firmware Upgrade** page, a user may update the device's hardware firmware. To update device firmware, simply click the **Browse** button, navigate to the location of the firmware file on your current system and select the file for use. A **Start** button will appear when a valid **.enc** file has been selected.

3). Click **Start** to begin the firmware update process.

SYSTEM LOG SETTINGS

Steps:

1). Opening the **Setup Tab>Maintenance** drop-down menu and clicking the **System Log** link will open the **System Log Settings** page.

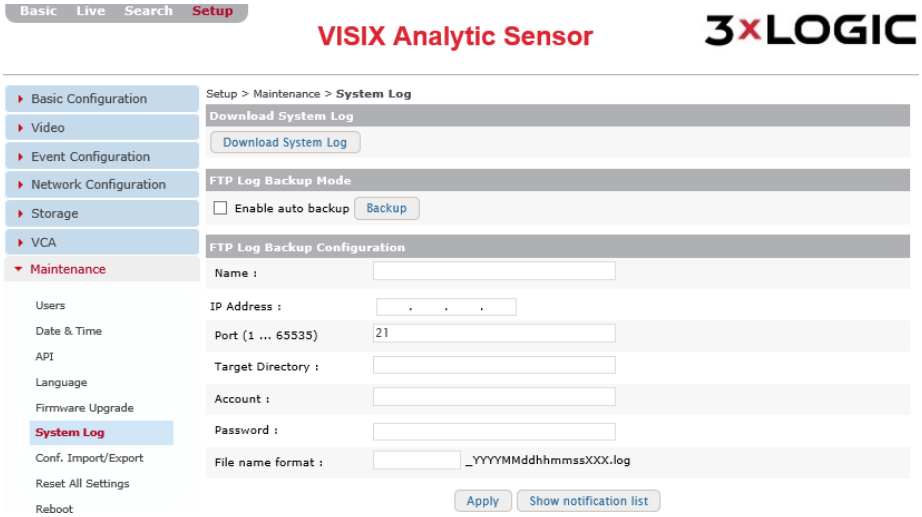


Figure 7-91 Setup Tab –Maintenance Menu –System Log Settings

2). From the System Log page, a user can click **Download System Log** for an updated copy of the log. If desired, check-off **Enable Auto Backup** and configure the following details for auto backup of the system log to an FTP service of your choosing.

FTP connection settings are described below:

FTP Setting	Description
Name	Name the FTP server. This name will be used to identify this particular FTP when selecting it for storage purposes.
IP Address/Port	Enter network connection values for the desired FTP Server.
Target Directory	Enter the target destination directory on the FTP for storing uploaded files.
Account/Password	Enter the user login credentials for the FTP. 3xLOGIC recommends using an administrative level account when possible to avoid permissions conflicts.
Filename Format	Assign the filename format for the .log files uploaded to the FTP.

3). If you have previously configured an FTP service via the FTP Notification settings, click **Show Notification List.** A list of configured FTP notifications will appear. To instantly load an FTP notification's FTP connection info into the System Log-FTP configuration form, select the desired notification from the list and click **Load Notification into Settings**.

4). Click **Apply** to save settings changes.

CONFIGURATION IMPORT/EXPORT SETTINGS

Steps:

1). Opening the Setup Tab>Maintenance drop-down menu and clicking the Configuration Import/Export link will open the Configuration Import/Export page.

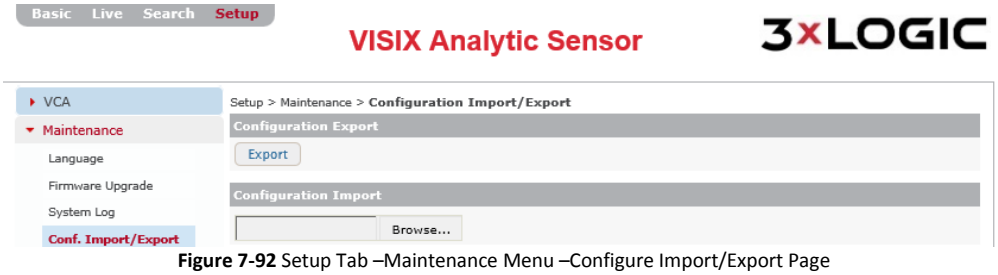


Figure 7-92 Setup Tab –Maintenance Menu –Configure Import/Export Page

2). From the **Configuration Import/Export** page, a user can export the cameras current settings configuration (**.dat** format) or import a settings configuration file to apply to the camera.

