Digital Watchdog
VMax+/VMaxA1 DVR

Installation Manual

V1.1

Updated: November 11, 2021

Contents

Introduction

Once the DVR/NVR/VMS has been set up it is ready to be tested with I-View. The following illustration shows the path of two message flows comprising a typical “Video Verification” scenario:

1-3 - An onsite alarm ‘event’ causes an SMTP message to be sent to the I-View Now system. The alarm event is usually the result of a simple contact closure wired into the back panel of the NVR/VMS.

4, 5 - The resulting message path I-View initiates upon receipt of the SMTP message to retrieve the ‘pre’ and ‘post’ alarm video associated with the alarm event. The number of pre and post seconds can vary but it’s usually not less than 3 and normally about 10 on either side of the alarm condition that initiates the sequence.

The user can view one or more consecutive alarm event ‘clips’ as they arrive from the I-View Now portal via a cell phone, or a PC or tablet device’s browser. With each clip is the ability to see one or more “Live Views” for various cameras associated with the NVR/VMS that generated the SMTP alarm.

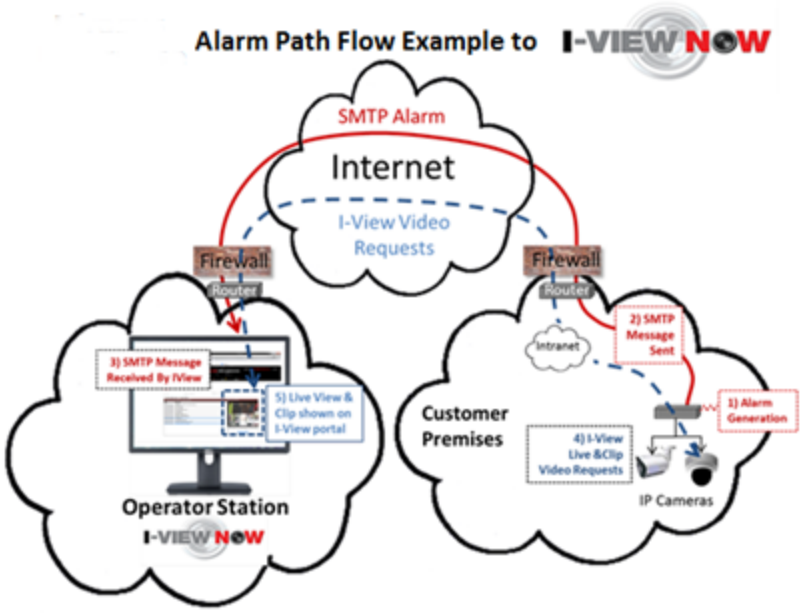


Figure 1

Workflow

The following steps describe a high level workflow to be followed in order to properly configure and install a Honeywell MODEL to work with I-View Now. Subsequent sections will provide more detail on each step outlined here.

1. **Network Setup:** Configure the DVR/NVR/VMS and router/firewall at the site so the DVR/NVR/VMS can connect to the Internet. Router/Firewall instructions will vary by location, manufacturer and site LAN configuration. In addition, data from this step needs to be input into the I-viewnow.com portal, such as the External IP Address for the site, as well as the "Client Port". These are necessary so that the I-View Now portal can gain access to the NVR/VMS for "Live Views" and retrieving video "Clips" associated with alarm events. Finally, a static IP must be available for the DVR/NVR/VMS on site which the router will send I-View requests to as well as services on specific ports.
2. **Configure SMTP email:** This will be used to communicate alerts and alarms to I-View Now. The SMTP server and SMTP ID provided on the "Installer Data" Worksheet obtained from the I-viewnow.com portal is necessary for this step.
3. **User Setup**: In the NVR/VMS please create an administrator account that has a unique password. I-View Now will be using this password to log into the device programmatically for 'Live View' and 'Clip' retrieval. As such I-View Now recommends using the suggested password on the "Installer Data" worksheet. If a password for the admin account on the NVR/VMS differs from the one provided on the worksheet, this needs to be communicated to I-View administrators in order to update the database.
4. **Port Forwarding:** Any ports required must be forwarded from the Router/firewalls external interface to the DVR's static internal address. In the I-View Now Portal, the add the forwarded port to the proper location
5. **Alarm Input Setup:** The technician will configure alarm inputs on the back of the DVR/NVR/VMS to perform two actions:
    1. Trigger recording on all connected cameras
    2. Send SMTP (email) alerts to I-View Now when an alarm event occurs
6. **Recording Setup:** The DVR/NVR/VMS can be set to record by schedule or by events. Event recording from alarm inputs is the recommended approach for I-View Now although other modes, such as motion detection, are possible with some caveats. These are described in more detail in this section.
7. **Configure I-View Now Entry Delay**: Entry delay is configured through the I-View Now portal.
8. **Test**: Here you will test the individual inputs on the DVR/NVR/VMS as they are connected to your alarm panel relays or other input devices. It is recommended that you test all inputs for functionality and to ensure the proper workflow is configured within the I-Viewnow.com portal.
9. **Troubleshooting:** This section is provided to help the technician troubleshoot common problems encountered while installing this particular type of NVR/VMS.

