User Guide

Valerus VMS

XX281-00-16

Updated for Valerus version 22R2

Vicon Industries Inc. does not warrant that the functions contained in this equipment will meet your requirements or that the operation will be entirely error free or perform precisely as described in the documentation. This system has not been designed to be used in life-critical situations and must not be used for this purpose.

Document Number: 8009-8281-00-16 Rev: 11/2022
Product specifications subject to change without notice
Copyright © 2022 Vicon Industries Inc. All rights reserved.

Vicon Industries Inc.
Tel: 631-952-2288) Fax: 631-951-2288
Toll Free: 800-645-9116
24-Hour Technical Support: 800-34-VICON (800-348-4266)
UK: 44/(0) 1489-566300
www.vicon-security.com

Table of Contents

Introduction **3**

Configuration **7**

- Network Devices 8
- Valerus-ViconNet Gateway 26
- Integration Partners 30
- Resources 32
- Maps 55
- Numeric ID 58
- Partner Resources 60
- Advanced 61
- External Events 65
- Alarms 67
- User Management 69
- System 76
- Maintenance 90

Search **94**

Using the Application Server Redundancy Function **102**

Monitoring **103**

- Resources (1) 103
- Display (2) 105

VAX **124**

Dashboard **125**

Alarms **134**

Shipping Instructions **136**

Vicon Standard Equipment Warranty **137**

Refer to Vicon's website, Support > Documentation, for the latest manuals and datasheets.

Introduction

Vicon's Valerus VMS is a browser-based application. It provides a web client with a single point of management for the entire system, no matter the size. All Recording Servers (NVRs), cameras and devices and other resources are added, configured and operated using the configuration section in the application. The VMS can be purchased as software only and installed on a PC meeting the minimum requirements or it can be purchased preinstalled on Vicon Valerus certified hardware offered exclusively by Vicon.

This manual describes how to configure and operate Vicon's Valerus video management software (VMS).

Starting the Application

Running the Application for the First Time

Being a fully web-based solution, it is necessary to browse to the Valerus Application Server, which is also serving as the web server, in the same way as browsing to any web site. Either enter the IP address of the Application Server in your web browser (if that IP address is not known, check the server on which Valerus Application Server was installed) or, if your network has defined server names, browse to that computer's name.

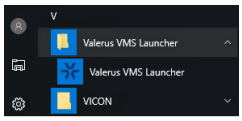
Tip! If the browser is being run on the same PC where the Application Server is running, browse to the local IP by using the loopback address:

- http://127.0.0.1 –or- http://localhost

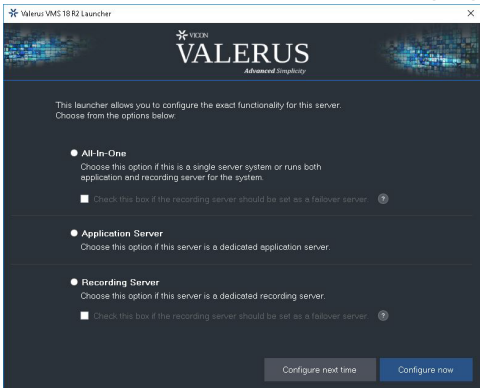
Each system requires only one Application Server. The Application Server can be either a dedicated unit or a Recording Server defined as an All-In-One unit that runs both the application and recording server for the system. If the Valerus software has been installed on customer-supplied hardware, follow the instructions in the Software Installation manual to define the server from the Valerus Launcher as All-In-One, a dedicated Application Server or a Recording Server. If your hardware was purchased from Vicon, and a dedicated Application Server (Model VLR-APPSRV) was purchased, this is the server. If the system only includes one or multiple Recording Server(s) purchased from Vicon, one of the Recording Servers must be defined as an All-In-One server from the Valerus Launcher.

Note: Along with the installation of Valerus come a number of necessary third party components, including one that handles NTP. Vicon recommends using this on the Application Server and disabling it on any NVRs that are in the system, as the NVRs synchronize with the time on the Application Server.

The Valerus Launcher can be accessed from the Windows Start menu.

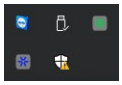


Click on the Valerus VMS Launcher to display the following screen.



From this screen, the server can be redefined as an All-In-One, Application Server or Recording Server by selecting that radio button and clicking Save. Additionally, from this screen an NVR can be designated as a failover NVR (note that an NVR can be *either* a standard NVR or a failover NVR, but not both).

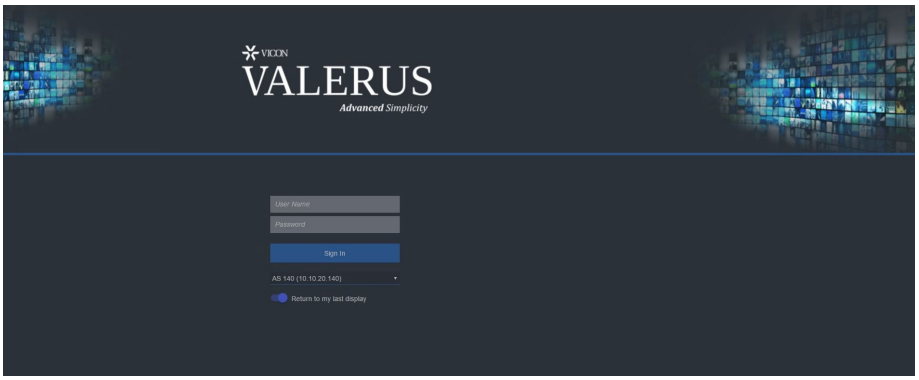
You can identify the type of server a unit is running in two ways. The Application Server will have a shortcut for Valerus on the desktop. Additionally, icons will display in the Windows Sys tray.



The Application Server will have a green icon and the Recording Server will have a blue icon; an All-In-One server will have both a green and blue icon in the tray. Any server in the system can later be redefined in this same manner, for example if the system grows and then requires a dedicated Application Server.

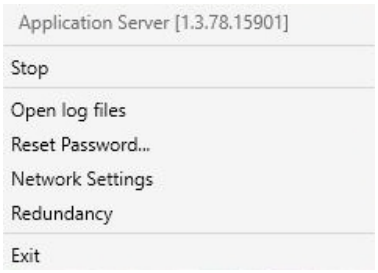
By default Valerus is using the standard port 80 for web access. The application will ONLY work with Internet Explorer 11 and on Chrome using the Valerus Chrome extension that can be found at the Google Chrome store; attempting to use a different web browser will not allow video to be displayed. If the default browser is not IE 11, a message will notify the user.

The login screen will open. The first time the system is accessed, the default settings will be in place. The default login is user name ADMIN (not case sensitive) and the password is 1234; the password can be changed in the Configuration screens for increased security. Click Sign in. For convenience, it is recommended to create a shortcut on your desktop to make subsequent logins easier.

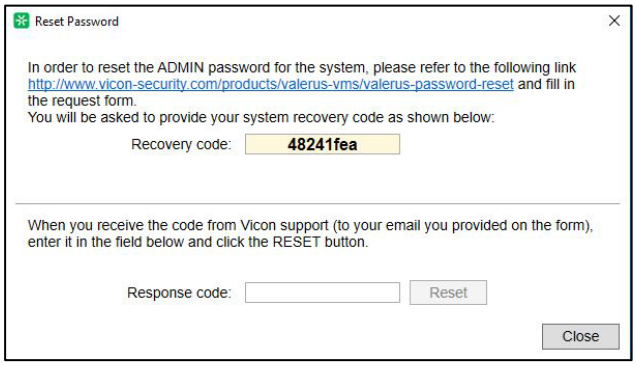


Note: In the rare occasion that the system locks up with an administrator password and that password has been lost, there is an option that will allow creating a request to Vicon Technical Support for a password reset.

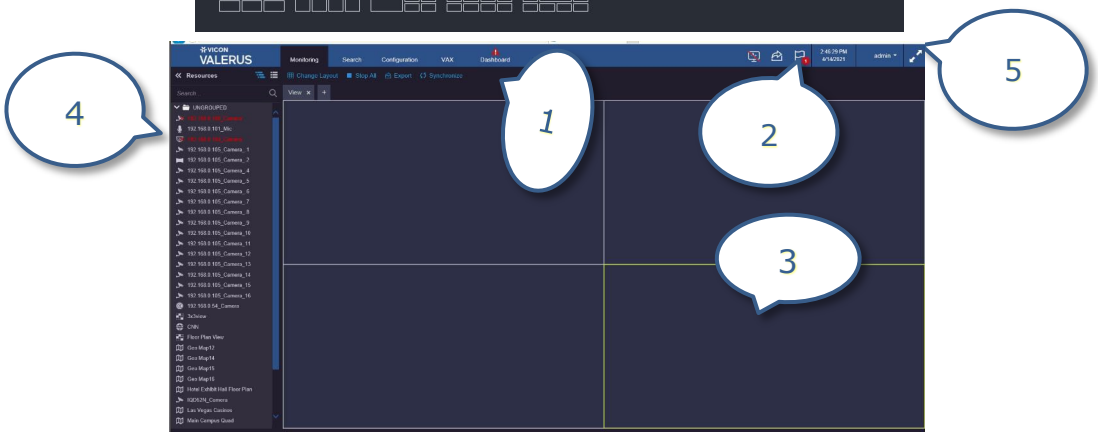
- Double or right click the Valerus icon. The following popup displays.



- Select Reset Password.
  - Selecting this option will open a window with a link to the password request page on the Vicon web site (click on the link for online access or copy and browse from any computer) and a recovery code to submit with the request (caps sensitive)
  - Vicon support will review the request and may contact you for further details to ensure resetting the password is indeed legitimate
  - When provided a response code (caps sensitive), you will need to enter it and click "reset"
  - After resetting, ADMIN password will be set back to its default 1234. Make sure to change it once logged back in.



The system opens up to the Monitoring screen and by default will open in 2x2 (quad) layout. Opening a new tab (+ symbol) will create a new tab called View and open a screen showing all the screen layouts to choose from. Click on the desired layout to switch to it or drag and drop cameras directly on the desired layout to switch and open. Additional information will be provided in the monitoring section of this manual.



1. Monitoring, Search, Configuration, VAX, Dashboard and Alarms tabs
2. About/User Settings/Logout
3. Video Display Area
4. Resources List
5. Full Screen

The Monitoring screen is where live and recorded video are displayed and is the main operator's screen. On the left side is a list of available Resources [cameras, microphones, URLs (web pages), digital inputs, relay outputs, views, tours and any defined groups]; this list can be presented in either a hierarchal view or a flat list of devices. There are some icons at the top that indicate Client Monitoring option, Export, Notifications or if the Application Server is not available .

Most of the screen is dedicated to the display area. When entering the application for the first time or before a layout has been defined, a choice of layouts is provided; the operator can click on a selected layout to switch to it or drag a device from the list onto the desired layout icon.

At the top of the screen there are tabs representing the different system applications: Monitoring, Search, Configuration, VAX, Dashboard and Alarms. The Search function provides a number of methods to look for specific video from a specific time and date: Thumbnail, Museum, Events Framework, Analytics and Event/Alarm searches. The Configuration tab will open the configuration screens, which provide everything needed to setup the system. The configuration screens are typically used by the system administrator. On a new system, the initial configuration must be done first so that the monitoring and other screens will become usable. The Dashboard screen provides an overview of the system components and their health. It shows a count of the healthy devices and if there are any warnings (non-critical issues) or errors (critical issues). The Alarms tab opens the Alarms Management area. Each of these tabs will be explained in detail in this guide. Each tab has an

icon in the top right corner when the mouse is hovered over it; clicking this icon detaches the tab and opens in a new window.

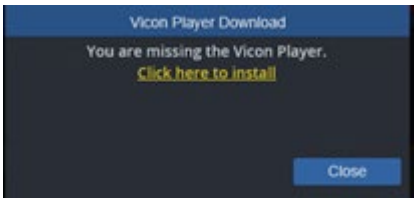
An in-depth Help system is available in certain sections. There are question mark symbols throughout the interface; hover your mouse to view text to explain your choices.

Video Player Status

The video player module needs to be installed in the browser upon first startup or when it has been updated; a warning icon will display to install the player on the top bar and in a video tile if the user tries to start the video. The player must be installed on every computer in the system connecting to Valerus.

To install the player:

1. When the icon displays, this may indicate that the player needs to be installed or updated.
2. Click the icon; a popup similar to that below displays. Click to install the player; a standard browser download message will display to install.



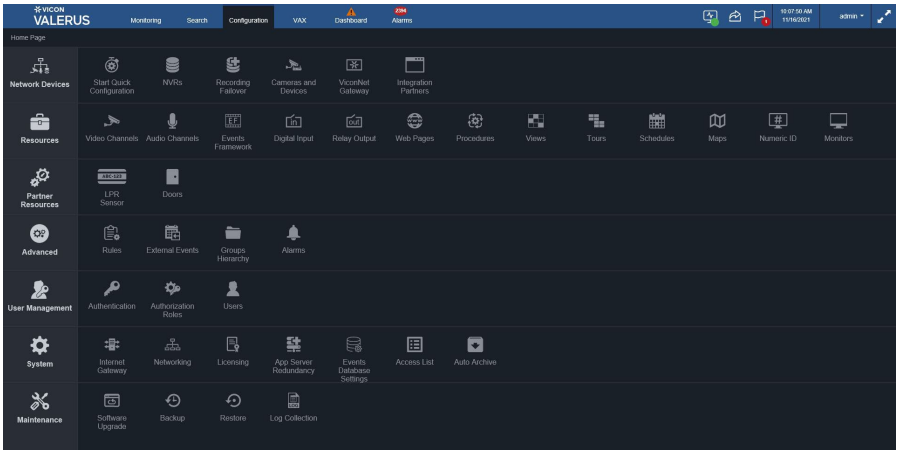
3. Below is an example of IE11 download message. Click Run to install.

4. Follow the installation instructions, close the browser and launch it again after the installation is complete. The player should now be installed and will work to display video. The system is ready to be configured.

Configuration

The Configuration application is used mostly by administrators to setup the system. Click on the ***Configuration*** tab to enter the setup screens. It is recommended that the configuration process be done in a specific order to ensure all the system components are added; if the Options list is followed from top to bottom, configuration will be accomplished properly. As an alternative, and for a very fast and easy deployment, a Quick Configuration process is available under Network devices. All of these options are described in detail below.

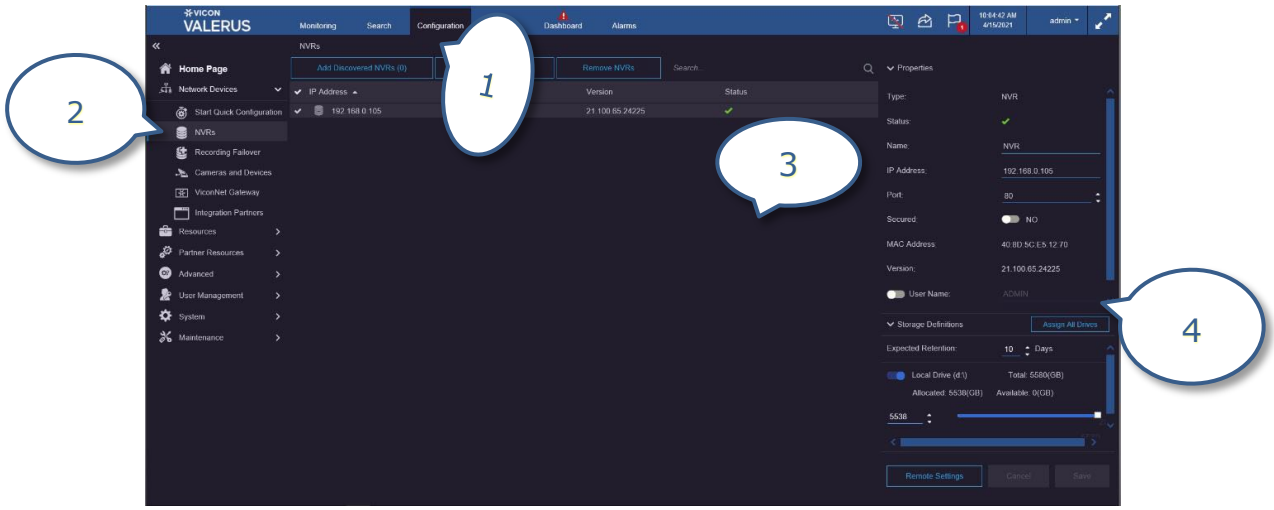
The first time Configuration is opened, a Home page displays. This page presents an overview of all the Configuration options and provides links to those specific setup screens. From here select what you want to configure. Entering Configuration later opens the last screen used; return to the Home page by clicking the Home Page at the top.



Note: Most screens provide a search field

that allows a search of the list on that screen; this is particularly useful in large systems with many devices or resources. A required field is indicated by red. A blue button indicates the button is active; a gray button is inactive.

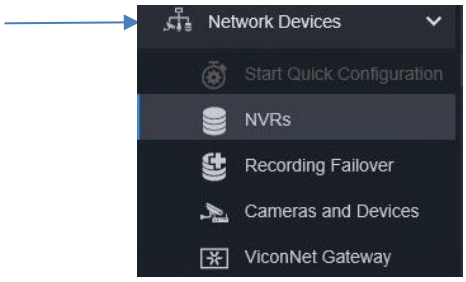
On the left side of the screen is the list of Configuration options. The middle section of the screen provides information about the devices being configured and the right side of the screen offers detailed information or ***Properties*** about each device in the system. Depending on the characteristics of the different devices, different options and properties will be presented.



1. Configuration tab
2. Configuration options list
3. List of NVRs in the system
4. Properties screen

Network Devices

From the Configuration Home Page, select ***Network Devices***; it is expanded by default. An exception to this is if the license has expired. In that case, the Configuration tab will open to the Licensing screen, where you can activate a license. This process is explained in detail under System configuration later in this manual.

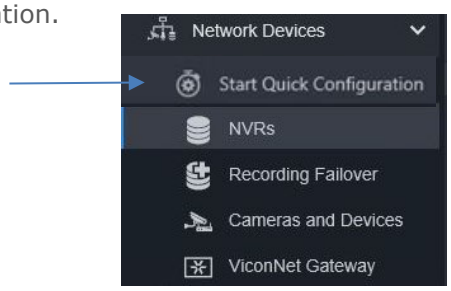


Quick Configuration

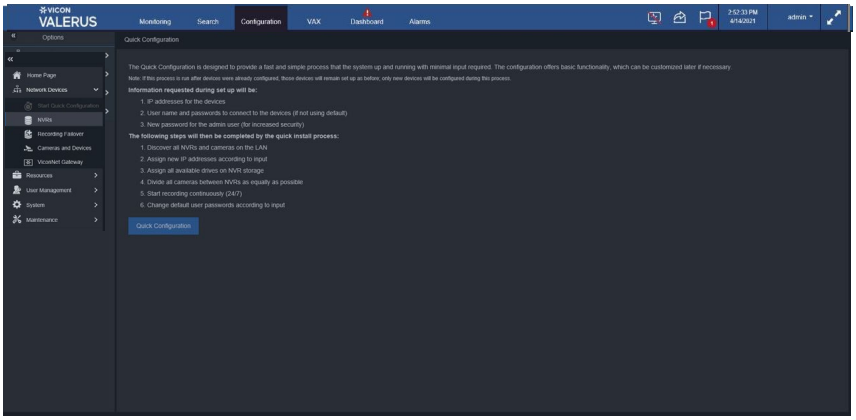
The simplest and easiest way to get the system up and running is to use the ***Quick Configuration***. This offers a streamlined process for typical and basic system setup with minimal input required. Information requested during set up will be:

- IP addresses for the devices: The process will assign IP addresses from a range of addresses that is most suitable for private networks without a specific network scheme. If the devices are already configured with an IP address (static or DHCP) you will be able to skip this step.
    - If an IP range different than the default one is required, make sure to set the range correctly (according to subnetting rules), have enough free addresses and remember the Application Server will also use an address.
- User name and passwords to connect to the devices (if not using default): The system has a list of known user name and password combinations for most camera vendors. When a camera is discovered, the system will attempt using those to connect to it. In case different user names and passwords have been set up, enter them here so they can be used as well.
- New password for the admin user: It is recommended that the administrator password be changed for increased security; if defaults are kept in place, the password is known to anyone and the system configuration screens can be easily accessed.

Click Start Quick Configuration.



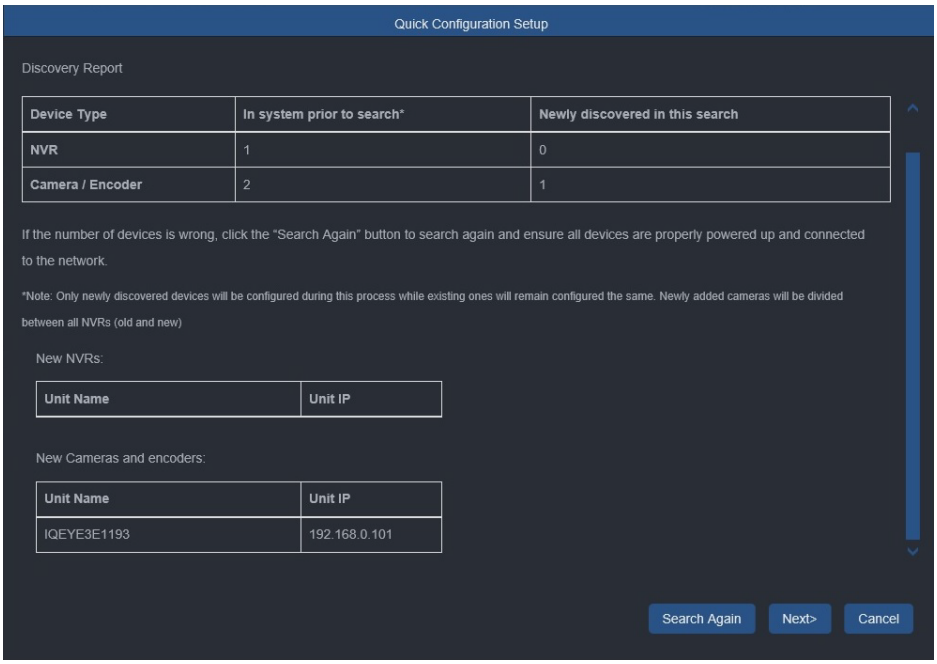
Clicking Start Quick Configuration opens an explanation page. Read the explanation. If you want to go ahead with the Quick Configuration, click the button.



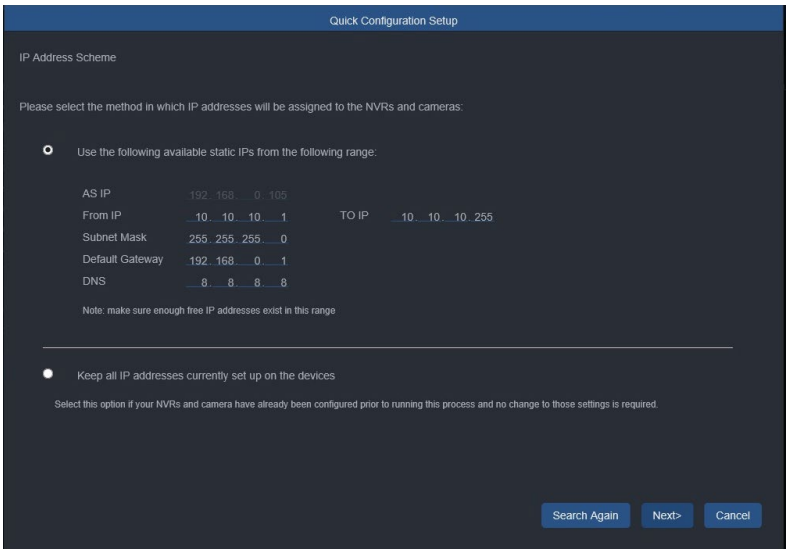
The following steps will then be completed by the quick install process:

- Discover all NVRs and cameras on the LAN: The server will search and find all devices that are on the same LAN as the server. If there are devices that you know are on the LAN and were not discovered, make sure that they are connected and powered and then click Search Again. When all devices have been discovered, click Next. Remember, the process can only discover NVRs and devices that are on the same LAN as the Application Server.

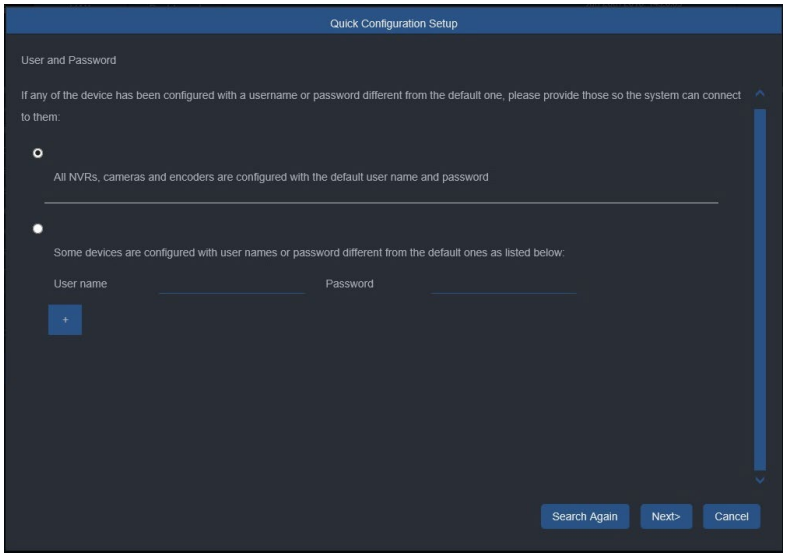
  Tip! If there are NVRs or other devices on a different VLAN or on a network not open for multicast discovery (i.e., certain WiFi, firewall), these will not be discovered automatically; these NVRs and devices can be added manually as explained later in this manual to allow discovery on those nodes.

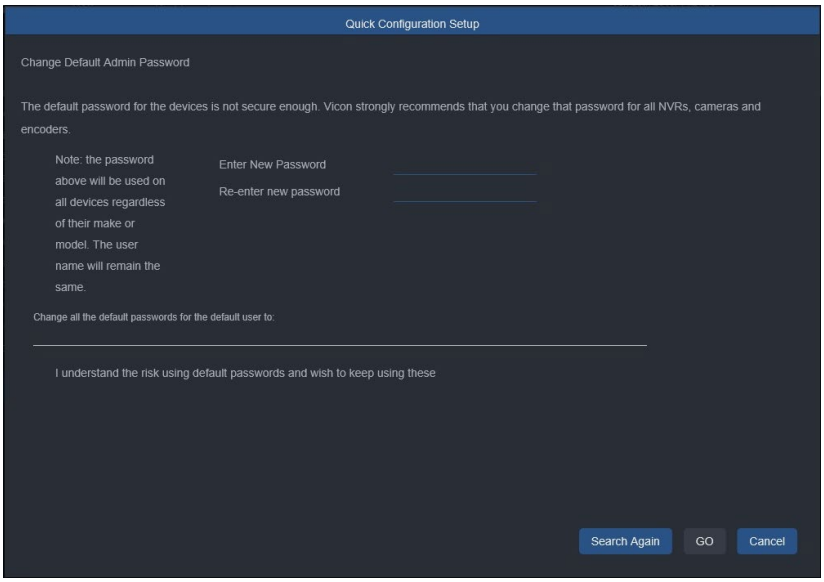


- Assign new IP addresses according to input: A screen displays with the default IP address range and allows you to change the IP addresses to an assigned valid range of your choice by clicking the radio button. Click the radio button below if all IP addresses are to remain as is and no change is required.

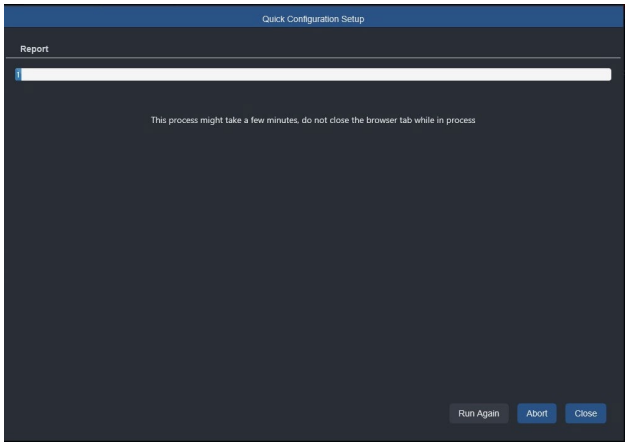


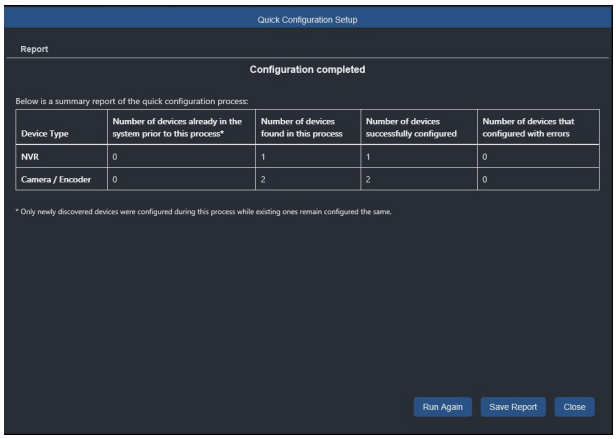
- By default the Quick Configuration will:
  - If IP assignment is needed, ping the IPs to ensure they are free and assign to the devices.
  - Assign all available drives on NVR for storage: All drives except the operating system drive (typically C:\ drive) will be assigned to the NVR and the system will allocate all available storage on the assigned drives for recording of devices.
  - Divide all cameras between NVRs as equally as possible: Cameras will be distributed among all available NVRs on the system by their model to allow equal distribution. Newly added cameras (when quick configuration is run again after some devices have already been added) will be added into both newly discovered and previously added NVRs.
  - Start recording video continuously (24/7): All cameras will be configured to record 24/7 by default.
- Setup user and password credentials. Change default user passwords according to input: For increased security, passwords will be set according to those selected by you; although it is not recommended, you can leave default passwords after reading Vicon's warning.





- After the Quick Configuration screens are completed, click Go. The configuration process will begin and may take a few minutes to complete, depending on system complexity. A Configuration completed message will display showing a summary of the NVRs and Cameras/Devices that were successfully configured as well as a list of failures if such exist.





- If you now go into the main Configuration area, you will see that NVRs and devices were added and display on their respective screens, NVR storage allocation was done and devices were split evenly between NVRs. Any modifications and customization required can now be done, as explained in the detailed configuration steps below.

Note: If this quick configuration process is run after devices were already configured, those devices will remain setup as before; only new devices will be configured during this process.

Step by Step Configuration

Quick Configuration, although very efficient and time saving, may sometimes not allow the flexibility required. For example, there are cases when NVRs cannot be discovered automatically and need to be added manually or when the even distribution of cameras is not sufficient and manual allocation is needed or simply when a step-by-step setup makes more sense. Configuration must be done in the correct order. Follow the steps below to complete setup.

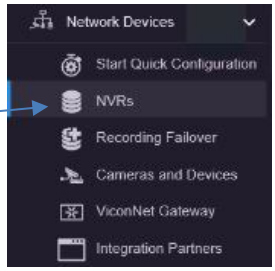
Tip: The order in which the options list is shown represents the logical order of laying down the system "building blocks": Application server on top, NVRs added to the Application server and IP devices (cameras and devices) added to the NVRs. At this stage the physical blocks are added and their different resources can be configured and used.

Note: Because the Network Settings (IPV4/IPV6 and HTTP/HTTPS) impact on the NVR and Camera and Devices settings, if you want to restrict any devices it is important to configure the Network Settings for these BEFORE adding in the Discovered NVRS and Discovered Devices.

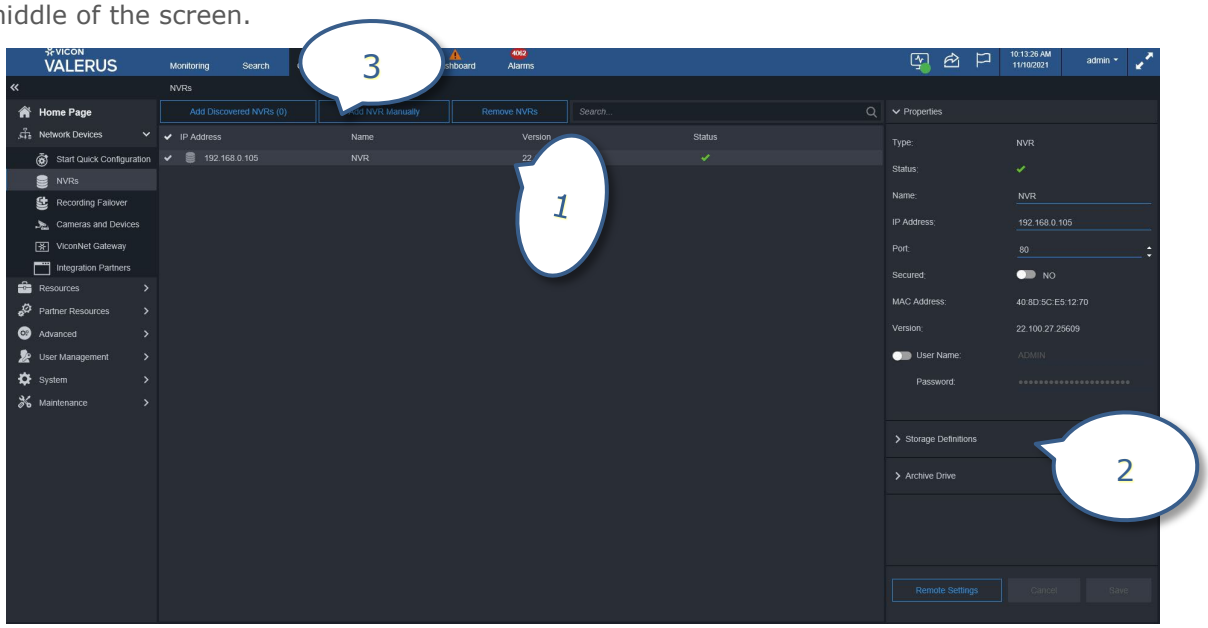
Recording Servers (NVRs)

The first step in configuration is to add the ***NVRs*** to the system. There is no limit to the number of NVRs that can be in the system.

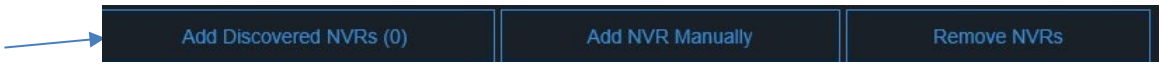
- Click on NVRs to open the NVR setup.



- If any NVRs were setup in the Quick Configuration or previously configured, they will be listed in the middle of the screen.

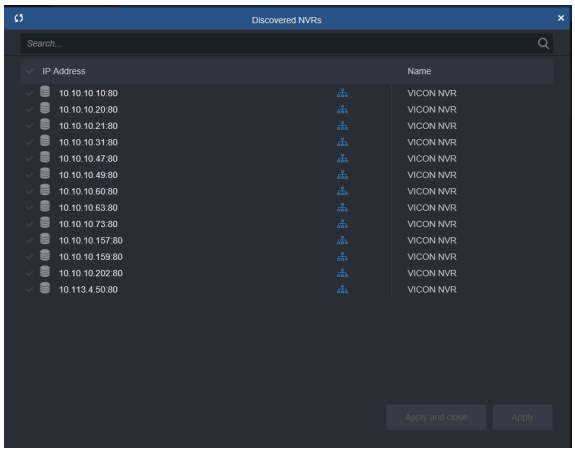


1. List of configured NVRs
2. Properties of selected NVR
3. Options to add or remove NVRs

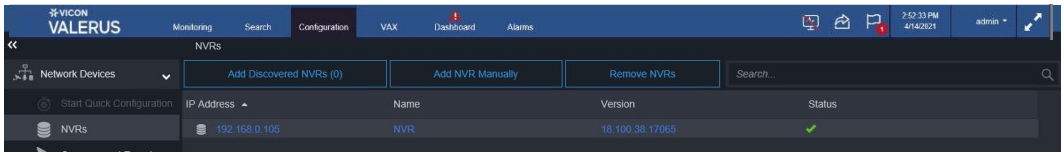


- NVRs can be added to the system in two ways, either from the list of NVRs discovered by the server or added manually The Add discovered NVRs provides a list of NVRs that were auto-discovered by the system that are not already on your list; a number in parenthesis on the button indicates how many NVRs were discovered on this LAN (once it is added to the system it is no longer in the Add discovered count). If you know that more than this number of NVRs has been installed, check their connectivity and if they are on a different network (or VLAN, etc.); they can be added manually.
- Click the ***Add Discovered NVRs*** tab at the top of the NVR screen; a popup with a list of the discovered NVRs will display; use the dropdown arrow to view the list. Note that there may be two IP addresses listed for the same device. This is because the Network Settings for IPV4/IPV6 and HTTP/HTTPS impact on what is presented here. This list can be refreshed by clicking the refresh button in the top left corner. Select the NVR(s) to be added to the system by clicking the check mark next to the NVR. Clicking the check mark on the top bar will select all the NVRs. Multiple NVRs

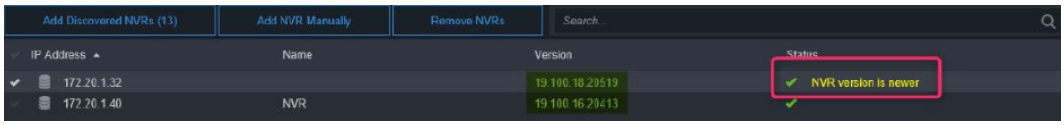
can also be selected holding the Control (Ctrl) key while clicking on the NVRs or by holding the Shift key and clicking the top and bottom NVRs in a selected range (standard Windows selection). Click Close and Apply when done or click Apply button to continue using this screen. Click the x in the right corner to close the popup menu.



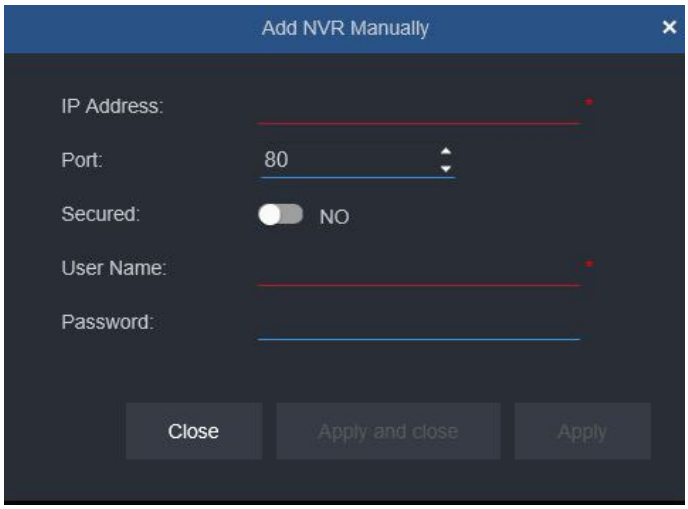
- The selected NVRs will now be listed with their IP address, version of software and the status. A green check indicates the NVR is recognized and can be further configured.



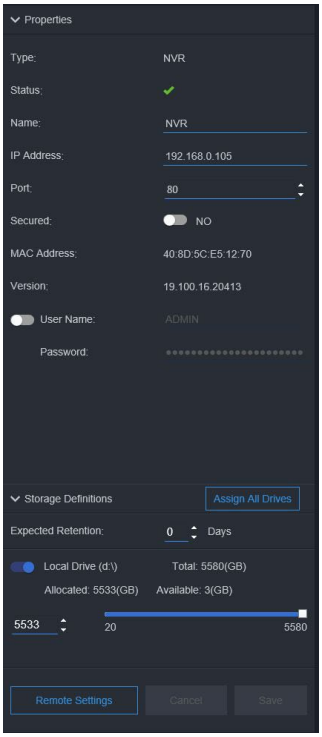
If an NVR is added whose version is newer than the Application Server, there will be a notice.



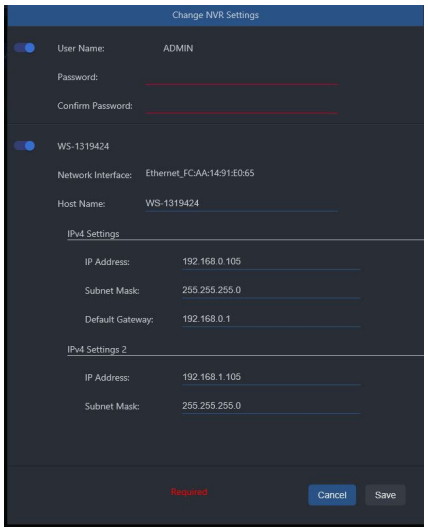
- To add an NVR that was not on the discovered list (for example on a different VLAN), click ***Add NVR Manually***. A popup displays to enter the IP address of the NVR, its port and a user name and password. Also select whether this NVR is using secured communication (Yes/No; using a secured HTTPS connection). Click Apply. A Close and Apply and Close button are provided to close the popup. This NVR is added to the list with all of its pertinent information and can now be configured.



- The ***NVR Properties*** screen displays to the right, providing information on the currently selected NVR. Clicking on the arrow head next to the word properties collapses the screen to display just the storage definitions.



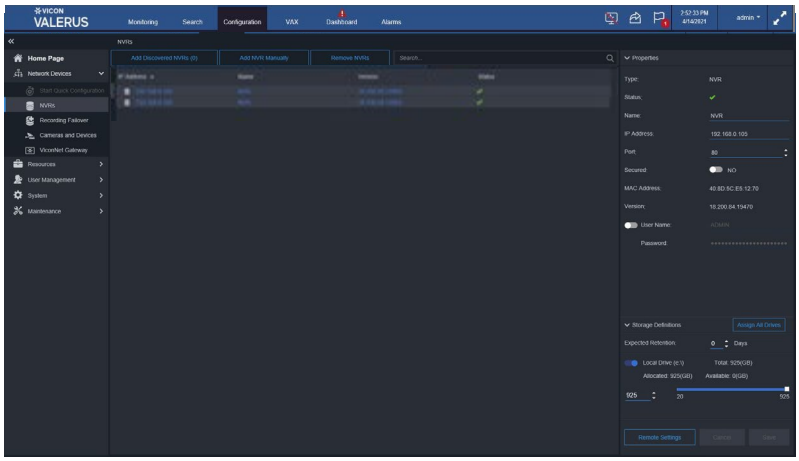
- By default, the NVR is added without a name and will be listed by its IP address. If a name is added in the field, that will also display in the NVR list.
- The IP address and port of the NVR is shown and can be changed. The address and port are what the Application Server will use in order to connect to the NVR and needs to be updated in any case where the NVR has changed its IP address and/or port.
- The Valerus version is provided here for easy reference.
- The user name and password shown are what the Application Server will use in order to connect to the NVR and will need to be updated if changed. Click the switch next to it to allow editing.
- A Remote Settings button is provided and can be used to change some of the credentials for the NVR itself. Different from the connection details described before, these will make changes to the NVR itself. Clicking Remote Settings opens a dialog box.



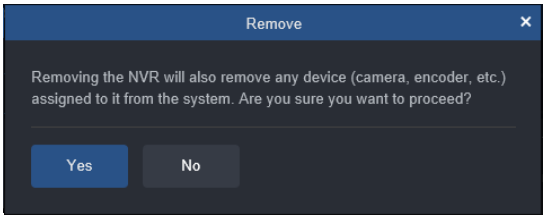
- Click the button to activate the fields you want to modify, password and/or your device credentials. The ADMIN password for the NVR can be changed (the ADMIN name cannot be modified). Required

fields are noted in red. After your changes are made, click Save or Cancel to close without saving the new settings.

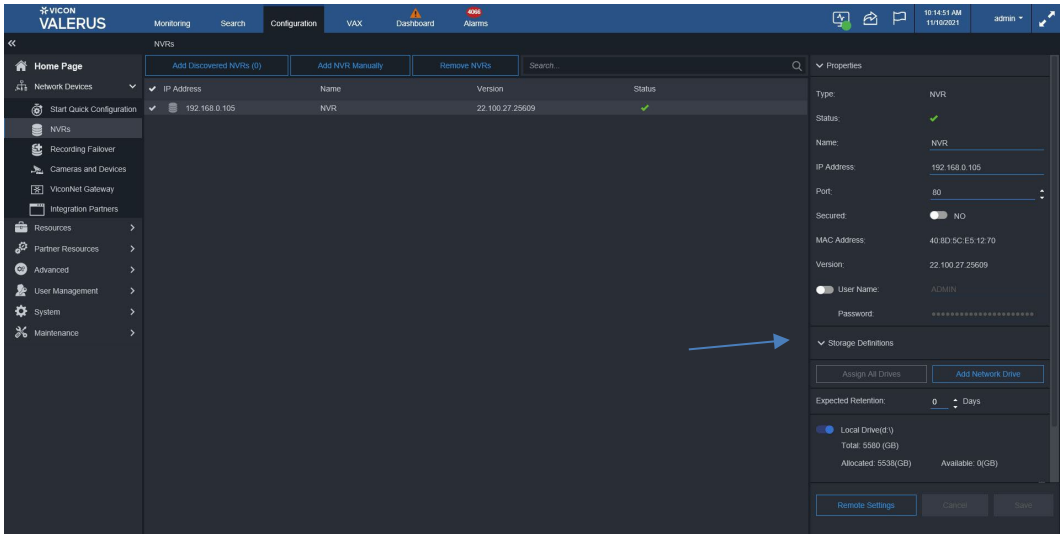
- If the IP details of the NVR need to be changed, it can be done in the lower section of this pop-up. Note that depending on how the Network Mode is configured in the System, Network screen, there may be both IPv4 and IPv6 settings here.
- If multiple NVRs are selected (done using the check box or the Ctrl key), they can be configured together, but only for their common attributes. For example, all NVRs can be given the same password, but an IP address cannot be configured as it's unique per NVR. Check the NVRs you want to configure; the Properties box will change to display the common properties to allow those changes. Click Save or Cancel to close without saving changes.



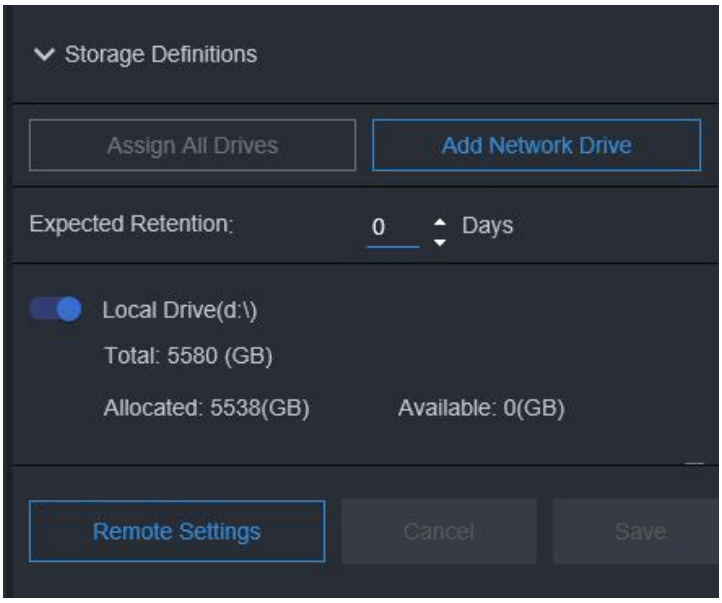
- NVRs can be deleted from the list. Check it in the list and click Remove NVR or click on the garbage pail icon in the row after Status. The following message displays.