3). To export the camera's current settings, click the **Export** button. The camera settings file will be downloaded to your browser's download destination.

4). To import settings, click the **Browse…** and navigate to the files location on your system. When a file is selected, an Import button will appear. Click **Import** to import settings from the selected file.

CAUTION:

Importing a settings file will overwrite all existing camera settings.

RESET ALL SETTINGS

Steps:

1). Opening the **Setup Tab>Maintenance** drop-down menu and clicking the **Reset All Settings** link will open the **Reset All Settings** page.

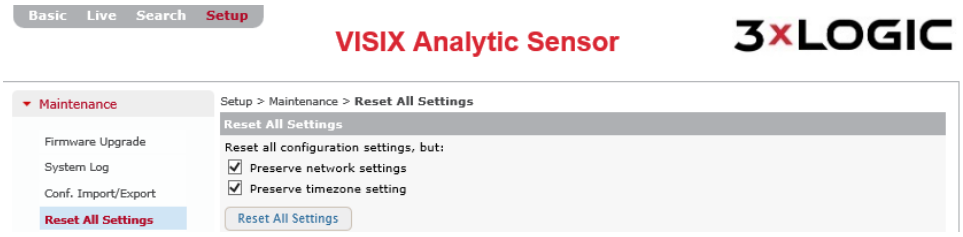


Figure 7-93 Setup Tab –Maintenance Menu –Reset All Settings

2). From the **Reset All Settings** page, a user may reset all camera settings to their factory default state.

3). Before resetting, a user may choose to preserve **Network** and **Time Zone** settings. Check-off **Preserve Network Settings** and/or **Preserve Time Zone Settings.**

4). After designating settings to be preserved, click **Reset All Settings** to restore settings to their factory defaults.

REBOOT

Steps:

1). Opening the **Setup Tab>Maintenance** drop-down menu and clicking the **Reboot** link will open the **Reset All Settings** page. To reboot the system, click 

and follow the on-screen instructions.

3XLOGIC

Steps:

1). Opening the **Setup Tab>Maintenance** drop-down menu and clicking the **3xLOGIC** link will open the **3xLOGIC VIGIL Camera Server Software** settings page.

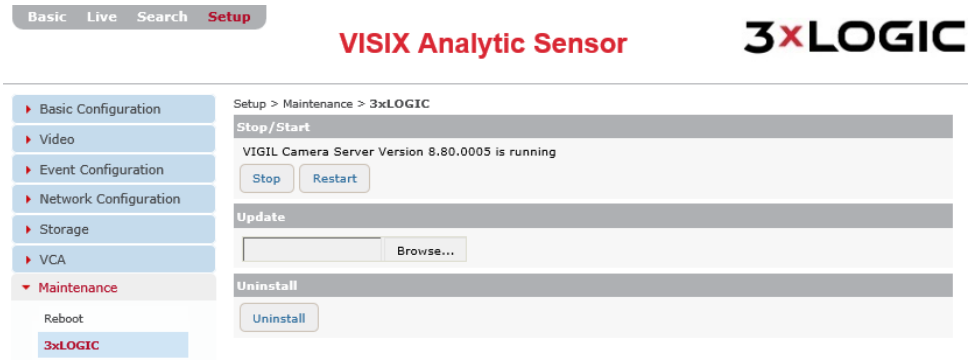


Figure 7-94 Setup Tab –Maintenance Menu –3xLOGIC Software Settings

2). From the **3xLOGIC VIGIL Camera Server** software settings page, a user can view the camera's current VIGIL Camera Server software version. The user can also **Stop** (shut down) or **Restart** the camera's VIGIL software by clicking the corresponding buttons.