Installation Worksheet

The I-View Now Portal Installation Worksheet is created after entering the DVR/NVR/VMS make and model into the system. A portion of an example worksheet is printed below. This sheet should be generated from the system before attempting to set up the site for integration with I-View as it enables setup of the DVR/NVR/VMS onsite login and password as well as the means to send SMTP messages back to the I-View Now server. There is a place on the form for recording the Location IP Address which is the external IP address used for the router at the site facing the Internet. In addition the ports on the external router that will be forwarded to the DVR/NVR/VMS should be noted on this form. This information needs to be input into the I-viewnow.com system so it will know the external IP address and ports used to communicate from the site through the router at the site and onto the DVR/NVR/VMS.

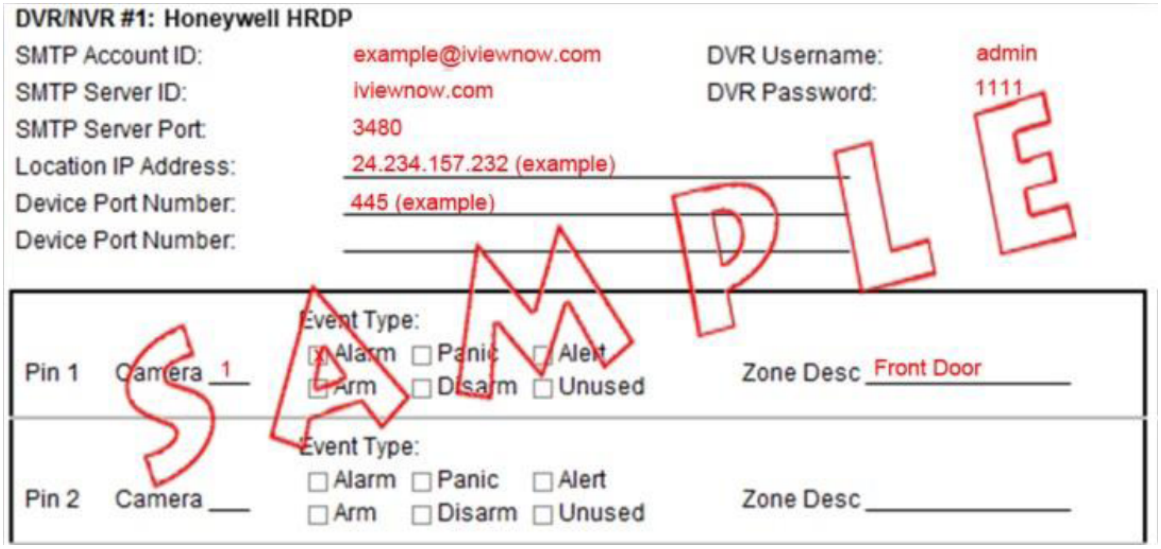


Figure 2

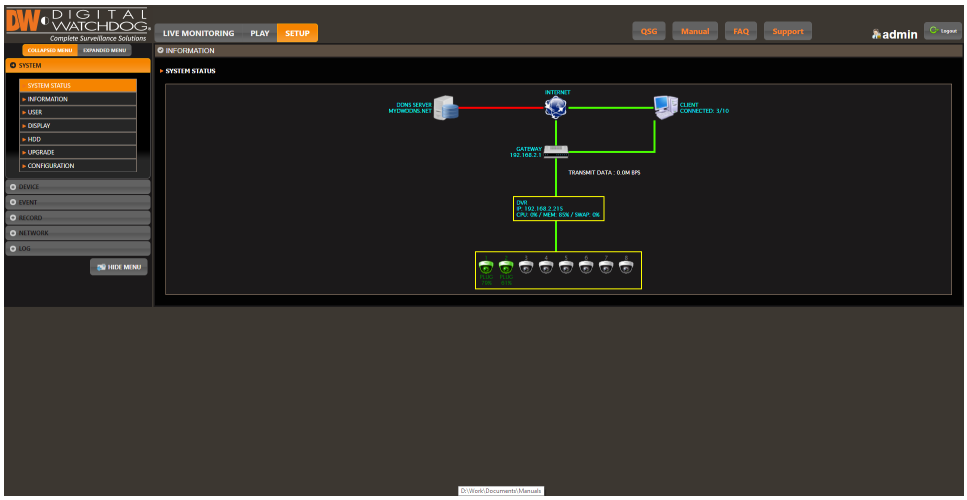