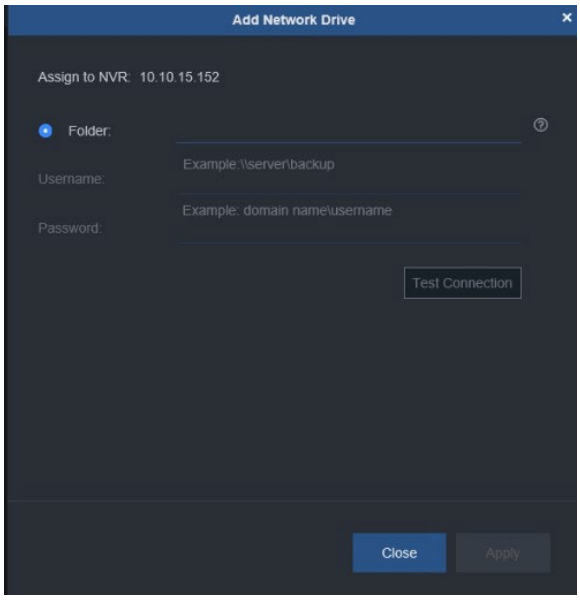


- Storage definitions must be set to allow devices to record to this NVR. The system allows using either local drives or mapping to a network location using standard network path addresses. The drive that contains the Operating System (typically the C:\) should not be used for recording unless it is the only choice.



- When Storage Definitions is selected, there are two choices, Assign All Drives (local) or Add Network Drive. When Add a Network Drive is selected, the screen below displays. Specify a network path and credentials to connect to it.



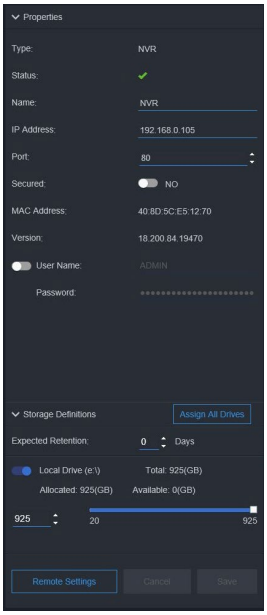


- Mapping a folder allows mapping to any location that is sharable (NAS or drive on a PC). It requires a full network path, which must be limited to 40 characters, the username to connect and the password. This is similar to mapping a network drive in Windows; the user access must allow read and write permission.
- The Test Connection button is used to verify that the connection and authentication are valid.
- *Important Note 1:* When mapping multiple NVRs to the same storage device (typically NAS), the storage setting must be done as a single folder and not split between different ones.

  Example:
  Using NAS on IP 192.168.1.9
  Good:
  NVR1 mapped to \\192.168.1.9\ValerusStorage will use 1TB
  NVR2 mapped to \\192.168.1.9\ValerusStorage will use 1TB
  The size of the ValerusStorage destination should allow enough for both NVRs to be configured so in the example above should be 2TB.
  Not good:
  NVR1 mapped to \\192.168.1.9\NVR1 will use 1TB
  NVR2 mapped to \\192.168.1.9\NVR2 will use 1TB
  The size of the NVR1 and NVR2 destinations is 1TB each
- Failing to use a common storage pool will result in the NVR available storage calculation failing and may harm recording.
- *Important Note 2*: Some network storage devices restrict the maximum file size they allow a system to write to them; this may impact the NVR's ability to reserve storage for recording. A file the size of the expected storage is created when the drive is picked by the NVR. If a storage device does not allow unlimited file size, it will require limiting the storage volume to the maximum file size. For example, if the limit is 4TB per file, to get 100TB, it will require providing the NVR 25 separate volumes of 4TB each. The correct way to do this, while following the same path rule explained above in Note 1, is to create subfolders for this specific NVR and using them as "drives." In our example, it will require 25 subfolders of 4TB each, as shown below.

  NVR1
  Mapped to \\192.168.1.9\ValerusStorage\A will use 4TB
  Mapped to \\192.168.1.9\ValerusStorage\B will use 4TB
  Mapped to \\192.168.1.9\ValerusStorage\C will use 4TB
  And so on.
- *Important Note 3*: Although allowed, it is not recommended to map both a local and a network drive for recording, as the access to the different locations may vary in speed.

- The Expected Retention of data (in days) can be set (is this just for local drives?). This setting is based on what is expected from the system according to how it is configured (using the storage calculator); it does not influence the recording done by the system. Note that if 0 days is selected, the system assumes no specific expectation of retention. From the Dashboard statistics, you can see if the retention expectations set here are being met or fall short. It is important to understand this is a user setting, not an actual limit. Refer to the Video Recording section for details on limit retention.

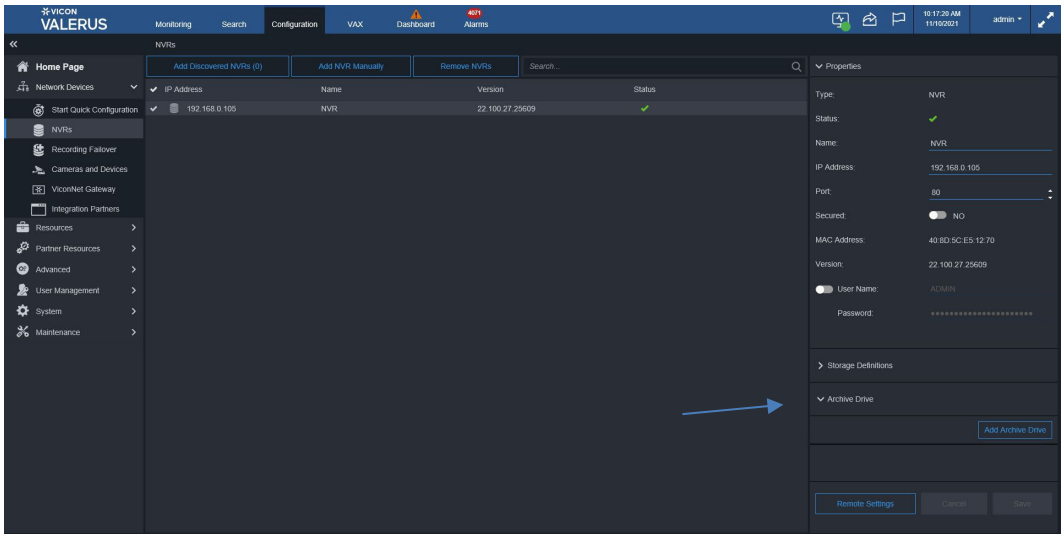


For convenience, there is an Assign All Drives button; when selected, the system will set all available drives to use their maximum storage capacity. Any physical drive can be used for storage except a USB stick. For a more controlled allocation of drives follow the steps below:

  - If only the C:\ drive is available, check the Local Drive box. Allocate space for recording storage using the slide bar or the number field up/down arrows. A 75 GB minimum storage space is required; if a drive does not have that available it will not display. If other drives are available for storage, select the drives to store video and allocate space on these drives.

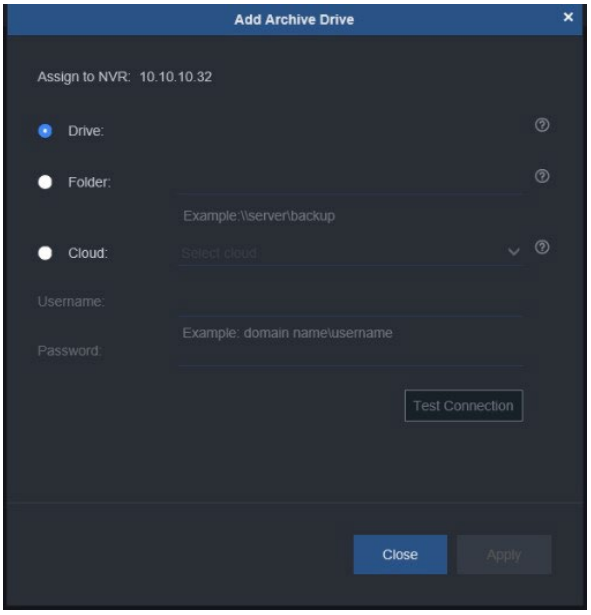
- Valerus allows defining and using a secondary storage location as a destination to move and store recordings. This allows splitting between local storage on the NVR (faster but more expensive) and longer time storage on lower cost solutions such as NAS. This still maintains the remote storage location connection and seamlessly supports access to that location for playback and search purposes while maintaining its own FIFO routine. For example, it is possible to choose to record 7 days on the local NVR and 90 days on a NAS, having access to both locations without the need to perform any complex restore process.

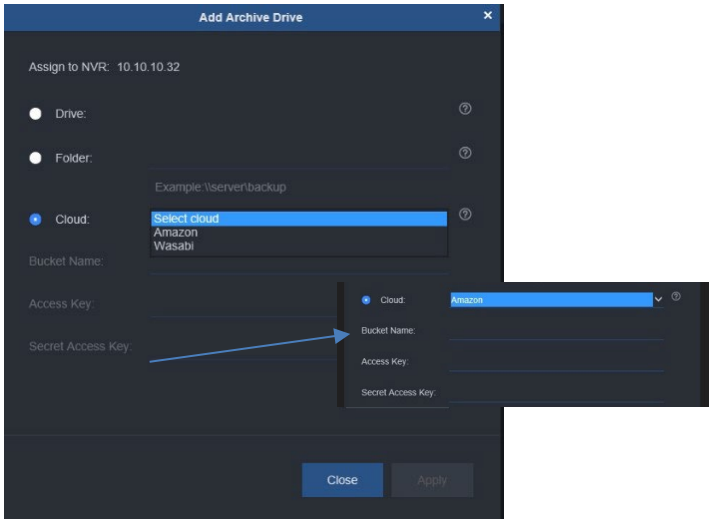
- Under Archive Drive, click Add Archive Drive. The following screen will display.



- The setup for Add Archive Drive is similar to the procedure for Add NVR Drive. There are two options, mapping to a drive or folder with a specific network path and credentials. Mapping a folder allows mapping to any location that is sharable [including Cloud storage (AWS or Wasabi; ENTERPRISE tier only), NAS or drive on a PC; note that either Cloud or NAS can be selected, not both]. A yellow triangle next to Archive Drive indicates that no storage has been allocated in the drive. It requires a full network path, which must be limited to 40 characters, the username to connect and the password. The Test Connection button is used to verify that the connection and authentication are valid. Additionally, Auto Archive can be set up. For details on setting that up, refer to the System section of this manual. New screen to show

  Note that the Cloud storage option must be setup in AWS/Wasabi by the customer prior to using it here. Use the details from AWS/Wasabi for the Bucket Name, Access Key and Secret Access Key required for the addition of Cloud archive.





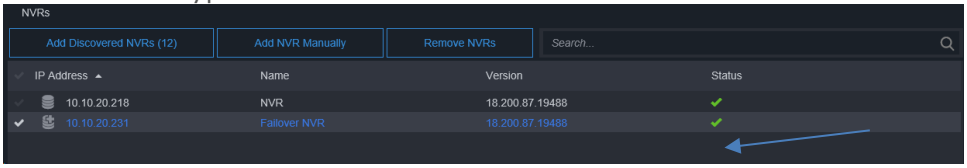
- Click the Save button to retain these settings. A Cancel button is provided to negate any settings made. If the page is closed without saving, a warning dialog box will display.

Tip: Avoid using the OS drive as a recording drive. It is strongly recommended to use a different physical drive if available or at least partition the drive and use a different partition. Using the OS drive for recording may have an impact on overall NVR performance.

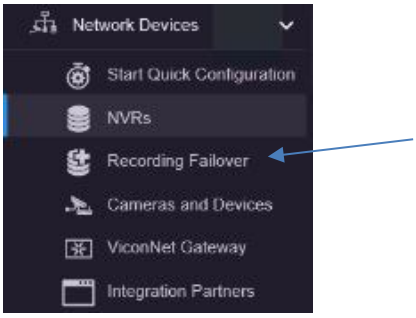
Recording Failover

Valerus allows an NVR to be configured as a failover NVR to act as a backup in the case of an NVR failure. The failover NVR is a dedicated PC and is *not* one of the system's NVRs.

Note: The Recording Failover capability requires an ENTERPRISE license. Additionally, the NVR must be defined as a failover NVR in the Valerus Launcher and then added to Valerus in the same way a standard NVR is added. Refer to the previous section to add the failover NVR. In the NVR list, the failover NVR will show with the different icon and failover type.

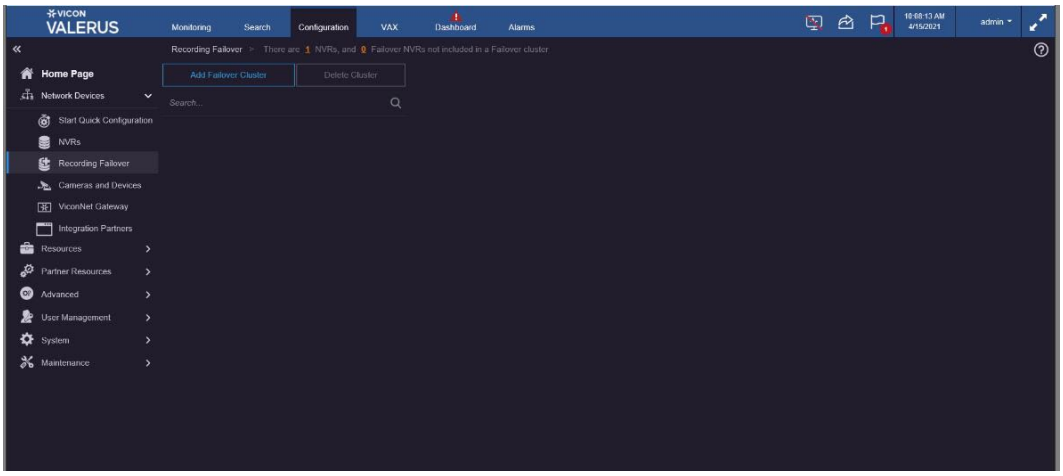


Proceed to the Recording Failover tab. The following screen displays.

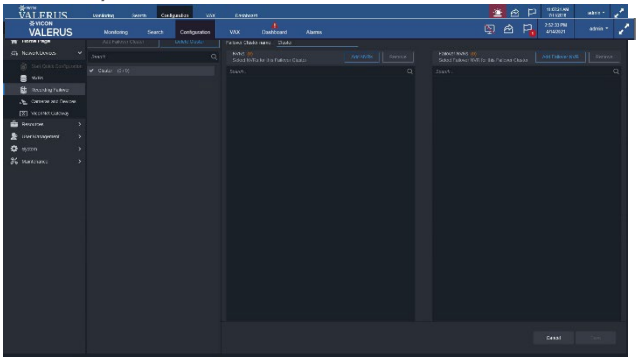


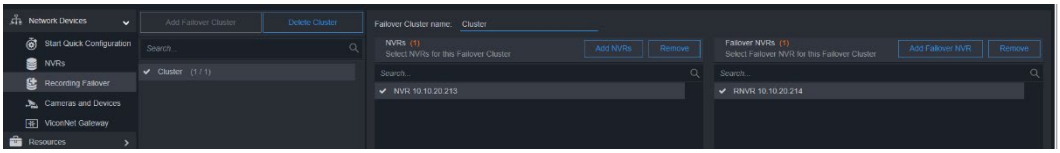
From this screen, define ***Clusters*** of NVRs and the association of failover NVRs that will be the backup.

- A single failover NVR can serve as a failover for multiple NVRs; once the failover NVR is in use (actively backing up a failed NVR), it is not available for failures of other NVRs in that cluster. Each device can be in only one cluster. At least one NVR and one Failover NVR must be in the system to form a cluster.
- You can also decide to have several failover NVRs in the same cluster and then, if one is actively backing up a failed NVR, the next one will be standing by for another failure.



- Click ***Recording Failover*** to open the setup screen.
- Click ***Add Failover Cluster***. The following screen displays. A summary of the system NVRs and Failover NVRs is at the top; this list is based on the NVRs and failover NVRs already added to the system. Click ***Add NVRs*** to select which NVRs will be in this cluster. Then click Add Failover NVR to designate which failover NVR will back up this cluster of NVRs.
  - The summary will always show if certain NVRs are still not members of a cluster.





- Click Save to complete configuration of the cluster. A cluster can be removed by selecting the cluster and then clicking the ***Delete Cluster*** button.

Once Recording Failover is configured, if an NVR fails, the system will automatically find the defined Failover NVR; failover will occur within 30 seconds. There will be a Dashboard message that an NVR failed and which failover has taken over.

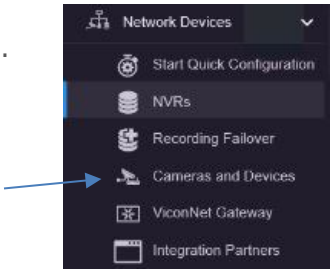
Note that except for the expected short gap in recording until the failover starts, the system behavior is transparent and user experience is not changed. Valerus will automatically switch playback to and from the failover NVRs without having to know when an event occurred.

The failover NVR has its own recording database and its own FIFO schedule.

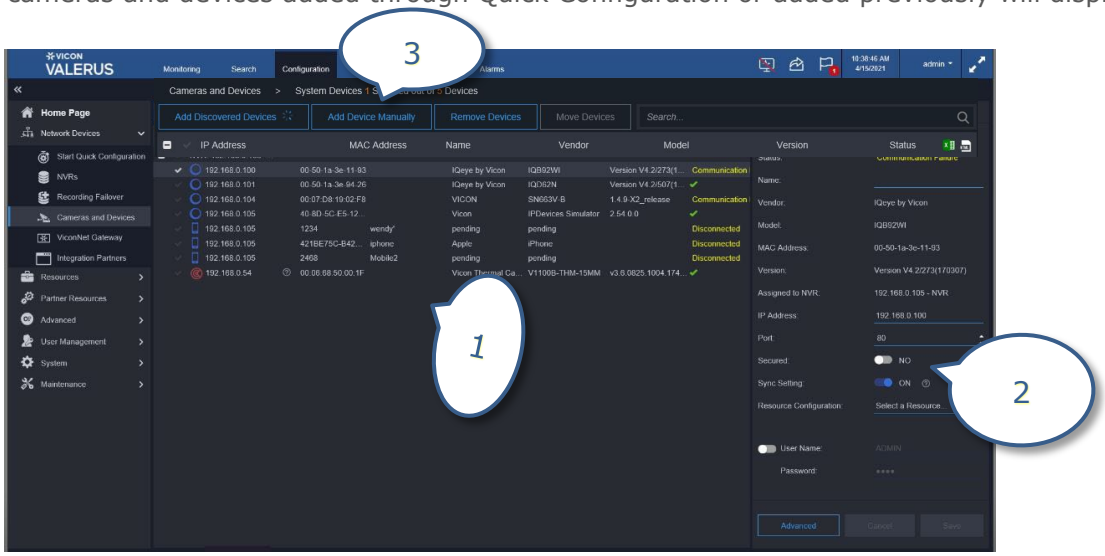
Cameras and Devices

Once the NVRs are configured (at least one NVR must be added to the system for this step; a message will display if no NVR has been added), cameras and devices, including mobile devices (ENT), can be added to the system and configured, requiring that they be assigned to an NVR; a device cannot be on multiple NVRs. Any ONVIF device is supported by the system. An ONVIF device supports at least standard ONVIF-S protocol and uses standard ONVIF protocol; RTSP devices are cameras and devices that support Real Time Streaming Protocol; although they may not support ONVIF, their streams may be added. Devices are listed under the NVR they are associated with; the number in parenthesis next to the NVR name indicates how many devices are currently associated with it.

- Click ***Cameras and Devices*** to open the setup screen.

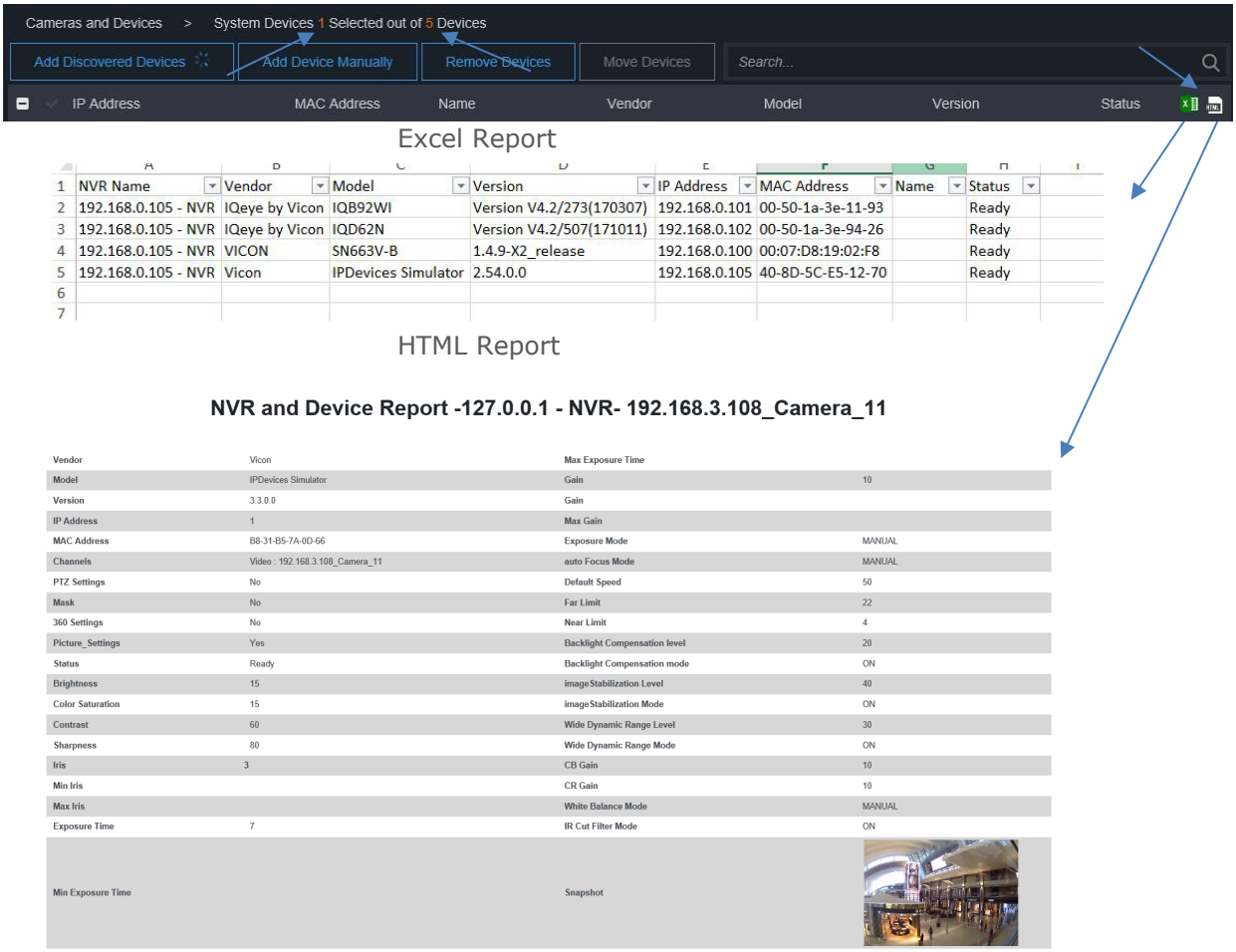


- Any cameras and devices added through Quick Configuration or added previously will display in the list.



1. List of configured cameras and devices per NVR, including MAC address
2. Properties of selected camera or device
3. Options to add, remove or move devices

- The number of devices selected in the list displays next to System Devices; Selected out of indicates how many devices are on the system. There is an Excel icon and an HTML icon in the right corner . Clicking the Excel icon allows you to save a report for all NVRs and all devices in an Excel format, including MAC address and Numeric ID, if assigned. Clicking the HTML icon provides a more structured report that can be to the server; in addition, the HTML report contains the channel snapshot as saved in Video Channels, showing the view from the specific camera. New with HTML report icon.



- Similar to NVRs, devices are added to the system in two ways, either from a list of devices discovered by the Application Server and NVRs or added manually. The Add Discovered Devices option provides a list of devices that were auto-discovered by the system and are not already on your list; the number in parenthesis indicates how many such devices were found on this network (once a device is added to an NVR it is no longer in the Add Discovered count). If you know that more than this number of devices has been installed, check their connectivity and if they are on a different network (or VLAN, etc.) they can be added manually.
- Click on the ***Add Discovered Devices*** tab at the top of the Cameras and Devices screen. A popup displays with a list of NVRs in the system on the left, along with the number of devices that specific NVR discovered and the number of devices already assigned to it; use the dropdown arrow to view the entire list. The first time this is done, a message will display asking to provide credentials for those devices that do not have any (user name and password); if the device has credentials, they will not be affected. Additionally, the first time a camera is being added, the VMS will ask and store a user name and password in case an ONVIF profile Q camera, which requires a known user and password in the VMS, is added to the system. Note that there may be two IP addresses listed for the same device. This is because the Network Settings for IPV4/IPV6 and HTTP/HTTPS impact on what is

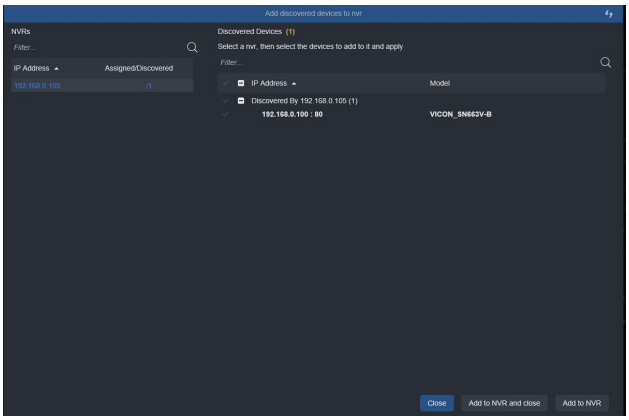
presented here. This list can be refreshed by clicking the refresh button in the top right corner. When an NVR is selected by clicking on it, two lists are displayed on the right side of the popup:

- List of all devices this specific NVR did not discover but were discovered by other NVRs (if such devices exist).
- List of devices discovered by this NVR but not yet assigned to it.

- In networks where there are NVRs on different nodes of the network, having two lists offers the ability to distinguish which NVRs and devices are on the same network node.

  When all NVRs and devices are on the same network, it is expected that all NVRs will be able to discover all devices and that there are no network constraints that might restrict certain NVRs to record certain devices. On the other hand, if there are NVRs and devices on different nodes, for example in a campus where different buildings are on a different VLANs, it might make more sense to assign the devices in a certain building to the NVR in that same building and not to stream back to another NVR. Knowing which NVR can discover those devices helps in making that decision.

- Select the devices to be added to the selected NVR. A device can be selected by clicking the check mark next to the device. Clicking the check mark on the top bar will select all the devices in the list. Multiple devices can also be selected holding the Control (Ctrl) key while clicking on the devices or by holding the Shift key and clicking the top and bottom devices in a selected range (standard Windows selection). Click Add to NVR and close when done or click Add to NVR button to continue using this screen. A Close button is provided to close the popup. The selected devices will now be listed with the IP address, vendor, model, version of software and the status. A green check indicates the device is recognized, meets the defined ONVIF profile and can be configured.

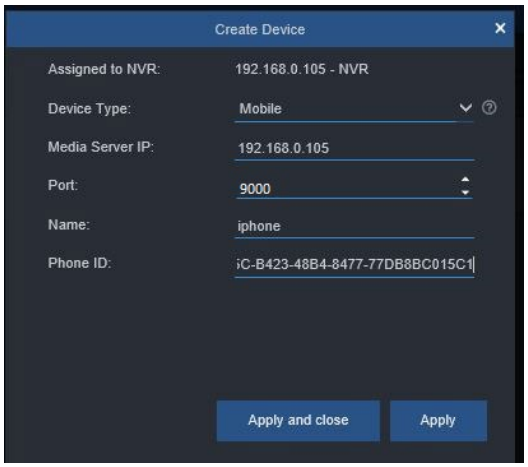


Note: On rare occasions, there may be the message "NVR Device Database Mismatch" instead of the green check; this message will also appear in the Dashboard. This means that the NVR is not receiving the expected settings for the device as defined in Configuration/Resources; the defined settings do not match the settings coming from the camera itself. This may happen, for example, if the camera settings are changed directly from the camera's web interface instead of from the VMS Configuration page (all camera settings should be done directly from the VMS). The NVR will keep trying every 30 minutes to match the defined settings. The camera will display video, but the display may not be as intended, i.e., different resolution or fps.

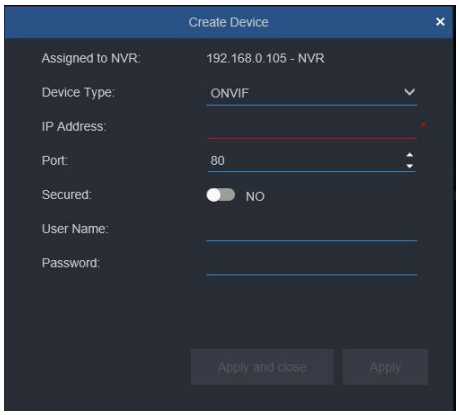
- To add a device that was not on the discovered list for any reason, click the ***Add Device Manually***. A popup displays to enter the device protocol (ONVIF, Events Framework, Mobile, ADAM-6050 or

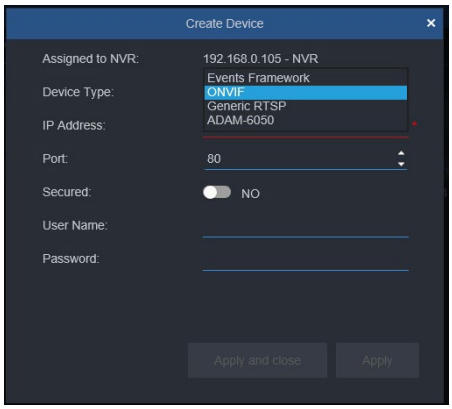
Generic RTSP), the NVR it will be assigned to, port, whether it should be secured (Yes/No; using a secured HTTPS connection) and user name and password for the device. Click Apply to continue using the screen. Click Apply and Close when finished. A Cancel button is also provided to close the popup. The device will be added to the list with all of its pertinent information.

- When adding a mobile device (Apple or Android phone or tablet), the latest Valerus App for mobile devices must be on the device. These are available at the Apple or Google Store. You also must provide the IP address of the Media Server (which should be configured prior to this step) on your Valerus system. Each mobile device has a unique identifier; when entering this ID be sure to include all letters, numbers and symbols (i.e., -) included in the ID. Multiple devices can be on connected to a Media Server as long as they have a unique ID. Refer to the manual on connecting mobile devices for details on how to add a Media Server and find this identifier. Once added, the mobile device displays as any other in the Resources list.



- Adding a device using its Generic RTSP address takes advantage of a capability most devices offer - to stream video and audio using an RTSP protocol. This will allow getting the streams from devices that are not ONVIF compatible and view and record them in Valerus. Adding a device in this way will allow you to define each stream by its RTSP address (these may vary between manufacturers and should be documented by them). A choice of resolutions is provided, up to 12 MP. An example of this follows:



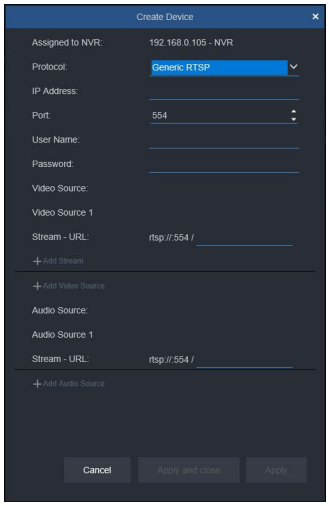


This example uses an encoder and shows how all channels can be added:

- In this example, the encoder has 8 video inputs and supports 2 streams for each input.
- The RTSP address is defined as follows:
  - Channels are numbered from "0" being the first channel to "7" being the 8th channel.
  - RTSP port used is 5554.
  - For every channel, the **first** stream address is RTSP://xxx.xxx.xxx.xxx/live/mainN (where xxx.xxx.xxx.xxx is the unit IP, N is the channel number 0-7).

- For every channel, the **second** stream address is RTSP://xxx.xxx.xxx.xxx/n/live/secondN (where xxx.xxx.xxx.xxx is the unit IP, N is the channel number 0-7).

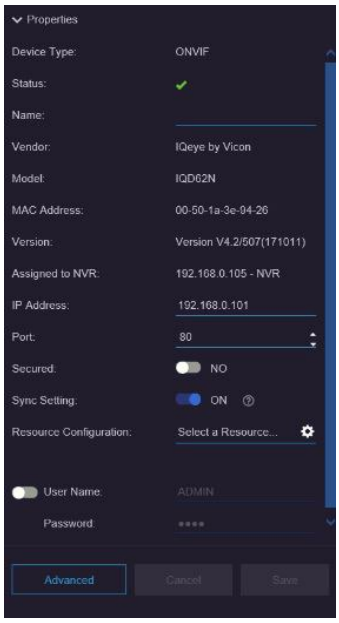
- Each channel with the two streams is setup as shown in the setup screen below. Note the option to add more sources (when multiple inputs exist) and more streams.



Note that at this time there is no way to edit the unit once added, so please make sure to add all channels at the same time.

Once added every source will show as a video resource exactly as other cameras and allow setting its properties. See the note regarding these channels under the video channel settings.

- The ***Properties*** screen displays to the right, providing credentials on the currently selected device. If a name is added in the field, that will also display in the list. Click the User Name button to allow the user name and password to be modified. Clicking the arrow head next to Properties collapses the Properties screen.



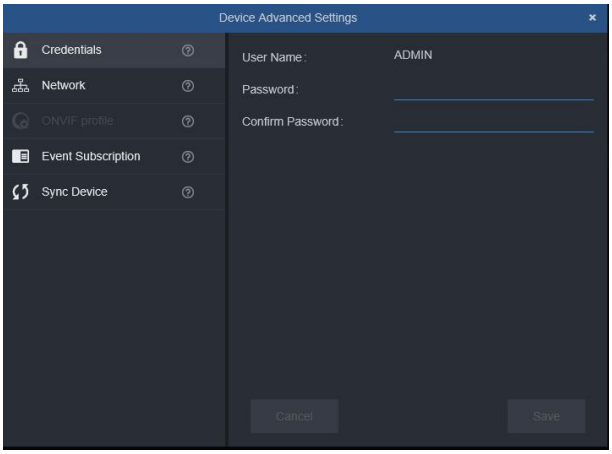
- By default, the device is added without a name and is listed by its IP address. If a name is added in the field, that will also display in the list.

- The IP address and port of the device is shown and can be changed. The address and port are what the Application Server will use to connect to the device and needs to be updated in any case where

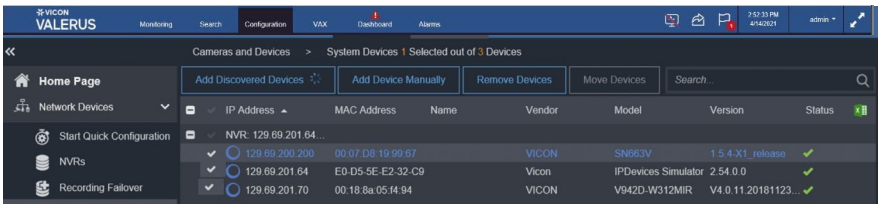
the device has changed its IP address and/or port. Enable the Secured button by clicking the button to YES (turns blue). This is used when you are using a secured HTTPS connection.

- The user name and password shown are what the Application Server will use in order to connect to the device. This will need to be updated if changed. Click the switch next to these fields to allow editing.
- By default, Valerus will sync the setting to the camera to ensure they match the VMS; this is done every 30 minutes. The Sync Setting allows this to be turned off to stop the sync if it is necessary to

  set the camera manually and keep those settings for another need. Note, it is recommended to keep the sync and allow Valerus to control the camera unless a real need comes up.
- An Advanced button is provided and can be used to change some of the credentials for the device itself. Clicking Advanced button opens a dialog box.

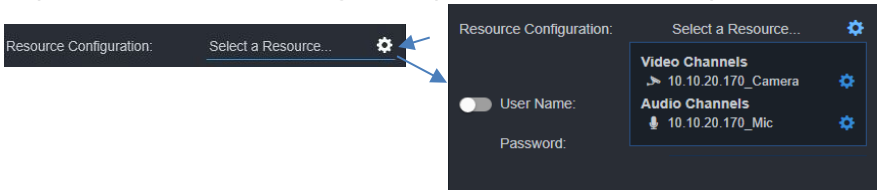


- From the Device Advanced Settings, several settings can be modified. From Credentials, the password for the device can be changed (the ADMIN name cannot be modified). Required fields are noted in red. After your changes are made, click Save or Cancel to close without saving the new settings.
- From Network, if the IP details of the device need to be changed, it can be done directly from the Properties screen. Note that depending on how the Network Mode is configured in the System, Network screen, there may be both IPv4 and IPv6 settings here.
- The ONVIF profile allows setting between profile S and profile T (default) for cameras that support both and may require a change.
- Event Subscription allows setting the way Valerus receives events from the cameras. By default Valerus will do this automatically, but some cameras may not work well and it is possible to manually select a method or disable this completely (to prevent event subscription failures).
- Sync Device will initiate a database sync with a device instead of waiting for it automatically, which may be required after certain changes occur.
- If multiple devices of the same model are selected (can be done using the check box or Control (Ctrl) key, they can be configured together, but only for similar properties. Check the devices you want to configure. The properties box will display with the common fields. Set the properties for all these cameras. Click Save.

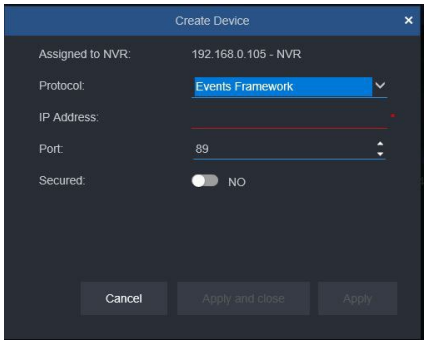


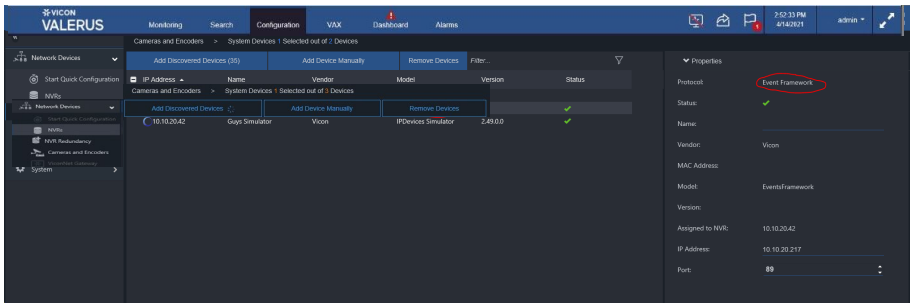
- Devices can be deleted from the list. Check it in the list and click Remove Devices or click on the garbage pail icon next to the Status indicator.

- Devices can be moved to another NVR, done for example to balance resources on the system. Click the Move Devices button and select another NVR to move this device to.
- A camera already in the system can be replaced with a new one (MAC address change); the existing settings will remain. When Valerus detects that a device IP address has a new MAC, the Admin will be prompted to approve the change. Upon approval, the new MAC address will be updated.
- From the Properties section, a settings icon provides a link directly to the Resource configuration screen.



- The VEF Streaming Engine is added manually in the Cameras and Devices Configuration screen.
- Once added, the VEF device will be listed as any other device and configured in Resources.





Valerus-ViconNet Gateway

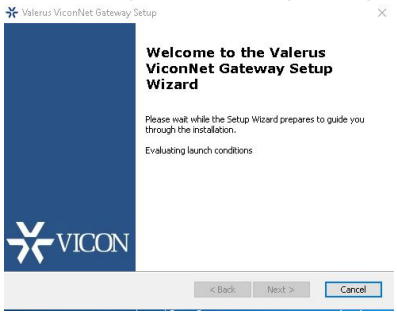
The Valerus-ViconNet Gateway is a module designed to provide a simple migration path to allow bridging existing ViconNet systems to a Valerus VMS. Refer to Valerus-ViconNet Gateway manual for details about this configuration.

Configuration in the ViconNet System

- The ViconNet Gateway uses the device groups set in the Nucleus to connect to existing ViconNet systems and select which cameras to bridge to Valerus.
- A group must be created that contains all the selected cameras that are to be connected. If multiple Gateways are used, multiple groups can be created (all under the same working group set), each consisting of the cameras for a specific server. If groups already exist, they can be used as long as they list all the cameras needed. Go to your ViconNet Nucleus and enter *System Setting*, *Device Group Sets*, *Working Set* to create the group.

Configuring the Gateway

- Download the Valerus-ViconNet Gateway software from the Vicon website on the Software Download page. Note that this download contains two installation files in one zip file, Gateway software and ViconNet version 8.3. Unzip the file and save the two installations.
- Install the Valerus-ViconNet Gateway on the assigned server; follow the installation steps in the setup wizard. If there are multiple Gateway servers in your system, install this on each of them.

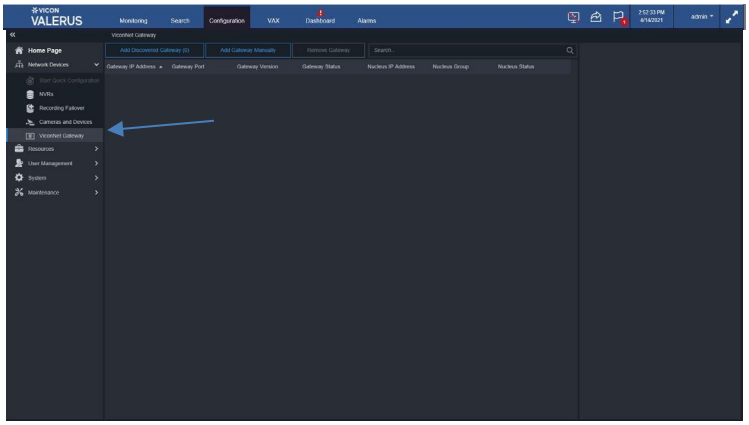


- Install ViconNet 8.3 on the same server on which the Gateway software was installed; there is no need to upgrade other ViconNet devices, as only the Gateway has to run this version. At the end of the installation choose not to run ViconNet on system startup. Run the ViconNet software once and then exit ViconNet. If the Gateway will be running on the Application Server in a new Valerus installation, be sure to choose *Application Server only* at the end of the install.

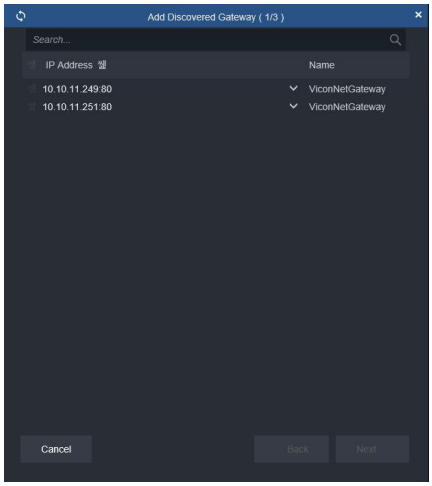
Valerus System

- Make sure the Valerus Application Server and all NVRs in the system are running a minimum of Valerus version 18.
- The Valerus license must be updated with the Gateway license. In a new installation, if the Gateway was part of the license, it should be in place; if this is an upgrade, the activation key needs to be updated. Each Gateway in the system requires a license.

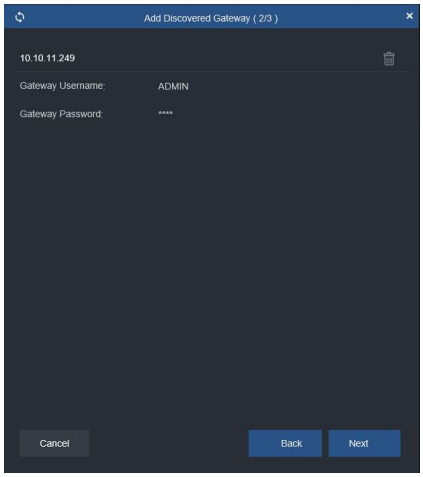
- Go to the Configuration tab. Click Network Devices and select the ViconNet Gateway option.



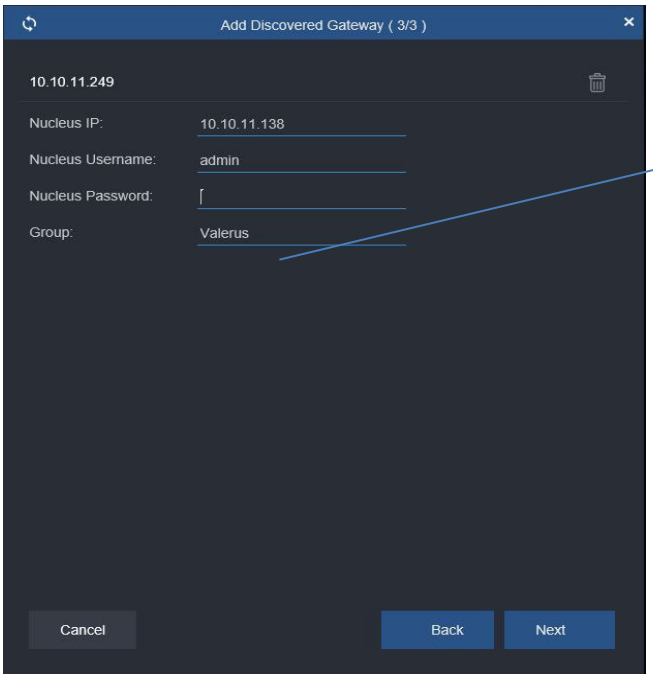
- Click on the Add Discovered Gateway to show the list of Gateways found on the network.

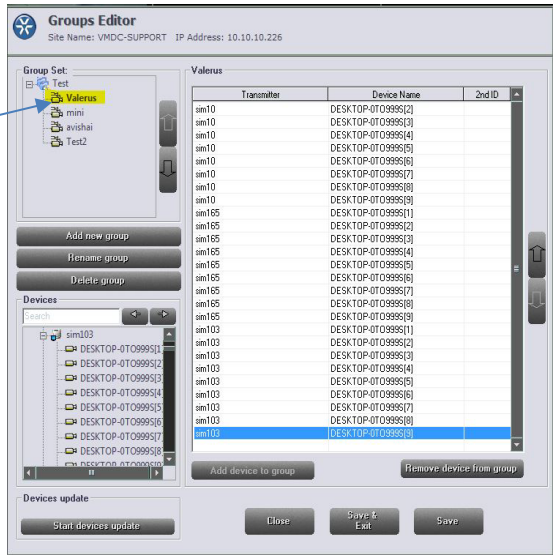


- Select the Valerus-ViconNet Gateway to be added from the list. Click Next.
- The Gateway User name and Password defaults are ADMIN, 1234. Click Next.

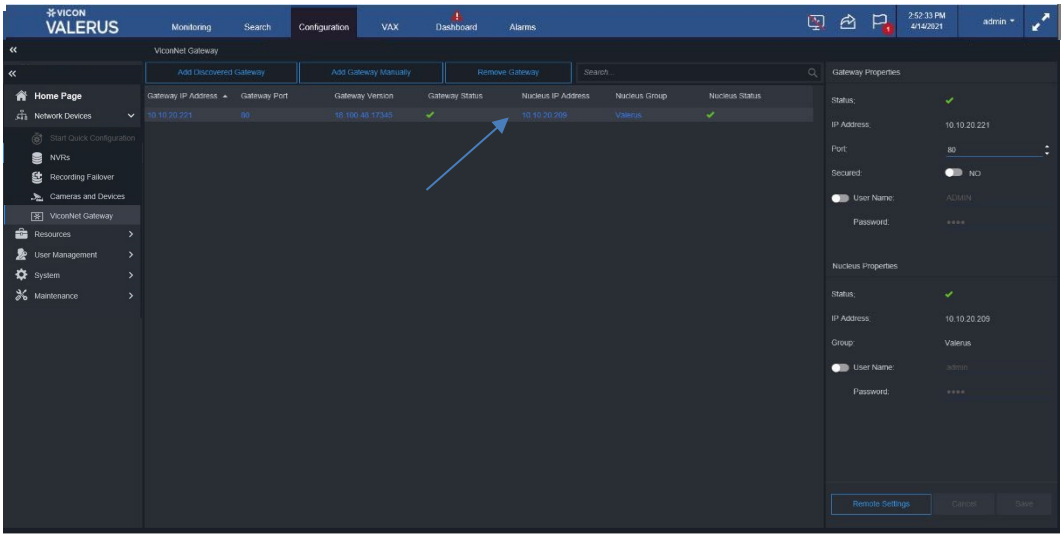


- A green check mark indicates that the Gateway has been connected. If the credentials have changed, update them here. Click Next.
- You will be asked for the Nucleus information allowing the Gateway to connect and communicate with the pre-assigned camera group. Fill in all the details as shown in the example below: Nucleus IP, the IP address of the ViconNet Nucleus; Nucleus Username and Nucleus Password have the same login credentials as the ViconNet administrator login credentials. Group is the Group name inside the ViconNet Working Group Set that contains the cameras from ViconNet to be added to the Gateway. Click Next.