3). A user may also update the camera's VIGIL Server Camera software from this page. To begin, click the **Browse** button in the **Update** section. This will deploy a standard file browser. Navigate to the update file on your system and select it. An **Update** button will appear when valid file has been chosen. Click **Update** to begin the software update process.

4). To uninstall the current VIGIL Server Camera software, click the **Uninstall** button.

7.8 Activation Menu

ACTIVATE

Steps:

1). Opening the **Setup Tab>Activation** drop-down menu and clicking the **Activate l**ink will open the **Activation** settings page.

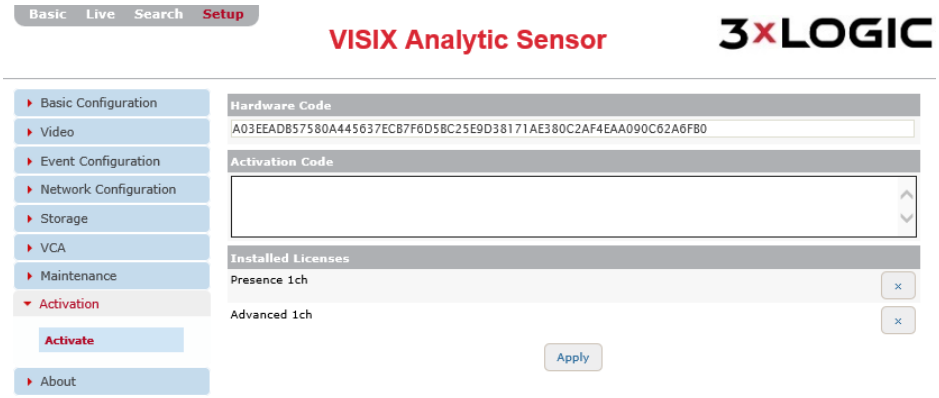


Figure 7-95 Setup Tab –Activation Menu –Activation Form

2). From the **Activation** settings page, a user may view the camera's **Hardware Code** and any installed licenses. To register new license, enter the activation code into the **Activation Code** text field. Valid codes will be automatically processed and the corresponding license will appear in the **Installed Licenses** list.

3). Click **Apply** to save settings changes.

7.9 About Menu

INFORMATION

Steps:

1). Opening the **Setup Tab> About** drop-down menu and clicking the **Information** link will open the camera information page.