Retrieve the IP address by asking the Customer/IT department for the IP address, or visit http://whatismyip.org while on-site for a possible correct address; however, verify with the IT department that the IP address discovered is valid to use as a target from the I-View servers. The IT Site Administration must enable port forwarding from their router/firewalls to the port address.

Default DVR Login

Plug a monitor into the VGA output on the device, plug the mouse provided with the DVR into the front USB port of the device. The menus presented in this manual may vary depending on the model and firmware version.

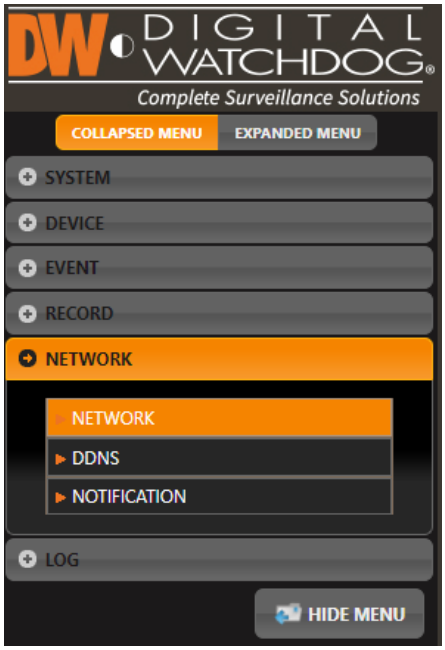
Default User: admin
Default Password: empty (no password)

Once logged in, you should see a display similar to below



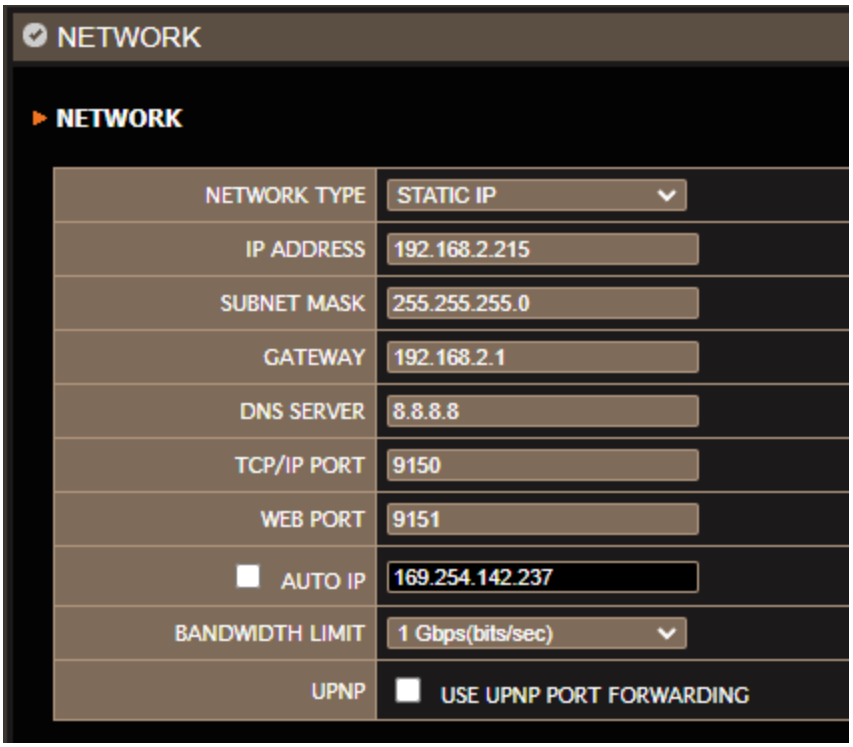
Network Configuration

After logging into the device for the first time and setting the proper login and password, the first setting that should be changed is the IP address. The DVR requires a static internal IP address at the site behind the router/firewalls. In addition, one or more communication ports will have to be forwarded to it from the firewall/router on site. Select NETWORK from the menu on the left.