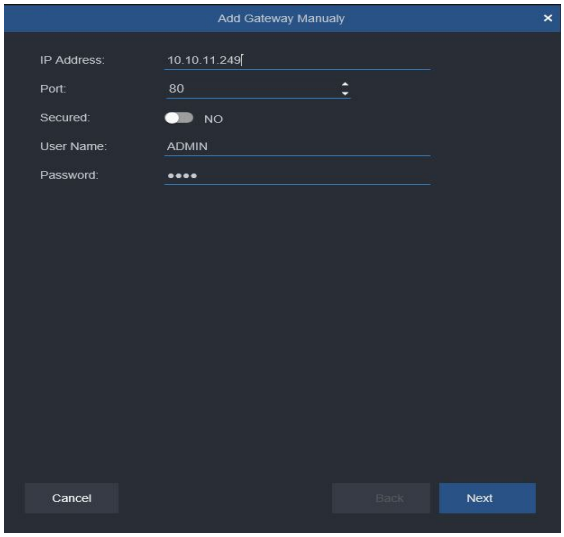


- If all the information entered is correct, the following screen should display; Gateway Status should show Online and Nucleus Status should show green check mark.



- If the Gateway Status shows Offline, make sure that the Gateway Service is running on the computer that it is installed on, or that the computer itself did not go offline; if the Nucleus status does not have a green check mark, make sure that the Nucleus is online and can be reached on the network by the Gateway computer.
- If the Gateway is located on another network or another VLAN and the Gateway computer can be pinged, it may not be discovered automatically by Valerus. In this case, use the Add Gateway Manually.

  Enter the Gateway IP address and port of the Gateway computer to be added. The remainder of the steps are identical to the Add Discovered Gateway procedure. See the image below.

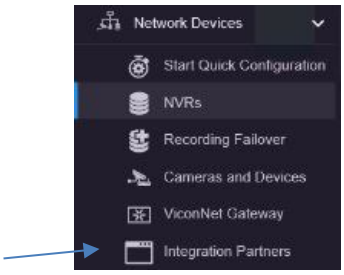


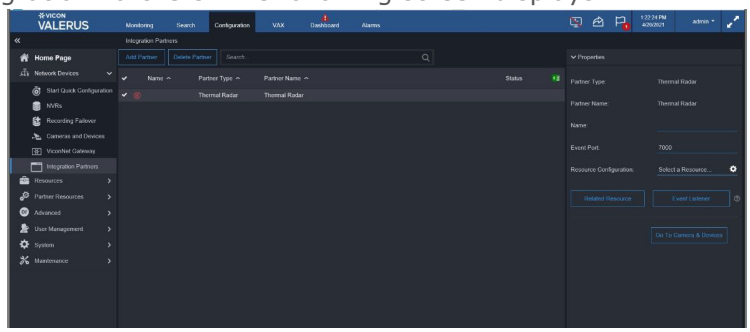
- Once the Gateway installation and configuration are completed, it will show in the Valerus system as if all the cameras are on one virtual encoder and all the Resources coming through the Gateway will be populated. All Resources coming through the Gateway in the Resources list and relevant parameters can be set.
- Remember that when using the Gateway, all the recording still takes place on the ViconNet system, so in Valerus these channels will not be configurable for streams and recording. Masking, if needed, will need to be defined in Valerus for the channels even if they have masking in ViconNet.

Integration Partners

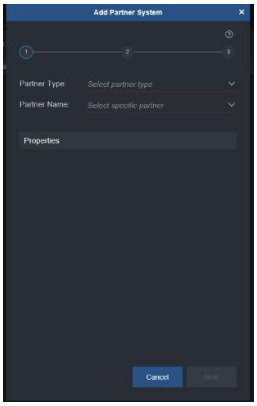
Valerus allows integration with different 3rd party partner applications. Currently available partners are Thermal Radar, Neural Labs LPR, Vicon LPR solution and VAX Access Control. Refer to the User Guides for VAX Access Control, Vicon LPR and Neural Labs LPR for details.

- Under Network Devices, select Integration Partners. The following screen displays.

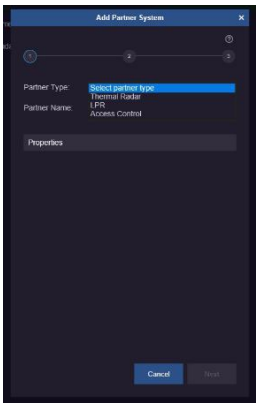




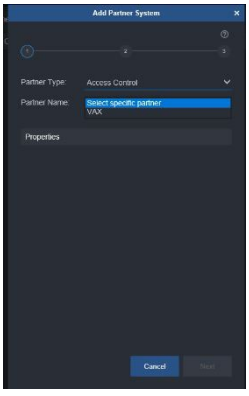
- Select New to add in a new partner. The following screen displays.

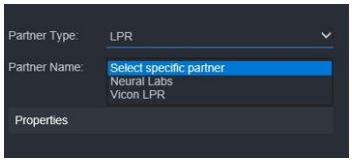


- From the Partner type, select Thermal Radar, LPR, Vicon LPR or Access Control. Note that this list will be continually updated.

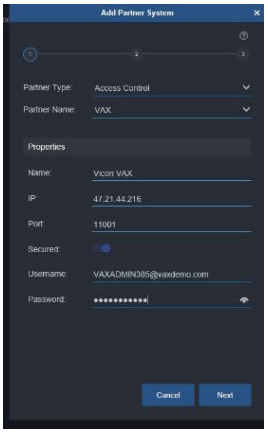


- From Partner Name, depending on what Partner type was selected, select Thermal Radar, Neural LPR, Vicon LPR or VAX, respectively. Note that this list will be continually updated. Enter all the information in the Properties fields. Select Next.

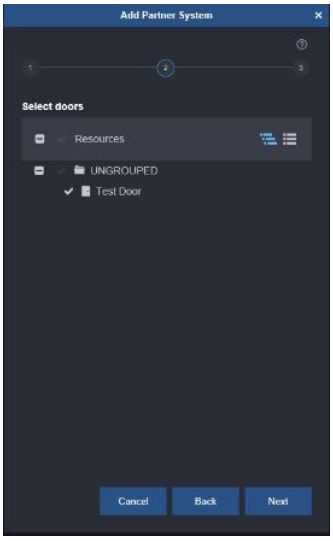


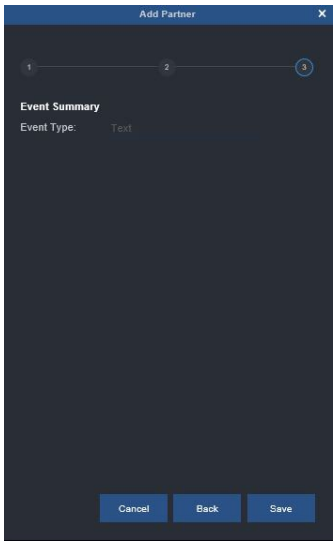


- Complete the Properties section of the Add Partner form. The User and Password are the default settings for the device; change them if this device is using different ones. Click Next.

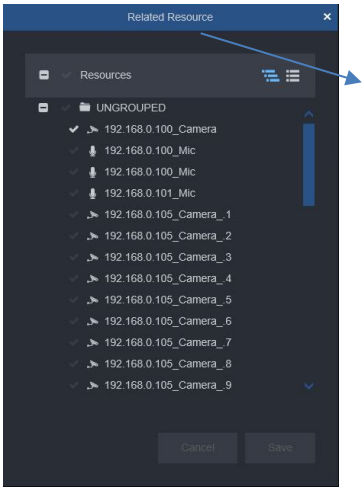


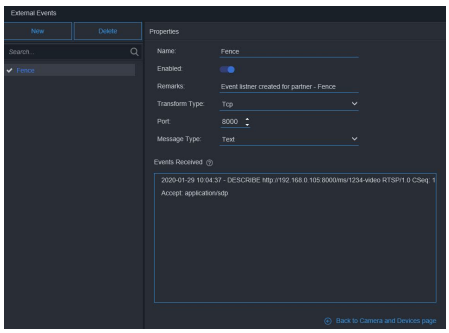
- From the Resources screen, select a resource (this screen will change depending on the partner selected). Note that for VAX integration, any Digital Inputs and Relay Outputs created in VAX are automatically added in Valerus to be configured as any other of those Resources. Click Next to setup the Event Summary. Click Save.



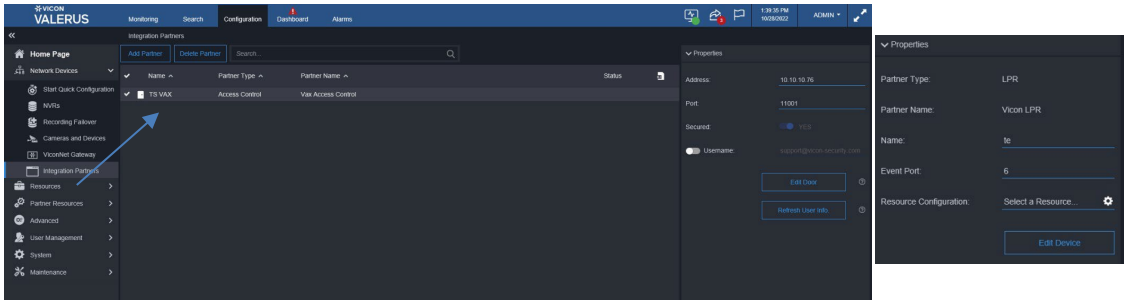


- The Event Listener, for Thermal Radar, will take you to the External Events screen to enable capturing events. Refer to the External Events section for details.





- Once completed, the Partner will be added to the Integration Partner list and will be in the Resources list.

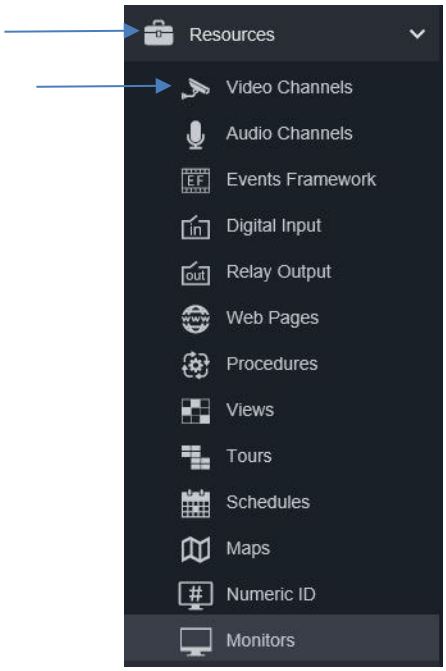


- Buttons are provided to Edit Door (VAX)/Edit Devices (LPR) information; a button is provided to Refresh User info for the cardholder picture, once it is updated in VAX.

Resources

After the system has been built with all the physical devices connected in the Network Devices area, the resources can now be configured. All the system resources are organized by type under the ***Resources*** section.

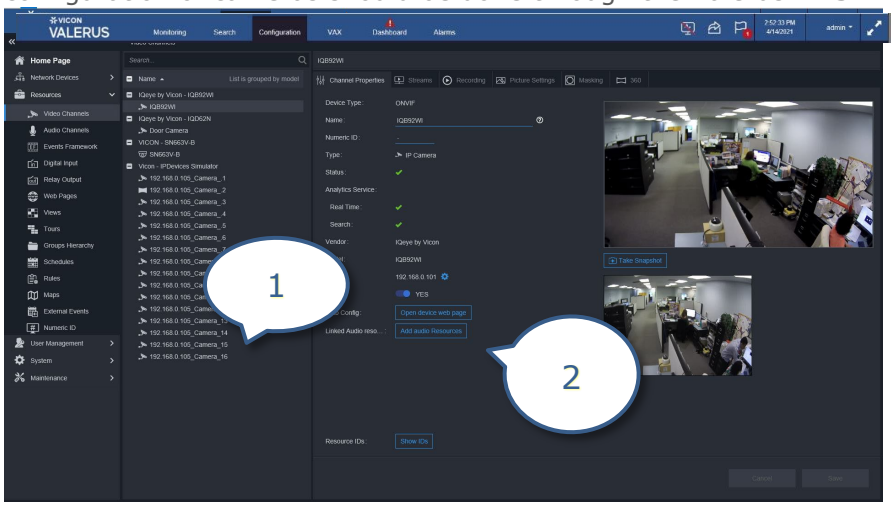
This includes Video Channels, Audio Channels, Events Framework, Digital Input, Relay Output, Web Pages, Procedures, Views, Tours, Schedules, Maps and Numeric ID. These are all described in detail below.



Video Channels

This category refers to the video ability of the cameras and devices previously added to the system. These channels are grouped by their model, which allows groups of video channels to be configured for common settings in one action. The settings available depend upon the specific camera/device model being configured.

Note: All configuration of cameras should be done through the Valerus VMS.

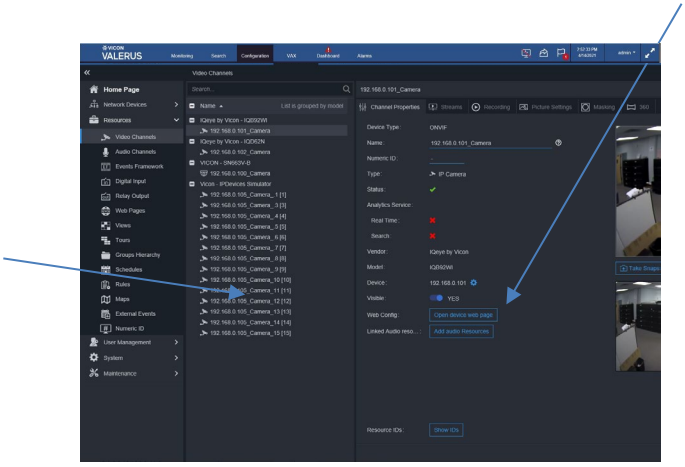


1. List of video channels grouped by model
2. Camera settings; choices vary by specific model

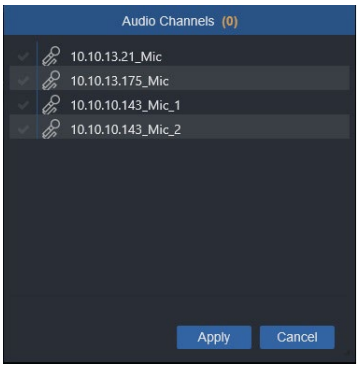
Channel Properties

- Select a channel from the list. The Channel Properties displays, including the protocol, name of the camera/device and the type of camera/device it is. You will also see the vendor and exact model name and the camera/device's IP address. If the camera is being analyzed by SmartAnalytics, it will be indicated with a green check (enabled) or red x (not available). A Numeric ID can be added in the field here.
- If the Show Player button is activated (Yes), the live video will display in place of the camera icon. Additionally, there is a Snapshot view. This can serve as a visual identification of the camera as a reference. Clicking Take Snapshot will open a popup asking if the system should take a snapshot of just the selected camera or all resources; selecting All Resources is helpful in systems with many resources and a snapshot is wanted for all of them. Take Snapshot will show a snapshot of the current live video; this can then be compared to Live view to confirm any camera setting changes.

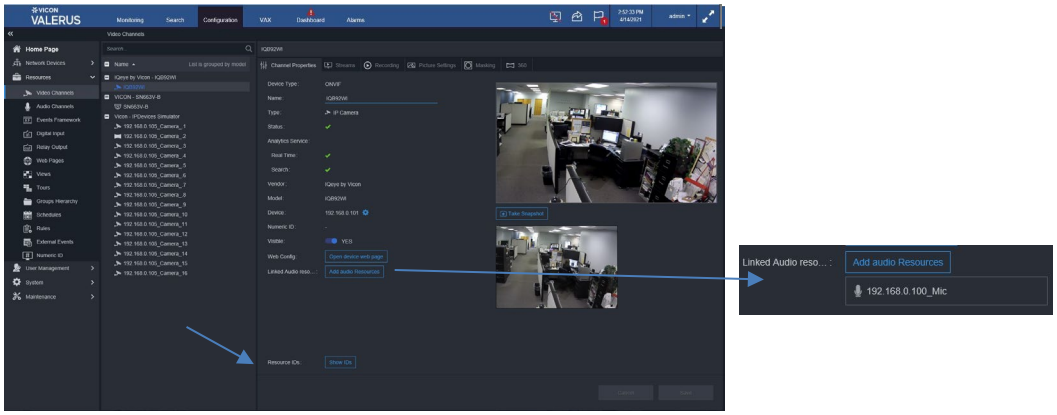
- The video channel name field will show by default its IP address and type. The name can be edited here and will be used on all lists. In the case of using a multiple channel device, such as an encoder, a number in square brackets is automatically added to the name so the physical input number will still be identified; be sure not to use square brackets at the end when naming devices, as they will be automatically removed. Next to Device there is a settings icon; clicking the icon will link to the NVR screen.



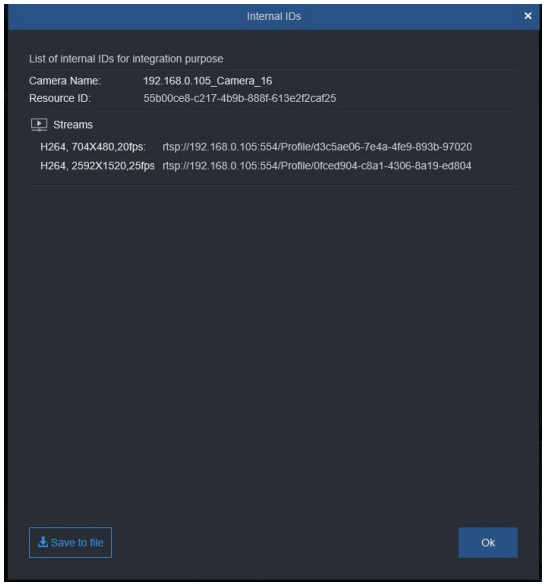
- By default the video channel is set to appear in the Resource list on the monitoring screen. If you would prefer that it not appear in the list, for example if it is viewing a covert location and the channel should not be seen, make sure Visible is set to No by clicking the button.
- A link to "Open device web page" is provided to the device web interface to review the specific features of the camera or if certain features need to be configured and are not configurable by the VMS. Otherwise, all configuration should be done through the VMS.
- The video of this camera/device can be linked to audio resources (up to 2 audio channels per video channel) so that they will be grouped for use. Click the Add audio Resources; select the microphone to be linked from the popup list. When this is done, the cameras icon on the Resource list will show it has linked audio. Live and playback will automatically include video and audio; this is convenient in certain types of situations, for example in an interrogation room so the interview can be both seen and heard together without having to start the video and audio separately.



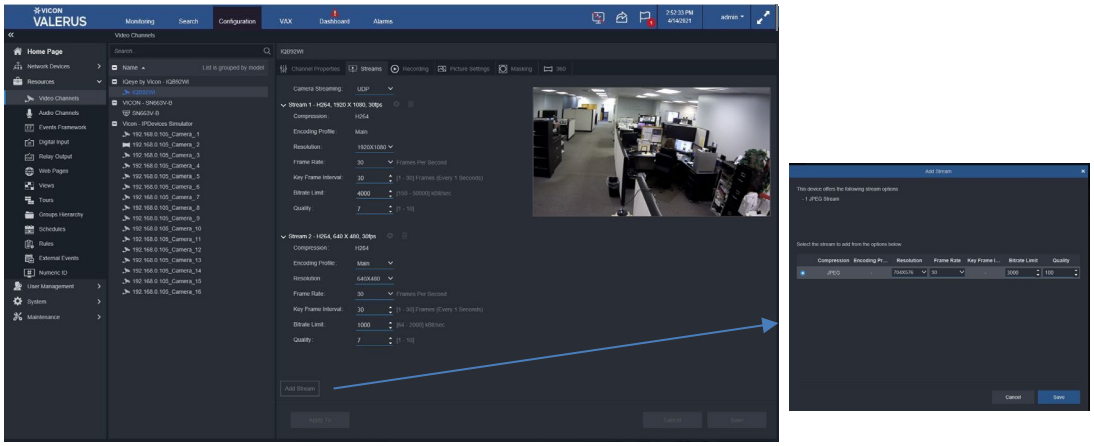
- Click Apply. Click Cancel to close without saving these settings. A list of the linked audio devices will display below the Add audio resources button.



- For Resource IDs, selecting Show ID allows you to save a text file with information about that camera that can be useful when working with integrated parties that need this information.

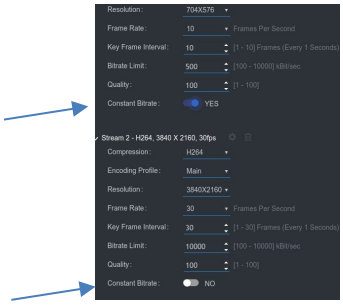


Streams



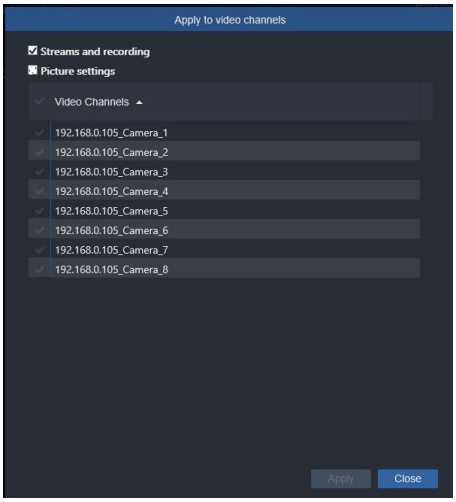
- Many cameras/devices offer multiple video streams. The stream tab allows configuration of up to two streams per camera, with an option to add a stream if the camera has that capability; click the Add Stream button. These streams will be used to set up recording and used by the Monitoring screen.
- Protocol, Compression, BitRate, Frame Rates, etc. are all defined here. The VMS default settings, enforced by default once the device is added to the system, are:
    - One Stream – top resolution supported by the camera/device and maximum frame rate; Second Stream – VGA (D1) resolution and maximum fps available. Clicking on the stream collapses the fields.

Each of these settings can be changed; the list of available options is based on the specific device capabilities (the camera tells the VMS what it can support). Some cameras have the option to select Constant Bitrate on or off. Click to enable. Note that either H.264 or H.265 must be selected for any given camera; compressions cannot be mixed and have different streams of the same camera use a different compression.



Note: If Generic RTSP has been chosen as the protocol for the device, these stream parameters are set in the unit. However, it is still important to select the same parameters on this screen as those set in the device, as Valerus uses these settings when it determines which stream to display (Monitoring).

- Saving the need to make the same settings to multiple cameras/device s of the same type, these settings can be applied to a group of cameras/devices of the same model. At the bottom of the screen there is an Apply To button. Clicking it opens a popup that will allow you to assign these same settings to other cameras/devices of the same model in the system. Select the camera/device(s) from the list. Multiple selection is supported by checking the box next to the camera or by using the Ctrl and Shift keys and clicking the channels; all cameras/devices can be selected by clicking the check box in the gray title bar. Click Apply and then Close.

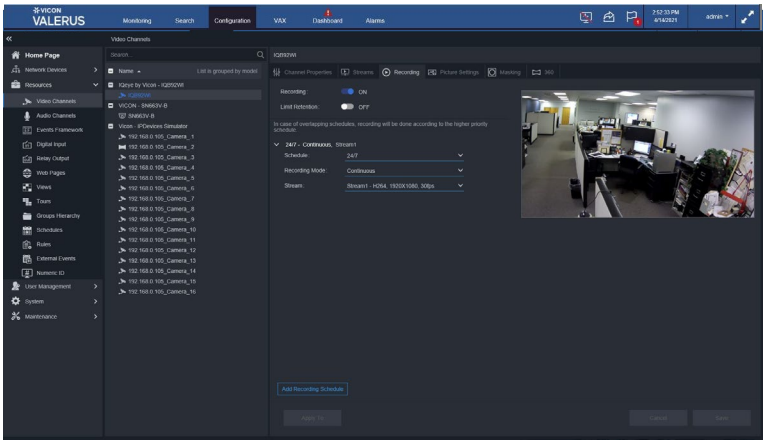


- Click Save or Cancel to close without saving these settings.

Tip: Typically, there is a certain similarity between camera type (indoor, outdoor, PTZ, etc.), which allows sharing the same settings with the cameras of the same type. For a quick configuration, select one channel representing the group, configure it and then apply these settings to all similar devices.

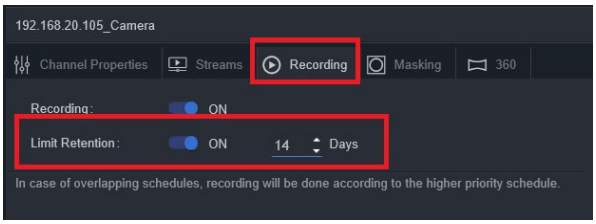
Recording

- Each device can be set to record video. Recording of video is turned On by default when the device is added to a recording server; click the button to toggle recording On/Off. Remember that for any type of recording, it is essential that enough recording space is available in order to get the expected results.



- The default setting (OFF) for the NVR retention is based on a FIFO (first in first out) algorithm and will use the allocated storage to its full size and then overwrite the oldest files to maintain the maximum number of days on the drive.
- Where limiting the number of days for retention is required, either as means to better utilize the available storage or where legally there is a limit on the number of days allowed to be stored, click the Limit Retention button to On to select the maximum number of days to hold recorded video in storage before it will be overwritten. The storage algorithm will use as much storage as needed to get the defined number of days and may not use the entire allocated space.
- For example, if there is space allowing 14 days of storage, but the channels have been set to a maximum of 7 days, only about half the storage will be utilized. In a case where the retention limit number of days is increased (example, from 7 to 10 days), the system will utilize the available storage and immediately record additional days; however, in a case where the retention limit has been set after the system has been running in full FIFO for a while, it will adjust the storage over a certain period of time until it stabilizes on the required number of days. This may take some time (even up to a week) based on the number of channels, data rate and reduction of days.

Note: When setting a recording limit after the system has been recording for a while, it is important to verify that the system does not have more recording days than the expected retention. For example, if the expected retention is 30 days, make sure that the system has not recorded more than 30 days already. In the case where the system has extra recording days, those will need to be properly purged; consult Vicon Technical Support for instruction on how to do this correctly.

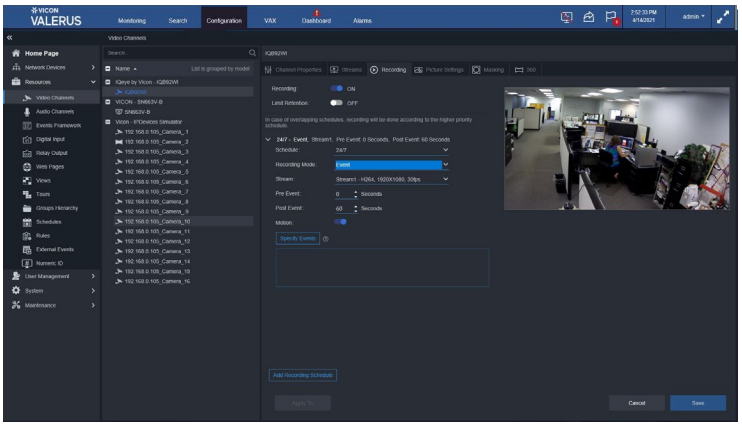


- Select a schedule for recording from the dropdown list. The default setting is 24/7. Any schedules that have been previously configured will be listed here as well. As a convenience, selecting new schedule opens the Schedule settings screen and another schedule can be created directly from here.
- If additional recording schedules are required, for example one for weekdays and one for weekends, click the plus symbol to open another schedule. Note that if 24/7 is selected as the first schedule, no other schedule is necessary, as the camera will be recording all the time. If a

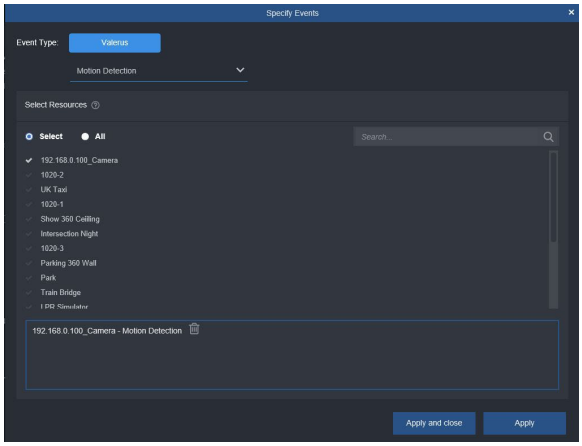
second events-based schedule is created (i.e., weekends) that overlaps with a 24/7 schedule, the event schedule has priority; an event is considered to have priority over ongoing recording. Therefore, in the example, there will only be recording on the weekend if the event occurs, even though 24/7 was selected for the first schedule.

Tip: When designing the system, understand the expected recording at different times and create your schedule accordingly.

- Select a recording mode from the dropdown list, Continuous, Event or Continuous & Event (if the camera has more than one stream). The sub-menu will change according to the selection.
- If Event is selected, both pre and post event recording can be set for a specific number of seconds. When the event occurs, video will be recorded for a preset time of up to 30 seconds per channel before (pre; event saved in memory until it needs to be saved on the drive) and after (post) the event, resulting in a video segment that shows exactly what happened just before and after the event.
- If Continuous & Event is selected, there is no need for pre-event recording, as the event is already recording continuously; the event will be recorded from a secondary stream, which is specified here.



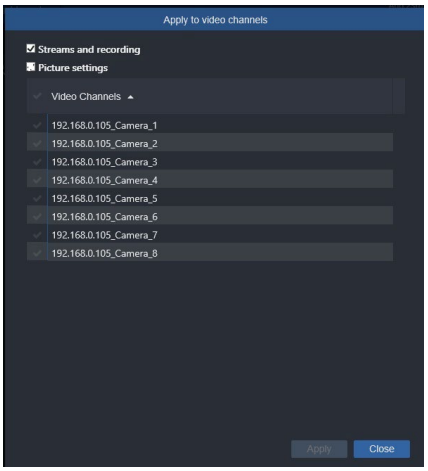
- Event Recording is enabled for motion on the specific camera being configured by default, as this is the most common event; it can be disabled by clicking the button. Recording upon other events can also be configured. *Note that external events are not supported for recording rules at this time.*
- Click Specify events to determine what events across the system will be included in this channel's event for recording. Select the event type from the Valerus dropdown list on top: Motion Detection, Digital Input, Tamper, Audio Level Detection, Camera Connection Lost, Relay, Native Camera Analytics, Thermal Camera Events and Recording Problem are options included currently and will be relevant depending on the system and its capabilities (for example, native camera analytics is not available on all cameras). With the Selected radio button checked, select the cameras from the list to associate with this event. Selecting the Any radio button on the Specify event screen means that if this event type occurs on any device in the list, it will trigger event recording on the video channel being configured. Multiple event types can be selected and will display in the box at the bottom. When all the events have been selected, click Apply or Apply and close; click Close to shut the popup without making any changes. All of the events will be listed under Specify events.



Important Note: There is a question mark symbol next to Specify events that will explain the logic of your choices. When specifying more than one event to trigger recording, the recording will start if an event is reported by ANY of the sources specified. Recording events is working as a logical *OR* between multiple events. The same applies if the Any event option is selected.

Tip: This method allows selecting, for every video channel, which events from which cameras are considered a trigger. It allows for a very specific configuration.

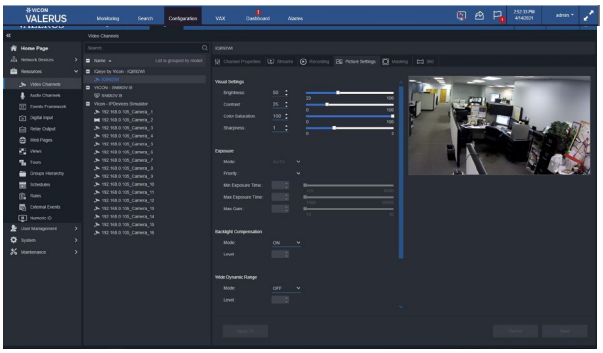
- Select which camera stream will record at which time, based on your former selection.
- To collapse the schedule display list, when there are many schedules, click the arrow head.
- Saving the need to make the same settings to multiple cameras/devices of the same type, these settings can be applied to a group of cameras/devices of the same model. At the bottom of the screen there is an Apply To button. Clicking it opens a popup that will allow you to assign these same settings to other cameras/devices of the same model in the system. Select the camera/device(s) from the list. Multiple selection is supported by checking the box next to the camera or by using the Ctrl and Shift keys and clicking the channels; all cameras/devices can be selected by clicking the check box in the gray title bar. Click Apply and then Close.



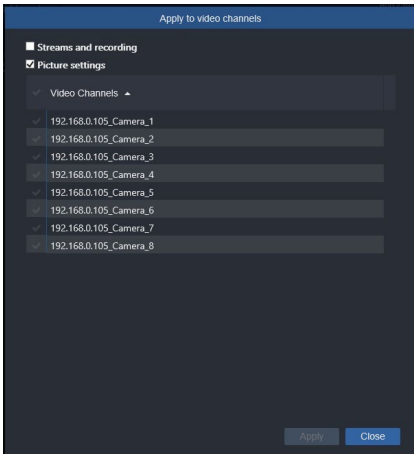
- Click Save or Cancel to close without saving these settings.

Picture Settings

- The Picture Settings screen provides adjustments for Visual Settings (brightness, contrast, saturation, etc.), Focus, Exposure and other camera features. The settings offered are camera dependent and will vary between models and cameras with different settings.



- Saving the need to make the same settings to multiple cameras/devices of the same type, these settings can be applied to a group of cameras/devices of the same model. At the bottom of the screen there is an Apply To button. Clicking it opens a popup that will allow you to assign these same settings to other cameras/devices of the same model in the system. Select the camera/device(s) from the list. Multiple selection is supported by checking the box next to the camera or by using the Ctrl and Shift keys and clicking the channels; all cameras/devices can be selected by clicking the check box in the gray title bar. Click Apply and then Close.

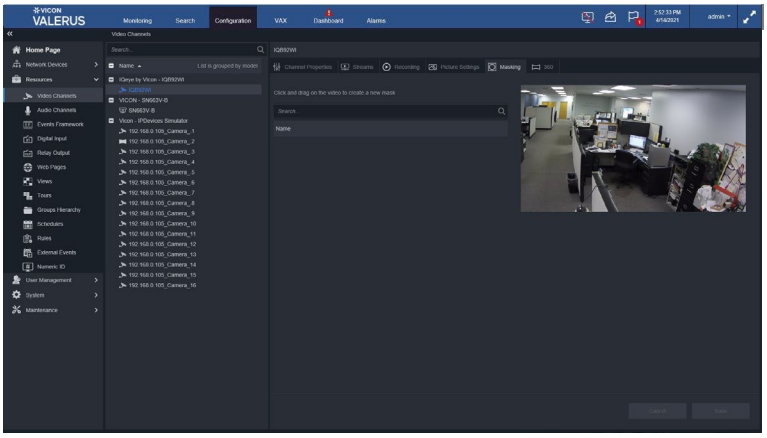


- Click Save or Cancel to close without saving these settings.

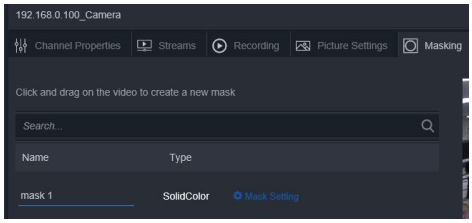
Privacy Masks

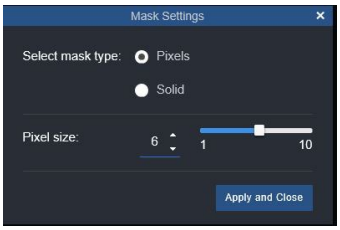
In cases where it is necessary to protect sensitive areas of the video from being seen, they can be pixelated so that only a vague outline is visible without any detail. This mask is created in the VMS, which is different from doing it in the camera, and allows unmasking of video if needed.

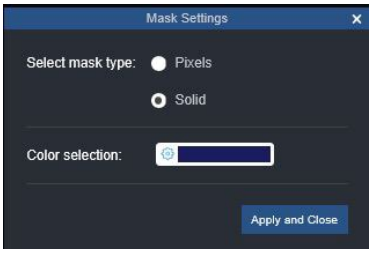
- Click on the Masking tab to create privacy masks on the video. The number of masks created appears in parenthesis.



- Using the mouse cursor, draw the mask in the location it is needed. The mask location and size can be modified; place the cursor inside the mask and move it or place the cursor on the borders or corners to change the size (cursor changes to arrows).
- Once the mask is configured, a default name of mask populates the field; a custom name can be entered in its place if needed.
- Click Mask Settings to open a popup to customize the type of mask, pixelated or solid. The sliding scale of pixel size affects how blurry the mask will be. If solid is selected, a color palette will open providing an array of color choices for the mask. When finished, click Apply and Close.

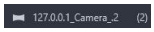


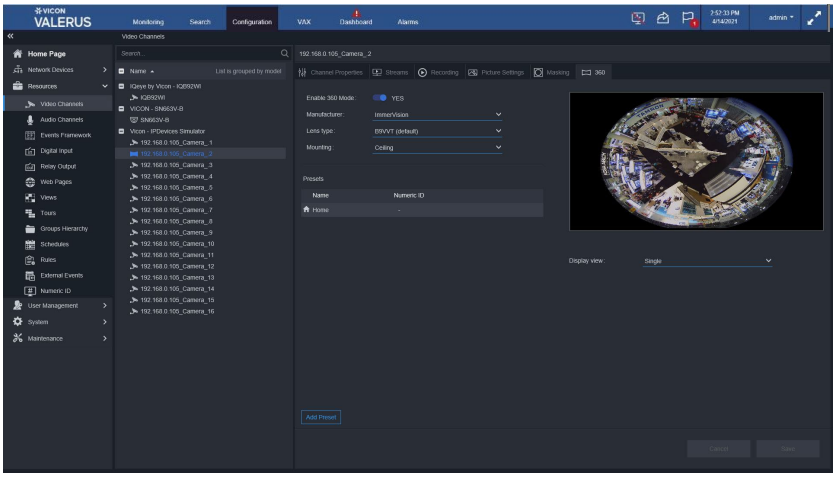




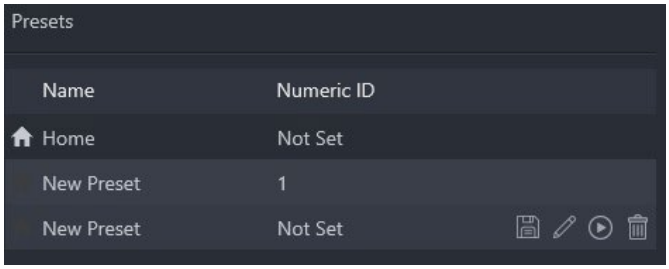
- To create another mask, click the plus sign.
- If more than one mask is created, the active mask is outlined in red. A mask can be removed by clicking the x in the right corner.

360

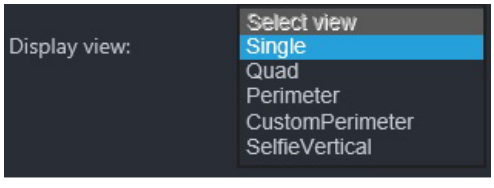
Valerus supports setting up hemispheric (panoramic) cameras with a fisheye lens. This 360 feature will display for all cameras; since this feature is based on the lens type, not the camera, the VMS cannot know the lens on the camera. However, it will only allow configuration to an appropriate camera/lens. Note that a 360 camera has a distinctive icon in the Resources list  .



- Cameras with fisheye (360°) can be configured from the 360 tab.
- Click the Enable 360 Mode button to configure the camera.
- Select the manufacturer of the lens from the dropdown list. Currently Immervision lens type is supported. Note that selecting the wrong lens may result in video not displaying at all.
- Select the lens type from the dropdown list. By default it is compatible with Vicon (B9VVT).
- Select the mounting method of the camera. This setting does impact on some of the views available. Refer to the camera manual for details.
- Preset positions enable users to pre-define and save camera information to create specific views that can be called up for display, similar to a PTZ camera. These are often used when it is necessary for an operator to go from one frequently viewed position to the next very quickly.



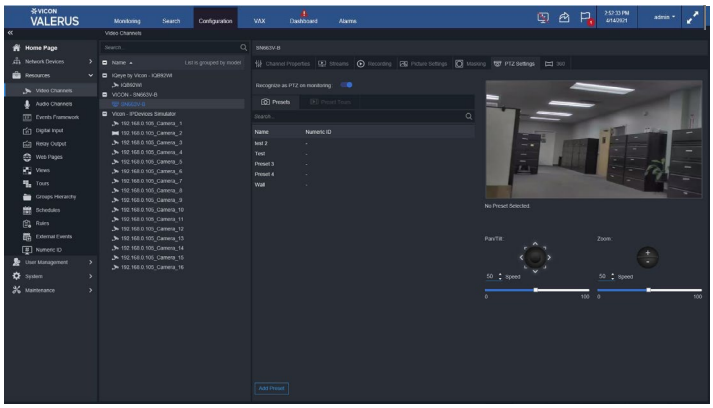
- Presets can be set for the panoramic camera/lens. Click the Add Preset button to add a preset. Move the camera to the position you want to save as a preset. Icons will display to Save the preset, Edit the preset name, Go to the preset and Delete the preset. These presets will then be available from the Live view in the Monitoring screen. If using a keypad/PLC, be sure to set a Numeric ID here.
- The camera offers a number of built-in preset display views. Select the Display view from the dropdown list, Single, Quad, Perimeter, CustomPerimeter or SelfieVertical. The selection will be reflected in the video displaying on the page.



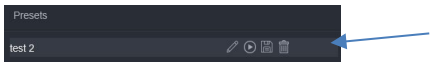
PTZ Settings

When a PTZ camera is added to the system, the PTZ tab is enabled automatically.

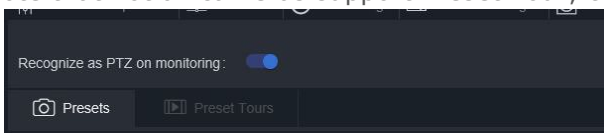
- The Recognize as PTZ on monitoring is enabled by default. This can be disabled as needed.
- Presets can be configured from the PTZ Settings tab. This is only available for PTZ cameras.



- Preset positions enable users to pre-define and save camera information to create specific views that can be called up for display. These are often used when it is necessary for an operator to go from one frequently viewed position to the next very quickly.
- To store a preset, click the Add Preset button. A default preset name will be added to the Presets list. Using the Pan/Tilt and Zoom controls (buttons in Configuration or on the video in Monitoring), move the camera to the position and zoom you want to save as a preset position. Click the save icon (floppy disk icon). Use the arrow button to move the camera to the preset and the pencil icon to edit the preset parameters. A garbage pail is provided to delete this preset.

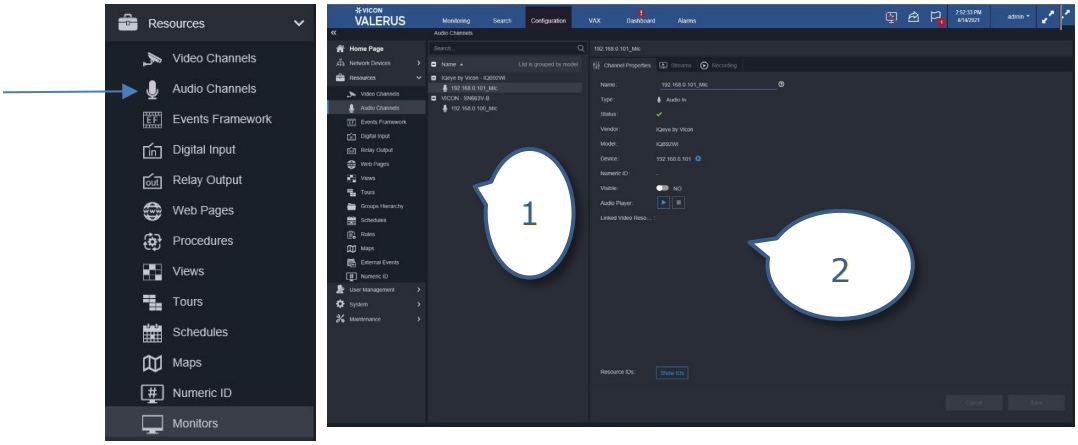


- Preset Tours can be created from previously created presets. A series of presets can be combined into one tour. This tour can then be selected and viewed from the Live video in Monitoring. Note that not all cameras support Preset Tour; the tab will remain grayed out.



Audio Channels

This category includes the microphones in the system connected through IP cameras and devices. Similar to video channels, the microphones are sorted by model type, which allows groups of microphones to be configured for common settings. The microphone should be configured through the VMS, but in some cameras and devices, these have to be enabled in the device web interface first.



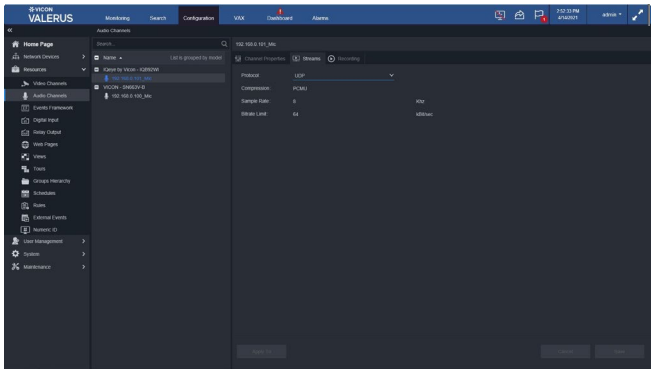
1. List of microphones grouped by microphone type
2. Microphone settings; choices vary by specific microphone

Channel Properties

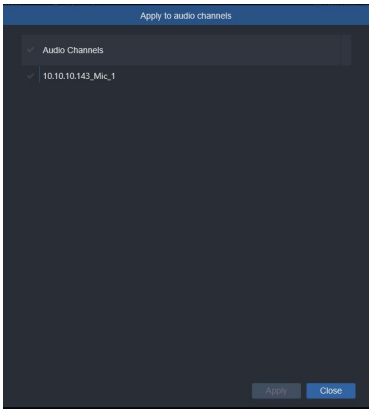
- Select a microphone from the list. The Channel Properties displays, including the type of microphone and its vendor and exact model. The IP address of the device handling this microphone is displayed and a green check appears in status if the system recognizes it. A Numeric ID can be added in the field here.
- Click the Visible button to Yes for this microphone to appear in the Resources list on the Monitoring screen. By default audio channels are set to be not visible.
- To preview the audio, press the play icon on Audio Player.
- If the audio from this camera has been linked to video from the Video Channel screen, it will display here; refer to video channel audio linking for details.
- Save changes or click Cancel to close without saving.
- For Resource IDs, selecting Show ID allows you to save a text file with information about that camera that can be useful when working with integrated parties that need this information.

Stream Settings

- Protocol, Compression, Sample Rate and Bitrate Limit are all defined here.
- The parameters that can be configured are determined by the specific microphone. In certain cases, the parameters are set and cannot be changed. If a parameter can be changed, a field box with a dropdown displays.