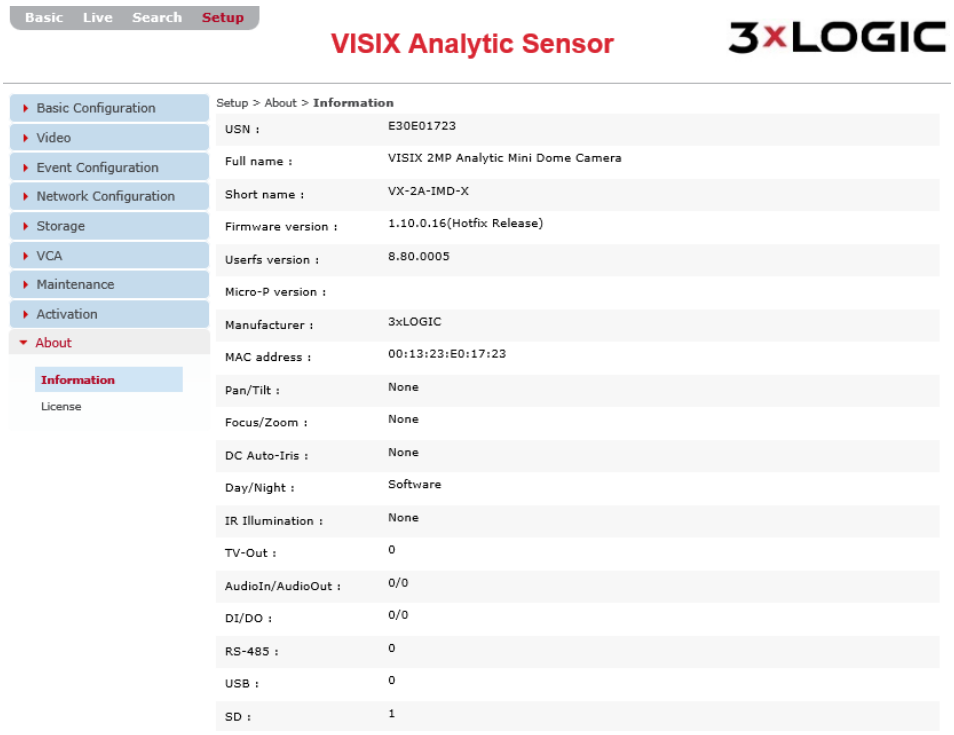


Figure 7-96 Setup Tab –About Menu –Information Form

The Information page provides a user with at-a-glance information regarding the following camera components/specifications:

- Serial Number
- Full and Short Names
- Firmware Version
- VIGIL Server Camera (Userfs) Software Version
- Micro-P Version
- Manufacturer Name
- MAC Address
- Pan/Tilt Capability
- Focus/zoom Capability
- DC-Auto Iris Info
- Day/Night Mode Info
- IR Illumination Specs
- TV-Out
- Audio In/Audio Out
- DI/DO
- RS-485
- USB
- SD

LICENSE

Steps:

1). Opening the **Setup Tab>About** drop-down menu and clicking the **About** link will open the License information page.