Be sure to write on the installation note on the external IP address representing the Internet facing location where the device is installed (Location IP Address). This value is typically the IP address of the router facing the Internet for the site. In addition, the TCP/IP Port Number is vital to enable the router to 'port forward' incoming I-View requests to the device. The IT staff responsible for the site needs to assist you in ensuring these prerequisites are in effect in their network facilities.

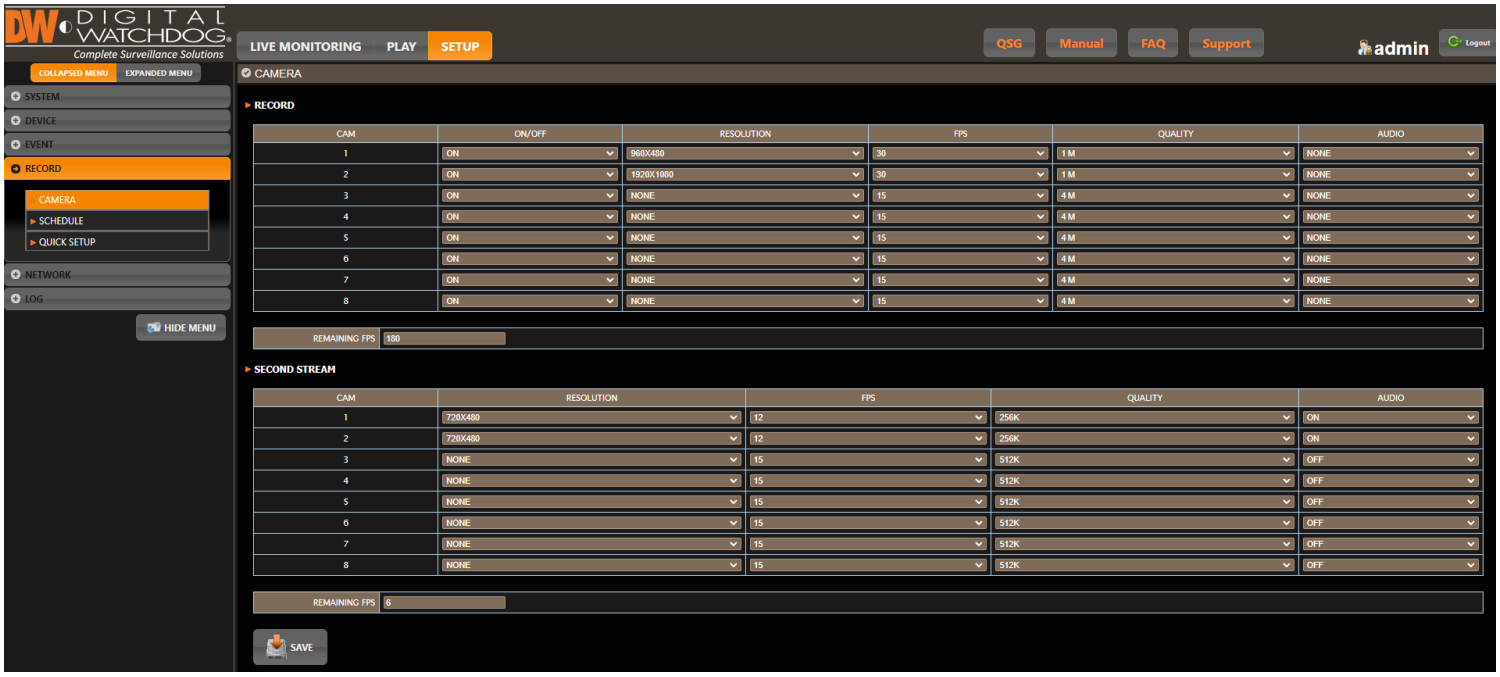
This is what the screen should look like after bringing up the NETWORK panel. Each field has an explanation intending to describe how to configure the various settings to prepare the system for integration with I-View:



IP & Port Config

- Network Type: Static
- IP, Subnet, Gateway: Site provided
- DNS: Use 8.8.8.8 / 8.8.4.4 for Primary / Secondary unless site provided
- TCP/IP Port / Web Port: Use defaults unless the site provides instruction.

Camera Configuration



Camera's will be configured on a per-device basis. Be sure to follow the instructions for the camera's being connected.

Video Quality Configuration Guidelines

With the variety of cameras available, we've determined some guidelines for the best experience.