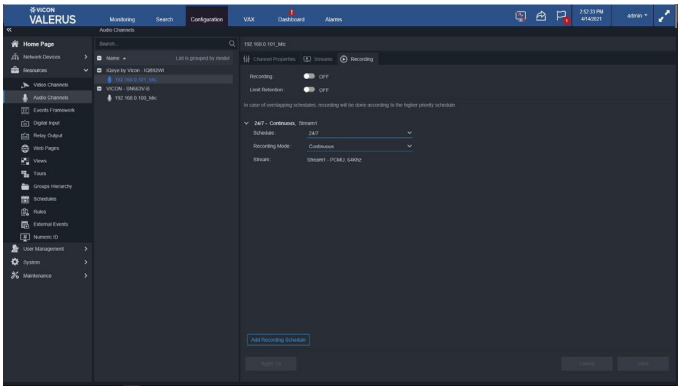
- To avoid having to make the same settings to multiple microphones of the same type, these settings can be applied to a group of microphones. At the bottom of the screen is an Apply To button. Clicking it opens a popup that will allow you to assign these same settings to other microphones in the system; the system recognizes which settings can be adjusted for multiple microphones and will only list those cameras. Select the microphone(s) from the list; all microphones can be selected by clicking the arrow in the gray title bar. Click Apply and then Close.



- Click Save or Cancel to close without saving these settings.

Recording

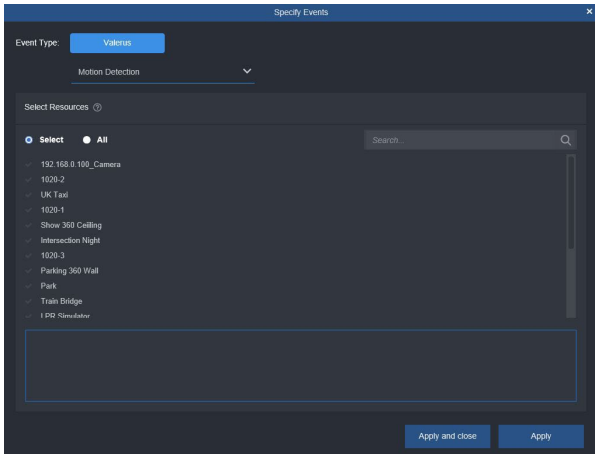
- Each device can be set to record audio. Unlike video, audio recording is turned Off by default. To record audio use the button to toggle recording to On.



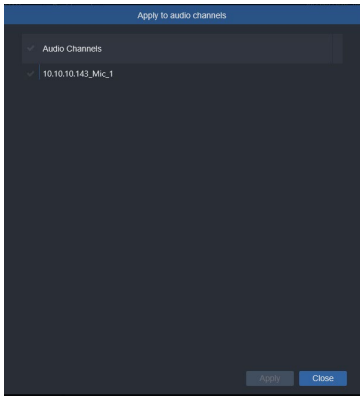
- Click the Limit Retention button to On to select the maximum number of days to hold recorded audio in storage before it will be overwritten (even if there is still free space on the drive). If this is turned Off (default), recording will continue until the storage is filled and then be overwritten according to FIFO. Refer to the Video Recording section for details on limit retention.
- To create a schedule for recording, click the Add Recording Schedule button and select a schedule from the dropdown list. Recording 24/7 and any schedules that have been previously configured will be listed here. Additionally, selecting new schedule opens the Schedule settings screen and another schedule can be created directly from here.
- If additional recording schedules are required, for example one for weekdays and one for weekends, click the Add Recording Schedule button to open another schedule. Note that if 24/7 is selected as the first schedule, no other schedule is necessary, as the camera will be recording all the time. If a second event based schedule is created (i.e., weekends) that overlaps with a 24/7 schedule, the event schedule has priority; an event is considered to have priority over ongoing recording. Therefore, in the example, there will be no recording on the weekend except if the event occurs, even though 24/7 was selected for the first schedule.

Tip: When designing the system, understand the expected recording at different times and create your schedule accordingly.

- Select a recording mode from the dropdown list, Event or Continuous. The sub-menu will change according to the selection.
- If Event is selected, both pre and post event recording can be set for a specific number of seconds. When the event occurs, audio will be recorded for a preset time of up to 30 seconds per channel before (pre; event saved in memory until it needs to be saved on the drive) and after (post) the event, resulting in an audio segment that shows exactly what happened just before and after the event. Select Specify Events to select the Event Type. Select the event from the dropdown list. Click Apply and close to finish or Apply to make more selections.



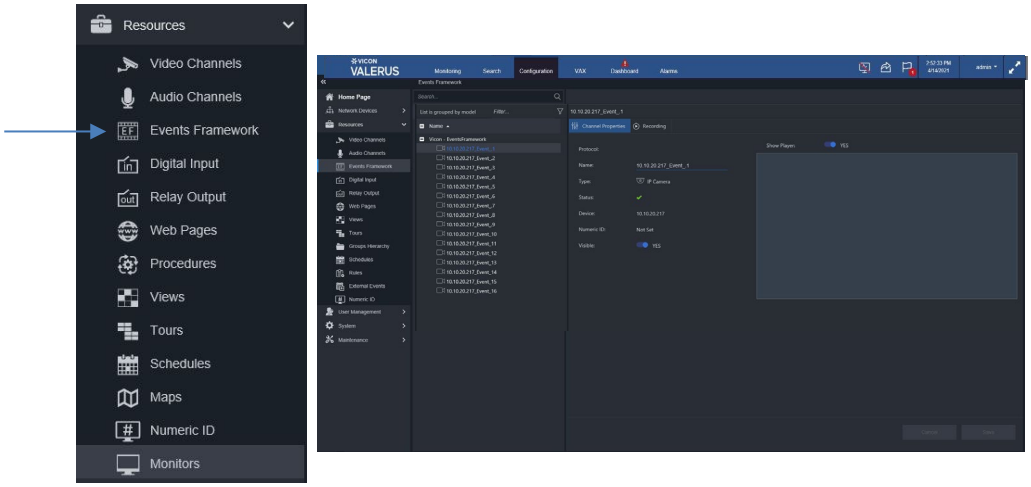
- To avoid having to make the same settings to multiple microphones of the same type, these settings can be applied to a group of microphones. At the bottom of the screen is an Apply To button. Clicking it opens a popup that will allow you to assign these same settings to other microphones in the system; the system recognizes which settings can be adjusted for multiple microphones and will only list those cameras. Select the microphone(s) from the list; all microphones can be selected by clicking the arrow in the gray title bar. Click Apply and then Close.



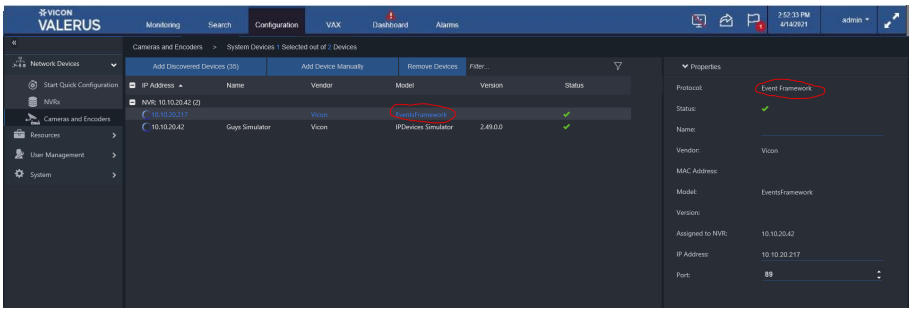
- Save changes or click Cancel to close without saving.

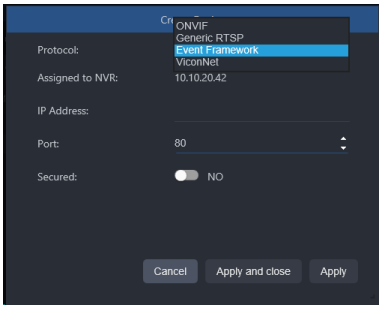
Events Framework

The Valerus Events Framework is an add-on to Valerus that allows it to integrate with external partners' systems. After the VEF device has been added in the Cameras and Devices, it will be listed in the Resources section of Configuration and available for view in the Monitoring screen.



- The VEF Streaming Engine is added manually in the Cameras and Devices Configuration screen. Click Add Device Manually and select Events Framework.

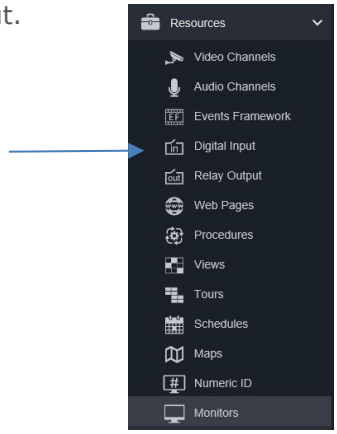


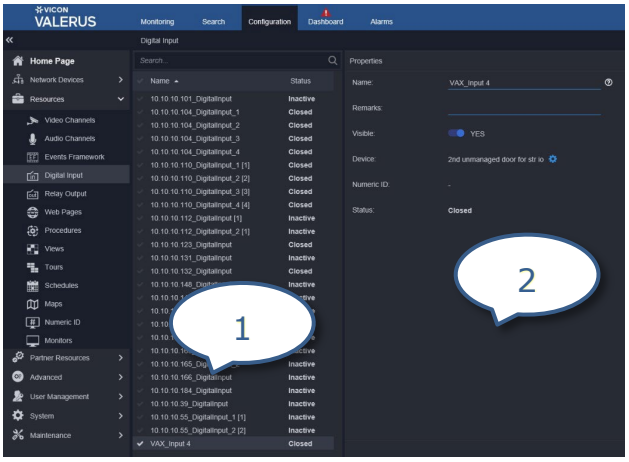


- Once added, the VEF device will be listed as any other device and will show in the Resources section of Configuration; it is not enabled or recorded by default but can be made visible and available for view in the Monitoring screen by clicking Visible to yes.

Digital Input

This category includes the alarms inputs (sensors) for devices on the system. The status column is dynamic, as the inputs may change from Closed to Open. These can be used in Rules setup. When integrated with VAX, any digital inputs created in VAX are automatically added into Valerus and Rules can be setup to react to VAX inputs just as any other input.





1. List of digital inputs available
2. Input properties

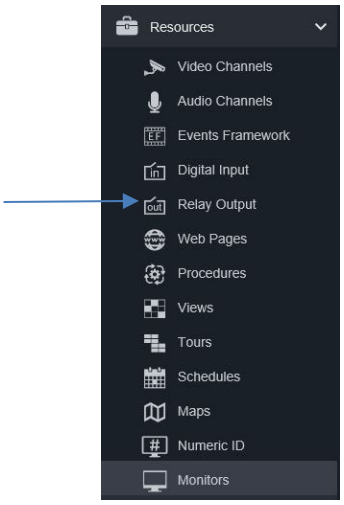
Properties

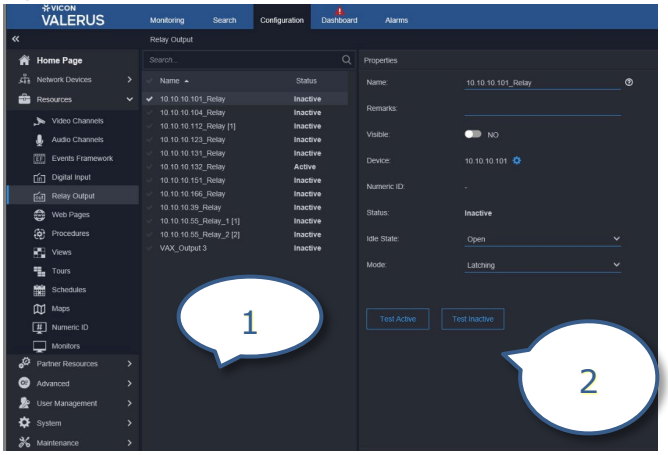
- Click on Digital Inputs to open the Properties screen for a list of available digital inputs. Select the input you want to configure.
- Give the input a name if needed and add any description to help identify it. A Numeric ID can be added in the field here.
- Enable the input to allow communication with it as well as appear in the Resources list on the Monitoring screen. By default the digital input (DI) is not visible on the Monitoring screen in the Resources list.
- The Device field is the IP address of the device handling this DI. There is a Device Configuration link next to this that will take you back to the Device screen.

- The current status of the input is displayed, open or closed.
- Save changes or click Cancel to close without saving.

Relay Output

Relay outputs can be configured. The status column is dynamic, as the outputs change from Inactive to Active (green). These can be used in Rules setup and can be controlled manually from the Resources list on the Monitoring screen. When integrated with VAX, VAX Relay Outputs are automatically added into Valerus and can be configured in the same way as any other output.





1. List of relay outputs available
2. Output properties

Tip: Although the term relay is being used, the actual output may be a TTL or a digital output. Be sure to check the specification for the device to use it correctly.

Properties

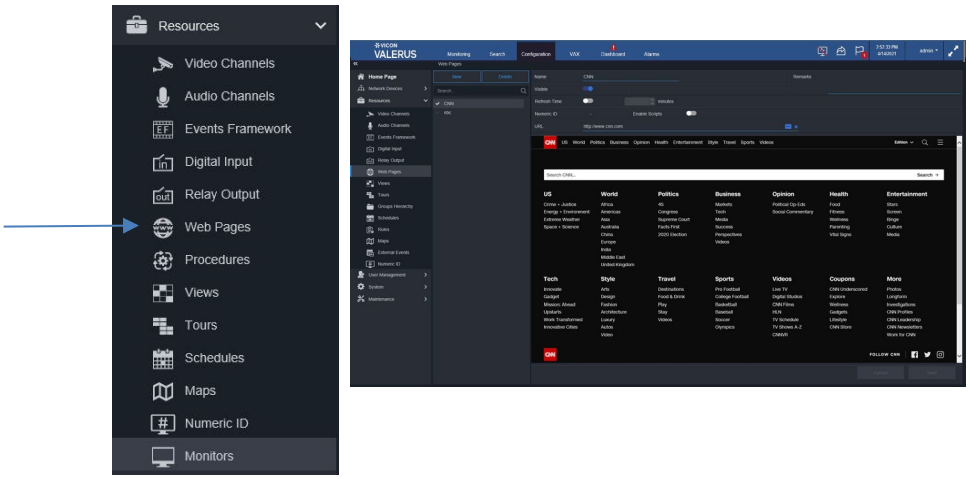
- Click on Relay Outputs to open the Properties screen for a list of available relay outputs. Select the relay output you want to configure.
- The output can be given a specific name and helpful identification details can be added in the Description field. A Numeric ID can be added in the field here.
- Click the Visible button to Yes for this output to appear in the Resources list on the Monitoring screen.

- The Device field is the IP address of the device handling this relay. There is a Device Configuration link next to this that will take you back to the Device screen.

- Select the Idle State (when contact is inactive) as Closed or Open and the Mode as Bistable (Momentary; maintains contact position as long as it is held) or Monostable (Latching; maintains contact position indefinitely).
- Save changes or click Cancel to close without saving.

Web Pages

If there are web pages that are used regularly, web links of their URLs can be saved for easy access. An example would be a news website the operator would like displayed or operating procedures that are saved in a web page format for easy access and display upon an event. Note that websites that do not allow opening in an I-Frame cannot be used in Valerus.



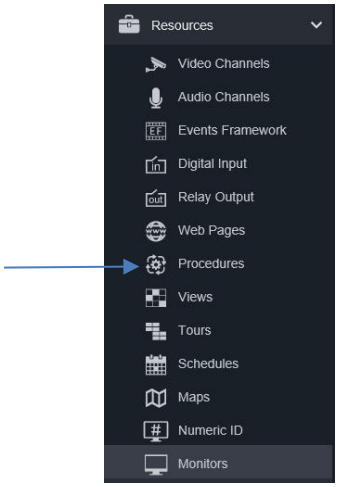
- From the Web Pages screen, click the New button.
- Enter the name of web page if needed, add any pertinent remarks and its URL in the appropriate fields. Once the URL is entered, click on the arrow on the right to browse to the exact page or click the Enter key. A Numeric ID can be added in the field here.
- The web page is Visible by default and will show on the Resources list on the Monitoring page; click the Visible button to remove it from the Resources list. It can be accessed directly from the Resources list and display in a tile in the same way as a device, instead of having to open a browser.
- Clicking the Refresh Time button allows setting the duration of time in minutes for the web site to be refreshed. This is meant to allow web pages that have changing content but do not refresh automatically to remain current.

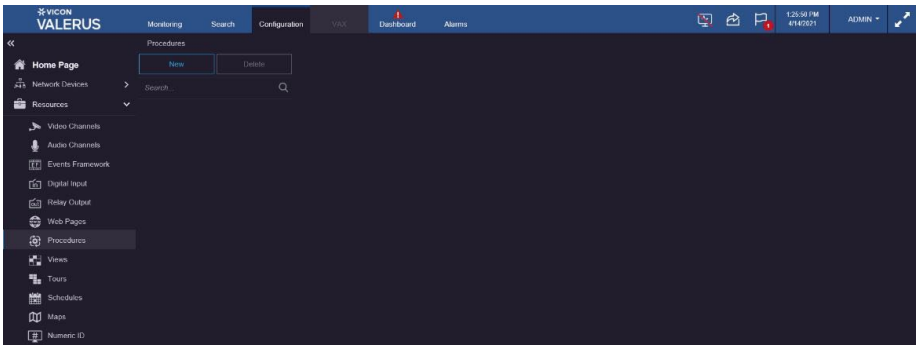
A user can create their own webpage to use in the system. This would be convenient for creating a procedure to follow in specific situations. The page would be readily available to access the procedure.

- Create the page in an html format, either using HTML tools or saving a Word document as HTML.
- Copy the page or folder with pages to the Application Server under C:\VII.HTMLDocs.
- When creating the web page, the URL to use will be http://xxx.xxx.xxx.xxx/htmldocs/PageName
  - xxx.xxx.xxx.xxx is the IP address of the Application Server computer.
  - PageName is the name of the web page created.

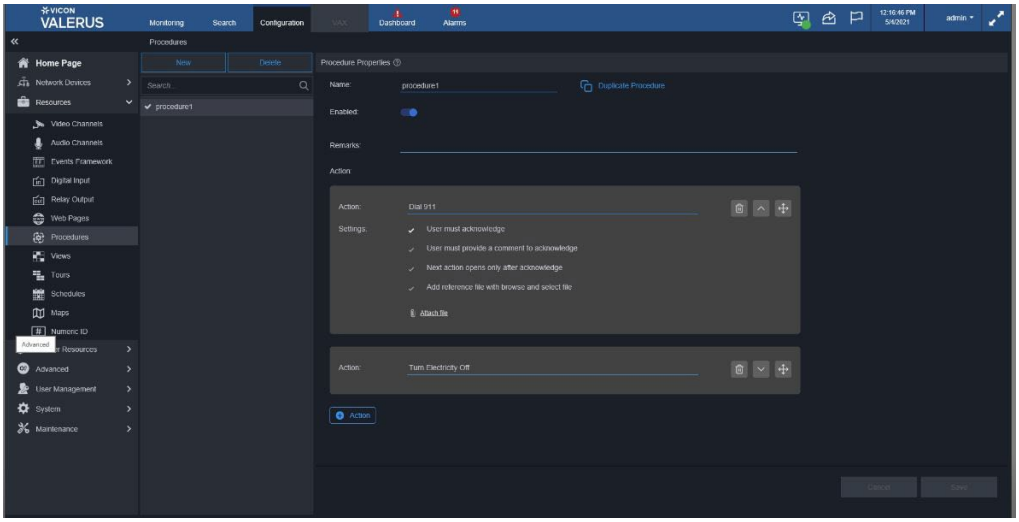
Procedures

Procedures are used for Alarms Management, in the Advanced Alarm section and on the Alarms tab. It is an optional tool used to set up a step-by-step protocol for what should happen when an alarm occurs. *Procedures must be created before defining the alarms so they can be selected and included in the alarm creation process*. ***Refer to the Alarms Management Guide for details on setup.***





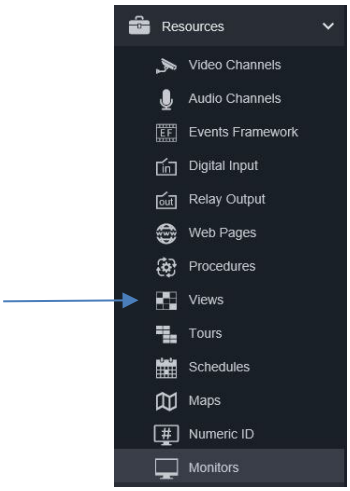
- Click Procedures to open the screen to configure a Procedure. Click New. The procedure editor screen displays. Enter the information for the following options.



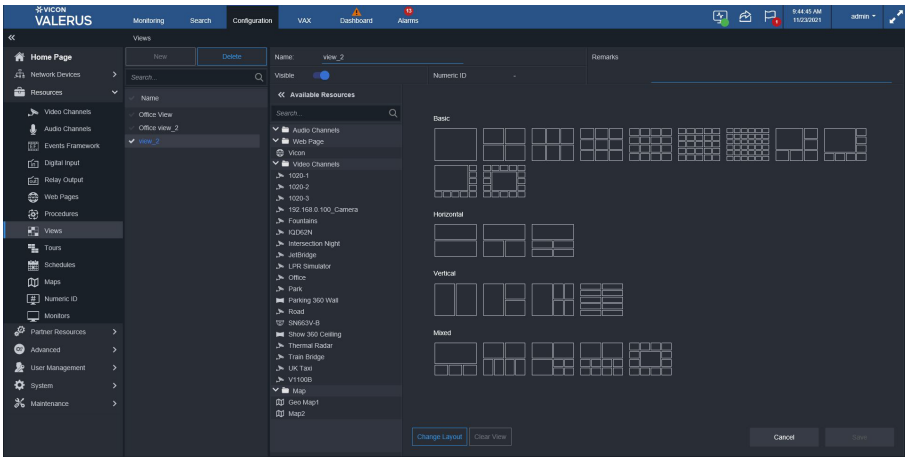
- Name: Assign a name to the procedure in the Name field.
- Duplicate procedure: If you want to base this new procedure on an existing one, select Duplicate procedure link and select the similar procedure to create a copy that can be modified and saved as a new one.
- Enable the procedure with the slide button.
- Remarks: Add in any Remarks that might help to describe or assist with this procedure (optional field).
- Actions: One empty action is displayed for a new procedure; for each action provide the details of the specific settings.
- On each action window, there is an option to delete it, collapse it and move it to change the order of actions by dragging them up or down.

Views

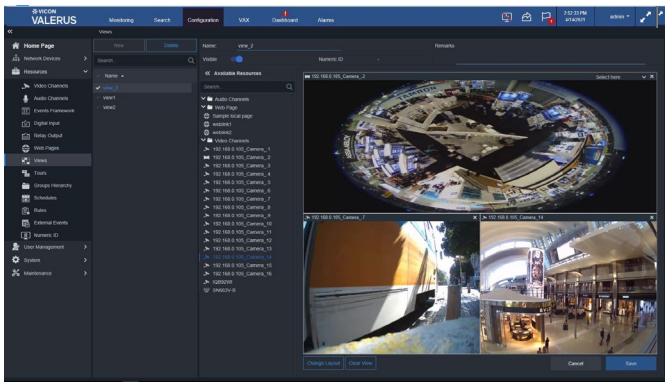
A specific layout and the data content within the view (i.e., video, audio and web pages) displayed on the Monitoring screen is called a view. Individual display layouts of specific resources can be created and saved as views. These can be visible in the Resources list. Dragging a View from the Resources list opens that view up in a new display tab, saving the need to open resources individually. A View can also be called on event (see Rules).



- Click Views to open the screen to configure new views. Click New button.
- The list of Available resources and layouts displays. Select a layout from the wide variety of choices that are provided, including up to a 36 device display and horizontal, vertical and mixed views. The Available Resources list can be expanded or collapsed by clicking on the arrow heads above the list.



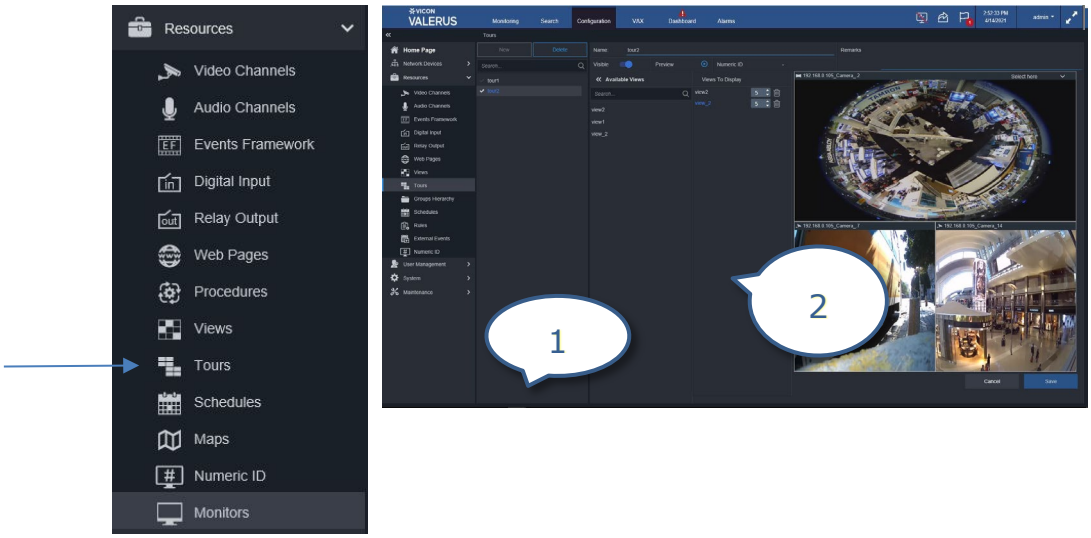
- From the Available Resources list, drag the device to display into each tile of the layout in the same way as on the Monitoring screen. Note that in the Configuration screen, a snapshot of the resource displays, not live video, so that if a webpage is in the view only the IP address will show here; this improves performance.



- Enter a name if needed for this specific view. A Numeric ID can be added in the field here.
- Views are visible by default. Clicking the Visible button determines if this view is on the Resources list on the Monitoring page. A Remarks field provides space for any notes or information on this view.
- A view can be deleted by clicking the garbage pail icon on the right.
- Click Change layout to see a choice of other layout displays for these same cameras. The viewing areas can be deleted using the Clear View button.
- Save changes or click Cancel to close without saving.

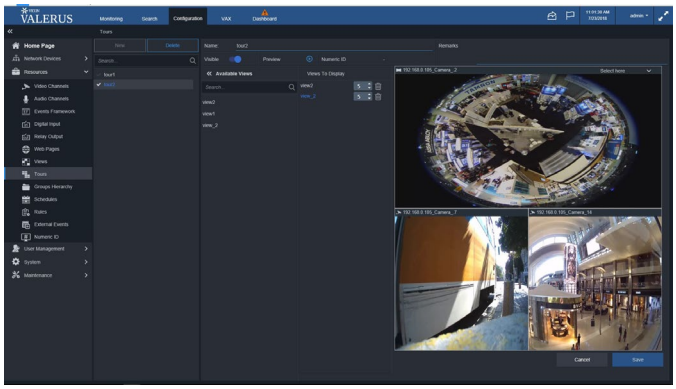
Tours

A tour is a series of previously created views, each shown for a designated amount of time, as steps in the tour.



1. List of tours
2. Tour setup

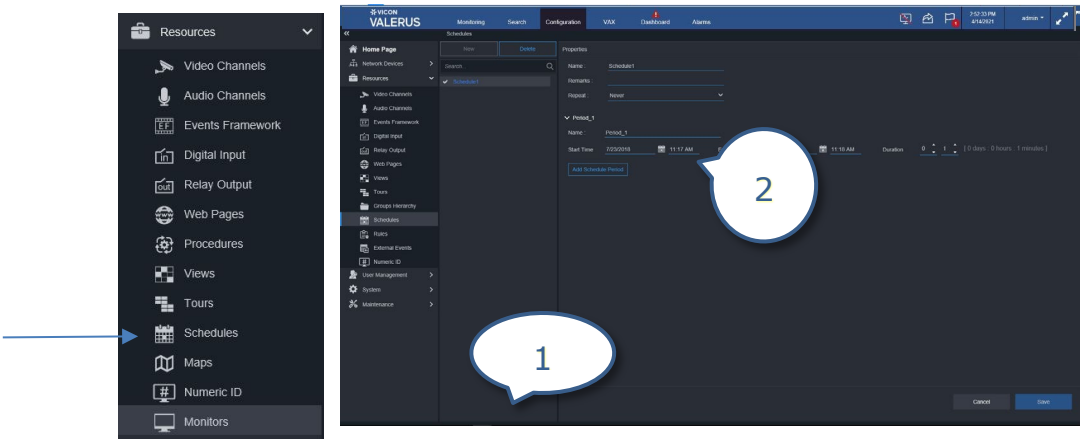
- Click Tour to display to Tour screen. Click New button.
- Enter a name for the tour if needed. A Numeric ID can be added in the field here.
- Tours are visible by default. Clicking the Visible button determines if this tour is on the Resources list on the Monitoring page. A Remarks field provides space for any notes or information on this tour.
- Views must be created from the Views configuration before a tour can be setup. From the Available views list, select the views that will be the steps in the tour and drag them into the next column in the desired order to be shown; a preview of the selected view displays. Select the duration of how long each view will display; make sure to configure this per view. The Available views list can be expanded or collapsed by clicking on the arrow heads above the list in case a larger viewing area is desired. Note that in the Configuration screen, a snapshot of the resource displays, not live video, so that if a webpage is in the view only the IP address will show here; this improves performance.
- The View can be given a numeric ID from that configuration screen, so it can then be called up from the keypad.



- A view in the tour or a tour itself can be deleted by clicking it to the garbage pail icon on the right.
- Click Save or Cancel this configuration.

Schedules

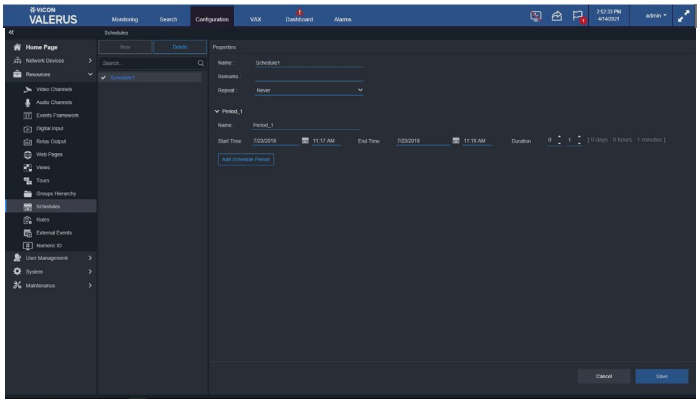
Schedules can be created and then used in the recording configuration as well as for rules. Using specific schedules instead of the default 24/7 allows fine tuning the system behavior; for example, create a schedule for weekdays and the weekend in a school. It is important to remember when configuring multiple schedules that there may be an overlap in time, and the system will prioritize one schedule (explained in detail below).



1. List of available Schedules

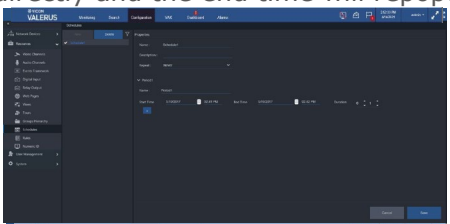
- Schedule properties

- From the Schedules screen, click New to start creating a new schedule.

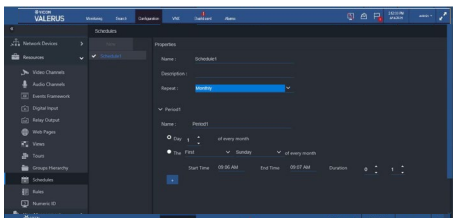


- Give the schedule a name in the Name field. Enter informative text in the Remarks field as needed.
- From the Repeat dropdown list, select how often this schedule should repeat, Weekly, Monthly, Yearly or Never. How often a schedule is set to repeat will set its priority level when schedules overlap; for example, a yearly schedule has priority over a monthly schedule which has priority over a weekly schedule which has priority over a daily one.
- In the Period area, the specific times this schedule will activate are set. The fields that display in the Period section depend on the repeat selection and dynamically change accordingly.
    - A Never repeat schedule is a one time schedule that has a start and end time on a specific day selected from the calendar. Name the period in the Title field if needed. From the calendar icons, select the start and end days for this period. Then set the start and end times (hours:minutes in 24 hour mode). The Duration fields calculate how long the period lasts from the start and end times; the duration can also be modified here and the end time will repopulate to match it.
    - A Weekly schedule sets the days and times this schedule will activate. Name the period in the Title field. Select the days of the week this schedule should run and then set the start and end times (hours:minutes in 24 hour mode). The Duration fields calculate how long the period lasts from the start and end times; the duration can also be modified directly and the end time will repopulate to match it.
    - For Monthly, select the day and month this schedule should activate and then the start and end times (hours:minutes in 24 hour mode). The Duration fields calculate how long the period lasts from the start and end times; the duration can also be modified directly and the end time will repopulate to match it.
    - For Yearly, select the day and month of each year this schedule should activate and then the start and end times (hours:minutes in 24 hour mode). The Duration fields calculate how long the period lasts from the start and end times; the duration can also be modified directly and the end time will repopulate to match it.

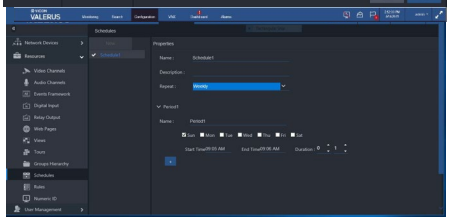
Never (Once)



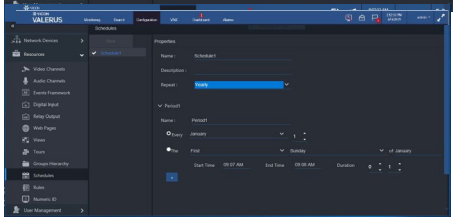
Monthly



Weekly



Yearly

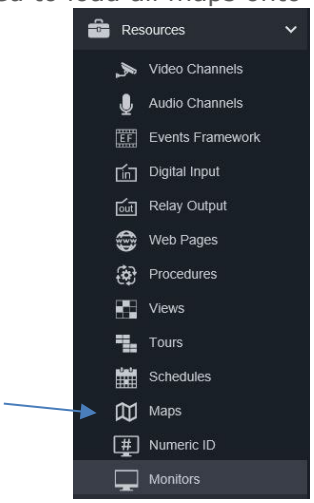


- Another period can be added to an existing schedule by clicking the Add Schedule Period button. This allows, for example, the creation in one schedule a period for working hours, another for night time and another for weekends.
- A schedule can be deleted by clicking the garbage pail icon.
- Click Save or Cancel this configuration.

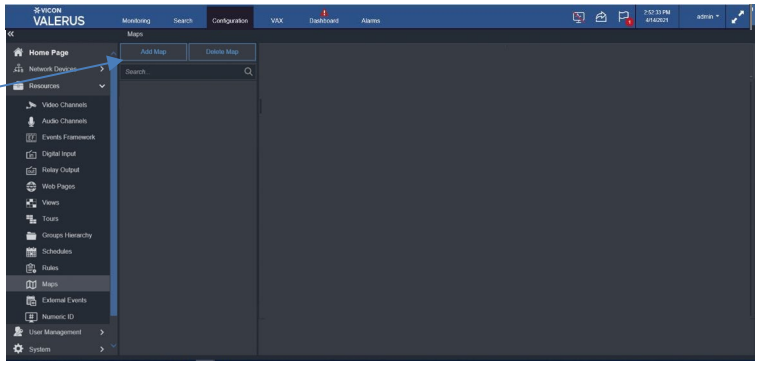
Tip: Once a schedule is created, it can be used for recording and rules, which saves the need to create multiple schedules. Be sure to name schedules and their internal periods with precise names so it is easy to identify and use them.

Maps

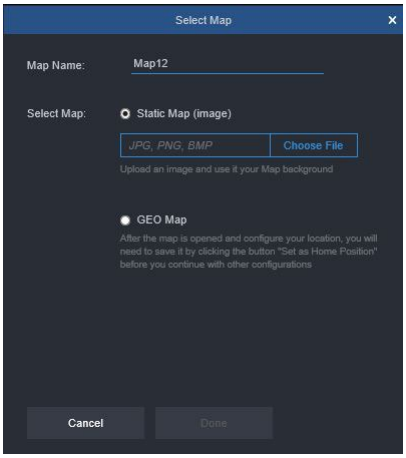
Valerus offers a mapping function (PRO tier and higher). The map can be a static picture (jpg or png) that allows an overlay of camera/device/resource icons placed directly on it or a live GEO map (requires internet). The video from the cameras can then be viewed live or in playback. After a map is created it is then listed in the Resources list on the Monitoring screen to be viewed. Note that maps are pictures that have been previously saved to your unit; it is recommended to load all maps onto your system first, before starting the configuration process.



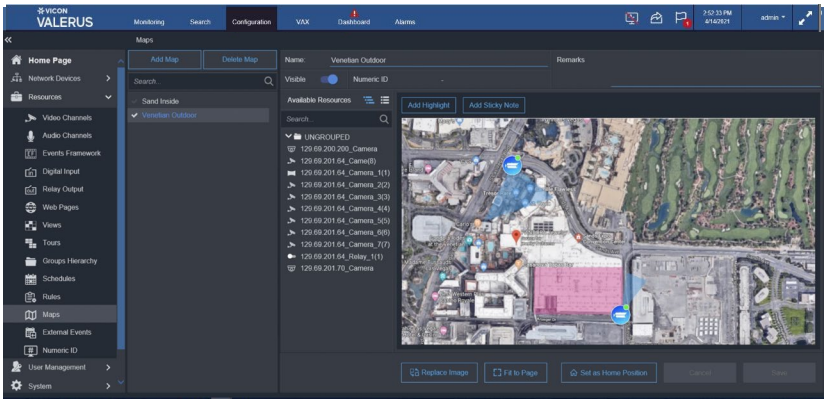
- Select Maps from the Resources list. The Maps screen displays, from which a map can be added, modified or deleted.



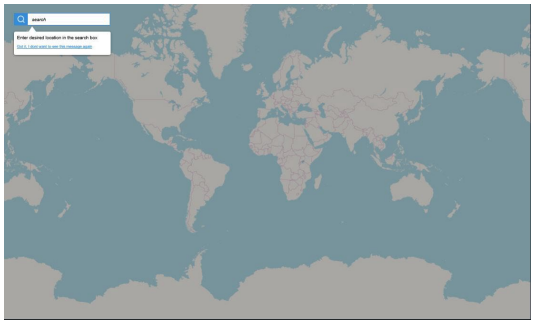
- Click the Add Map button. The following popup screen displays. Two types of maps can be added, Static Map, which is an image that has been saved to your server, or a GEO Map, which requires an internet connection to use the online map server. A GEO map is used for a large-scale geographic area where you can then pinpoint an exact location. Because it is online, it will constantly update and there is no limit to zooming.

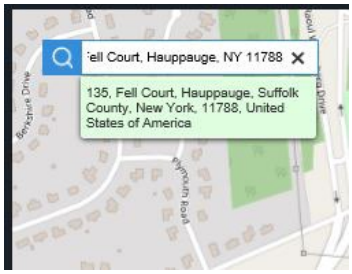


- For a Static Map, select the map by clicking Choose File. Enter a name for the map and click Save; the map is now listed on the Maps page and can be configured. Enter any pertinent Remarks to identify or define the map. Click the slider button to make this map visible on the **Resources** list on the **Monitoring** screen. The map can be given a Numeric ID as needed, just like any other resource.



- If GEO map is selected, click Done. A map of the world displays with a search field on it. Enter the location you want to pinpoint in the search field and click Enter; the mouse scroll wheel can also be used to zoom. The map of the area will display. Click *Set as Home* button. The map can now be configured. Enter any pertinent Remarks to identify or define the map. Click the slider button to make this map visible on the **Resources** list on the **Monitoring** screen. The map can be given a Numeric ID as needed, just like any other resource.

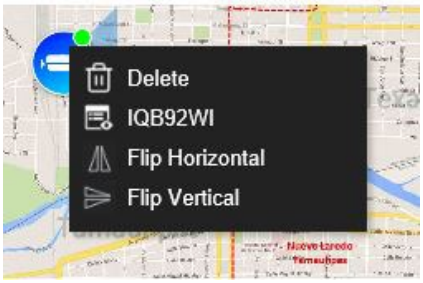




- A list of Available Resources displays, including video, audio, relay, digital input, views and tours; any of these resources can be placed on the map in the desired location to be viewed. If Integration Partners have been configured, access control doors and LPR sensors will also be available.

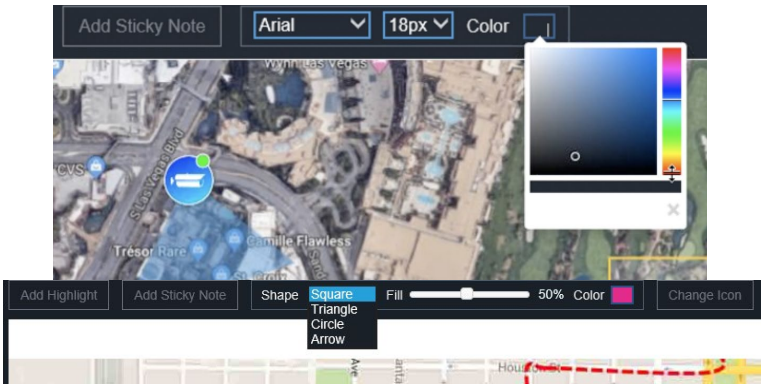
- To place a resource on the map, drag the resource to a location on the map. The resource will be identified by an icon for the type of camera or other resource. Click Change Icon to display a selection of icons to change it to, as needed. Additionally, the icon is different for when it is idle, active or in alarm state, and what these states mean varies per resource; for example, an idle camera/microphone means not recording whereas for alarm input/output it means no alarm state, while active for a camera/microphone means recording and for input/output indicates an alarm state.
- A funnel from the camera illustrates the direction and coverage of that camera. The funnel area can be changed by double clicking it and grabbing the small circles at the corners to change it; note that for a 360 camera the funnel is a circle, not a triangle, but can still be sized by grabbing the small circle at the edge. The camera/mic/tour/view direction can be adjusted by clicking the icon; a symbol displays to rotate the icon as needed. Right click the icon to view a dropdown to identify the resource or delete it; additionally, for a camera, you can reposition it by flipping it horizontally or vertically. You can zoom in and out of the map using the mouse wheel.

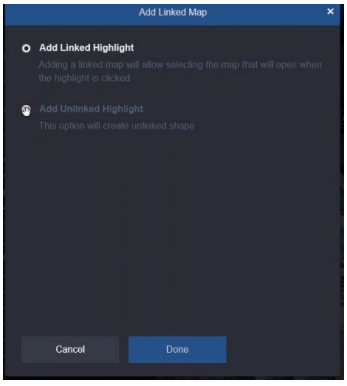
Change camera icons



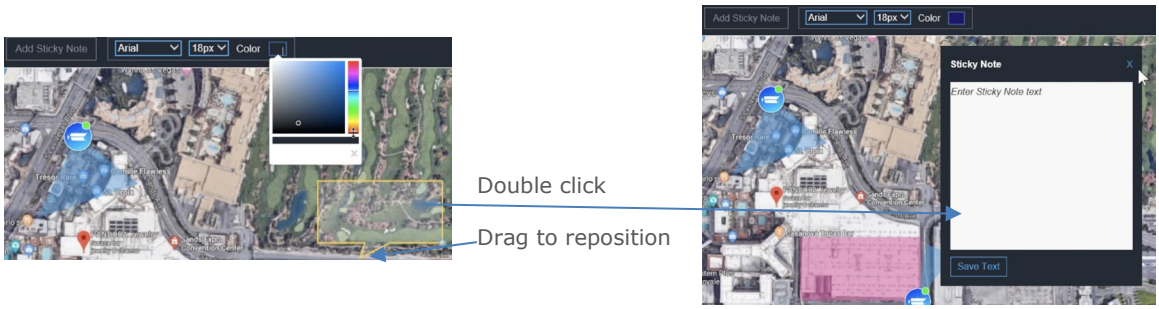
Adjust camera view and position

- Click on Add Highlight to highlight an area on a map in a variety of shapes (square, triangle, circle or arrow) and colors by using the Shape and Color tabs; the color tab provides a slider to set the transparency fill of the shape. The default shape is square and the default color is pink. This feature can be used to either simply highlight an area or used to link to another map.
- When Add Highlight is clicked, a screen displays to add a linked or unlinked highlight (see below). If Add Linked Highlight (default) is selected, click Done and another screen displays with a list of existing maps to link to. Select the map and click Done; when the highlight is clicked in the Monitoring screen, the linked map will display.
- Text can be added to the highlight by double clicking it; a dialog box opens to add any descriptive text, for example what map it is linking to. Using the arrow shape is often helpful to link portions of a large map. If the map of a large area is broken down into smaller sections for a better view, the arrow shape can be linked to another part of that map, to the right, left, up or down. Right click to delete the highlight.





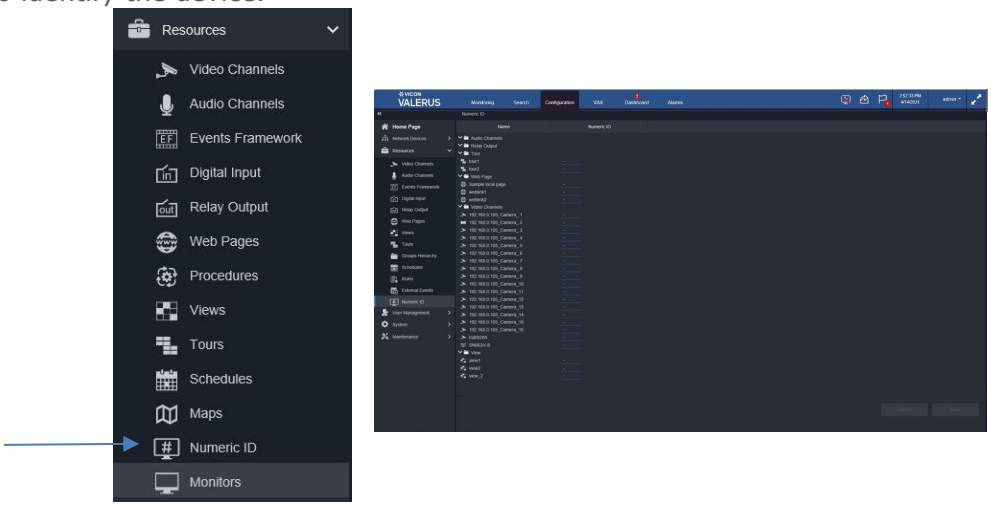
- Click on Add Sticky Note to insert a "sticky note" on a map; double click to add text with any information needed. Font and size can be selected. Be aware that the sticky note may not display at certain zoom levels. Zoom out if the sticky note text is not displaying. The sticky note can be used to point to a specific place on the map by grabbing its "tail" and dragging it to point to that place; the sticky note can be resized by a circle at its point and dragging.



- There is a button at the bottom that toggles between Actual Size and Fit to page. Clicking this will resize the map as needed. Clicking Replace Image will allow changing out the map, for example if the building has added a wing, but the icons from the original map will remain in place. You may have to move the icons around, as needed, but you will not have to recreate any of the resources already in place. The map can be set to a Home position which will determine how the map opens on the **Monitoring** screen.