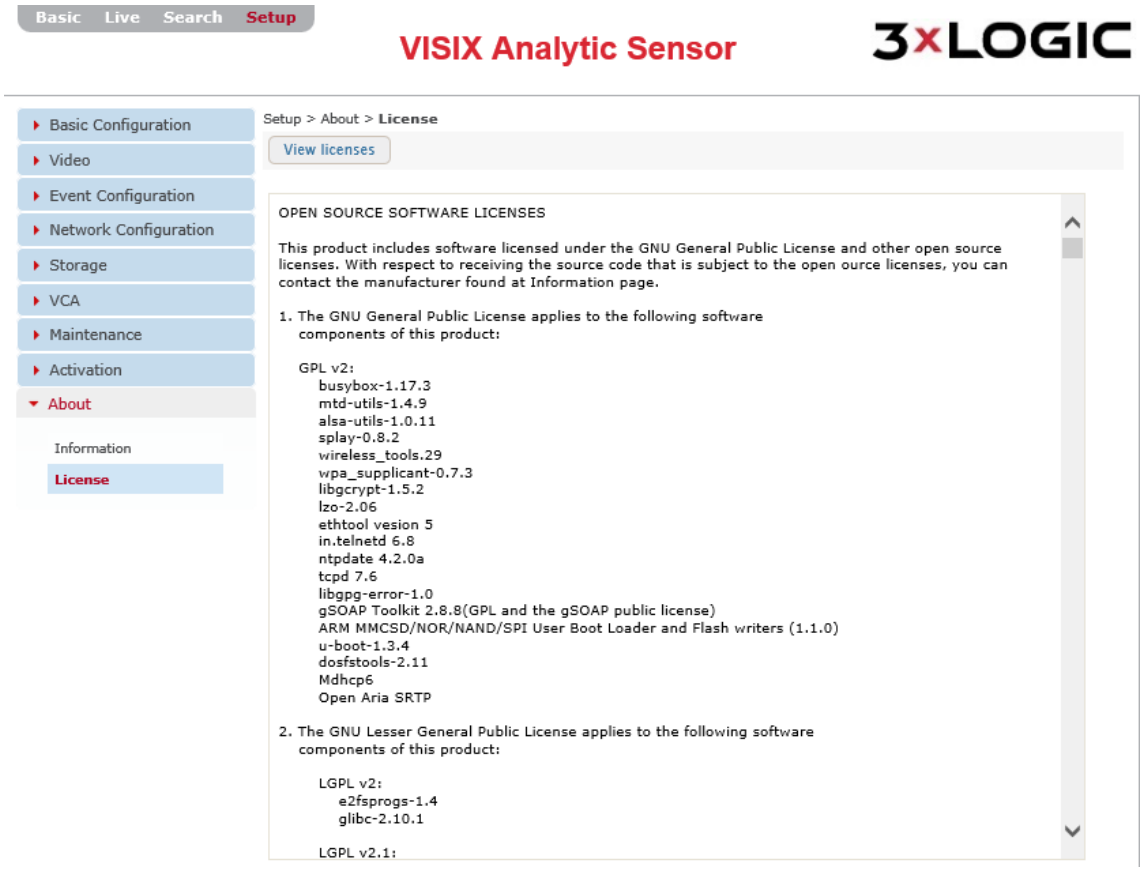


Figure 7-94 Setup Tab –About Menu –License Information

2). The **License Information** page provides a user with at-a-glance information regarding the licensing for several of the camera and software components.

8 IP Address – Hexadecimal/Decimal Conversion Table

Refer to the following table when converting the MAC address of the device to the IP address:

Hex	Dec	Hex	Dec	Hex	Dec	Hex	Dec	Hex	Dec	Hex	Dec	Hex	Dec
0	0	25	37	4A	74	6F	111	94	148	B9	185	DE	222
1	1	26	38	4B	75	70	112	95	149	BA	186	DF	223
2	2	27	39	4C	76	71	113	96	150	BB	187	E0	224
3	3	28	40	4D	77	72	114	97	151	BC	188	E1	225
4	4	29	41	4E	78	73	115	98	152	BD	189	E2	226
5	5	2A	42	4F	79	74	116	99	153	BE	190	E3	227
6	6	2B	43	50	80	75	117	9A	154	BF	191	E4	228
7	7	2C	44	51	81	76	118	9B	155	C0	192	E5	229
8	8	2D	45	52	82	77	119	9C	156	C1	193	E6	230
9	9	2E	46	53	83	78	120	9D	157	C2	194	E7	231
0A	10	2F	47	54	84	79	121	9E	158	C3	195	E8	232
0B	11	30	48	55	85	7A	122	9F	159	C4	196	E9	233
0C	12	31	49	56	86	7B	123	A0	160	C5	197	EA	234
0D	13	32	50	57	87	7C	124	A1	161	C6	198	EB	235
0E	14	33	51	58	88	7D	125	A2	162	C7	199	EC	236
0F	15	34	52	59	89	7E	126	A3	163	C8	200	ED	237
10	16	35	53	5A	90	7F	127	A4	164	C9	201	EE	238
11	17	36	54	5B	91	80	128	A5	165	CA	202	EF	239
12	18	37	55	5C	92	81	129	A6	166	CB	203	F0	240
13	19	38	56	5D	93	82	130	A7	167	CC	204	F1	241
14	20	39	57	5E	94	83	131	A8	168	CD	205	F2	242
15	21	3A	58	5F	95	84	132	A9	169	CE	206	F3	243
16	22	3B	59	60	96	85	133	AA	170	CF	207	F4	244
17	23	3C	60	61	97	86	134	AB	171	D0	208	F5	245
18	24	3D	61	62	98	87	135	AC	172	D1	209	F6	246
19	25	3E	62	63	99	88	136	AD	173	D2	210	F7	247
1A	26	3F	63	64	100	89	137	AE	174	D3	211	F8	248
1B	27	40	64	65	101	8A	138	AF	175	D4	212	F9	249
1C	28	41	65	66	102	8B	139	B0	176	D5	213	FA	250
1D	29	42	66	67	103	8C	140	B1	177	D6	214	FB	251
1E	30	43	67	68	104	8D	141	B2	178	D7	215	FC	252
1F	31	44	68	69	105	8E	142	B3	179	D8	216	FD	253
20	32	45	69	6A	106	8F	143	B4	180	D9	217	FE	254
21	33	46	70	6B	107	90	144	B5	181	DA	218	FF	255
22	34	47	71	6C	108	91	145	B6	182	DB	219		
23	35	48	72	6D	109	92	146	B7	183	DC	220		
24	36	49	73	6E	110	93	147	B8	184	DD	221		

9 Revision History

MAN#	DATE(M/D/Y)	Comments
11-2015-1	11/02/2015	Styled
01-2016-22	01/22/2016	Finalized initial draft.