Video Stream: We're looking for any secondary stream data first, which is generally more compressed, smaller in size, and a lower frame rate. Select 256k Quality, audio on or off, depending on camera

Video Size: Smallest, or second smallest resolution

Video Frame Rate: Between 7 – 15 frames per second. With network cameras, overall network bandwidth at the site requires attention. Start with 15, then start lower with 12 and so on if network speed is noticeably slow

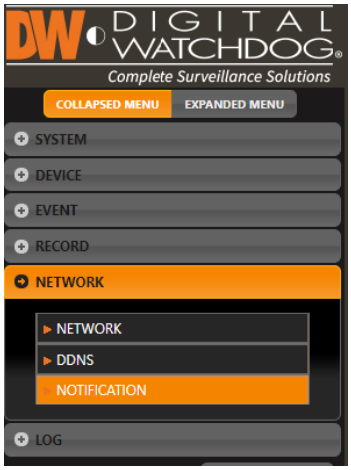
Entry Delay

Entry delay is configurable in the I-View Now Dealer Portal. Log in to configure.

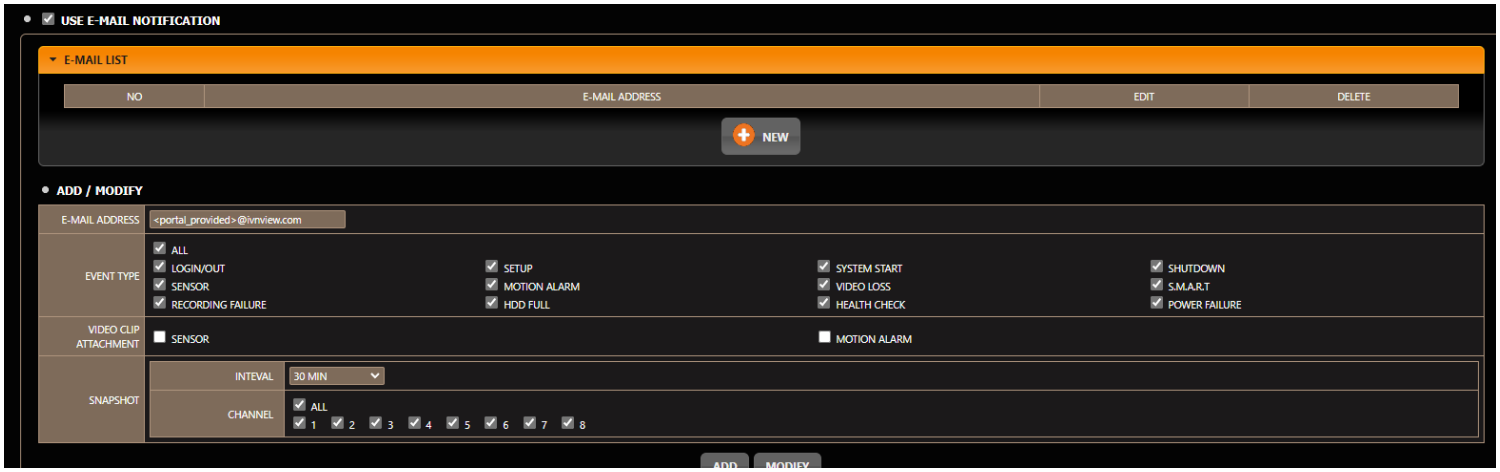
System Settings

Email

Go to the notification portion in the menu.