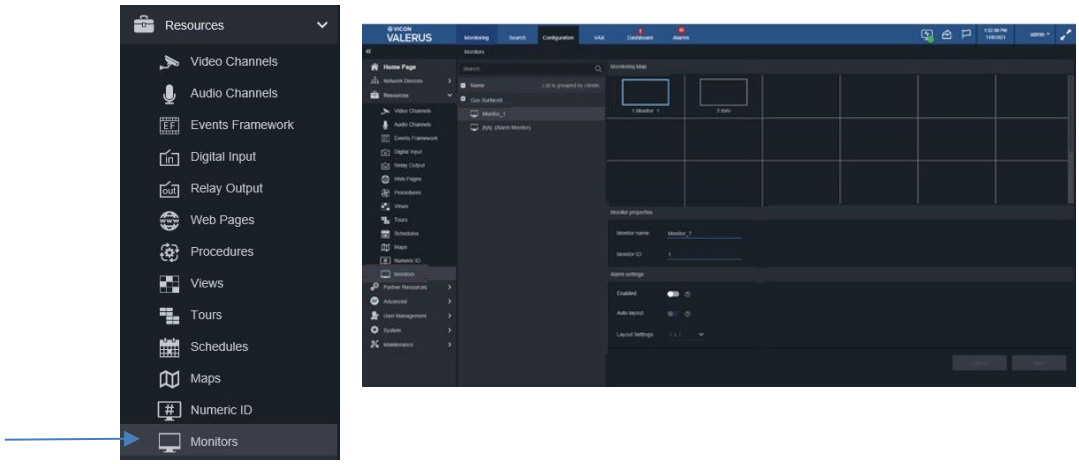
Numeric ID

If you are using a keypad or controller (PLC) with your system, a device must be assigned a numeric ID that allows the keypad to identify the device.



- Click on Numeric ID. A list of devices will display. A column next to the device is for Numeric ID. This will either display a number or have a dash in the field, indicating no ID is set.
- To give a device a numeric ID, click on the device. The Numeric ID field will become active. Enter the ID number into the field.
- If a number is repeated, it will display in red. Change the number; each device must have a unique number to identify it for the keypad/controller.
- Note that a monitor is not a resource and cannot be given an ID from here. This can be enabled through User Settings.
- The Numeric ID, when set, displays in parenthesis in the Resources List.

Monitors

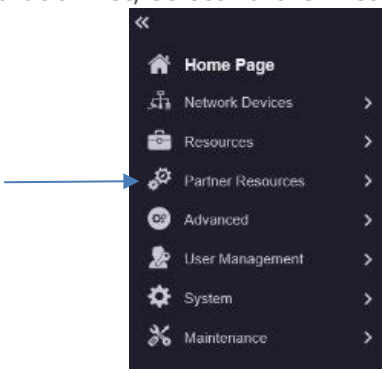


- Monitors provides a centralized approach for managing the monitors on the different Clients across the system. Once a Client sets their monitor(s) and syncs it, it will show on the Client list (on the left) and will be listed under the PC name. These monitors can be used with the VMDC feature.
- Monitors can be dragged to the right side and placed in any way required. Each monitor can be set with the following:
    - Name
    - Numeric ID. This should typically be unique, but in a case where there is a need for the same actions to show on different monitors (mirror action), they can be made the same.
    - Alarm setting:
        - Enabled/disabled (default). This will set a monitor as an alarm monitor; currently only a single monitor can be set as the alarm monitor for the system.
        - Auto Layout (Off by default). When set as the alarm monitor, determine if it is desired for the monitor to switch layouts when additional alarms occur or stay at a pre-defined layout. With auto layout, the monitor dynamically switches layouts to allow more alarms to be shown as they occur and then collapse back when those run out. For example, upon first alarm a single layout will show; when another alarm occurs, it switches to a 2x2 layout and show both alarms. When one of the alarms times out, the display switches back to single.
            - Every camera called up to an alarm monitor will show for 1 minute.
        - When auto layout is not enabled, a specific layout needs to be defined and the monitor remains in that layout. If more alarms come in than the number of available tiles, those will overwrite those currently displaying.

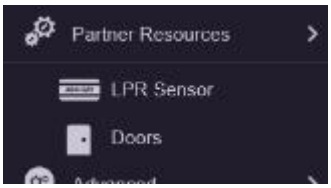
Partner Resources

If Integration Partners have been configured, from this screen you can configure Valerus resources to work with the partner. Refer to User Guides for VAX Access Control and Neural Labs LPR for details.

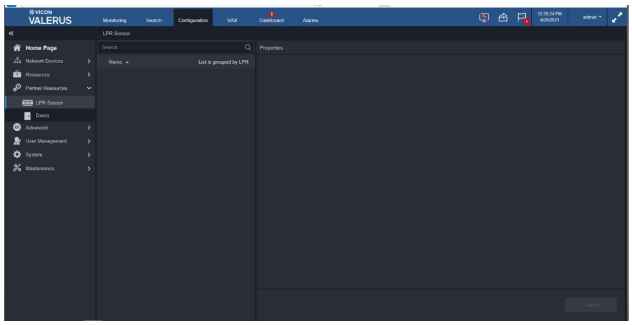
- From the Configuration list, select Partner Resources.

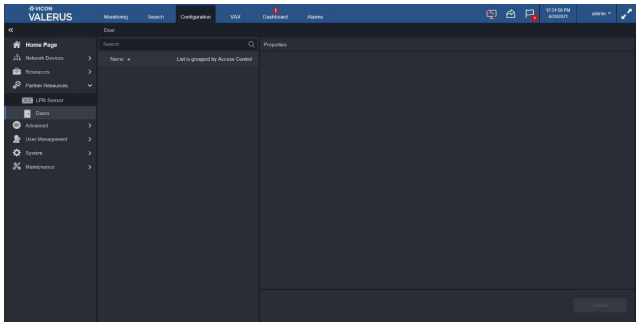


- If you are configuring an Access Control system, select Doors. If you are configuring an LPR system, select LPR Sensor.

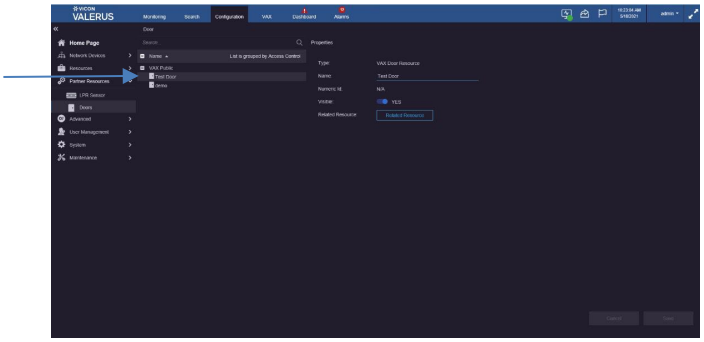


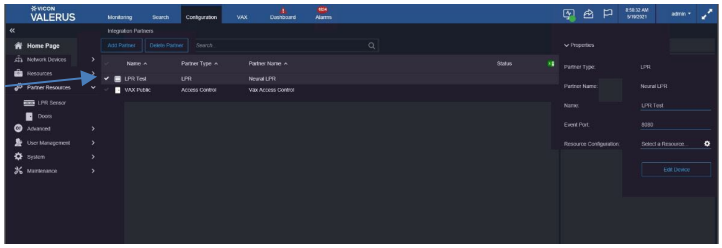
- The following screen will display, depending on your selection.





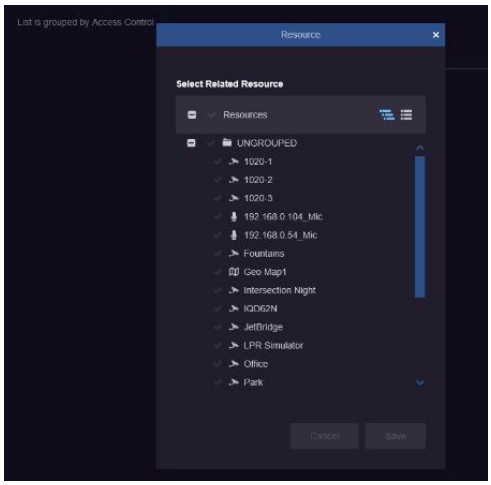
- When selecting Doors, a list of configured doors will display. When selection LPR Sensor, a list of sensors that were previously configured will display. Select the door/sensor you want to configure.





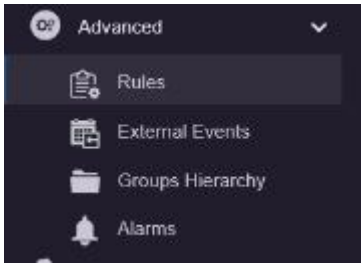
- In the Properties section, some of the fields will be populated based on how they have been previously configured, including the type of resource, its name and Numeric ID (if one has been assigned). The Visible button determines if this resource will be listed in the appropriate resources list and on the Map screen.

- Select Related Resources to open a list of available resources that can be associated to the door. Select the checkmark next to the desired resource(s); click Save. For example, if there is a camera at this door, it can be selected to display video at the door site when access was denied or if there is a camera near where the LPR camera is located (like a parking garage), it can be selected to display additional video with a different angle at the site where the car license plate is being read.



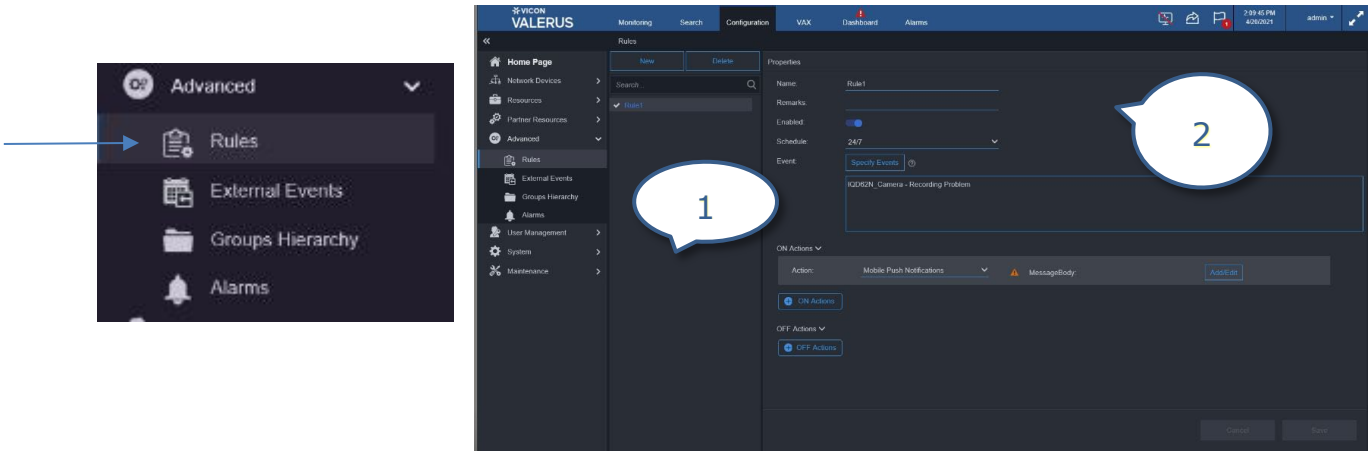
Advanced

The Advanced screen provides the configuration of Rules, External Events, Group Hierarchy and Alarms.



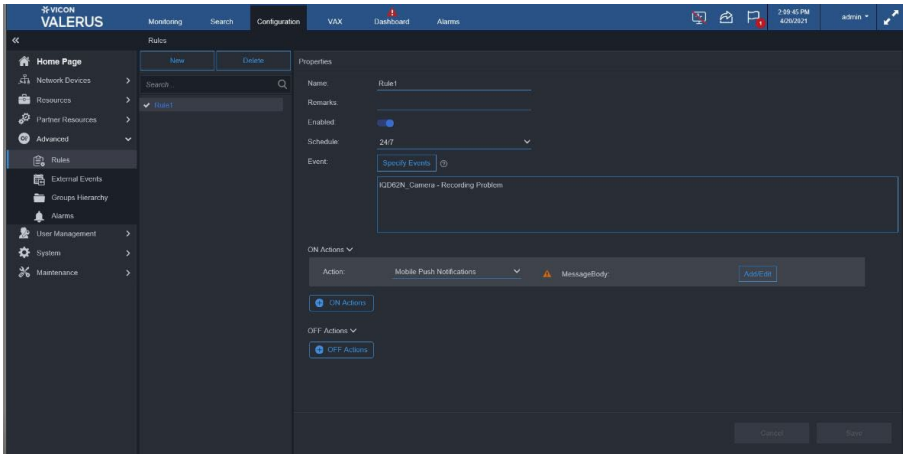
Rules

Rules are created to determine what happens when an event is triggered, defining a cause and an action.

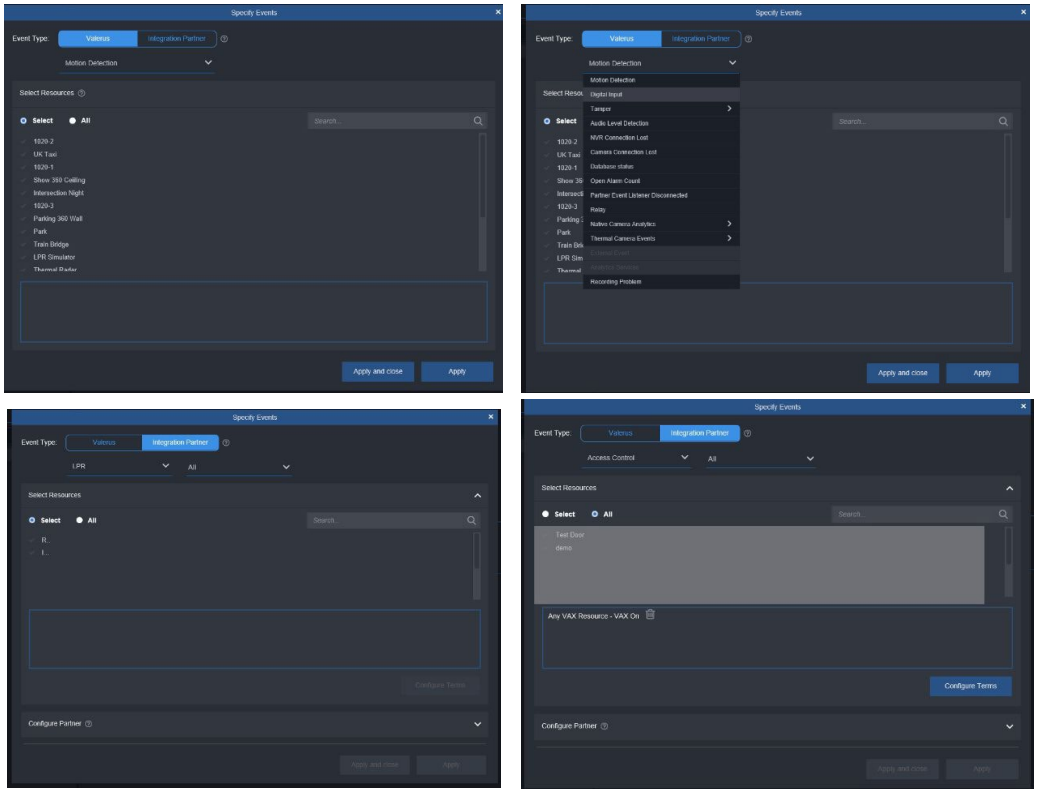


1. List of rules
2. Rule properties

- Click on Rules. From the Rules screen, click New to create a rule. The Properties screen will display.



- The rule can be given a name in the Name field.
- Configure the trigger for the rule by selecting an event. Click Specify Events. From the popup screen, select the event type, Valerus or Integration Partner. For Valerus, select from Motion Detection, Digital Input, Tamper, Audio Level Detection, NVR Connection Lost, Camera Connection Lost, Database status, Open Alarm Count, Partner Event Listener Disconnected, Relay, Native Camera Analytics, Thermal Camera Events, and Recording Problems; for Integration Partner, select LPR or Access Control.

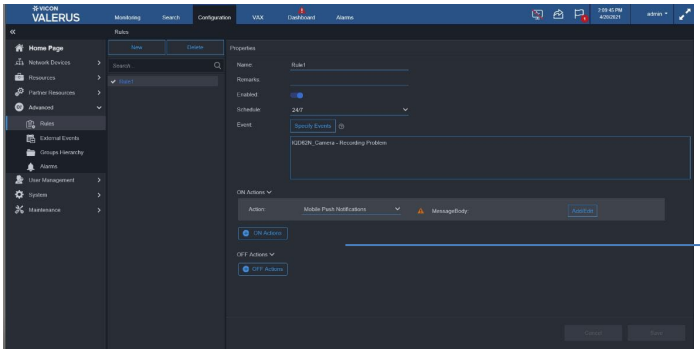


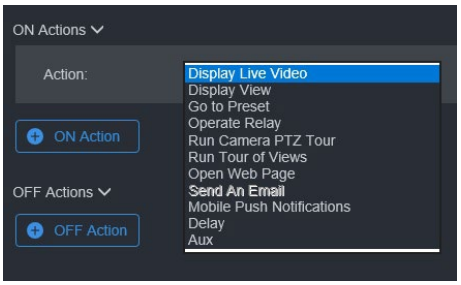
- For Valerus, with the Select radio button checked, choose the devices to associate with this event; multiple devices can be selected by holding the Control button and selecting the devices. The All radio button allows selecting all the devices in the list; when this event type occurs on all devices in the list, it will trigger the rule. If it is required to have multiple event types assigned to a single device, another rule can be created the device. Each event will display in the area at the bottom of the popup screen and can be deleted by clicking the garbage pail icon next to it. When events are configured, click Apply or if you are finished, click Apply and close. Click Close if no more events are to be configured.

- For Integration Partners, after selecting LPR or Access Control, select All (for all systems) or the specific system you are configuring from the dropdown list, currently Neural Labs or Vicon LPR for LPR or VAX for Access Control, respectively. From Select Resources, choose which unit has the event. For example, select the LPR sensor that will read a suspicious license plate. Click Configure Terms to define the parameters for the event. Select a parameter and an expression (i.e., Equals, Contains) from the dropdown list; enter a Value. When events are configured, click Apply or if you are finished, click Apply and close. Click Close if no more events are to be configured.

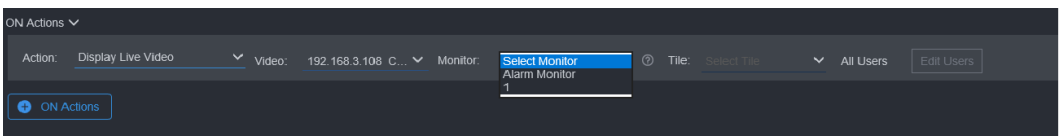
Important Note: There is a question mark symbol next to Specify events that opens a popup that explains your choices. When specifying more than one event to trigger a rule, the actions will occur when an event is reported by ALL the sources specified at the same time. Rules work as a logical *AND* between multiple events. If the Any event option is selected, it will work as a logical *OR* between events.

- The events now display in the event box on the page. More events can be added in the same way. Triggers can be deleted here using the garbage pail icon next to them.
- From the schedule dropdown, select the schedule for this trigger. Available schedules include 24/7 (default) and any schedule previously created. A new schedule can be created from here, if necessary. Clicking New schedule from the list opens the Create New Schedule screen. Follow instructions under Schedules.
- The actions taken when the event occurs are defined under the ON Actions. Select an action from Display Live Video, Display View, Go to Preset, Operate Relay, Run Camera PTZ Tour, Run Tour of Views, Open Web Page, Send An Email (note that an email is text, not video), Mobile Push Notifications, Delay, Aux or, on Integrated Partners only, Related Resources. The actions in the dropdown list are camera and event dependent. Depending on this selection, select the camera, tour, view, etc. to respond. Specific users that an action will apply to can be selected; click Edit Users.

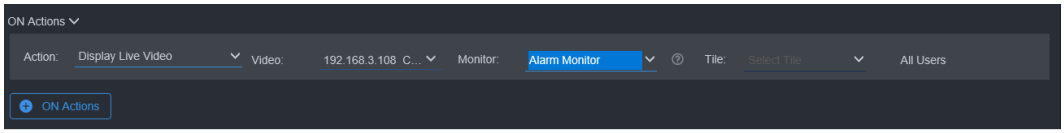




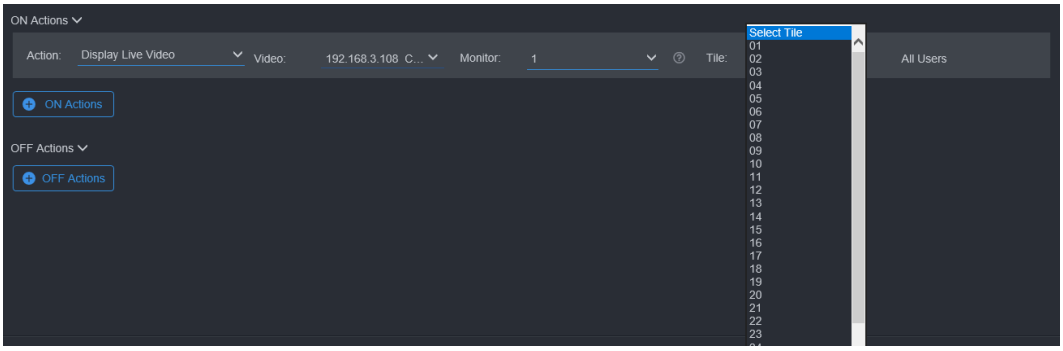
- When selecting the Display Live Video action, there is a dropdown list of monitors as they are configured in the Resources section to select from. This list allows selecting either an alarm monitor (if one has been configured) or a specific monitor by its Numeric ID.



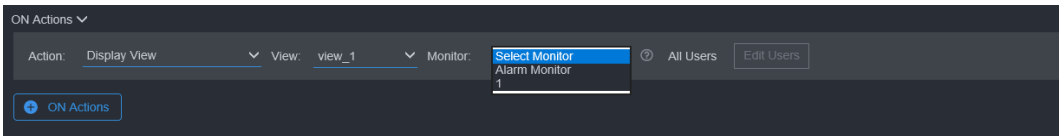
- When selecting an alarm monitor, the other configurations are grayed out and the camera will be shown on the designated alarm monitor, which operates according to its configuration.



- When selecting a specific monitor by number, it is necessary to select a specific tile on that monitor as well (1-36).



- When selecting the action to display a View, it behaves in the same way, except there is no tile selection for the monitor and the entire View is displayed.



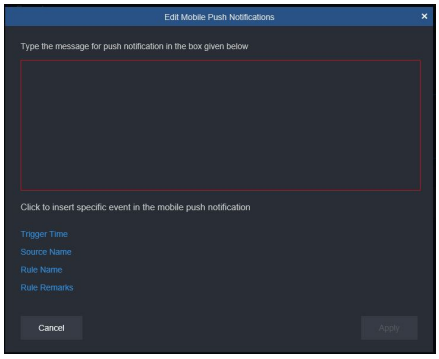
- In the same way, the action taken when the event is over can be configured by OFF Actions.
- Note that it is not necessary to configure both an ON and OFF Action for every event. Some events make sense to use only ON action, for example, when a door opens (sensor ON), display a camera. Some events make sense to use only an OFF actions, for example, when there is no motion, turn the light OFF. An example for both ON and OFF actions is when the door opens (sensor ON), sound a buzzer and when it closes (sensor OFF), stop the buzzer.
- Note that to enable the Send An Email option, the email server must be configured first. Refer to System>Networking section for details. If Send An Email is chosen as an Action, click Add/Edit; a popup displays to specify the recipients and write the body of the email. Enter the desired text; you can also click a variable from the list at the bottom to include that information in the notification. An example of this would be:

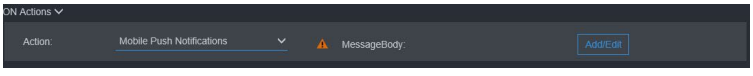
  - An event occurred on the Valerus system at %Trigger_Time%
  - The event was triggered by source %Source_Name%
  - The Rule that triggered this email is %Rule_Name%

- Note that for Push Notifications to work, the Application Server must have Internet connectivity as well as the mobile device. If Mobile Push Notifications is chosen as an Action, click Add/Edit; a popup displays to allow writing the notification text. Enter the desired text; you can also click a variable from the list at the bottom to include that information in the notification. An example of this would be:

  - An event occurred on the Valerus system at %Trigger_Time%
  - The event was triggered by source %Source_Name%
  - The Rule that triggered this email is %Rule_Name%

Note that the mobile device does not need the app running to receive messages.



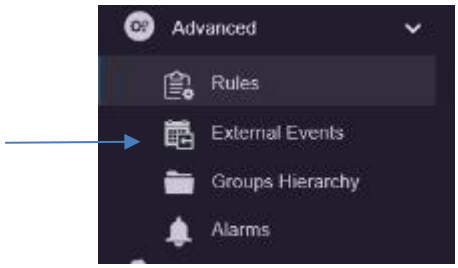


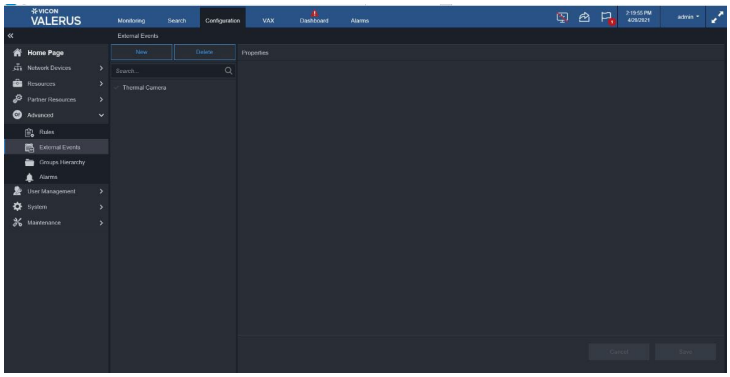
- Click Save or Cancel this configuration.

External Events

External Events occur from outside the Valerus system and generate from 3rd party systems such as LPRs, Access Control systems, etc. Valerus allows defining a "Listener" to listen on a specific port for external text events sent from those systems and then allows to create rules based on these external events. This is meant to enhance the integrations with such 3rd party systems as well as Valerus VEF, allowing specific events to be set to trigger actions in Valerus. *Note that external events are not supported for recording rules at this time.*

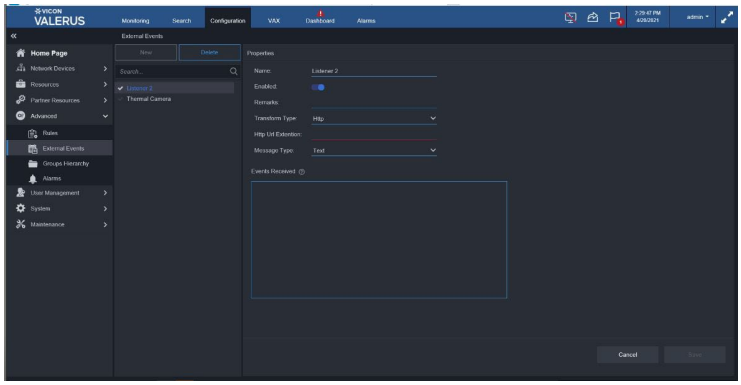
Once a Listener has been set up in Valerus, rules can be configured to read the events and act upon their content. The Listener is defined from this screen.

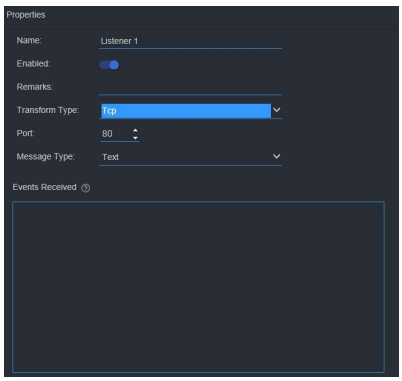




- Select External Events from the Advanced list. The screen above displays.
- Select New to create the Listener.
- Fill in all the fields and click to Enable or Disable the Listener. For the Transform Type, select Http, TCP; or UDP; for Http, enter the URL and for TCP enter the Port. Message Type can be Json, Text or Xml.

  The exact protocol and format of the event messages varies between manufacturers and requires understanding of the other system's behavior.



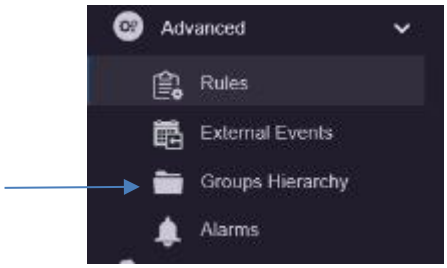


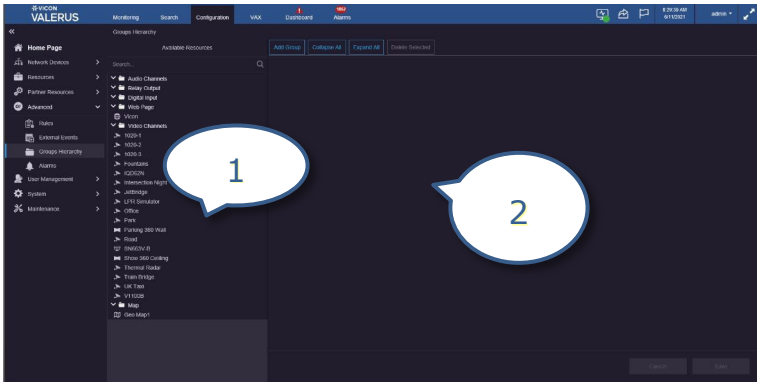
- At the bottom of the screen there is a window that serves as a console and will show the events that the selected Listener has received. This allows easy confirmation of the communication between the two systems.

Groups Hierarchy

The Groups Hierarchy is meant to create a geographical view of the system. From here, you can build a system "tree" to determine which resources should be logically grouped and determine their relation to other groups. This also helps in streamlining the authorization and operation settings for the user roles from the System and Resource Authorization screens. For example, on a Campus, there would be a number of buildings, and each building could be divided into zones and each of these zones would have a number of floors. These areas can be

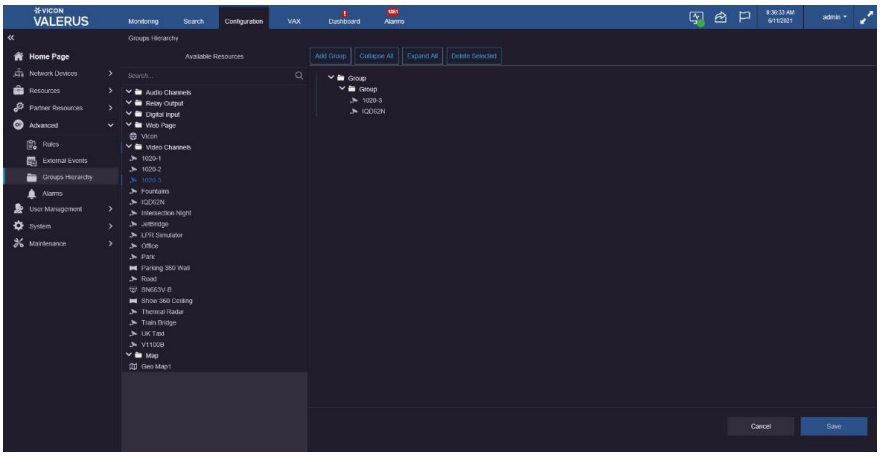
divided into groups and sub-groups and specific resources can be associated with each group and easily found in the Resources list on the Monitoring screen.





1. List of available resources (any resource that has been added previously)
2. List of groups

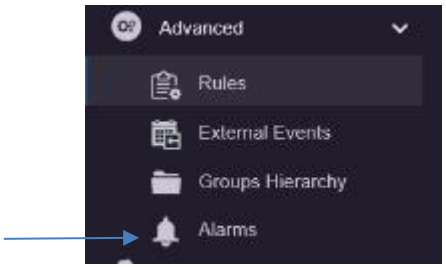
- Click Groups Hierarchy to open the page that lists all available resources that can be assigned to a group. The list on the right will be empty the first time this is done.
- Start by clicking Add Group to create a new main group. Multiple groups can be created or the entire list can be built under a single group.



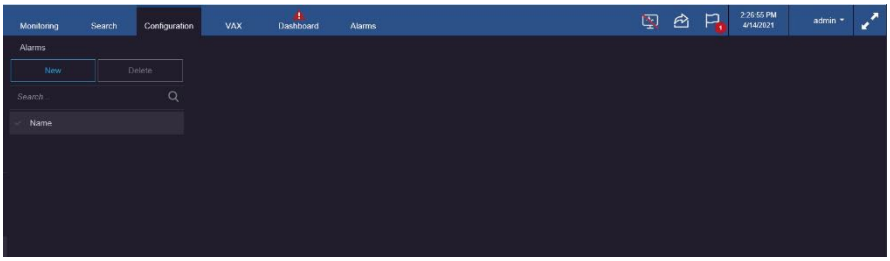
- The new group appears in the area to the right. Hovering over the group name displays buttons that allow you to edit the name (pencil), delete (garbage pail), add a sub-group (plus) or copy this group. The group name can be changed by selecting the pencil. The default group name becomes active and you can change the name; press Enter when done. Devices can be added to any group by dragging them from the Available Resources list to the group name; all the devices added to a group will list under the group name.
- Additional groups can be added by clicking Add Group again. Sub Groups of a group are created by clicking the plus symbol from the tools next to the group.
- Sub Groups and resources can be moved into another group in the hierarchy by dragging and dropping. The ability of move one main group inside another group is blocked.
- Groups and devices are deleted by clicking the garbage pail icon on the right.
- Multiple selection of groups and devices can be done using the Ctrl and Shift keys. When multiple items are selected, using the Delete Selected button deletes them all.
- Click Save or Cancel this configuration.

Alarms

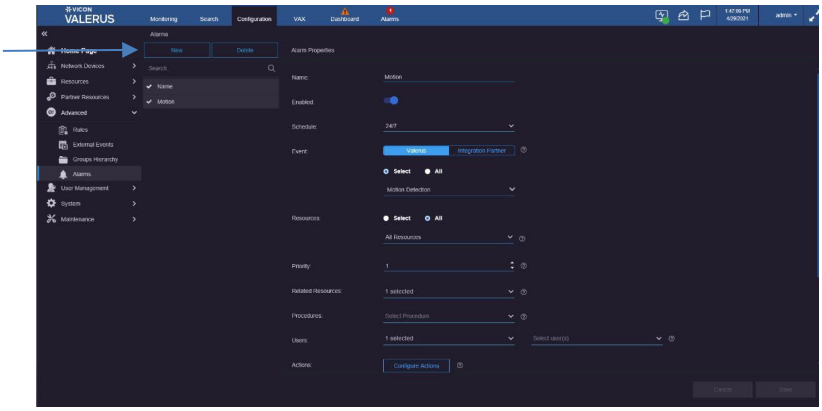
The Alarms screen defines which events are elevated to an alarm level, what resources are bundled with it and the life cycle for the alarm. Note: The Alarms Management feature is available for the PRO (with limited functionality) and ENTERPRISE tiers. ***Refer to the Alarms Management Guide for details.***



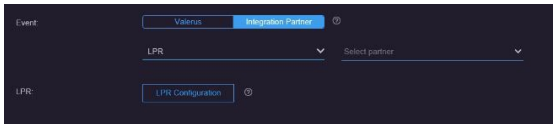
- Click alarms to open the alarms page.



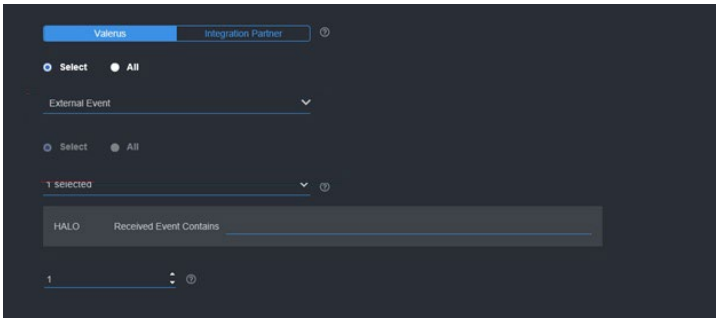
- Click the New button to open the alarms editor to define a new alarm.



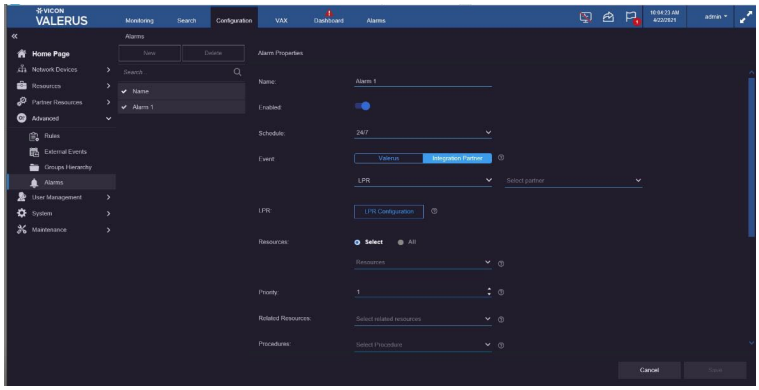
- Assign a name to the alarm in the Name field.
- The Enable/Disable button allows the alarm to be temporarily disabled as needed without deleting it.
- Select a schedule from the dropdown list to define a schedule for this specific alarm, using an existing schedule or creating a new schedule using the scheduling system in Valerus. It is important to identify the correct schedule for each alarm to minimize the number of unwanted alarms.
- In the Event field, select the events that will be the trigger of this alarm from the two options, events generated from Valerus or events coming from an Integration Partner. The display will change accordingly.

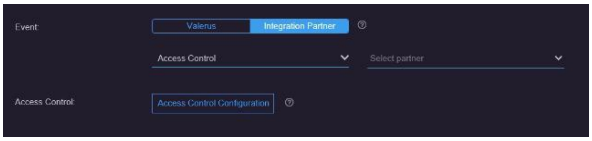


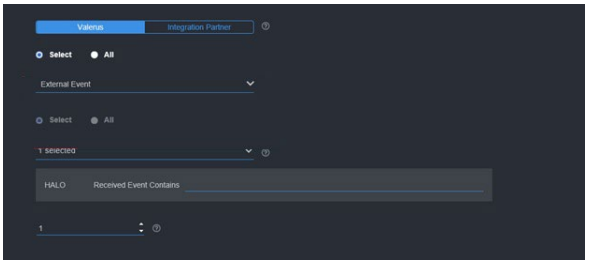
- For Valerus events, using the Select button, select the event type from the dropdown; an All button can be used to select all event types in the list. Note that it is usually not recommended to define All events as alarms, as this will overload the system by elevating any event in the system to the Alarms Management system. When selecting external event as the triggering resource, it is possible to specify the listener and the message that should be received from the external source as the trigger of the alarm.



- When the alarm is set to trigger by an Integration Partner event, select the event type from the dropdown list, for example LPR or Access Control, and the specific partner from the next dropdown (this list is expected to update as new partners are added). ***Refer to the user guides for VAX Access Control, Vicon LPR or Neural Labs LPR for details.***

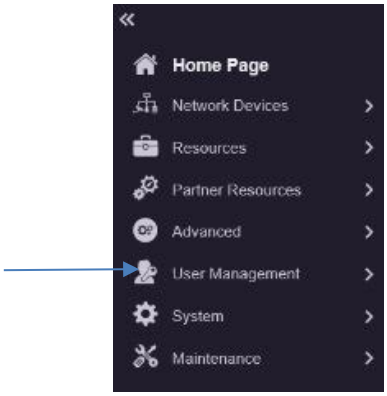


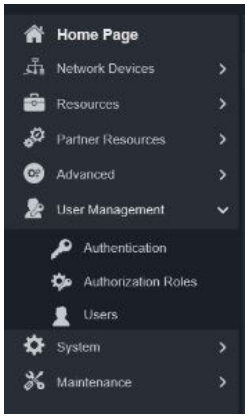




User Management

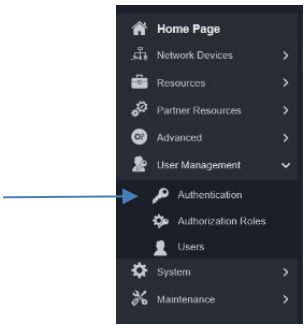
User Management sets up the privileges and authorizations for users of the system. Authentication determines if the users are managed by the local Application Server database or an active directory server. From here, users can be added to the system, authentication roles can be created and users can then be added with specific authorizations. The privileges for each user in the system is defined in the System and Resource Authorization screens tabs at the top.

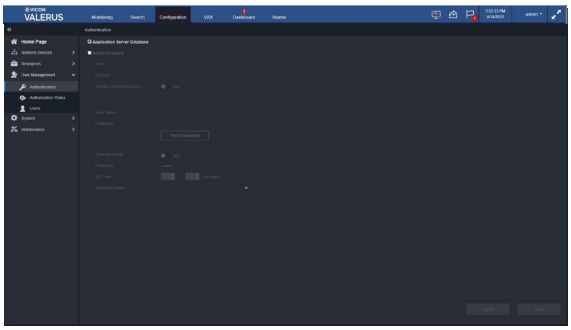




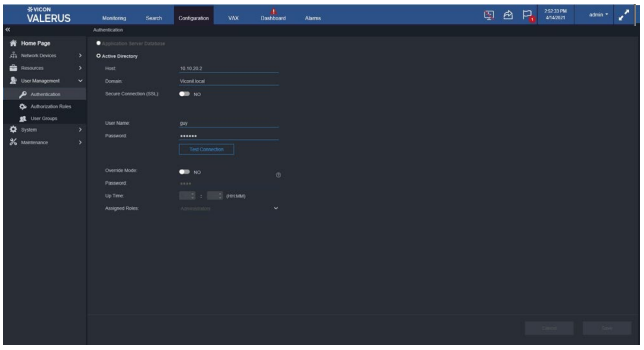
Authentication

From Authentication, the user database source is configured. Choose from the local Application Server database or an active directory server used on the network.





- When the local database is to be used (default state) for the user list, check the Application Server Database radio button.
- If connecting to an active directory server (existing on the network) is desired, check the Active Directory radio button. The IP address of the Active Directory server and the credentials to connect are defined here. When connected to an active directory server, the users and their groups are managed by the active directory.



- Enter the host IP or name and domain details for the active directory server. Only an authorized domain user can access it and retrieve information. Use the Test Connection button to verify that

the credentials are correct and connection can be established. Once connected to the active directory, it will allow importing user groups; see details in the User Groups and Users sections below.

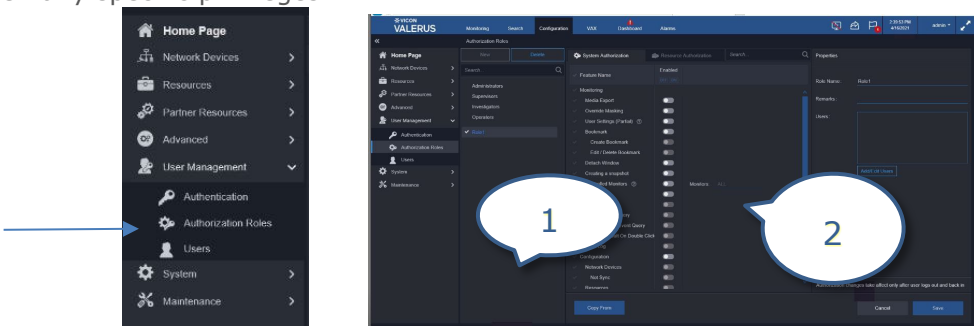
- It is required to know if this connection needs to be secure (SSL; ensures that all data passed between the web server and browsers remain secured and integral). Check with your IT staff to confirm whether the system demands this secure connection and turn it on if needed.
- The Override button can be enabled if needed. This is used in the rare event that the active directory server is down and access to it is impossible, which will prevent users from logging in to the system (systems running and users already logged in are not affected by such an issue). The VMS, even when set to active directory mode, still maintains a local account for the user.

  ADMIN (see more details under Users) and this user can set up a temporary password to allow login for any user without a connection to the active directory. The emergency mode and special password have an expiration time and remains valid for the time period designated, up to 24 hours, so that if the administrator does not shut this off mode; it will shut off automatically.
- Click Save or Cancel this configuration.

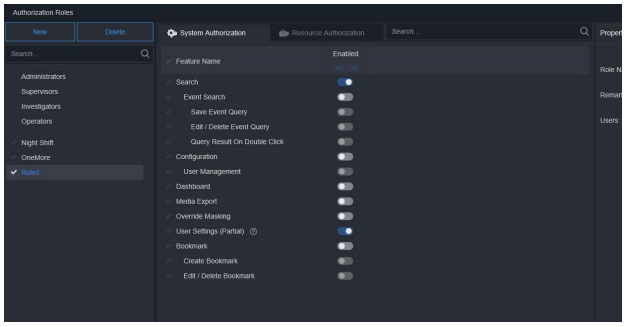
Authorization Roles

The Valerus VMS, similar to other IT centric systems, manages user privileges by grouping users under authorization roles. This allows setting privileges to these roles (for example the security guards), so any user with that role inherits those privileges without having to make individual settings for each user.

When working in the default mode, where the users are managed by the Application Server itself (different than the active directory, which is discussed later), there are four levels of predefined Authorization Roles, Administrators, Supervisors, Investigators and Operators. Each of these levels has set different privileges to work within the system. These Authorization Roles cannot be modified or deleted, but users can be added to them. However, new Authorization Roles can be added to the system and be given any specific privileges.

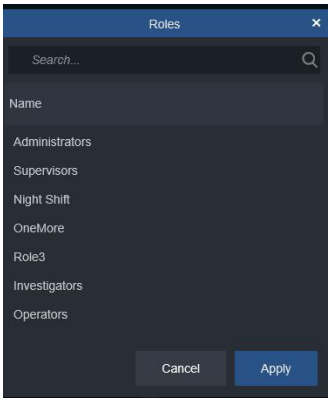


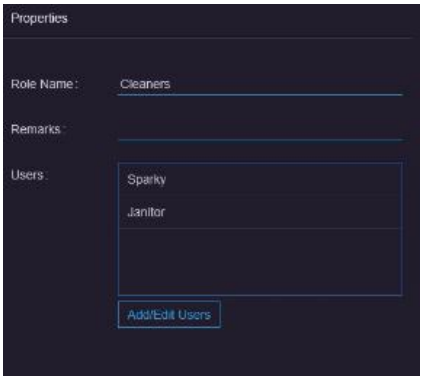
1. List of existing Authorization Roles
2. Authorization Roles details
   - A new Authorization Role is created by clicking New.
   - A new Role is added to the list.



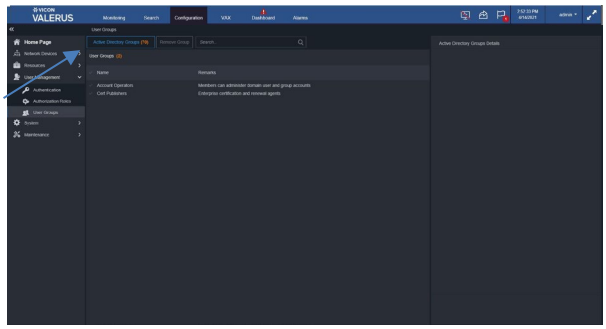
   - The Role can be named and users added to it. Each role has System Authorization and Resource Authorization tabs at the top. These will be explained below.

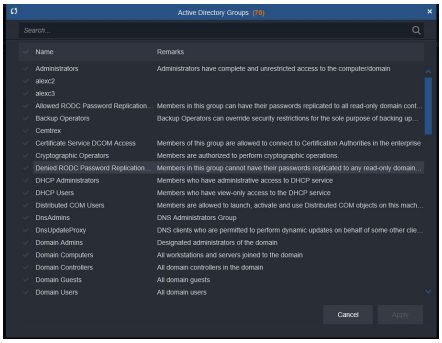
- For customer-defined roles, all the privileges can be set enabled ON/OFF.
- If you want to create another role that is similar to an existing role to save the need to configure all privileges, you can duplicate a role. Create a new Role and click Copy From. A popup will display. Select the Role you want to copy from and click Apply. The properties will remain the same as the original role but can be modified as needed. Users assigned to a role can be added or edited from the role properties list by clicking Add/Edit Users under the list of users.