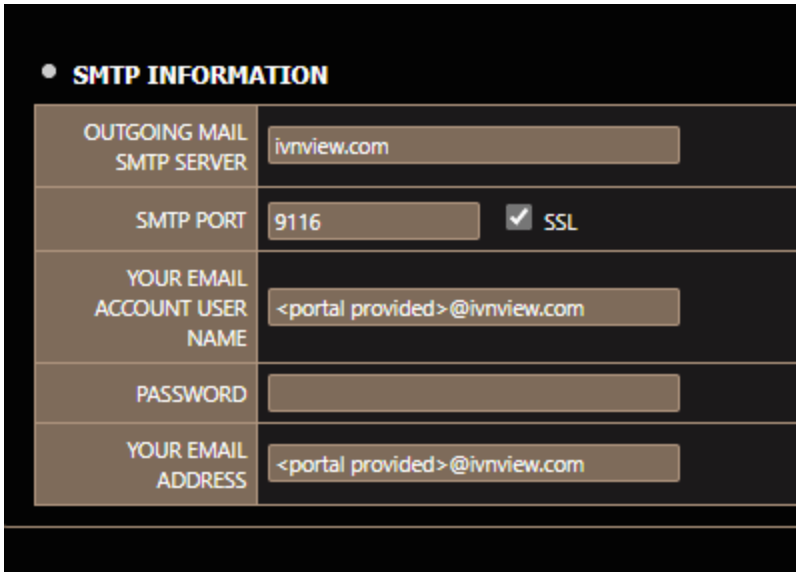


Check the box for “Use e-mail notification”. Select New, and with the email address provided to you, enter the information below, replacing the example email with the one provided. Press ADD when done.



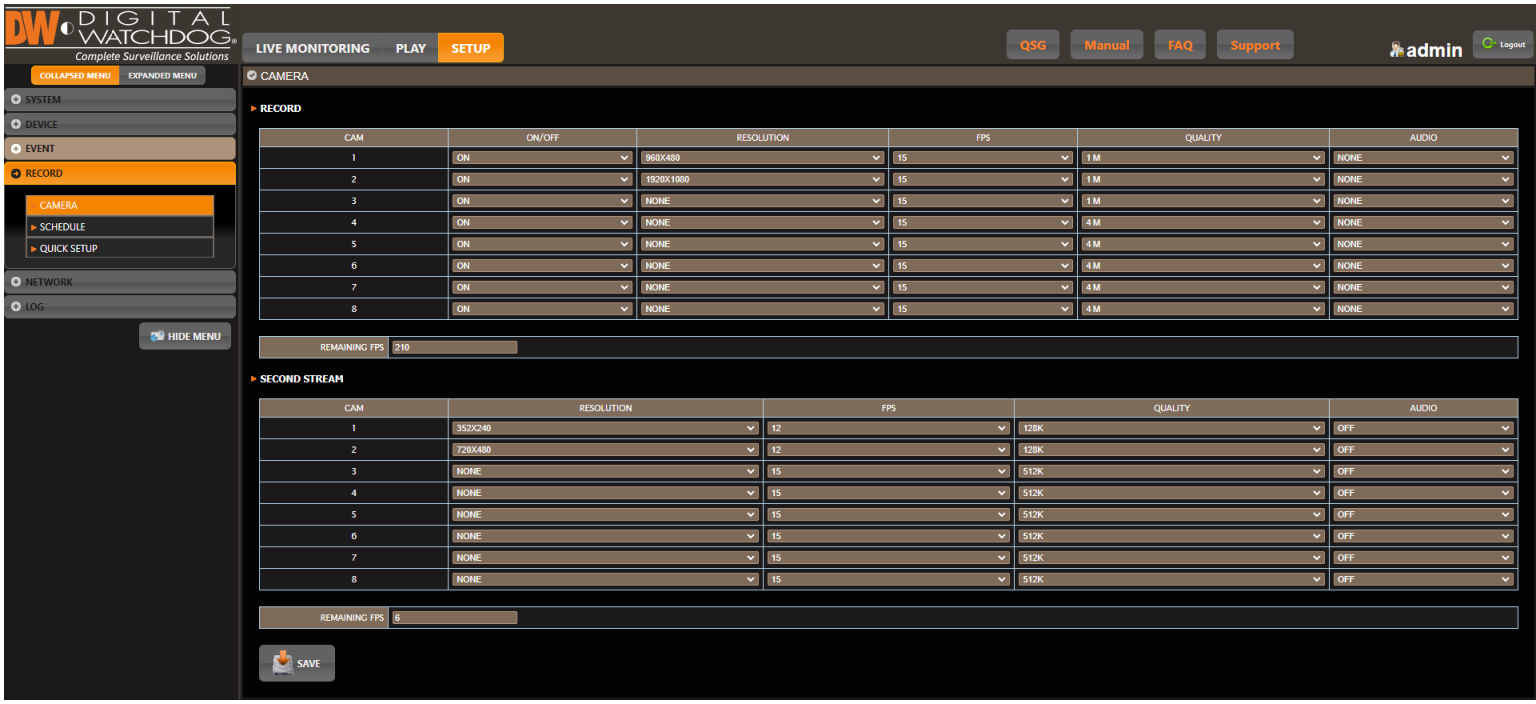
SMTP Settings

Replacing the email address, changing outgoing server and SMTP port to “ivnview.com”, and port 9116, then check the box for SSL.