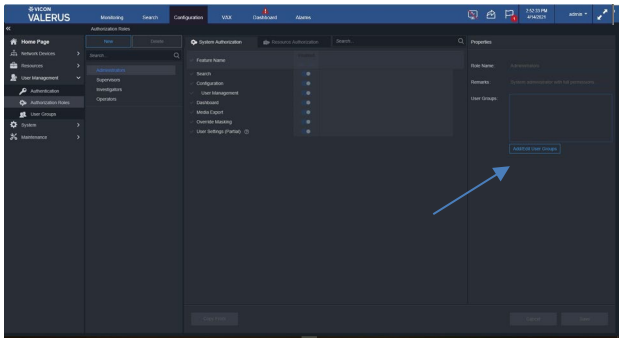


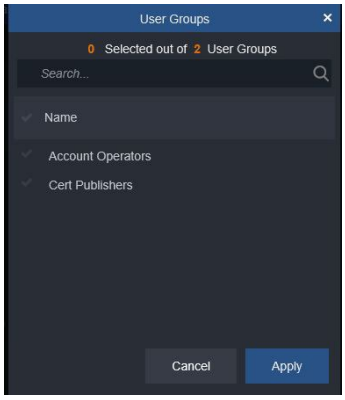
- If under Authentication, an Active Directory server, and not the local Application Server, was chosen to manage the user groups and roles, the screen will initially list only the override role (only including the ADMIN user and meant to put the system into override mode) allowing you to pick the desired user groups out of those in Active Directory.
- From User Groups screen, click the Active Directory Groups button to open the list of available user groups (number of groups shown in parentheses).





- Select the user groups you want to import holding the relevant users. It is recommended to have IT create groups dedicated to the VMS different roles to make this easier to manage.
- Multiple groups can be imported using the Ctrl and Shift keys to select a range of groups.
- Click Apply and close the pop-up screen.
- These User Groups can then be added to Authorization Roles by selecting the role and then clicking Add/Edit User Groups.



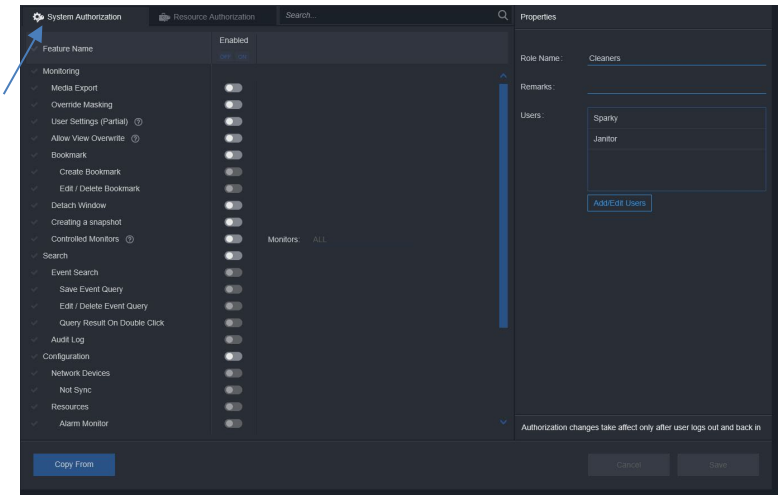


Note: When using an active directory server for user management, the users screen is not shown and all user credentials, as well as assignment to user groups, is done solely in the active directory server.

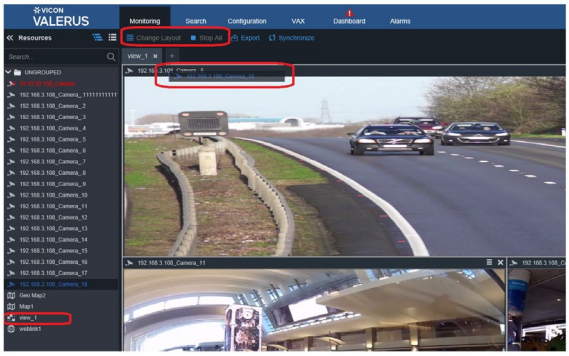
- A user group (except the override group) can be deleted by selecting it and clicking Remove group or clicking the garbage pail.
- Click Save or Cancel this configuration.

System Authorization

This screen summarizes which users can access what subcategories of Monitoring and Configuration. Each Authorization Role has specific permissions defining what functions that role is allowed to perform in the system.



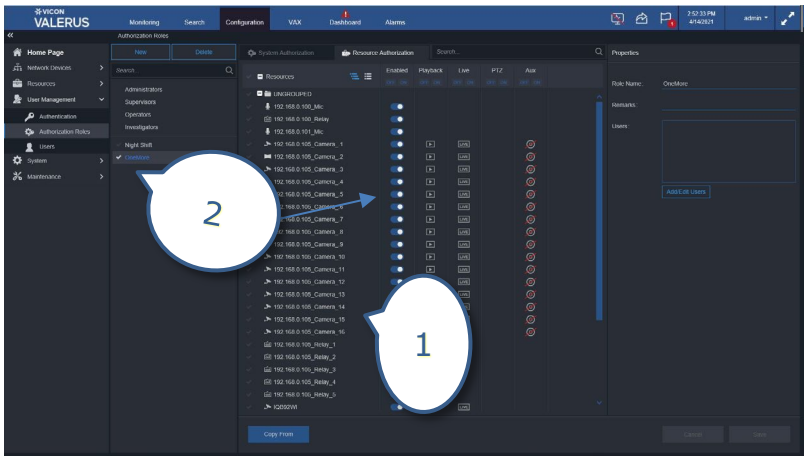
- The main functions are Monitoring, Search, Configuration, Dashboard and Alarms Management; subcategories include Media Export, Override Masking, User Settings (Partial), Bookmark, Detach Window, Creating a snapshot, Controlled Monitors, Event Search, Audit Log, Network Devices, Resources, Partner Resources, Advanced, User Management, System, and Maintenance.
- Select the Authorization Role from the list.
- Click a feature; the feature will be checked. Each feature has an Enabled ON/OFF button indicating what that role can do.
- Administrators, Supervisors, Operators and Investigators who have predefined permissions, as explained previously, cannot be changed.
- Allow View Overwrite, under Monitoring, provides additional control over the drag-and-drop behavior when showing a View. Since Views are often configured to display specific cameras for an intended purpose, it may be unacceptable to allow this configuration to be changed. When this authorization is disabled, the user will not be able to drag-and-drop cameras into the displayed view and a "No option" icon will display when attempted; additionally, the Stop All and Change Layout options will be grayed out to prevent changing the View.



- Controlled Monitors, when enabled, allows control of another client workstation using a Keyboard/PLC to allow switching cameras. To do this, all monitors must be numbered. The PLC driver must be installed on every Valerus unit you want to control. When Authorization Roles are configured, all monitors can be selected to allow control or specific monitors can be selected.
- Click Save or Cancel these setting.

Resource Authorization

Similar to System Authorization, each authorization role can be set to have different permissions to use the resources defined in the system. The Resources are listed by their group hierarchy if this was created.

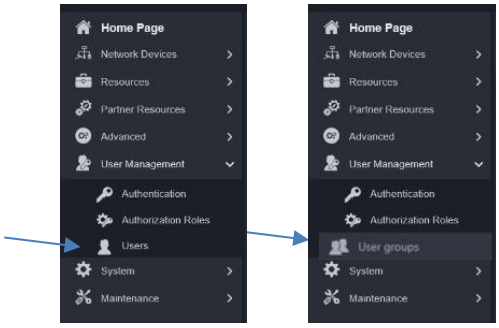


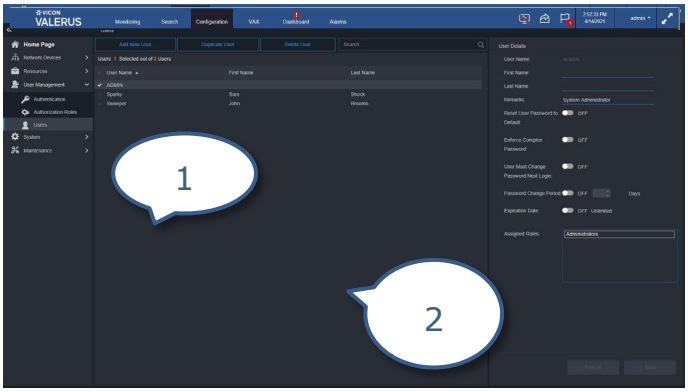
1. List of Resources and associated functions for each Authorization Role
2. List of Authorization Roles
   - A table of all resources in the system is listed.
   - For each resource, depending on its properties, there will be ON/OFF setup options to enable or disable Playback, Live, PTZ (if applicable) or Aux for any custom-created Authorization Role. Note that this cannot be changed for the fixed Administrators, Supervisors, Investigators and Operators.
   - When the resources are grouped in a certain hierarchy, a change to the role will apply to all the resources under it; for example, disabling playback for role ABC will disable it for all the resources in authorization role ABC, saving the need to configure each one separately.
   - If the settings for a certain resource within an authorization role are changed, it will NOT change the other resources nor the authorization role. For example, if you enable playback to a certain camera under an authorization role that has playback disabled, only that resource will get enabled and all the rest stay disabled.
   - Click Save or Cancel these setting.

Users

By default, the only user in the system is the ADMIN user; any number of Users can be added to the system. Valerus provides the ability to prepare a user list in advance in a standard Excel spreadsheet saved in CSV format. This allows a way to import user lists from other systems and arrange them for Valerus to use, as well as offering a single action, time saving option when multiple users need to be added to Valerus eliminating to process of adding them individually.

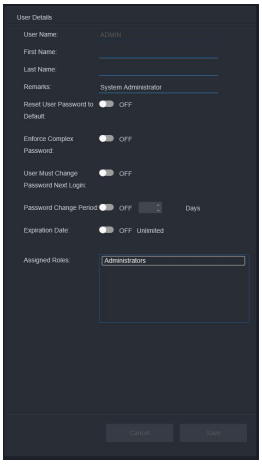
Note: When the VMS is configured to work with an Active Directory server for user management, the Users option will change to User Groups.

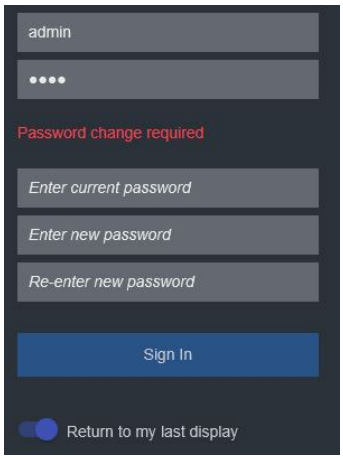




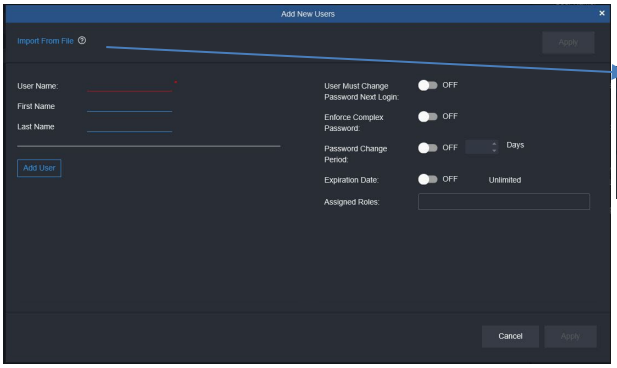
1. List of existing users
2. User details

- Click Users to open the User screen. A list of current users displays. Highlight the user to review the details to the right.
- If a user's password needs to be reset (typically if the user forgets it), that can be done here.
- You can Enforce Complex Password by sliding it to ON. This should be done as an added level of security. The requirements for the password are shown by hovering over the question mark: minimum of 8 and maximum of 20 characters, 1 capital letter, 1 lower case letter, 1 number, 1 symbol and cannot contain the user name.
- A user's password can be forced to change after a designated period of time or upon next login. When that user logs in, a message will display.

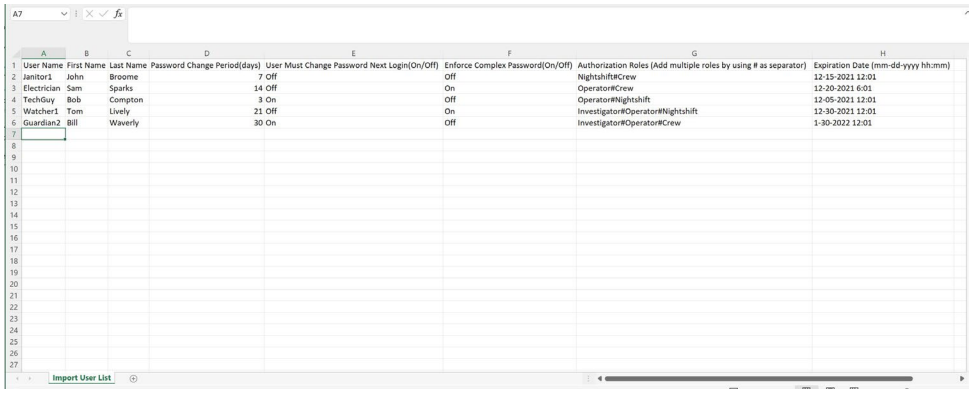




- To add a new user, click Add New User; a dialog box displays to enter user name, which will be used for log in, and the user's details.



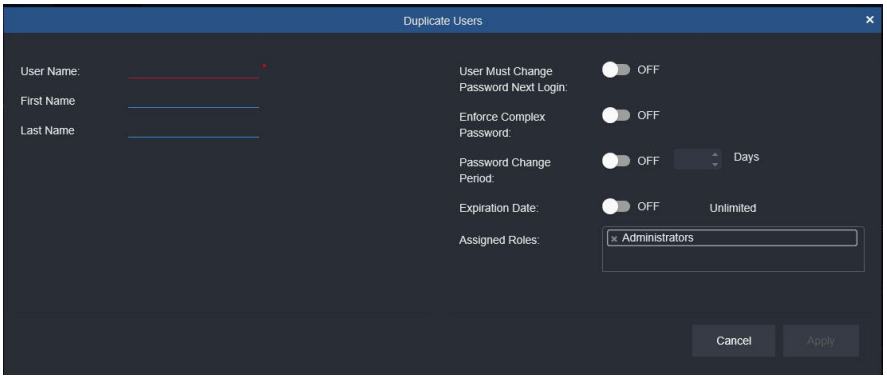
- There is an option to read from a file; this is useful if multiple users need to be added. There is a link to download a sample CSV file to use as a template for import. For first time users, it is recommended to download the sample file, open it in Excel and add users based on the predefined columns. Be sure you have Excel on your system.
- The information to be provided for each new user in the sheet is identical to the fields in the Add User form in Valerus. Enter a User name to be used for log in (mandatory) a first and last name, password change period, if needed, enforce complex password (On/Off – leave blank) and assign authorization roles; at least one role needs to be specified, role names must match the name previously entered in Roles and multiple roles can be entered, using # as a separator between role names. Refer to the information for add user in this section for details.



User Name	First Name	Last Name	Password Change Period(days)	User Must Change Password Next Login(On/Off)	Enforce Complex Password(On/Off)	Authorization Roles (Add multiple roles by using # as separator)	Expiration Date (mm-dd-yyyy hh:mm)
Janitor1	John	Broome	7	Off	Off	Nightshift#Crew	12-15-2021 12:01
Electrician	Sam	Sparks	14	Off	On	Operator#Crew	12-20-2021 6:01
TechGuy	Bob	Compton	3	On	Off	Operator#Nightshift	12-05-2021 12:01
Watcher1	Tom	Lively	21	Off	On	Investigator#Operator#Nightshift	12-30-2021 12:01
Guardian2	Bill	Waverly	30	On	Off	Investigator#Operator#Crew	1-30-2022 12:01

- Once the users file is complete, click on the Import From File link and select the file. Click the Apply button to upload and watch to the progress information. Note that only new users in the file will be imported. If users in the file already exist in Valerus, they will be skipped, even if changes were made to it, and show as an import error; new users will be imported successfully.
- Any new user created has a password of 1234 by default; it is highly recommended to force a change of passwords from the default. Click the button if this user should change the password from default after first login. Depending on your system policy, you can activate the change period and specify the number of days any password stays valid before the user has to change it (for example setting this to 90 days will make the system request a password change every 90 days). The specific user can be set so this account will expire after a certain date, for example for temporary staff, or it can remain Unlimited. If an expiration has been set, the user will no longer be able to log in past that date. An option to Enforce Complex Password is provided (see above).
- Assign this user to a role. The user will then have the privileges as those assigned to that role. A user can be a member of more than one role if needed.
- To add another user similar to the one just added (the same role), click Add New User again and repeat the process. This is meant to allow quickly adding all users that are members of a certain role together. If a new user for another role needs to be added, these additions must first be saved (Apply) and the add process repeated.

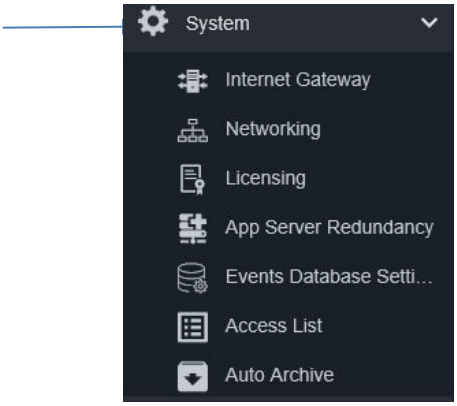
- Users can be deleted by clicking the garbage pail icon on the right or highlighting the user and clicking Remove User.
- When all new users in this role have been added, click Apply.
- As a shortcut to create new users, a new user with the same or similar details as an existing user can be created. Click on the existing user and then click Duplicate User. A popup box will display. Create a user name and fill in the name details if necessary. Click Apply and this user will appear in the list. Any detail can be changed as needed.



- If any user is selected and the details are changed directly from the User screen, press Save or Cancel these setting.

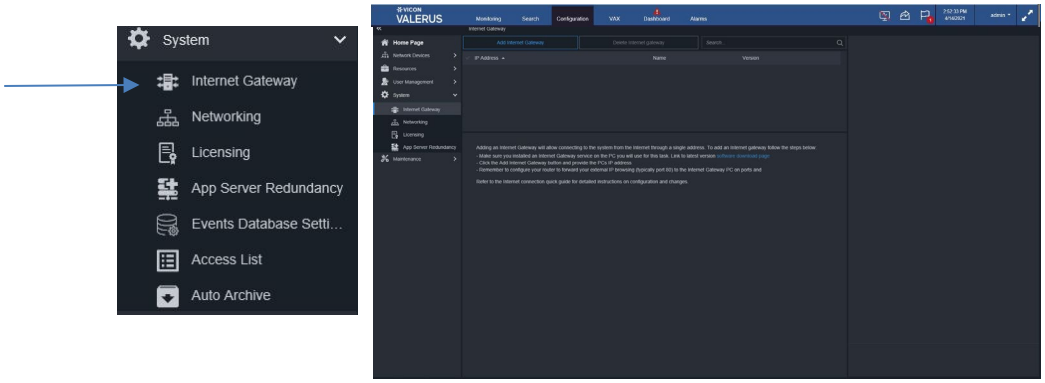
System

The System menus include general system settings and allow modifications to the workings of the system, including setting up an Internet Gateway, Networking, Licensing, App Server Redundancy and Events Database Settings menus. Additionally, an Access List can be created to restrict access to certain PCs.



Internet Gateway

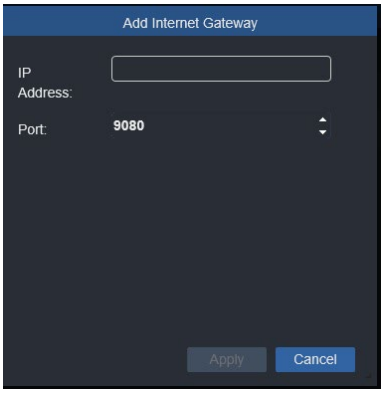
An internet gateway is a module that can be enabled in order to allow internet connectivity to the VMS. It controls traffic and acts as a single point of communication to all cameras in the system via the Internet network, instead of needing to configure access to each NVR and camera separately. The Internet Gateway needs to be connected to the Application Server and NVRs on one side and to the internet on the other side. Every connection to the Internet Gateway from the internet will be automatically redirected to the VMS system and returning responses and video is sent through the gateway to the requestor.



- Prior to configuring an Internet Gateway to allow such connectivity, the Internet Gateway module needs to be installed on the appropriate server. There is a link on the page to download the latest version if necessary. There are two typical configurations:
    - Internet Gateway on a dedicated PC (recommended) – The Internet Gateway runs on its own computer. This allows full utilization of the computer resources and also ensures that problems with the Internet Gateway do not affect other modules in the system.
    - Internet Gateway on the Application Server – If it is not desirable or possible to dedicate a computer for the Internet Gateway, it can be installed on the same server running the Application Server.

Note: See Internet connectivity best practices guide for further details on installation and configuration.

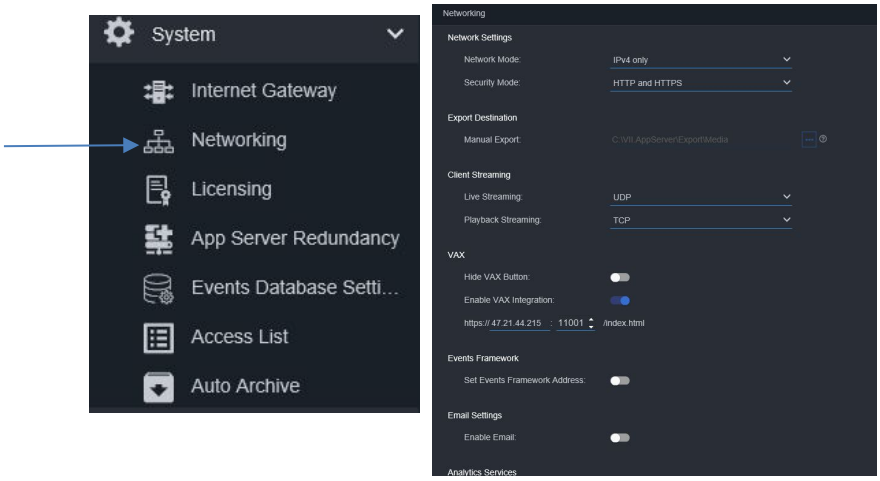
- Select Add Internet Gateway. A popup displays. Enter the IP address for the server that you installed the Internet Gateway on and the port number (default port is 9080).



- Click Apply or Cancel these settings.

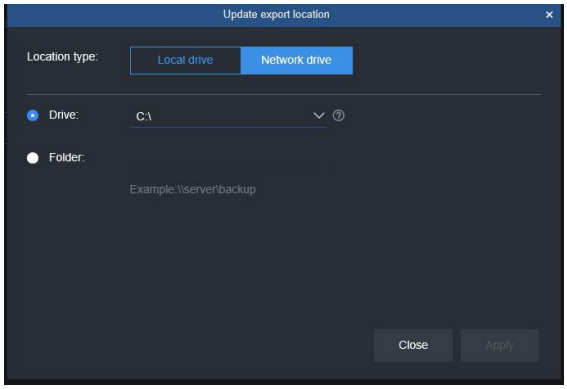
Networking

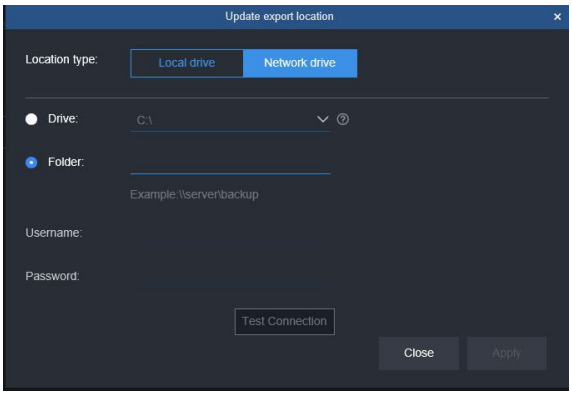
From this screen the system wide network behavior is set, and these are the default settings for the entire system. It will determine what protocols are used to stream live and playback video to and from the NVRs. TCP, UDP and HTTP are protocols used for sending data over the internet. This page is also used to configure Export Destination, connectivity to a VAX access control system and Email Settings.



Note that the Network Settings for Network and Security Mode must be set *before* setting the cameras, as they influence the NVR/camera display.

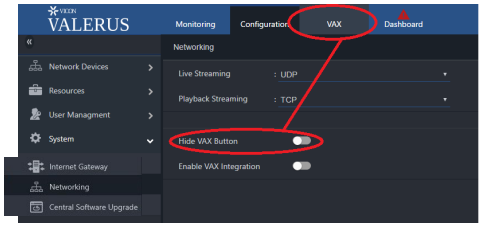
- Valerus supports both IPv4 and IPv6 address protocols. The selection here tells the Application Server which network will be supported, particularly if an NVR has more than one NIC; the unit will filter the addresses to pick from. Select the Network Mode, IPv4 only, IPv6 only or IPv4 + IPv6; the default is IPv4. Note that this affects what can be picked for the Cameras and Devices in Network Devices.
- The destination of exported video can be selected using the Manual Export. Click the icon to open a popup screen to define where the exported files should be saved. Included here is an option to map a network drive. In this case, Valerus uses a central location to store export files and share a NAS or drive can be used for this purpose. All exports are done by the server. Remember the Application Server must know this storage location, i.e., if a USB is selected it must be connected to the server.

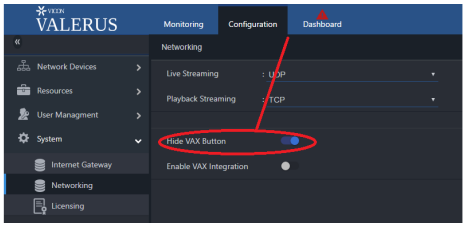




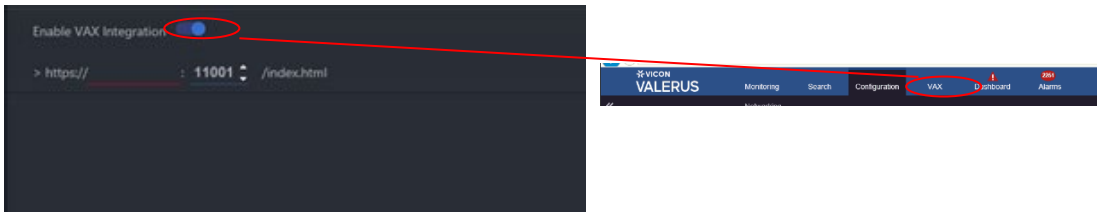
- Select Local drive or Network drive. If Local drive is selected, click Drive radio button and enter the local disk path. If Network drive is selected, select the Folder radio button and enter the User Name and Password.
- Mapping a folder allows mapping to any location that is sharable (NAS or drive on a PC). It requires a full network path to the folder, which must be limited to 40 characters, the username to connect and the password. This is similar to mapping a network drive in Windows; the user access must allow read and write permission.
- The Test Connection button is used to verify that the connection and authentication are valid. *Important Note:* When mapping multiple NVRs to the same storage device (typically NAS), the storage setting must be done as a single folder and not split between the different NVRs. Click Apply when finished.
- Valerus supports encrypted communication over HTTPS for added security. Select HTTPS only or HTTP and HTTPS; the default is HTTP and signed. Make sure your device is configured accordingly.
- Select the protocols to be used for Client Streaming, Live (UDP/TCP/HTTP) and Playback (TCP/HTTP). The default settings are UDP for live streaming and TCP for playback.
- If your system includes a VAX system connected to this Valerus VMS, do the following:
    - The VAX button (tab) on the Valerus interface can be hidden by selecting the Hide VAX button. This is helpful if your system will not integrate with VAX access control.
    - Click the Enable VAX Integration button to show the URL field.
    - Enter the IP address of the VAX server and change the port as needed.
    - Once configured, the VAX application tab on the top bar will be enabled (turn blue)

VAX Visible

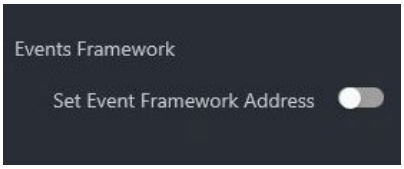




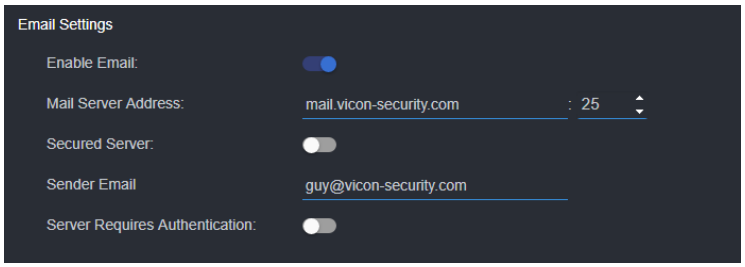
VAX Hidden



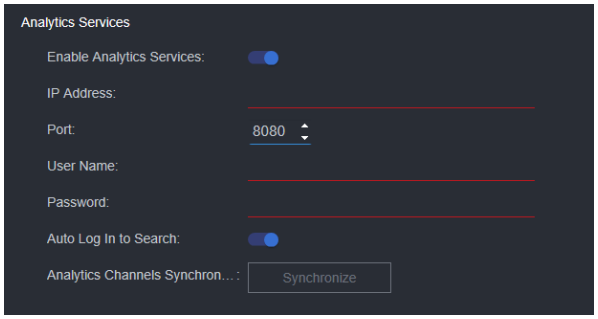
- If your system supports the Events Framework add-on, enable the settings by clicking the button and set the IP address and port.



- Click Save or Cancel these settings.
- Under Email Settings, Enable Email to connect to an email server, which will allow sending mail alerts as an action in Rules. Enter the Mail Server Address and Sender Email. Enable Secured Server and Server Requires Authentication as needed for your specific system. This must be done before the Send An Email option can be can be used as an Action.

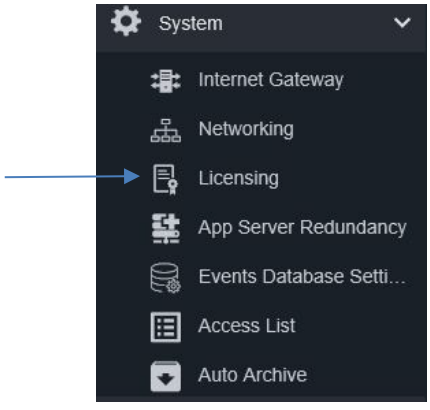


- Valerus SmartAnalytics requires a separate license. Analytics Services are enabled and configured from this screen. If your system has the SmartAnalytics add-on it is configured here.



Licensing

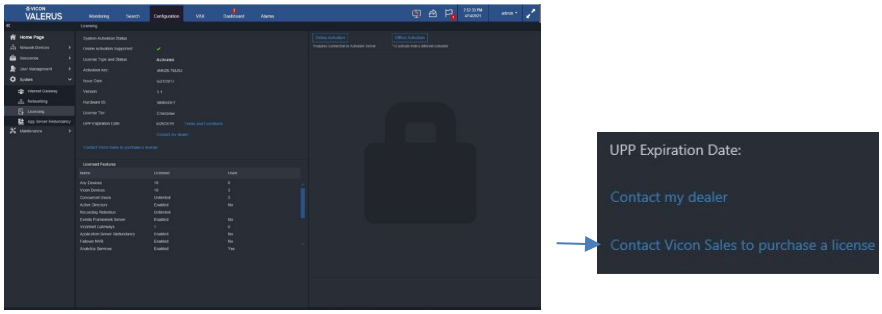
The Licensing screen shows the status of the current system. Online Activation requires access to the Vicon license server on the Internet; if you do not have access to the Internet, Offline Activation is also available.



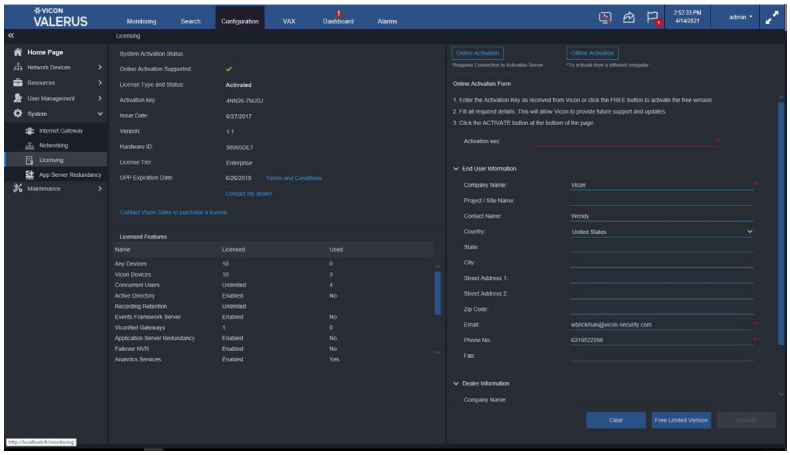
- A summary of the licensing status is outlined, including the license type and UPP if relevant.
- Activation can be done online or offline using the forms on the right. To activate online, the PC that Valerus is installed on *must* be connected to the Internet, at least temporarily.

Note: When initially installed, the Valerus system provides a 30-day evaluation period that is fully open. Within this time, the system must be activated with either the free (TRY) license or with a valid license purchased from Vicon (PRO or ENTERPRISE).

- If your system is not already activated, select the activation type, online or offline depending on the connection to the Internet server indicated on the left. A link is provided to see Vicon's Terms and Conditions. Additionally, there is a link to request a license.

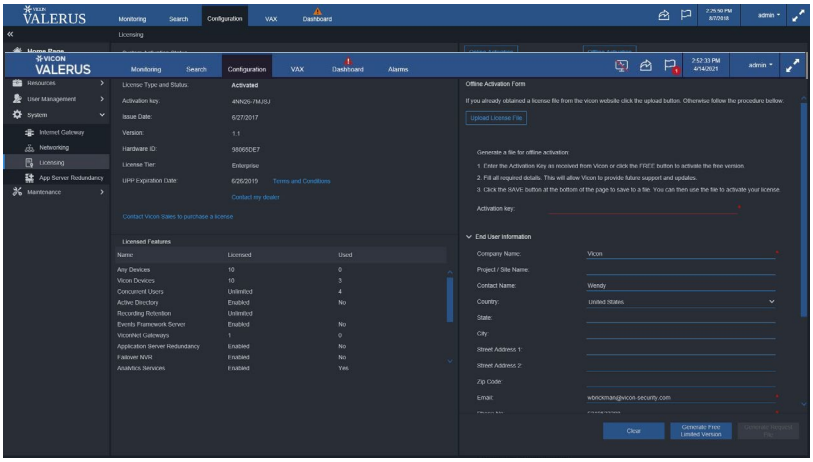


- For the Online activation process, click the Online Activation button and enter the unique Activation key you received upon purchase; this is the license for your system and will be used going forward. If you do not have an activation key and want to activate the free limited version (TRY), it will be available as an option at the end of the process. Complete the form as fully as possible and be sure to fill in any boxes with a red asterisk (*); note that the phone number should be entered without any dashes. Click Activate if a license has been purchased or Free Limited Version if this is how you want to activate; a Clear button is provided to erase the information entered on the form. You will now be connected to the Activation server that will complete the process.

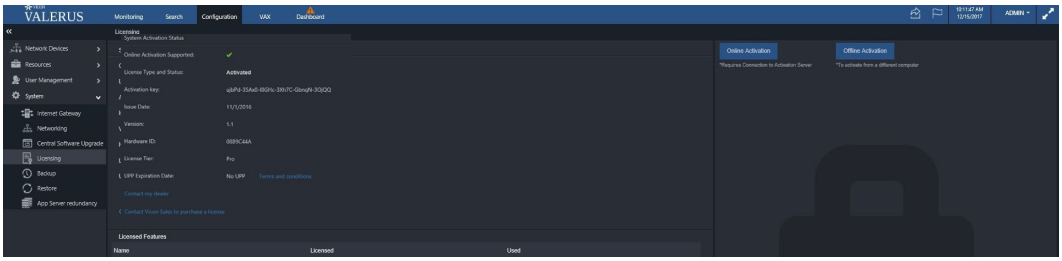


- For the Offline activation process, click the Offline Activation button and follow the procedure to generate a file that can be taken to another computer with Internet connectivity and activated through the Vicon website. Enter the unique Activation key received with your purchase or, if you do not have an activation key and want to activate, the free limited version will be available to you. To activate the free version, fill in the activation key Valerus.Free.1.1. Complete the form as fully as possible and be sure to fill in any boxes with a red asterisk (*); note that the phone number should be entered without any dashes. Click Generate Request File (the Free Limited Version button is for future use). A license request file will be generated and you will be prompted to download a file named ActivationRequest.dat; save the file to a thumb drive that will be used later on a computer connected to the Internet to complete the activation process.

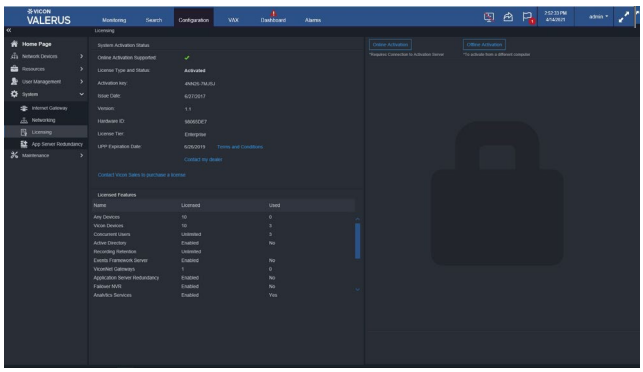
On the Vicon website, browse to the Valerus offline activation page (Support>Software Registration>Activate Valerus VMS Offline)) and follow the instructions; click on Choose File and navigate to the thumb drive with the ActivationRequest.dat file. Click Upload. Confirm your details to receive your ActivationResponse.dat file. When the license file is received, download and save it to the thumb drive. Now return to the Application Server with the thumb drive. On the licensing screen Offline Activation form, click Upload License File on the top of the page; select the ActivationResponse.dat file. Valerus will restart to complete the activation process.



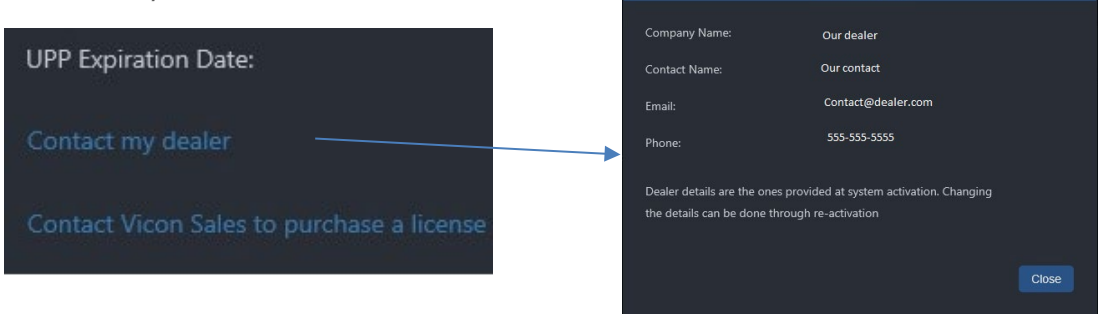
When a license expires, there is a notification on the Dashboard. Additionally, the Monitoring tab is no longer visible and the only Configuration page available is the Licensing page.



When a valid license is activated, the page will repopulate with all the correct information. A system Refresh may be required before the system is updated.



This page also provides a link to access your dealer information. This is a quick way to access dealer details directly from the system.

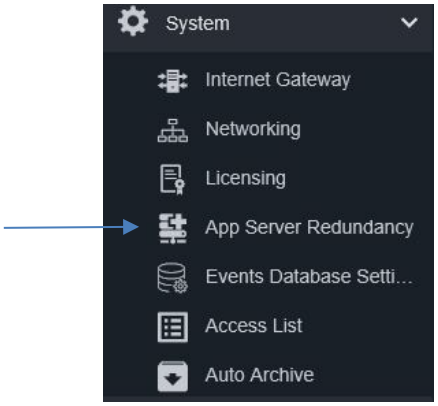


A list of Licensed Features provides an overview of the system capabilities and what is being used.

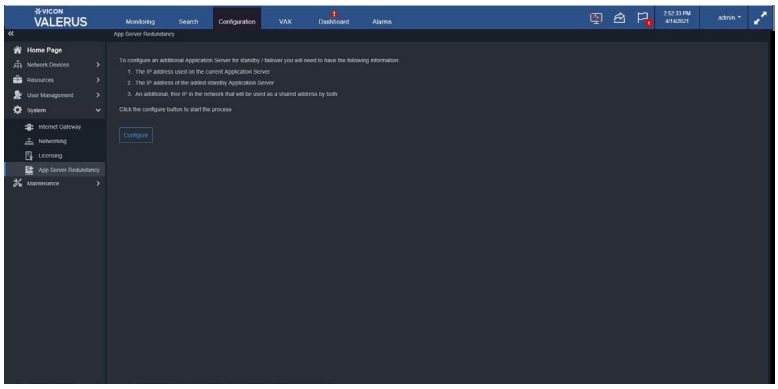
App Server Redundancy

The Valerus Application Server, which also functions as the web server, has a critical role in the system. Therefore, it is possible to add and define a redundant, backup server in the Valerus system in the event it experiences a failure. Once this backup server is defined, Valerus constantly replicates the system settings to this server. Note that this feature requires a minimum of Valerus version 18. This backup server remains idle until it is needed. Refer to the Application Server Redundancy Function section in this manual for how to activate the Redundant Application Server if needed.

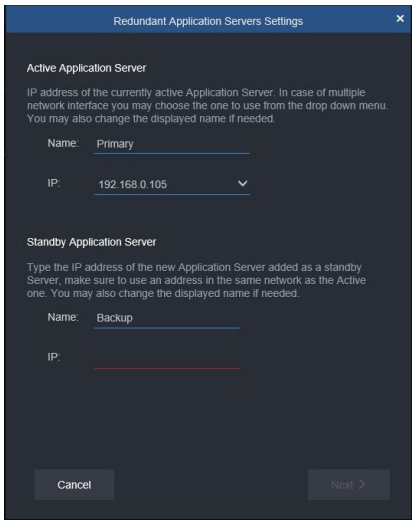
Note: In order to have a redundant Application Server, the system must be in the PRO or ENTERPRISE tier. A redundant Application Server license must be ordered. Two activation keys will be provided, one for primary and one for the secondary Application Server; these keys will have the same number, but the secondary will end with RED and cannot be used on its own.

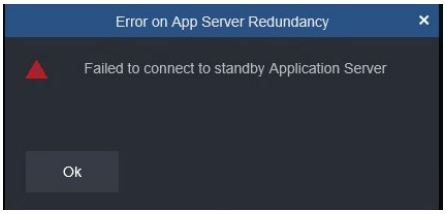


- Be sure to have the IP address of the current Application Server, the IP address of the secondary redundant server and a free IP address in the same network range at hand to setup redundancy.
- Click Configure from the opening Redundant Application screen. A Settings form will pop up.

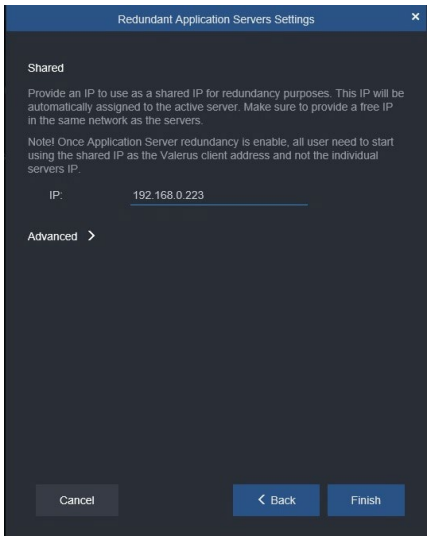


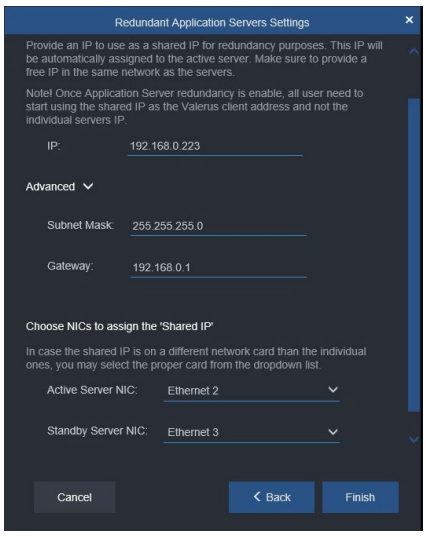
- The information on the active Application Server is filled in by default. You can enter a name for the redundant server (Backup displays by default but can be changed) and its IP address. Select Next. Valerus will attempt to connect to both servers and will send a notification if a problem is detected.



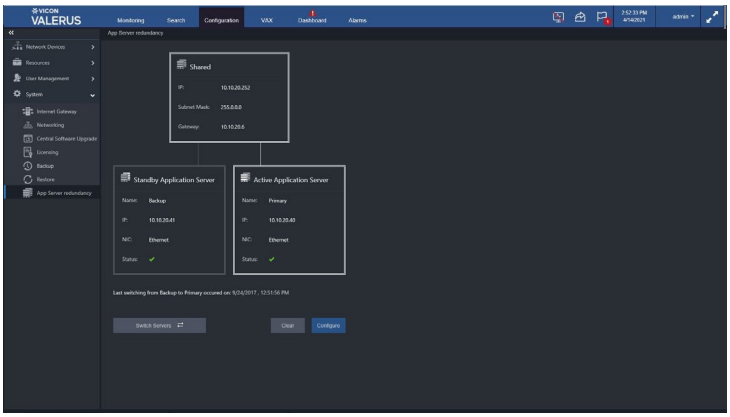


- Enter a Shared IP address; this IP will be used by the active server, whichever one it is, allowing Valerus users to always browse to the same address instead of having to know which server is active at any given time. This IP address must be a free IP on the same network as the servers. When entered, Valerus will connect to this IP. If the address entered is not valid, Valerus will prevent using this IP, so there will be no confusion. There is an Advanced tab provided in case the default settings need to be edited. Clicking it will allow you to modify the Subnet and Gateway addresses if needed as well as select the network if there are multiple network connections for the PCs.

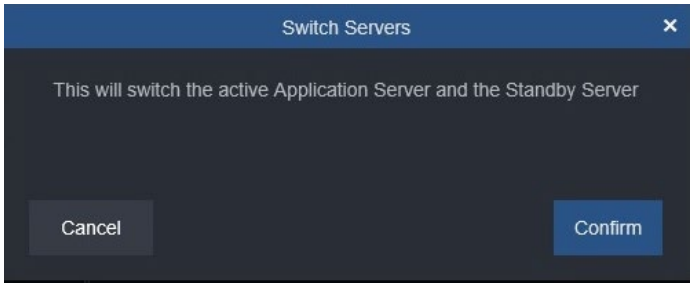




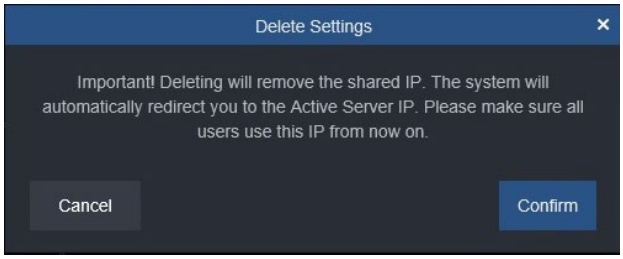
- Click Finish. Two servers, an active Application Server and a Standby Application Server, are now configured (both should have a green check mark indicating they are online and ready).



- You can switch between Application Server and Standby Server from this screen by clicking the Switch Servers button. If you want to switch, click Confirm on the notification. This option requires both servers to be online and cannot be used if one has failed.
- At this time, make sure to instruct all users to browse to the shared IP, and not to the server's assigned IP; this will ensure that on failure they keep their connection.



- If you need to delete the Application Server Redundancy, the shared IP will be deleted as well. The following message will display. Confirm to delete.