Once complete, save settings. Send a test email and it should say successful. If not, check the settings and try again

Record Settings



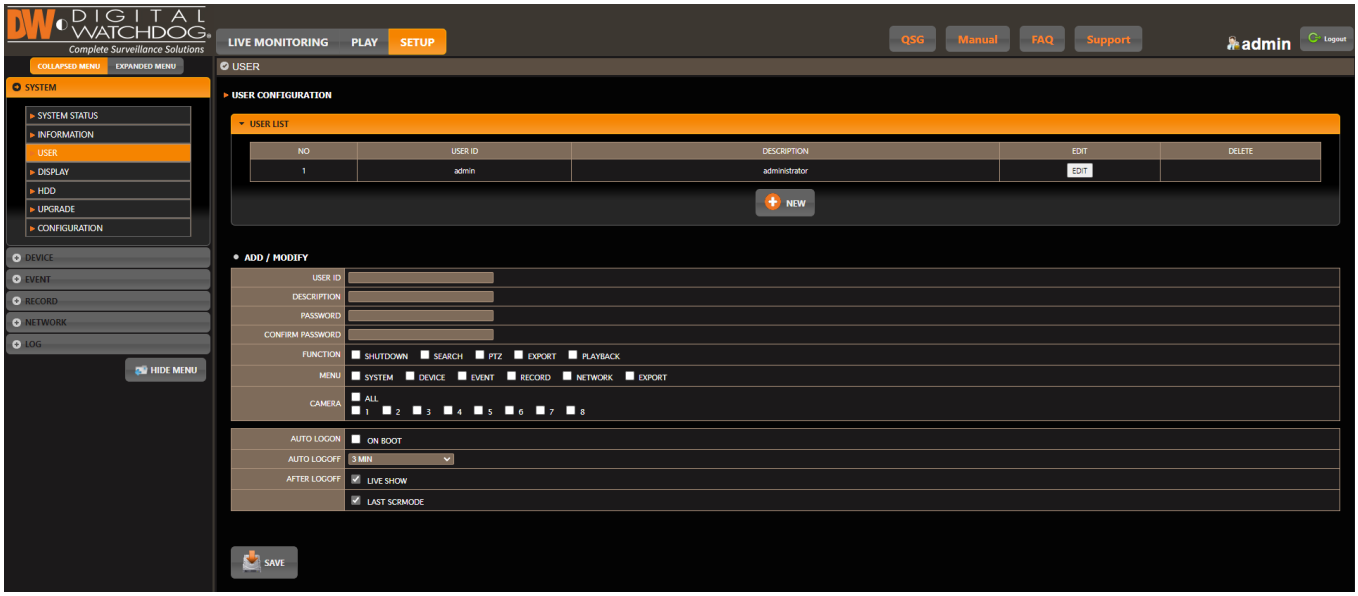
Use the configuration above. Make the secondary stream quality 128k, 12FPS, and the smallest or second smallest resolution.

Schedule

Configure the schedule to follow the example below, making sure to copy to other cameras.

User Management

You can add a user for the customer here. They should be entered without administrator permission, to ensure the I-View Now settings are not changed

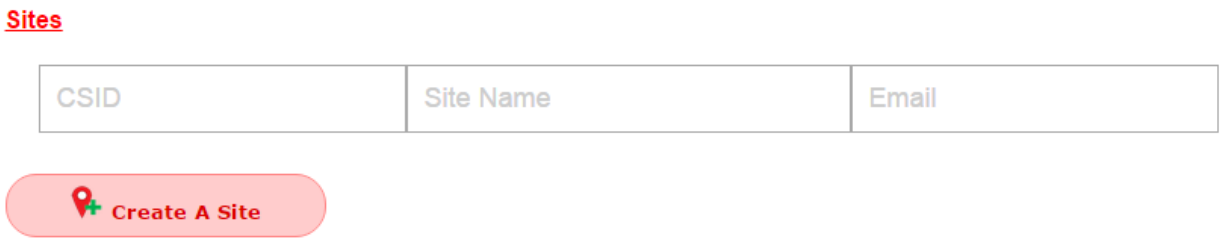


Configuration Testing

Test everything at the location to ensure normal alarm signals work, and entry delay works. If something is found to not be working correctly, troubleshoot the system and verify all settings are correct and try again.

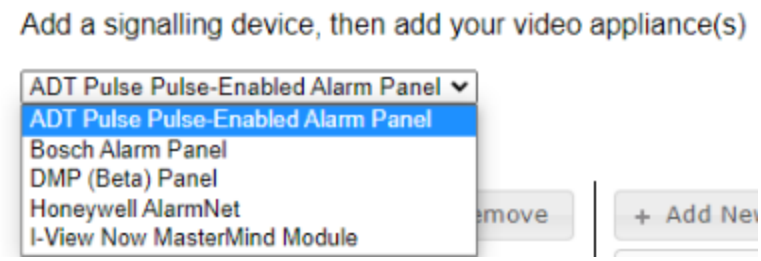
Creating the Device in the I-View Now Portal

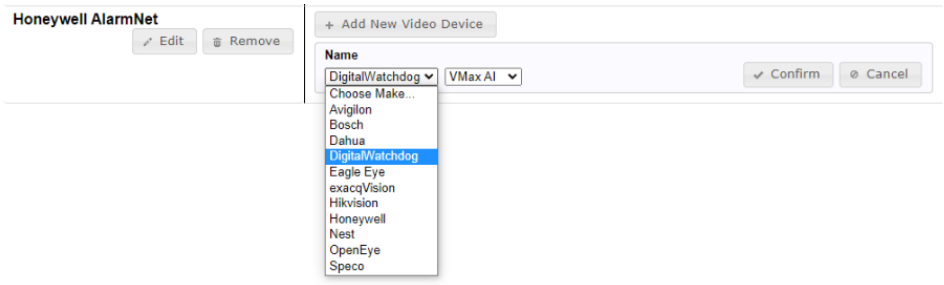
Click on Create A Site:



Complete the site setup form as needed.

Edit the site and add a device





Please make sure you properly configure the username and password information correctly. It should match the username and password for one of your administrator accounts such that it has access to Live, Events, Playback and AVI/JPEG Export at the minimum.

The generated SMTP Account ID needs to be added in the Sender email address on the Server Settings Section and in the Recipient(s) field on the Message Setting Section.

So in the Sender email address field please enter the SMTP Account ID value there. For example I would enter test@ivnview.com in the Sender email address field.

On Message Settings Please enter the same SMTP Account ID value into the Receipts(s) field.

Location IP Address: Please enter in your external IP address.

Save, update device, once you're done with alarm inputs.

Glossary

This section includes terminology used throughout the manual. For further information on any term, type the name in Google with “wiki” at the end to see a complete definition.

1. DDNS - Dynamic DNS is a method, protocol, or network service that provides the capability for a networked device, such as a router or computer system using the Internet Protocol Suite, to notify a domain name server to change, in real time (ad-hoc) the active DNS configuration of its configured hostnames, addresses or other information stored in DNS
2. DHCP - Dynamic Host Configuration Protocol (DHCP) is a network application protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network.
3. NVR/VMS - Digital Video Recorder. This is typically an analog camera based recording system that provides a common interface into 4 to 16 cameras. In contrast, an NVR (Network Video Recorder) provides an IP based interface to cameras.
4. IP - Internet Protocol address. IP addresses are used to identify the I-View server, the site containing the NVR/VMS and the NVR/VMS itself. The site and I-View IP addresses are Internet routable which means they can be anywhere on the Internet. The NVR/VMS typically has a private address which is specific to the site. This is why the router/firewall at the site that faces the Internet must contain a port forwarding entry to allow for messages to be passed to the NVR/VMS from I-View as well as the NVR/VMS to communicate with the I-View via an SMTP email message or in response to a request for a clip or live view.
5. MAC Address - A media access control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet. Essentially, the MAC address can be thought of as one layer above the physical medium, e.g. wire or cable, and one level below the IP address. The MAC address is often assigned by the manufacturer.
6. Private Network - In the Internet addressing architecture, a private network is a network that uses private IP address space, following the standards set by RFC 1918 for IPv4 and RFC 4193 for IPv6. These addresses are commonly used for home, office, and enterprise local area networks (LANs), when globally routable addresses are not mandatory, or are not available for the intended network applications. Under Internet Protocol IPv4, private IP address spaces were originally defined in an effort to delay IPv4 address exhaustion, but they are also a feature of the next generation Internet Protocol, IPv6.
7. SMTP - Simple Mail Transfer Protocol is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.
8. PoE - Power over Ethernet, describes any of several standardized or ad-hoc systems which pass electrical power along with data on Ethernet cabling. This allows a single cable to provide both data connection and electrical power to devices such as IP cameras. ‘
9. VMS - Video management software. Allows for storing, recording and retrieval of video clips.
10. VCA (video content analysis)