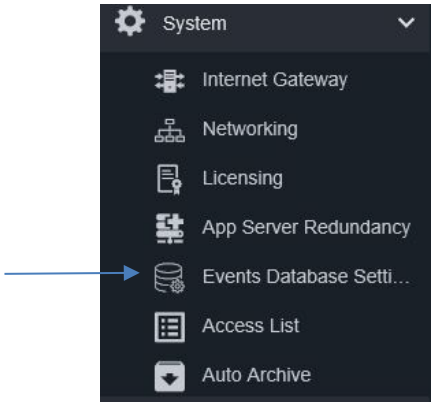


In case the primary Application Server fails, you will need to switch to the standby server from the actual server desktop. See Application Server Redundancy operation section.

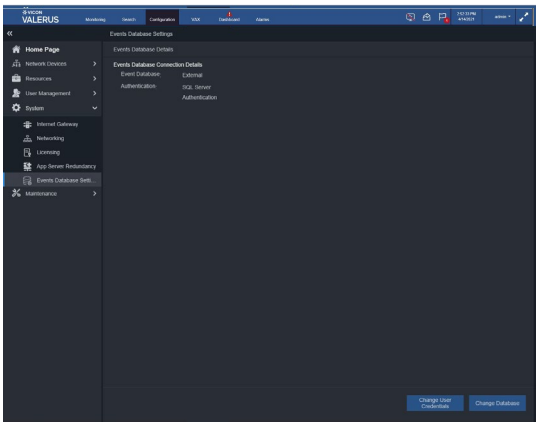
Note: Starting at Valerus version 20, an Events Database (Microsoft® SQL™) is included and installed on the Application Server by default. Valerus also provides the ability to connect to and use a different Microsoft SQL server for those who have their own server or want the database to run on a different PC than the one on the Application Server. To avoid the situation where, if the Application Server PC fails (and the Events Database along with it), the redundant server takes over and will not be able to access and save events, the Events Database **MUST** be configured to run on a separate unit that is accessible to both the Application Server and the redundant Application Server (the events will continue to be saved to that database). To change the location of the Events Database go to the configuration page; refer to the User Guide for details on how to do this.

Events Database Settings

Valerus includes the installation of a SQL Events Database onto the Application Server (version 20 minimum). This is a dedicated database for the storage of all events that occur in the system, both internal and external, including bookmarks. This is a Microsoft SQL server that includes a VII Operational instance. Only one database is required per system. If you want to change the database or change the user credentials, that is done from this page. If you want to use the preinstalled Events Database, nothing is required on this screen.

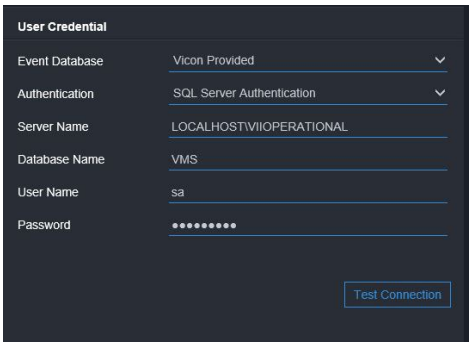


- Select Events Database Settings from the System dropdown. The following screen displays.

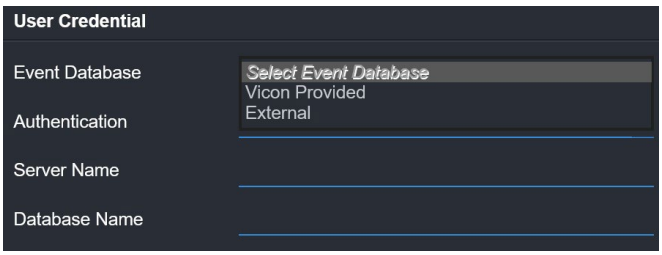


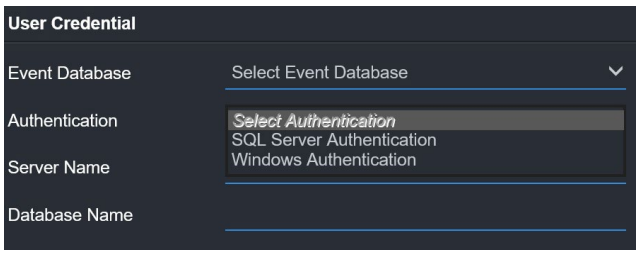
- For a typical system where the database is on the Application Server, if the user needs to define the database, the default settings are shown below.

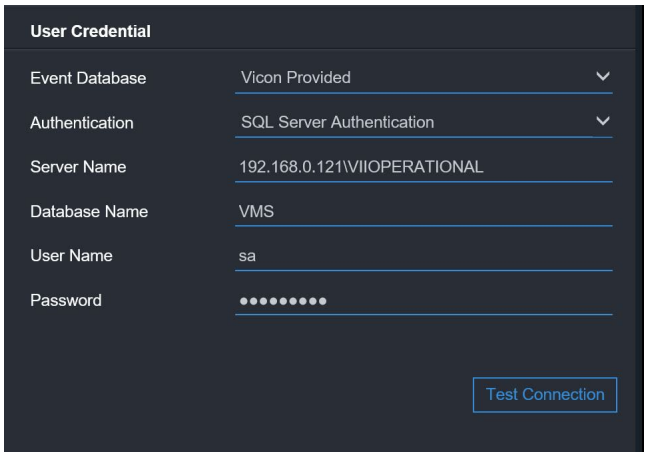
Default Events Database Settings:
Events Database: Vicon Provided;
Authentication: SQL Server Authentication;
Server Name: LOCALHOST\VIIOPERATIONAL;
Database Name: VMS;
User Name: sa



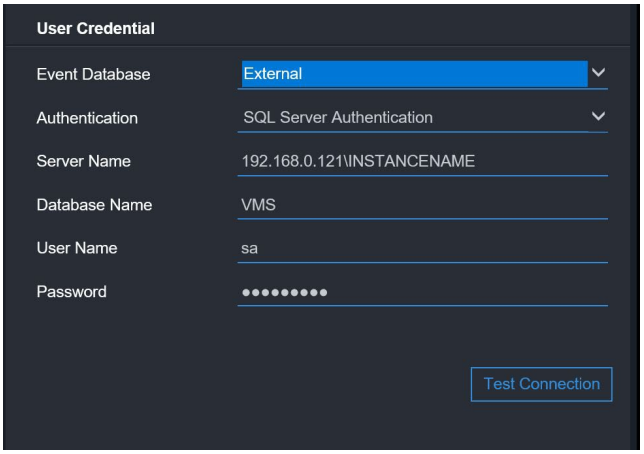
- Valerus provides the ability to connect to and use a different Microsoft SQL server for those who have their own server or want the database to run on a different server other than on the Application Server.
- Click Change Database if it is required to use a different database. The following displays. Select the Event Database type from the dropdown, Vicon Provided for a Vicon database installed on another PC or External for a customer-provided SQL server, and the Authentication, SQL Server or Windows. Enter a Server Name\Instance name and the Database Name: VMS. Refer to the manual on Creating Events Database for details.





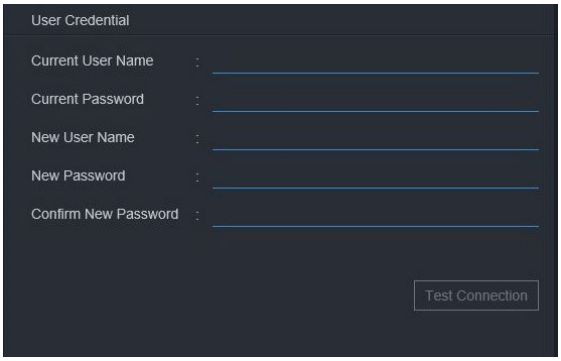


Vicon Events Database on Separate Server



Events Database on Customer-Provided SQL Server

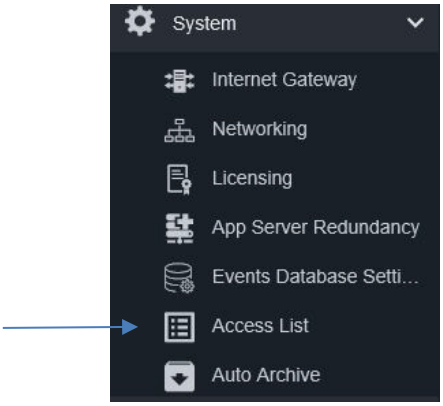
- A test connection button is provided to assure that the connection can be made using the details provided. Click Save when complete or Cancel to abort the change.
- Click Change User Credentials. The following displays. Enter the current user name and password and the new user name and password and confirm.



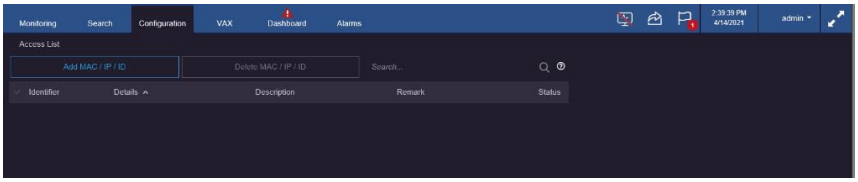
- A test connection button is provided to assure the connection to the database. Click Save when complete or Cancel to abort the change.

Access List

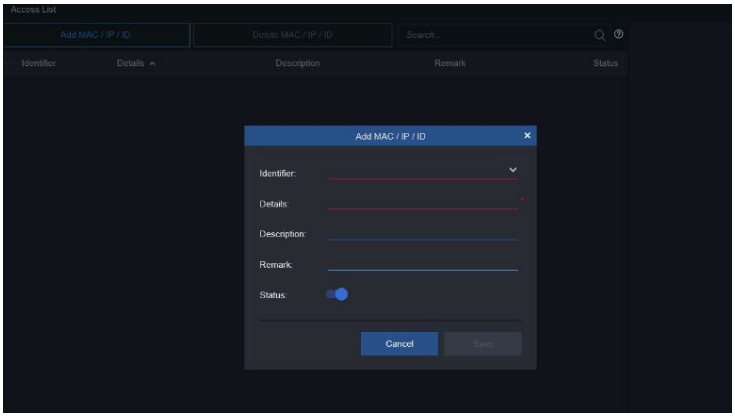
As added security in network management, Valerus' Access List provides the ability to restrict access to the system. From this screen, you can create a whitelist of computers that are permitted to have access to the system. Not adding any PCs to the Access List will allow any Client PC to connect. To limit access, add those PCs to the list; once a PC is added to the list, access will be limited to only those PCs on the list. The built-in ADMIN user can always connect from any PC, regardless of Access List configuration.



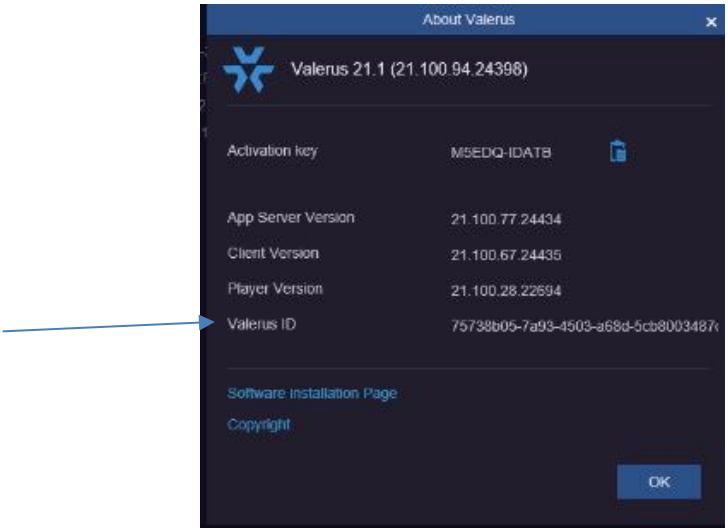
- Select Access List from the System dropdown. The following screen displays.



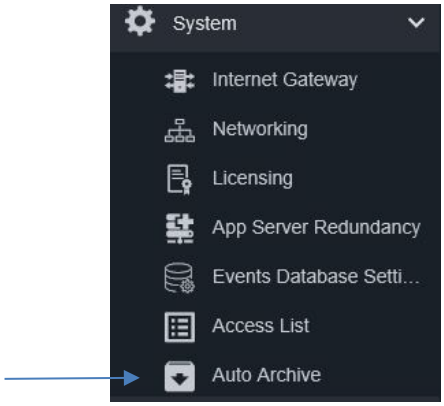
- Units can be identified by MAC, IP address or Valerus ID (see details on Valerus ID following). Click Add MAC/IP/ID button to add a PC to the Access List. The following screen will display. Be sure to add the correct identifier and detail or login from the Client PC will not be allowed, including the Application Server. Note that the limited access is based on the hardware, not the user.



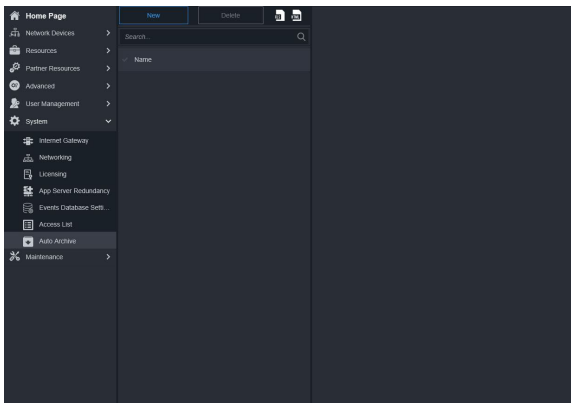
- Select the identifier, IP, Valerus ID or MAC address, and any details about this PC. A description and Remark can be added, as needed. Turn the Status on by having the button blue. Click Save or Cancel and the PC will not be added.
- If you want to remove a PC from the list, select the unit from the list. And click the Delete MAC/IP/ID button.
- If an unauthorized PC tries to login, a message will be sent to the Dashboard.
- Your Valerus ID can be gotten from the About screen. Valerus ID is an optional item that is set up from Advanced Monitoring. Refer to that section of the manual for details.
    - The Valerus ID used here for access limitation is a unique computer ID generated when the Advanced Monitoring service is installed and running on the Client PC. The ID will be listed in the About section of the User Settings. It can be used as an alternative to the IP or MAC.



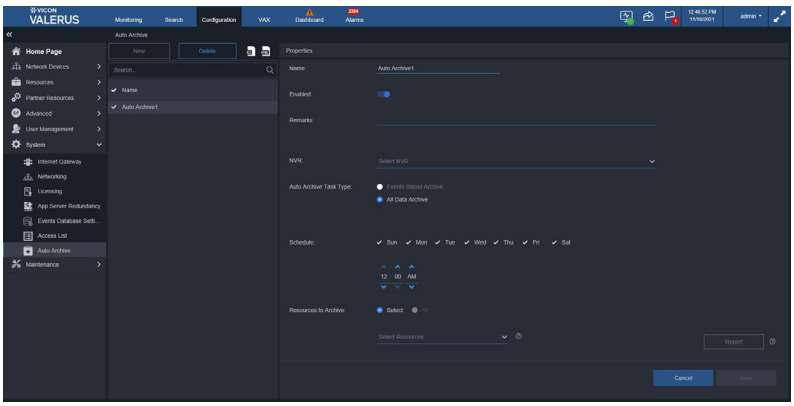
Auto Archiving



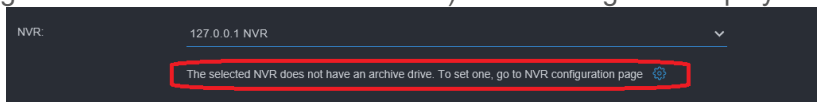
Valerus provides the ability to automatically archive video. Different than exporting clips, which results in a standard MP4 clip not part of the Valerus recording, the archive is a live repository in a secondary storage location and is managed by the same NVR recording to it (FIFO based on archive drive size).



- The method used for the archiving process is by defining separate archive “jobs” for each NVR. It is also possible to define different archive jobs for different NVRs and even for different cameras, as required. There are two methods supported for the archive jobs. Click New to create the “job” to auto archive.



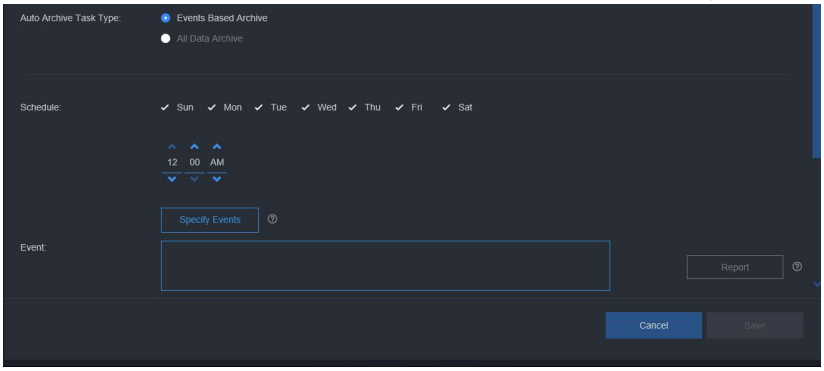
- All Data Archive: In this method, the entire recording is moved on schedule from the local recording location to the remote location. This can be a way to save on local storage and use less expensive NAS storage or as a means to move the recording to a data center for longer retention. In both cases, the NVR manages FIFO for local recording (ex., 7 days) and remote location (ex., 90 days) in parallel. Use the steps that follow to define an All Data Archive job.
    - Enter a name for the task, for example “NVR1 data.” As in any other Valerus screen, the specific archive task can be disabled or enabled and remarks can be added for any additional details.
    - Select the NVR that will run this task. Be sure that the NVR has its archive storage configured prior to setting the task (under Configuration – Network Devices – NVRs) or a message will display indicating to do so at this time.



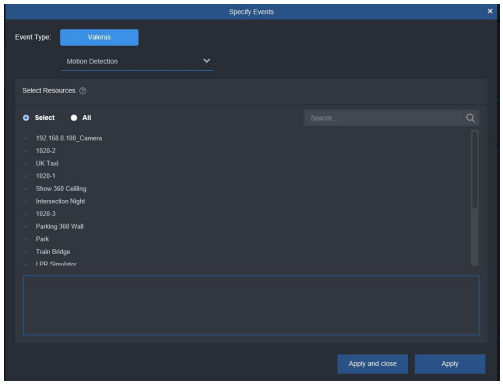
The destination storage drive that has previously been configured for that NVR will display; auto archiving can take place to the cloud storage (AWS/Wasabi) if that has been configured under archiving.

- Select if the task is for All data or for Events Based data (explained later in this section).
- Define the schedule that the task will start and run on. Best practice is to use a schedule that takes advantage of times when the network is relatively not busy, so the archive tasks can be completed without disruption; for example, running the task every day at midnight is a good way to utilize lower activity time.
- Define the resources on the NVR that are to be archived. This allows either selecting “All” or just specific resources recorded by this NVR if it is not necessary to archive all recordings; for example, only indoor cameras can be archived for longer retention while outdoor cameras only remain on the local storage.
- When complete, Save the task or click Cancel to remove the entry.

- Events Based Archive: This method allows defining the archive task around certain events that occurred in the system, for example only archiving events at the time of motion detection indoors or a digital input trigger when a door opens. This method provides a more granular archive, storing less data on the remote storage, which may allow longer retention for more significant recordings.
  - Select Events Based Archive to open the screen below for event configuration.



  - Specify the recorded events to be archived; the selection is similar to other Valerus screens that allow events selection. At this time, only native events can be used for archiving tasks; integrated partner events will be added in a future version.



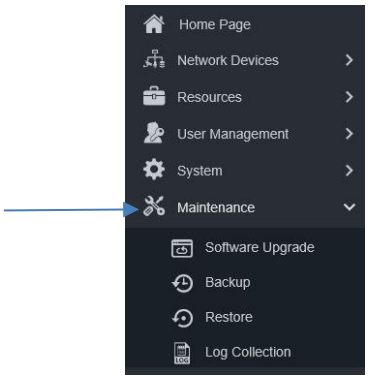
    - When selecting events, it is possible to select all or specific events.
    - The task will work for either event selected in a logical OR manner.
  - Define the resources on the NVR to be archived; keep in mind that if All events or multiple events have been selected, all the resources connected to any of those events will be archived. If it is necessary to define a more specific task, where certain events on certain cameras will archive certain channels, while other events on cameras archive other channels, make sure to define separate tasks accordingly.

- Select the pre and post event time to be archived; up to 60 seconds can be selected for each.
- The Report button on the bottom right is specific to each task and will only show when that task is selected. The report provides status of the task runs based on its schedule and also allow relaunching a task that failed.
- The Report buttons at the top produce a report related to all archive tasks.

- Important: The Auto Archive mechanism includes handling of failed events, for example when remote storage is unreachable, and will provide Dashboard notifications as well as retry to complete the task on the next schedule. Using the archived video for playback and searches does not require any specific configuration and is handled by the NVR automatically. The playback will be retrieved from the local or remote storage as if it is one recording location, as long as the NVR has access to the storage.

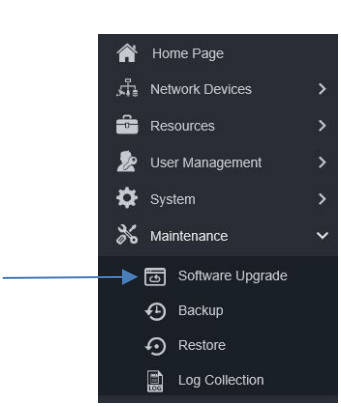
Maintenance

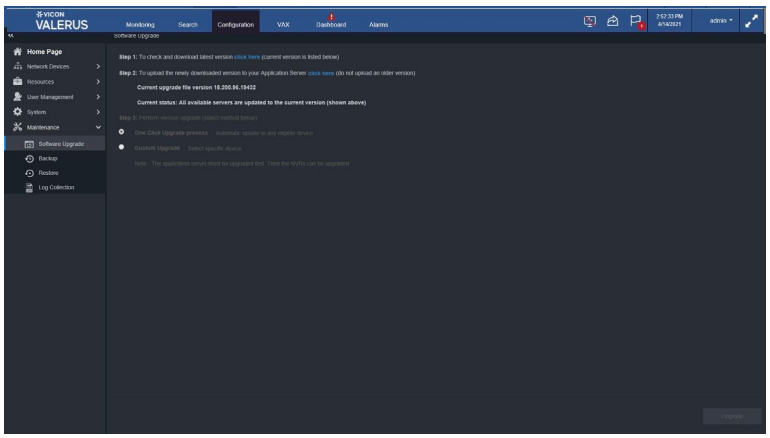
The Maintenance section provides menus that allow the user to keep their system updated, configure backup schedules and locations, restore or replace a server and collect system logs that are useful when troubleshooting.



Software Upgrade

The Software Upgrade screen provides a simple three step process to upgrade the system to the most current version. This download can be done from any client and then uploaded and pushed to all servers on the system. Note that this is only available for Valerus version 1.2 and higher.





- Step 1 is to check for the latest version; a link is provided to Vicon's website to review and download it as necessary.

  Note: There is a Current status notification on the screen that lets you know if all servers on the system are up to date; in this case, up to date means that all servers in the system are at the latest version of software that is ***on*** your system. There still may be a more current version posted on the Vicon website. There is also a message indicating that an NVR is running a newer

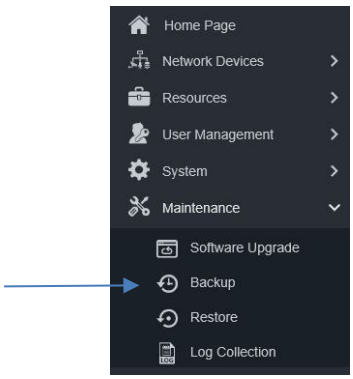
version than the system; this alerts the availability of a newer version. Also remember that you cannot downgrade your system to a lower version of software.

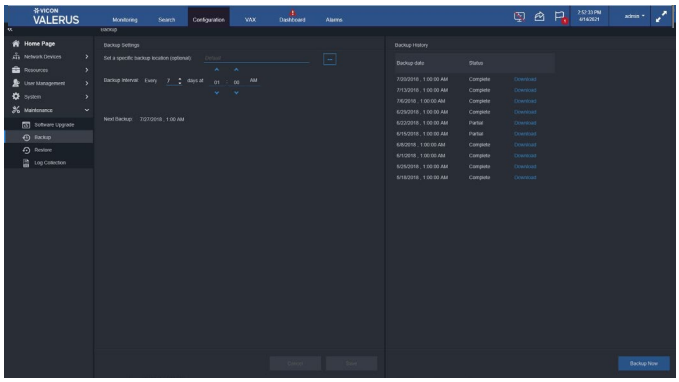
- Step 2 provides a link to upload the most current version downloaded in step 1 to the Application Server.
- Step 3 offers two methods of upgrade, a simple One Click Upgrade process that will upgrade all appropriate servers or a Custom Upgrade that allows the selection of specific servers to upgrade. It is important to remember that the Application Server must be upgraded before any NVR in the system is upgraded. Once uploaded, the new current version will display. Select the method that suits your needs.
- Click Upgrade. The system will go through the upgrade process. At the end of the process, servers will restart (reboot). You can go to the NVR screen to confirm that the new version is on your system.

  Note that in systems that include remote NVRs over a slower connection (Internet or similar), performing a remote upgrade on those may fail and upgrading on them should be done locally.

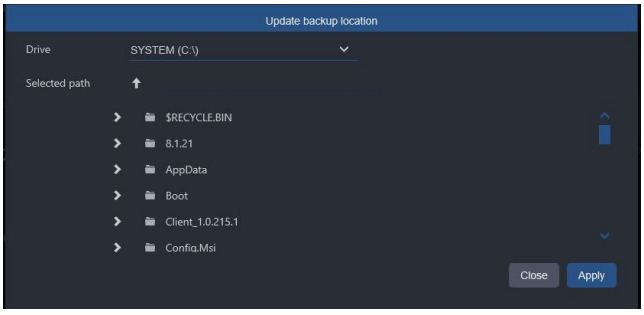
Backup

The system Configuration settings can be backed up in the case that a server fails or a new server replacement is being added to the system that will use the same settings. By default, the system is set up to backup settings every 7 days to the Application Server, but this can be customized. It is important to remember that it is the system settings that is being backed up, *not* recorded video, and this is for the full system, not just the unit you are working from.





- If you want to select a location for the backup file other than the default, click the three dots next to the field. There is a default location on the Application Server or select any location desired, including a USB drive. The screen below displays. Select Local drive or Network drive from Location type. From Local drive, select the path from the list provided. From Network drive, select Drive or Folder; for Drive, select a drive from the dropdown; for Folder, enter the folder location and its username and password. A Test Connection button is provided to confirm selections. When selections are complete, click Apply.



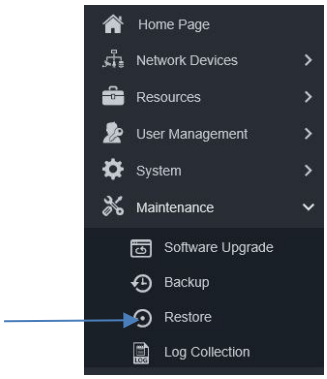
- Set the Backup Interval, in days, and a convenient time for the backup. There will be a display of when the next backup will occur.
- Use the buttons provided to include Procedures Data and Integration Partner Data.

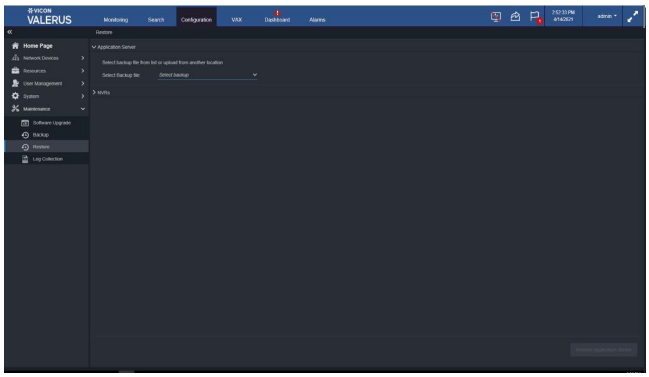
- Click Save to save these settings or Cancel the settings.
- Additionally, the screen provides a list of Backup history, and these can be downloaded as needed. Click the download link. A total of 10 backups will remain in history and be replaced FIFO.

- If it is required to backup immediately, for example if you recently made important changes to your system, there is a button provided to Backup Now.

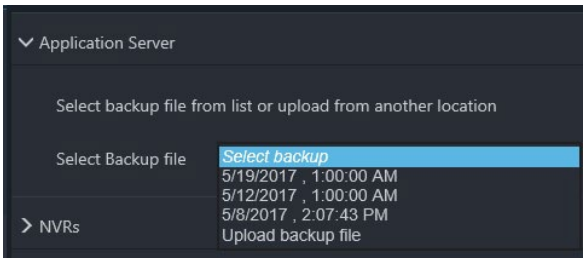
Restore

If a server fails, it can be restored or replaced. An Application Server can only be restored; an NVR can be restored or replaced. Using Restore will go back to the last known working (good) settings. Replace is used if a unit needs to be physically replaced because it has stopped functioning properly; the new NVR will have all the same settings as the unit being replaced.

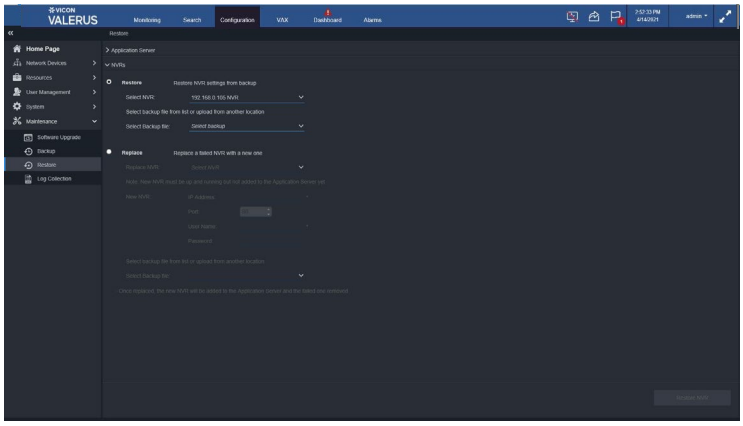




- To restore an Application Server to previous settings, select the backup file from the list provided (the list will include files saved on a network drive) or from the location the file resides; you can use a file that is stored elsewhere that is not on the list (i.e., USB). Click Restore Application Server.



- To restore an NVR to previous settings, select the NVR from the list and then select the backup file from the list provided or from the location the file resides. Click Restore NVR.

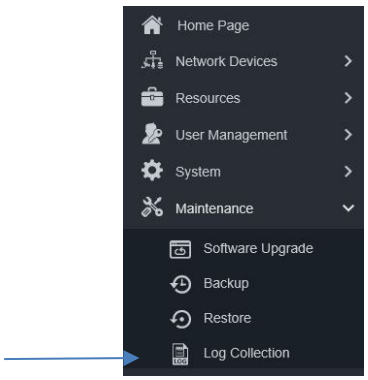


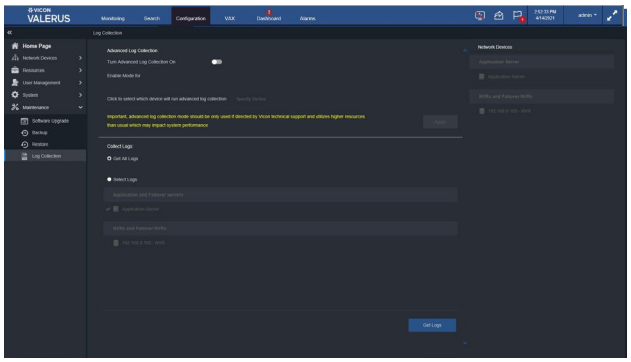
- To replace a failed NVR with a new NVR, connect the new NVR to the network (providing an IP address) but do NOT add it to the Valerus VMS; the new NVR will take on the identity of the failed NVR.

- Select the NVR to be replaced (unhealthy NVR); the list will only show NVRs that are currently offline (broken). Enter the IP address, port information, user name and password for the new NVR. If you accidentally enter an IP address that is already on the system, it will be blocked, preventing replacing a healthy NVR. Then select the backup file from the list provided or from the location the file resides.
- Click Replace NVR. The new NVR will be added to the Application Server and the failed NVR will be removed. The NVR will now have the exact settings as the unit replaced.

Log Collection

The Log Collection option allows the retrieval of system logs from all Valerus PCs without any special tool. An advanced logging tool helps in troubleshooting.



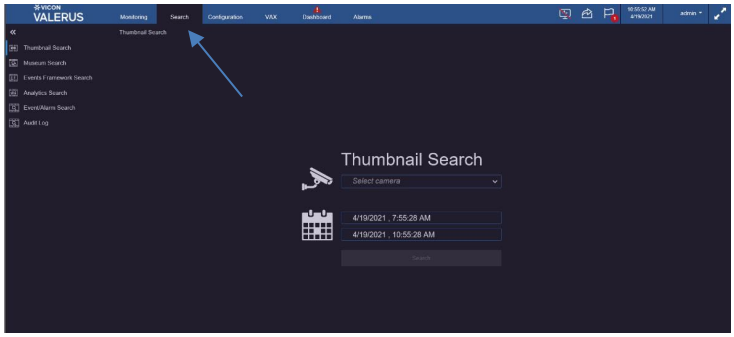


- The Advanced Log Collection can be turned on by clicking the button to enable it (turns blue). This function should ***only*** be used if directed to do so by Vicon Technical Support and should only be enabled for a limited amount of time that is set using the Enable Mode for button, as it uses an increased amount of resources utilization on your system. Select which device will run the advanced log collection by clicking Specify Device. Click Apply.
- From the Log Collection screen, select either Get All Logs or Select Logs.
- If Select Logs is chosen, choose the unit(s) that logs are needed from the Application and Failover servers or NVRs and Failovers NVRS.
- Click the Get Logs button at the bottom of the screen.

Search

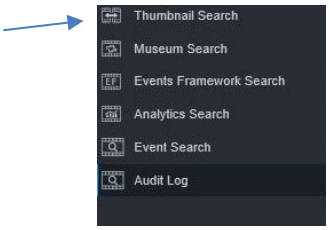
Valerus provides six efficient search tools to find recorded video, Thumbnail Search, Museum Search, Events Framework Search, Analytics Search, Event/Alarm Search and Audit Log. The video from these searches can then be easily exported from the Search interface. You can also get to the Search menu by right clicking on the device in the Resources list from the Monitoring screen. Note that if a pixelated privacy mask has been created for a resource, it will display as a gray box in Thumbnail and Museum Search result pictures but will be pixelated in the playback video.

Note that Thumbnail Search is included with all versions of Valerus; Museum Search, Events Framework Search, Analytics Search, Event/Alarm Search and Audit Log are Valerus PRO/ENTERPRISE features. Also note that Events Framework and Analytics are add-ons that require an additional license.

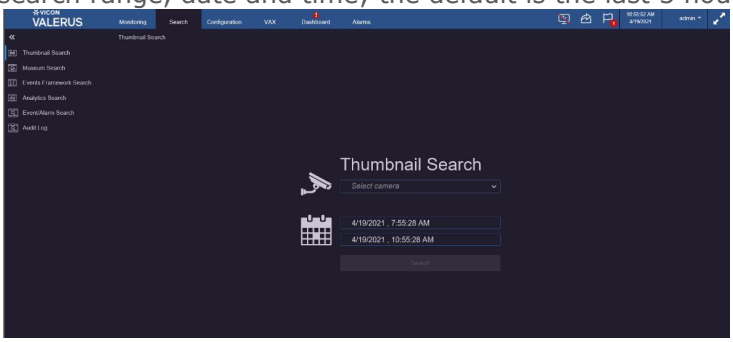


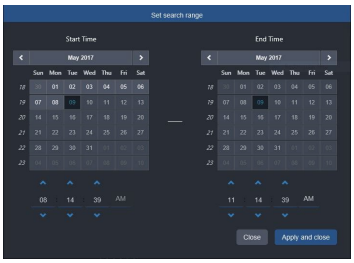
Thumbnail Search

The Thumbnail Search provides the ability to search a selected video segment from a specified interval of time for an exact clip of video. It provides a visual comparison between images along a timeline.

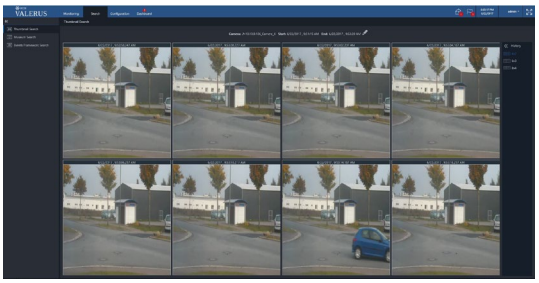


- From the Search screen, select Thumbnail Search.
- From the dropdown, select the camera you want to search for video on. From the calendar, select the search range, date and time; the default is the last 3 hours. Click Search.

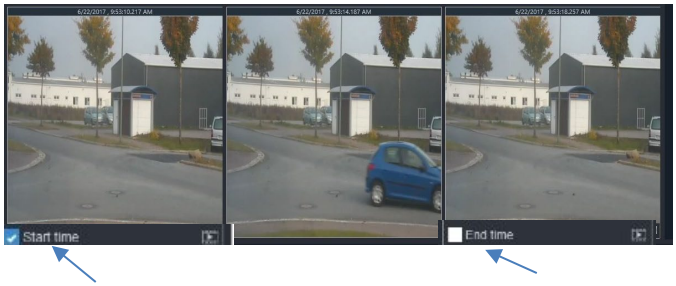




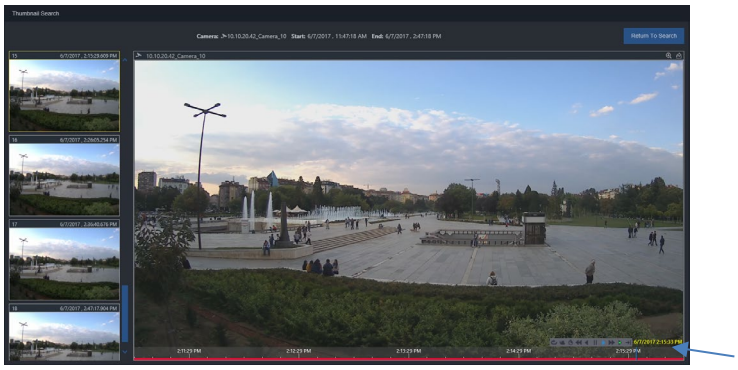
- A selection of video will display evenly distributed over the selected search time frame. The screen display format can be selected from 4x2, 6x3 (default) or 8x4.



- The search range can be narrowed by checking Start time and then End time on selected thumbnails. If you want to search between two adjacent thumbnails, click the Quick Cursor arrows symbol between the thumbnails. The thumbnail search will redistribute the same number of thumbnails over the smaller time range.



- Once the search is narrowed down, and the video you are looking for is found, double click on its thumbnail view or click playback to see it in a larger display. The remaining thumbnails will display in a list on the left side of the screen. Click on the playback symbol or double click in the list to display the video. This video opens up in playback at that time and can then be viewed and controlled as any other playback, including digital zoom and export of video using the icons in the right corner.

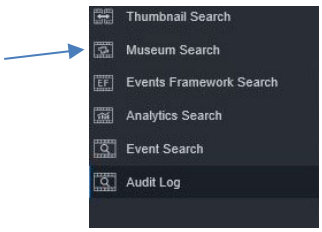


- Click Return to Search to go back to thumbnail view.
- To view a record of your searches click on History on the right side of the screen to review previous searches on this camera. Click again to collapse the list.

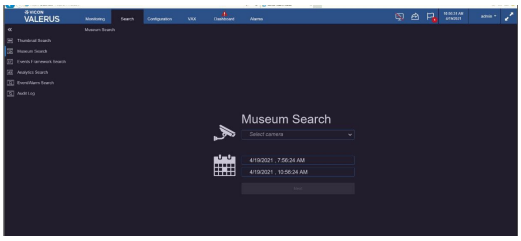
- Any time the search parameters need to change, click the pencil symbol next to the current camera search at the top of the screen.

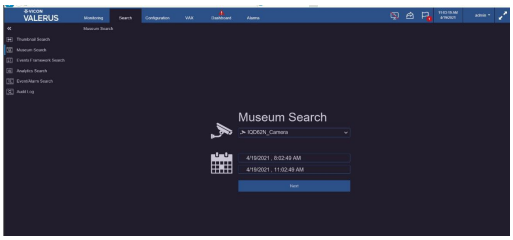
Museum Search

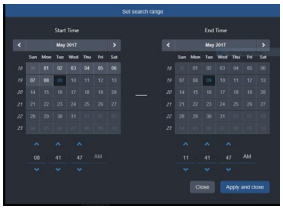
The Museum Search provides an accurate search for changes in a defined region of interest (ROI), such as a door opening or an object disappearing, reducing the time it would take to look through the entire database for the specific video needed. This is a special feature in Vicon cameras equipped with a unique algorithm to allow the search.



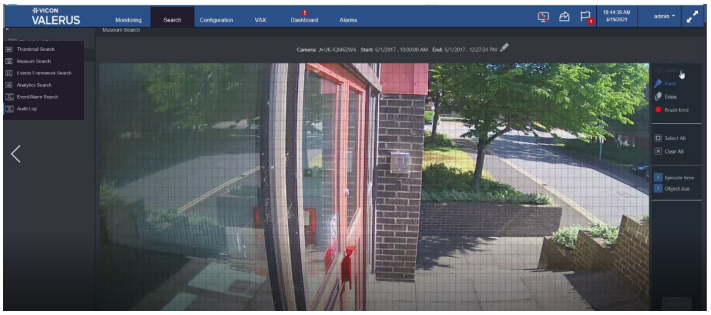
- From the Search screen, select Museum Search.
- From the dropdown, select the camera on which you want to search for video; note that the camera list will only display cameras that have the museum search capability. From the calendar, select the search range, date and time; the default is the last 3 hours. Click Next.

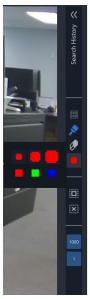




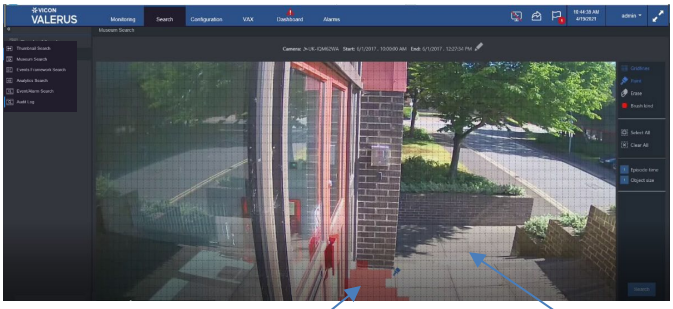


- A view from the camera will display. A list of tools will display on the right side of the screen for grids, paint, erase and brush options. Additionally, there is an option to select the entire image or clear the image of all selections and select the episode time and object size.

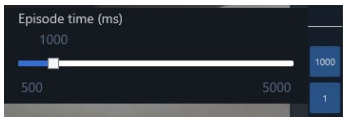


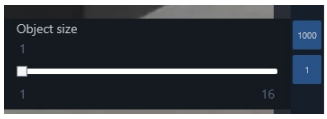


- Click Grids to toggle between viewing gridlines on the image and turning them off. Select a brush kind (color, size and shape) and then select the region of interest using the paint tool. Different colors can be used to highlight specific regions. Use the eraser tool to remove an area from the region of interest.

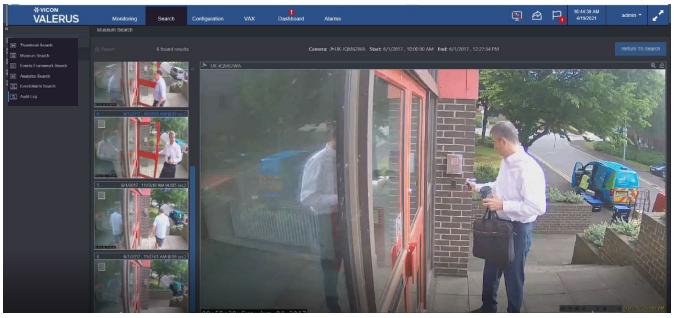


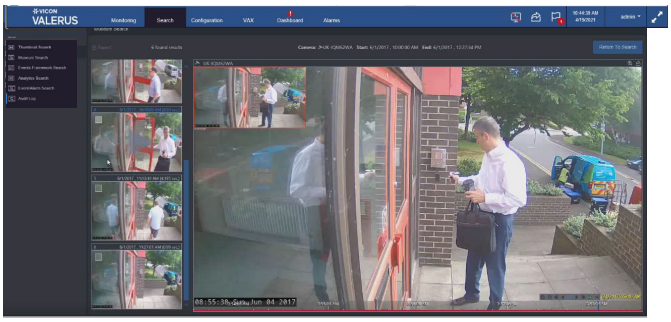
- The parameters of the search can be fine-tuned using Episode time and Object size sliders. The Episode time defines how long changes in the ROI have to occur to be considered an episode. Define the object size to define the sensitivity of the detection, how many blocks have to be involved before detected. The smaller these numbers, the more episodes will be detected.





- Click Search. Video from the selected time will display in a list 25 images at a time. Click the specific video to display and playback will start in the large display area. This can be controlled as any other playback video, including digital zoom and export of video using the icons in the right corner.





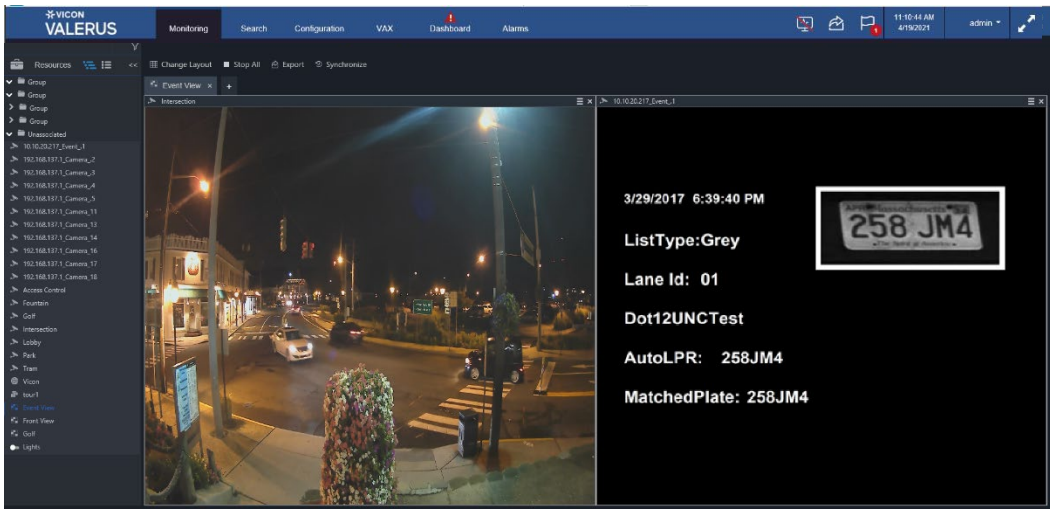
- Click Return to Search to clear the list of images and return to the original video.
- The search can be changed by clicking the pencil symbol next to the current camera search at the top of the screen.

Events Framework Search

The Valerus Events Framework is an add-on to the Valerus system that allows it to integrate external partners' systems and brings their event data to the VMS as a video feed that will be presented in a tile like any other resource. Using the Valerus Events Framework, Vicon offers a way to receive the different events (possibly from different systems), feed them into a common database so they can be searched later, and instead of having the VMS process the text and pictures, cope with overlaying it on video, etc., the framework wraps the event data as a video stream that the VMS can display like any camera in different tiles and views. By wrapping the event data as a video stream, the event becomes a resource in the Valerus VMS, just like video, audio, web and other channels and can be viewed live if needed, recorded and playback, and most commonly, used to call up as a result for an event query.

The Valerus Events Framework consists of three components: the VEF Server (module, usually running on the Application Server; it also holds the VEF license); the VEF Streaming Engine, a dedicated PC(s) that can handle up to 16 integration points; and the VEF vendor driver, a specific driver for the integrated vendor that runs on the VEF streaming engine; multiple vendor drivers can run on the VEF streaming engine. The VEF Streaming Engine is added manually in the Cameras and Devices Configuration screen. Refer to Configuration, Resources. Refer to the specific manual on the Valerus Events Framework for details on how it works.

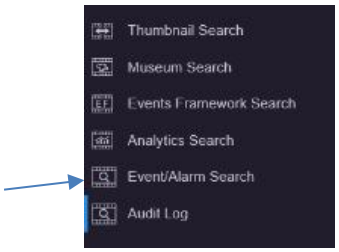
The Events Framework Search allows you to search for video clips and associated data that's been captured through a Valerus/third-party integration, for example License Plate Recognition.



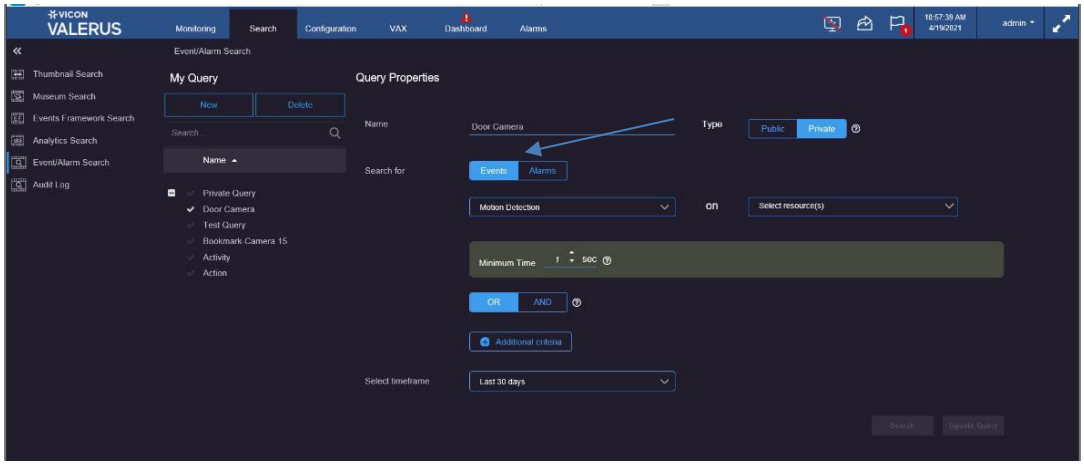
Event/Alarm Search

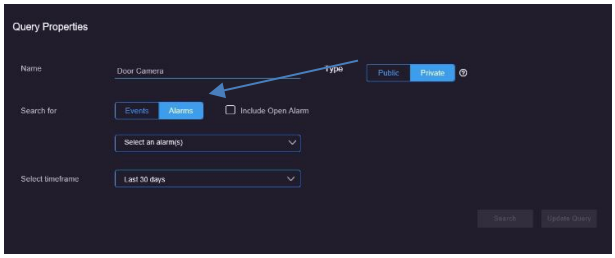
The Event/Alarm Search allows you to find any event that has occurred in the system, including bookmarks. These events are stored in the Events database in Valerus. Queries are defined to search for specific events in the storage database. ***Refer to the Alarms Management Guide for details on Alarm Search.***

- From the Search screen, select Event/Alarm Search.

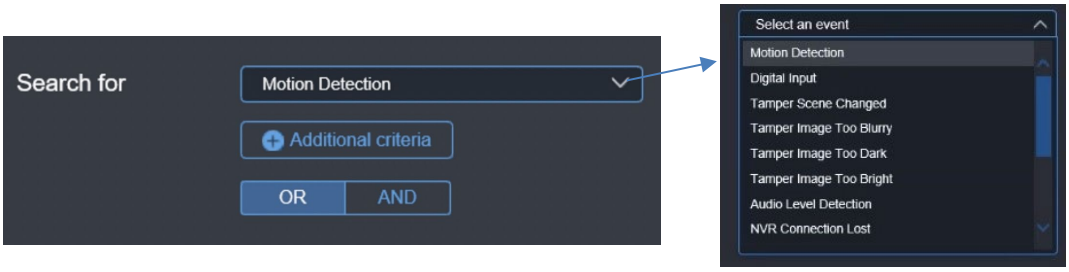


- The Query screen displays. From here a new query can be created or an existing query can be used to initiate a search (My Query). The query selects an event or alarm type on selected resource(s) at a defined time.

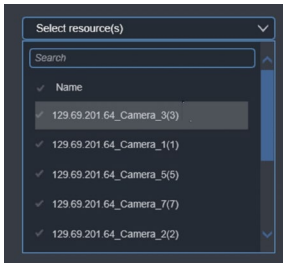




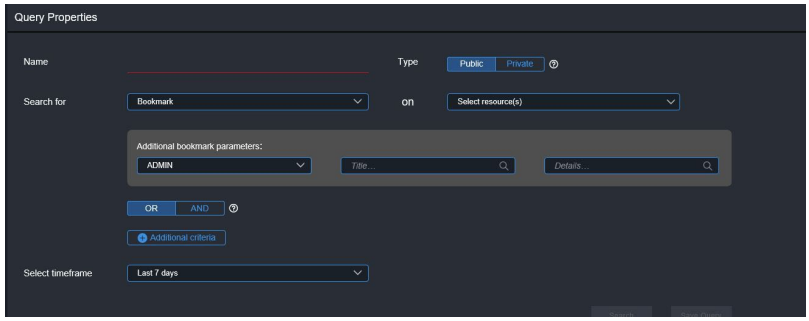
- Click the New button. From the *Search for* dropdown, select either Events or Alarms button. Then select the Event type or Alarm from dropdown lists; multiple event types can be added by clicking the Additional criteria button. For multiple events, the query must be made even more specific by using the AND/OR function to include a combination of events (AND) or any from among the selected events (OR). For Alarms, typically, this search is used to review historical alarms that have been closed, as the open alarms show on the Alarms Management screen; however, if there is a need to include the open alarms as well, check the box provided.



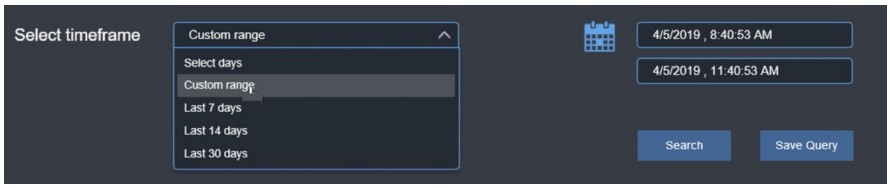
- For Events, from the *Select resource(s)* dropdown select the device(s) to search when the event(s) occurs. Multiple resources can be selected; click Name to select all for convenience if every device on the system is to be included in the search. For an LPR or VAX event, there is an *Advanced Filters* button that allows you to refine your search (including respective parameters for LPR Event search and VAX Event search).



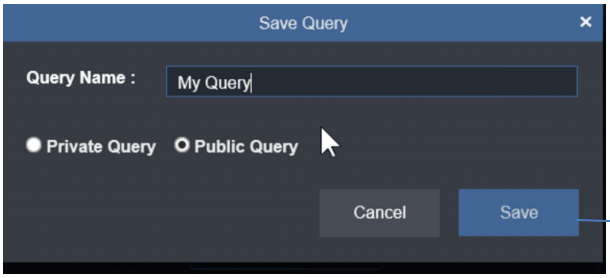
- When the event is a bookmark, you will also add in the parameters of who created it (a list of users is provided) and their title and details of the bookmark.

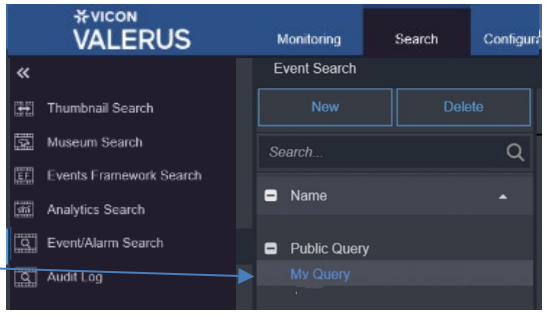


- From the *Select timeframe* dropdown list, select the number of days in the past you want to search. If a custom range is selected, a calendar will display to select the specific day and time for the search.

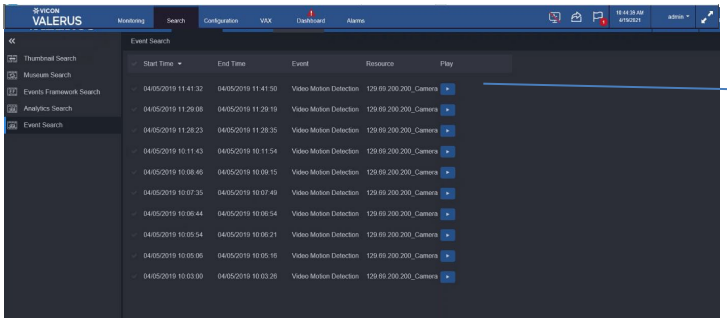


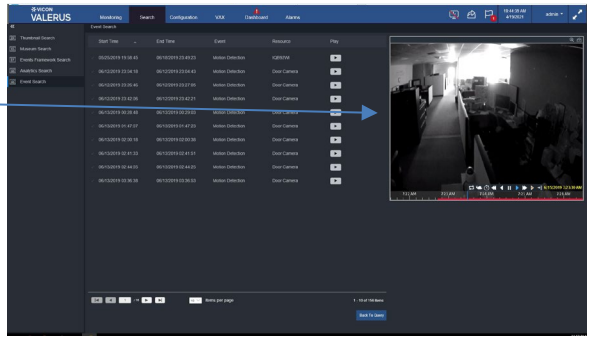
- After all the details are completed, click Save. The Query can be given a name and be made Private, for use by only this user, or Public for anyone on the system to use. Click Save or Cancel if you do not want to save this query. Once it is saved, it will be listed on the Event/Alarm Search page.



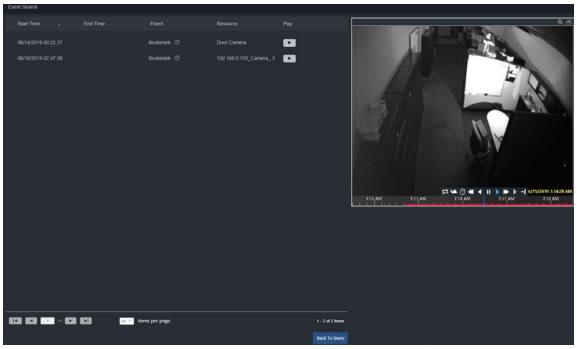


- Any query in the list can be selected and searched for. After the search is performed, a list of events displays. Each event can be selected and the video/audio played back for cameras and microphones; up to six (6) playback windows can display where AND queries were used. There are arrows at the bottom of the screen to page through all the queries. A button to go back to the query is provided. A report can be exported, in Excel or HTML format, to have a record of these events. Additionally, after selecting and playing an alarm/event, a Snapshot, Bookmark and Export (video and audio) can be created and is supported by the player.





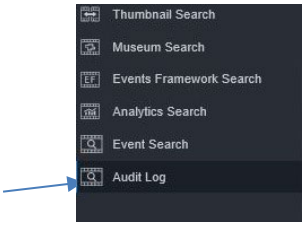
Playback of Bookmark



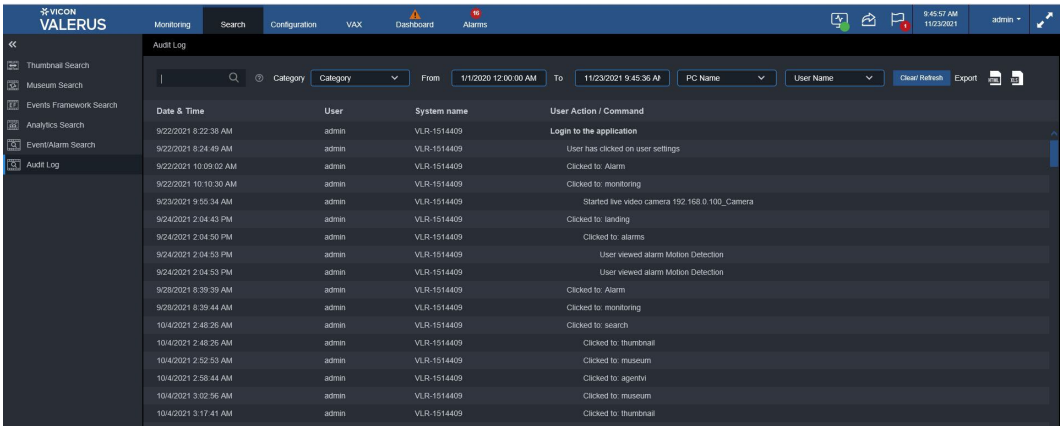
Audit Log

The Audit Log keeps a record of all actions that take place. This includes the information from Alarms Management, when the alarm occurred, whether it was handled, etc.

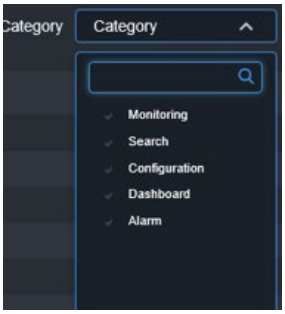
- From the Search screen, select Audit Log.



- From the Audit Log screen, select the From/To time frame to display the actions.



- Entering text in the Search field will perform a search for that word in the audit log. Search can be filtered by date/time, PC or User.
- A dropdown list is provided under Category for search, including Monitoring, Search, Configuration, Dashboard and Alarm. That category will be automatically selected when accessed from the Activity Map on the Dashboard or can be used directly on the audit log. The audit log allows selecting start and end times of more than 24 hours when doing a category search.

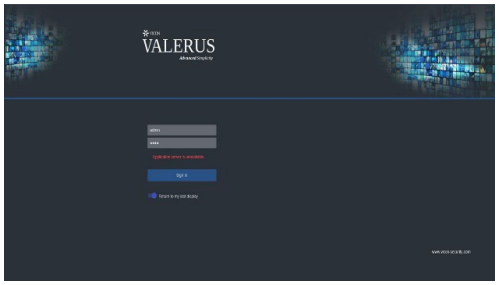


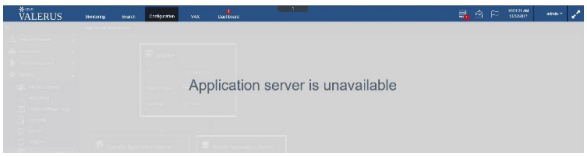
  - Select the PC Name and User Name from the dropdown lists.
  - A report in HTML or Excel format can be generated and exported for your records.
- Click Clear/Refresh to return to update the page.

Using the Application Server Redundancy Function

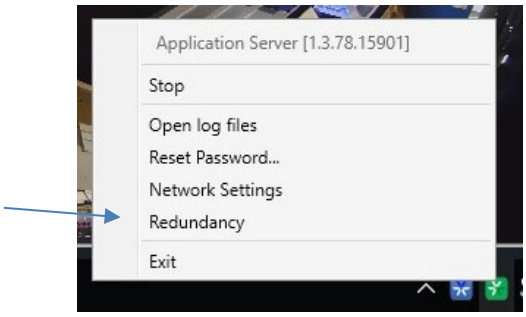
If the Application Server fails, it will be indicated on the interface with a red X on the Application Server icon at the top of the interface. After the switch is made to the redundant server, an icon will display to indicate that the system is working on the secondary server.

Any user already logged in while the server failed (and the redundant has not been activated) will remain logged in to the functioning Valerus system, but a user attempting to login will not be able to do so and will get a message that the Application server is unavailable. Additionally, there will be no access to Configuration available.

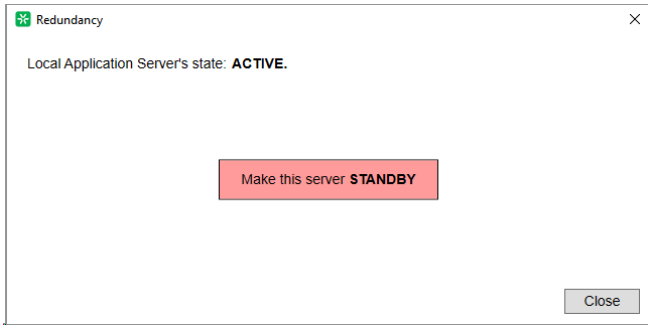


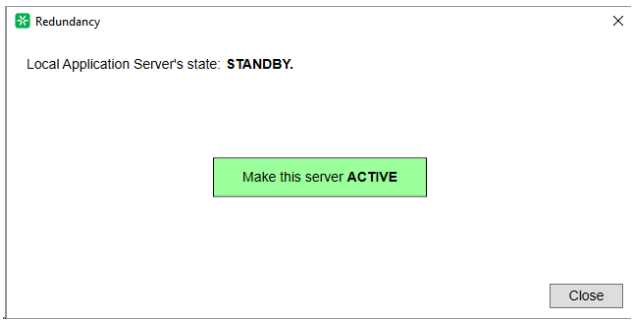


Controlling either Application Server's state (active or standby) is done with the click of a button (cold swap). If the primary server fails, you will need to access the backup server desktop (directly on the PC or using remote desktop or similar). Go to your system tray and right click the Application Server icon (green); if the icon is not in the system tray, you can run it by clicking on the Windows key, type application server and click on the Application Server utilities icon that displays. From the list that displays, select Redundancy to open the Redundancy panel.



From here, you will be able to click to make the Local Application Server Active, as it was in standby mode before (being the redundant server). The secondary redundant server will now take over. When the primary Application Server is repaired or replaced and brought back online, you will be able to click Redundancy again and make it Standby while the primary will be made Active.



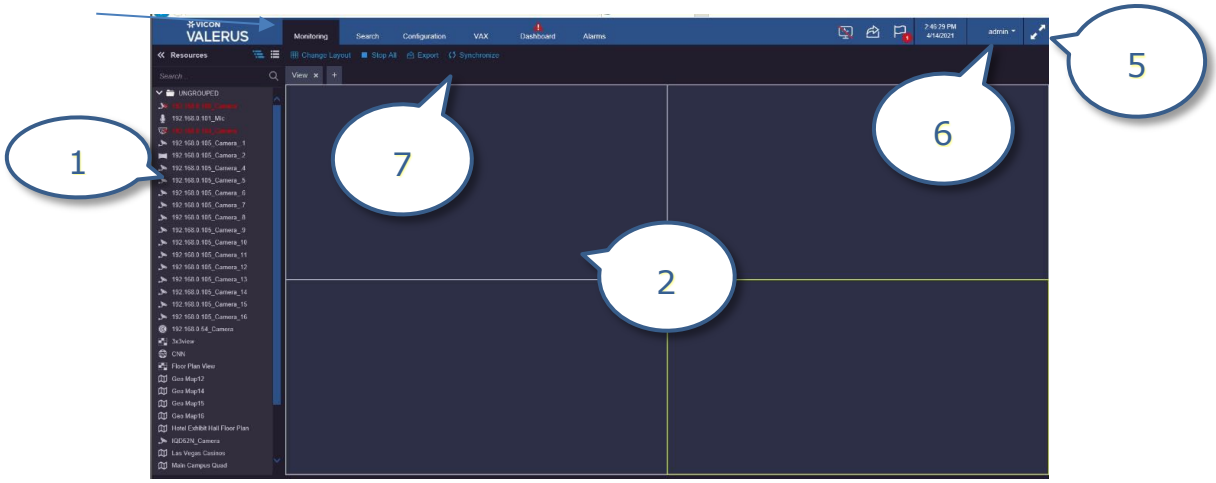


It is important to remember that only one of this pair should be Active at any given time and that normally the primary should be the Active one.

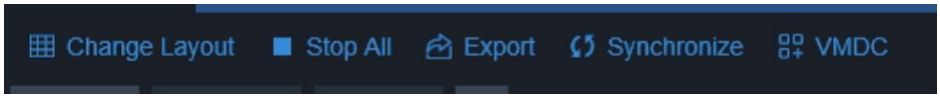
Monitoring

The VMS is operated from the Monitoring screen. This is where all devices on the system are listed and both live and recorded video is viewed. Click on the Monitoring tab at the top of the screen. The default display screen (2x2 quad) displays.

There are 4 levels of users, Administrators, who have all privileges, Supervisors and Investigators, who have limited privileges and Operators, who can only view live and playback video from the Monitoring screen.



General controls (7) for the Monitoring screen are located at the top of the screen. These are for Change Layout, Stop All, Export, Synchronize and VMDC. Each of these is explained in detail following.



Resources (1)

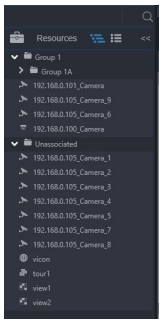
A list of available resources on the system is provided. The Resources list includes cameras, microphones, URLs (web pages), digital inputs, relay outputs, views, tours, mobile devices, partners and any defined groups. Each of these are represented by an icon as well as its name (refer to list below). If any device has been deleted from the system, there will be a folder of deleted channels in the Resources list, so that existing recorded data can be played back. These devices will be removed when the storage is filled, and the data is overwritten based on retention days set before their removal. Add in icons for Access Control Doors and LPR.

A – Group
B – Fixed Camera
C – PTZ Camera
D – Web page
E – Tour
F – View
G – Microphone
H – Removed Device
I – Access Control (Door)
J - LPR

This list can be presented in either a hierarchal view or a flat list of devices.

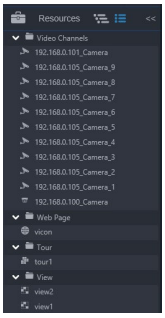
Hierarchy View (3)

In Hierarchy view, each device is listed under the group it is associated with. These are the groups configured in Groups Hierarchy. In systems with a large number of cameras, this can make locating the camera to view simpler, as it is identified with a specific group. If a device is not in a group, it will display as unassociated.

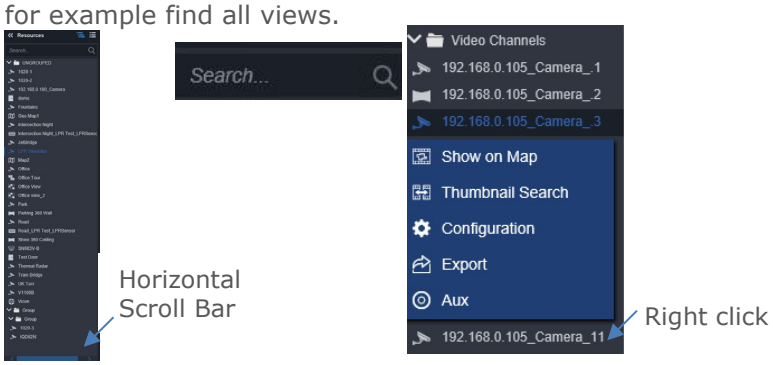


List View (4)

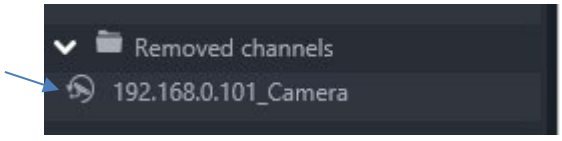
In the flat list view, devices are defined by resource type (video source, audio source, tour, etc.) and no groups are listed.



The Resources list can be collapsed by clicking the double arrows to provide a larger display area. Additionally, the Group lists can be collapsed by clicking the down arrow head. There is also a scroll bar at the bottom of the list that allows scrolling the list horizontally to read camera names with multiple characters that exceed the width of the Resources list. In large systems, it is sometimes difficult to find the exact device and group of devices in the list. You can right click any resource to get to a shortcut to the Search functions, Configuration, Show on Map and Export video, depending on what is available for that resource. A search function is provided to do a search of the list on that screen, for example find all views.



If a device is removed from the system, it will still display in the Resource list noted with an icon that will allow playback from the device. Additionally, removed devices will be listed in a dedicated group. The display of these devices can be turned off in the Users Settings screen.

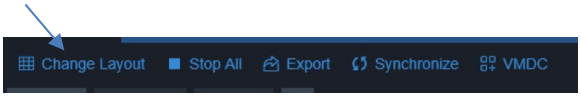


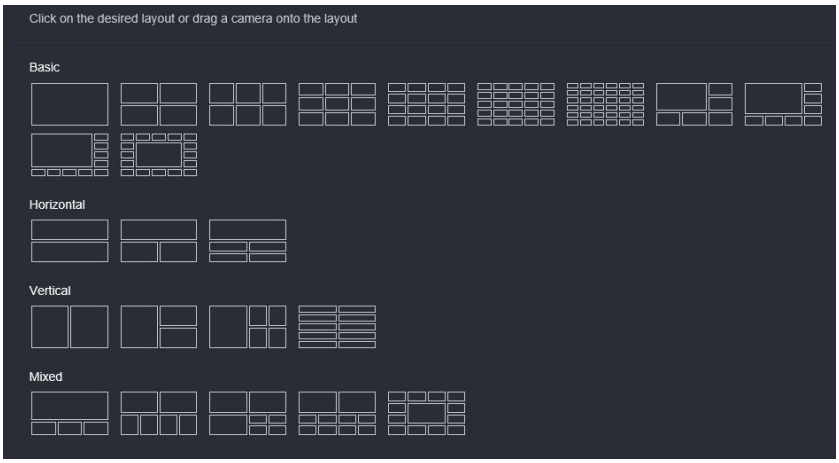
Display (2)

The default video display is quad (2x2) view; the default view can be changed and additional views can be created. Valerus supports multi-monitors.

View

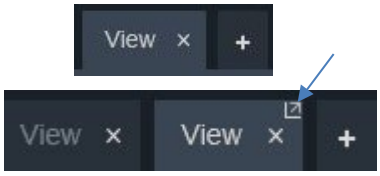
- To change the default view, click Change Layout to reveal a list of basic, horizontal, vertical and mixed layouts. Select the desired layout and it will display on the Monitoring screen.





New View

- It is often convenient to have several displays available for viewing, without having to change the main default view.
- Additional views are created by clicking the plus sign next to the View tab; a visual display of layout types opens. Click on the layout desired; a new view tab is created next to the View tab.

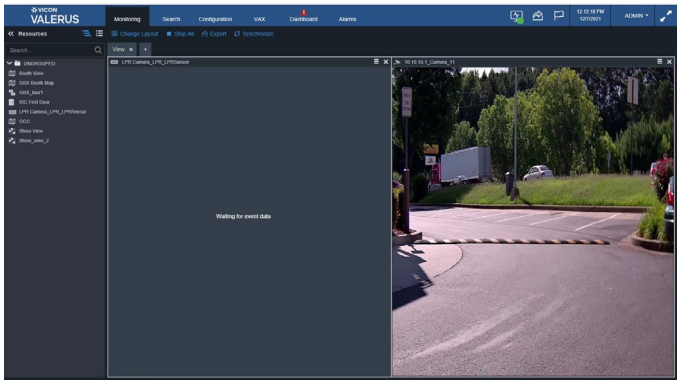


- As an alternative, any View created in Configuration and is in the Resources list can be dragged to the display area and a new tab will open up.
- Any View tab can be closed by clicking the "x" on the tab.
- Valerus supports multiple monitors, so any view or edge device can be displayed on another monitor. Click the View tab and drag it up a by the little arrow in the corner; a new window will open with that view. This can then be dragged to the other monitor. Note that popup blocking must be turned off in the browser to allow display on the second monitor.

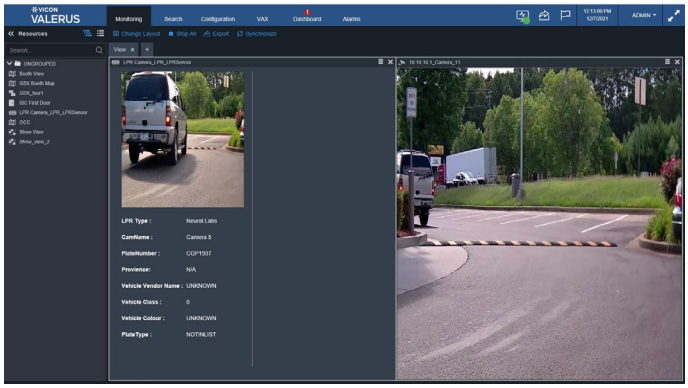
Live View

- To view video, audio or event data from a sensor, simply drag the resource, camera, microphone or integrated partner sensor (door or LPR), into the tile. Video/audio will start to display live. When a partner sensor is selected for display, it will display the event data for 30 seconds; if there is no event, the screen will display "Waiting for event data" on the tile. Audio does not take up a tile in the display area but displays in a small area under the video display area.

Partner Sensor – No Event



Partner Sensor –Event Occurs Display



If a video stream is lost because an NVR goes down, the Valerus failover will attempt to get the video directly from the camera. To indicate this, the word Alternate will display in the title bar.

- Double clicking the camera icon changes the view to single view; double click again to return to previous screen layout.
- To view a different camera/microphone/partner sensor in a tile already displaying video, drag it from the Resources list to the title bar above the video with the camera name to replace the video. Displays can be moved from tile to tile on the interface and the displays simply rearrange to accommodate the change.
- To stop displaying video/audio, click the x in the right corner of the title bar above the video. If a previously created view is dragged, it will open in a new tab.
- To display a configured View or Tour, drag it from the Resources list onto the display area. A new tab is added next to the View tab or any other View tabs that are currently available. These views and tours can be selected, viewed and operated as any other device in the list.
- Web pages that are visible in the Resources list can be dragged to the display area just as any other device. The web page displays in the tile and can be navigated as any website. Double clicking on the display will change the view to single view; double clicking again returns to the previous screen layout.
- Placing the cursor on the title bar above the video/audio that displays the device name reveals a series of icons for video/audio functions, including Snapshot, Bookmark, Search, PTZ (on PTZ cameras only), 360 (on 360 cameras), Play (for playback), Digital Zoom, Unmask, Configure and Export; audio icons include Volume, Configure and Export. Additionally, there is an icon for Search (i.e., Thumbnail or Museum Search) that will take you directly to the Search function if clicked; refer to that section for details on how to use those screens. These icons will display for a set amount of time and then disappear. If it is convenient to have these display continually,

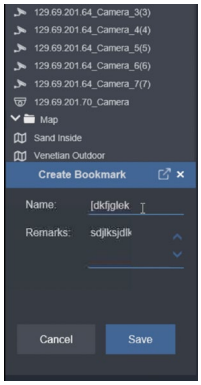
click the three line icon so it turns and the lines are vertical; click the icon to have the lines be horizontal and the icon bar will time out. When the icon is blue, it is selected.

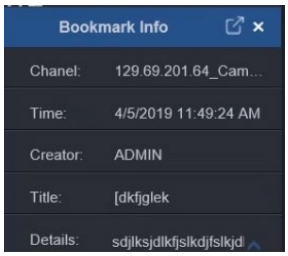
Video Controls

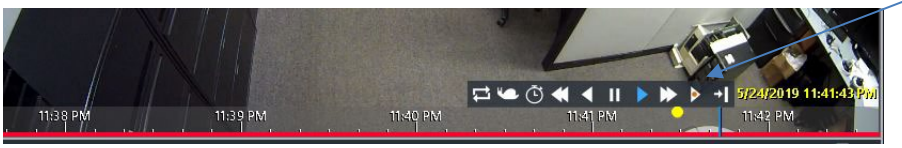
Audio Controls

- Snapshot – A photo of live or playback video can be taken by clicking the Snapshot icon on the toolbar ( ). The path for where the snapshot is saved is shown on the screen. This can be modified from User Settings. Note that the date and time indicates that of the creation of the snapshot and not the time and date the video occurred. The snapshot will be of whichever stream is displaying video.

- Bookmark – The operator, if authorized in User settings, can create a bookmark related to a specific video feed, live or playback, by clicking the bookmark icon (star) on the toolbar; this will open a bookmark dialog box with the time it was clicked. When a bookmark is created, its information is docked under the Resources area so it does not block any video, but it can be undocked and placed where convenient. The bookmark is accessible from the Playback screen timeline as well as searchable in the query form. This bookmark can be searched for using the Query feature. When in playback mode, the bookmark is noted by a large yellow dot. Hovering over the dot will display the title of the bookmark; clicking it opens full playback functionality.



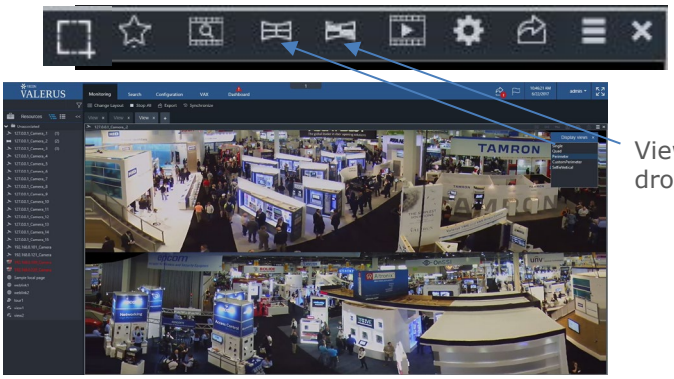




- When a PTZ camera is displaying, the cursor turns into a large arrow head that allows movement of the camera position. Additionally, zooming can be done using the mouse wheel or the +/- sign next to the PTZ symbol. Click the PTZ icon to select the preset or the tour you would like to view (for PTZ cameras only). The camera will immediately move to that position or tour.

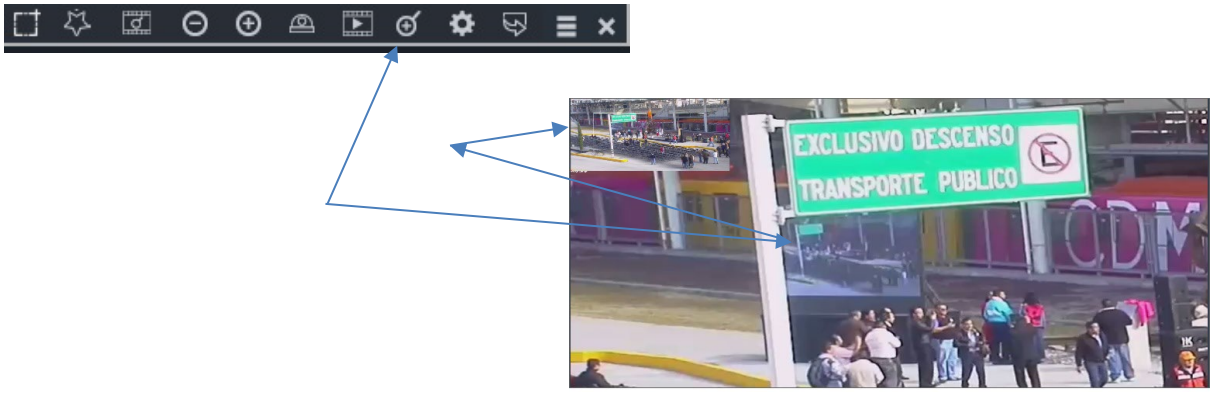
- When a hemispheric (360) camera is displaying, there are icons that open a view dropdown and a preset dropdown. There is no digital zoom, but you can zoom in using the mouse wheel or right

click and move the mouse into the area you want to zoom in to. After zooming, you can navigate the picture with a left mouse click and moving the mouse.

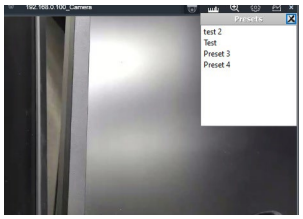


- Playback – This is used for playback and is explained in the Playback section that follows below.
- Digital Zoom – Use the digital zoom tool to zoom in to a specific area of the video display. A picture-in-picture of the entire screen will display in the left corner of the tile. Use the mouse wheel to fine tune the zoom amount or use the cursor to select a specific area to zoom in to.

  Clicking the mouse wheel in the picture-in-picture returns the display to 100%. Note that digital zoom is not available for hemispheric (panoramic 360°) cameras. Refer to that section for details on zooming.

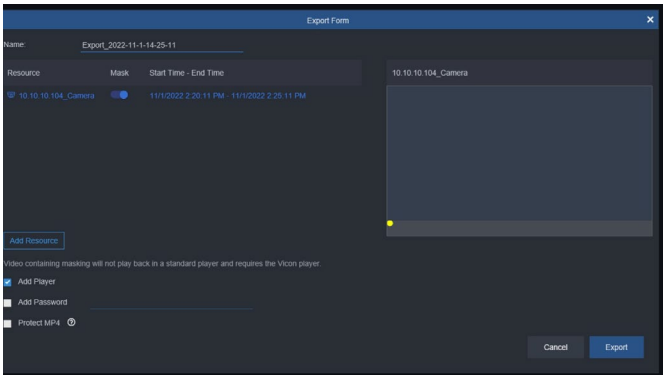


- Unmask – Select the Unmask icon to temporarily remove any mask on the video that was created in Configuration. Clicking Unmask again restores the mask.

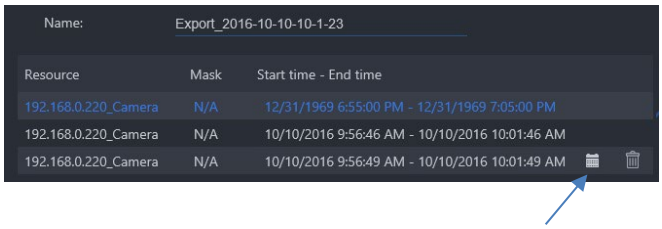


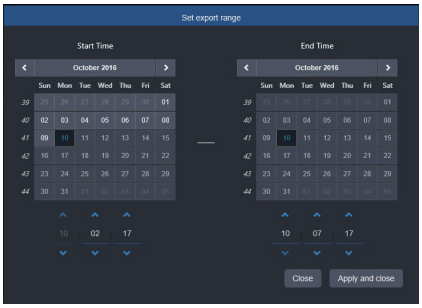
- Configure – Clicking the Configuration icon opens the Configuration screen for that device. This is a shortcut to make changes to that device's setup.

- Export – The Export icon is used to save a video clip from this camera. To save a clip, click the Export icon. A popup will display.



- Video/audio recorded in Valerus is not saved in a standard format (i.e., avi, mp4) but rather in a proprietary sequential file format. These files cannot be simply played by standard media players and must be exported to allow them to be viewed elsewhere than the Valerus system.
- A default name export will display; this can be modified, but the name cannot include any special characters or symbols other than a dash (-) or an underscore (_). Select the Start and End time for the video clip by clicking on the calendar icon; a popup screen will display. Select the exact start and end times for the video clip; when finished click Apply and close. If there is a mask on the video, it can be removed on the exported clip by clicking the Mask button; the mask remains on the live video display. The video loop function is supported and that loop can be exported.

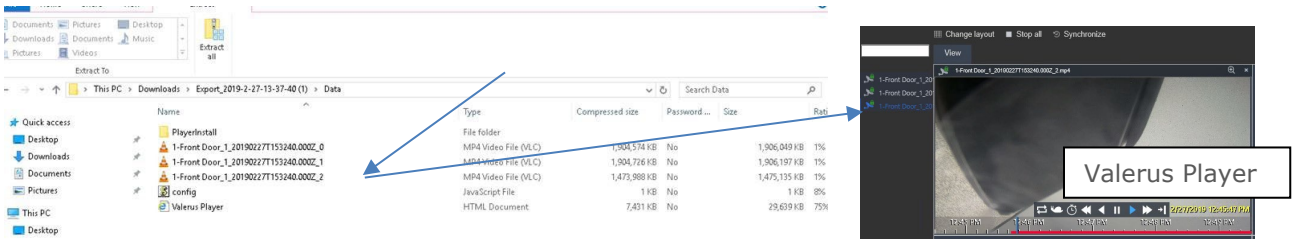




- Add another resource not in the list by clicking the plus sign; a list of resources will display. Select desired resource and click Add; if you have selected all the resources click Add and Close; click Close to close the popup without adding any resource. You can include the Player and a Password to the clip by checking those boxes; this way video can be viewed as in the VMS and is protected. For added security, you can block the MP4 video from being played in external players (like VLC) by checking the Protect MP4 option. Click Export to save the video on the Application Server (because the VMS is browser-based, video cannot be saved directly to a local device). The Export symbol will display a number that indicates that the export is in progress; click on the Export symbol for details on the progress of the export. A spinning circle indicates how the export is progressing. You can also click Abort to stop the export or Advanced for additional details. When the export reaches 100%, click download; a message (Windows standard) to save the video clip zip file to a local device of your choice will display. Video is exported in MP4 format.

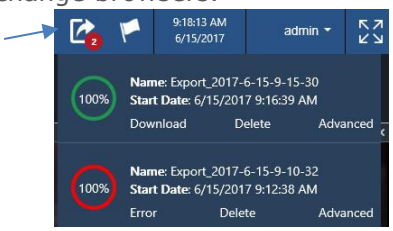
  Note: If the exported file size is larger than 2 GB, the video will be split into 2 GB size files and will show as multiple consecutive files using the camera name and a suffix number showing their order. This is done to support clients running on a 32-bit operating system that cannot handle file sizes larger than 2 GB.

  In the example below, an actual export file was split by Valerus into three (3) files. The camera name (1-Front Door) is the same for all three files and a numeric ID showing the order is added at the end (0-2). On the right-hand side you can see how these will show in the Valerus player, allowing the user to access the entire exported scene.



Download List

- When extracted (if a password was added in the Export form, you will need to provide it now), the exported video is in a folder. If the player was added in the Export form, it will be in the folder as Valerus_player.html. The file will now be Valerus Player.exe. If no player was exported, there will only be the MP4 files. When clicked, the Export Player automatically opens in Internet Explorer or in Microsoft Edge; if it is opened in a different browser a message will display to notify the user to change browsers.

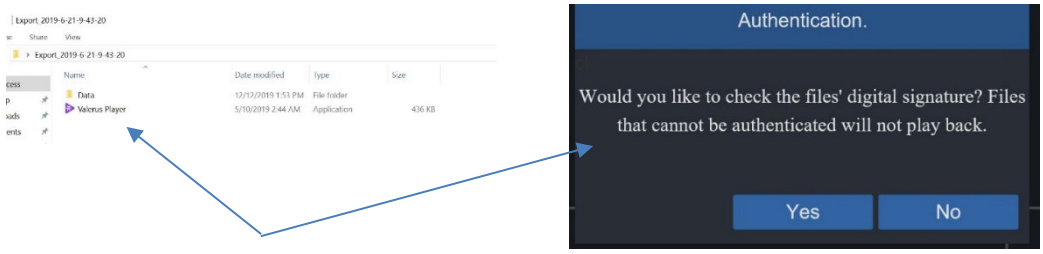


Note: Once the file is exported and downloaded to the client, it is recommended to delete it.

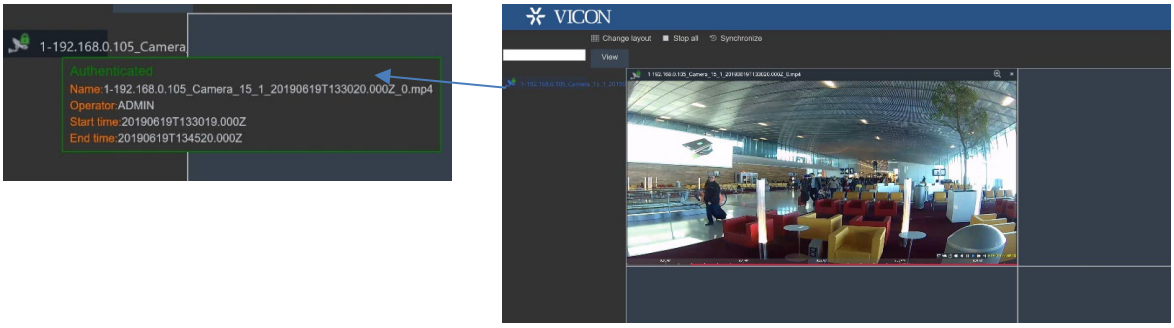
Authenticating Exported Video

- Valerus files can be exported and saved either as a simple MP4 clip that can be played in any media player or along with the special standalone Valerus player that supports additional functionality, including multi-camera playback, synch playback and authentication.
- At the time of export, all files are digitally signed using the system's SSL certificate. This SSL certificate will be used to verify that the files were not tampered with, ensuring the integrity of the recorded video.
- When you run the exported video from the folder, a popup will display offering the option to authenticate the files. Click Yes to run the authentication or No to skip the authentication process.

NOTE: A message asking to Allow blocked contents on the browser may display at the bottom of the screen. You need to allow this in order to proceed.



- The length of time the authentication process takes will depend upon the number of clips and their length. Once completed, the Valerus player will open and the files will be listed. Click the file to display information about the file and the Authentication confirmation. Drag the video to a tile for playback. The green lock icon indicates the file has been authenticated. If the file has been tampered with, it will show a red lock and will not allow it to be played back. If the authentication process was skipped, there will be no indication.



To maintain chain of custody, the exported camera source is displayed using its original camera name.

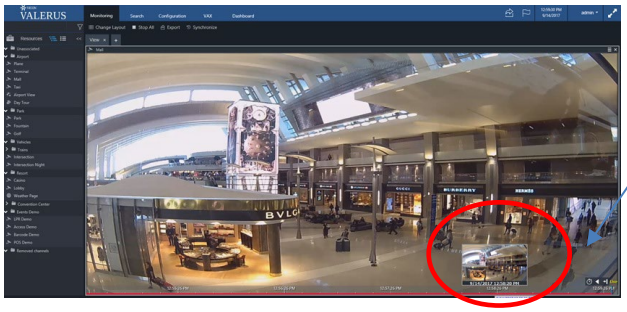
- Volume – The volume icon for audio displays a slide scale that allows you to lower and raise the loudness of the audio that is playing.

Playback

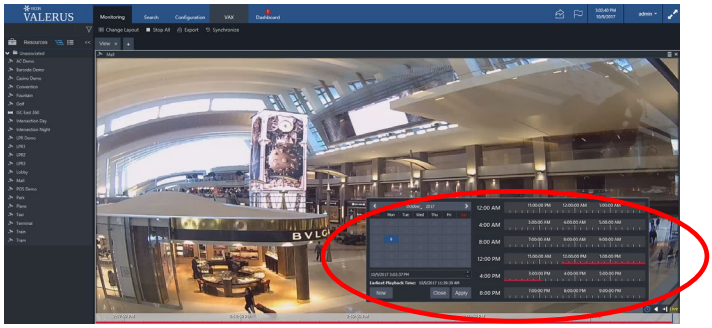
Video

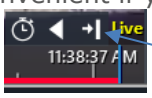
- To view recorded video, click on the Playback mode icon to display a timeline at the bottom of the video display (the Playback icon turns blue); icons for Play From Time, Backward (rewind) and Go to Current Time also display. There is also a clear indication that the video displaying is Live, even when the timeline is displayed.

- Playback can be started by clicking directly on the timeline. To playback from a specific date and time, click on the Play From Time clock icon; a calendar displays. Select the specific date and then enter the time, hour, minute and second. Click Apply. The video from that specific date and time displays on the screen. The playback icons change with more options. There is a blue playback cursor in the timeline that indicates the exact time the playback is displaying; this cursor can be moved to any time. The earliest playback time available is noted on the calendar. Hovering the mouse over an area in the timeline will display a thumbnail of the video at that time; this can be turned off in User Settings, Visual.



- If a bookmark has been created, clicking the yellow dot will put you directly into playback mode, with all the same functionality of standard playback.
- Use the icons to view video in: Loop mode, Slow mode, Play from Time, Fast rewind, Rewind, Pause, Forward, Fast Forward, Live view and Go to Current. Clicking the Loop mode icon will activate brackets around a time span that can be moved to the exact time desired for playback; this same time section of video will display repeatedly. Be sure that the blue playback curser is in the looped time brackets.
- When Playback from Time is called up, Valerus will show a 24-hour map of recording for the selected day. Right clicking on the red line brings up thumbnail of the video at that time.



- Clicking the Go to Current icon takes the video to the time where the blue cursor is in playback. This is convenient if you have been scrolling in the timeline and lost track of where the current playback time is. 

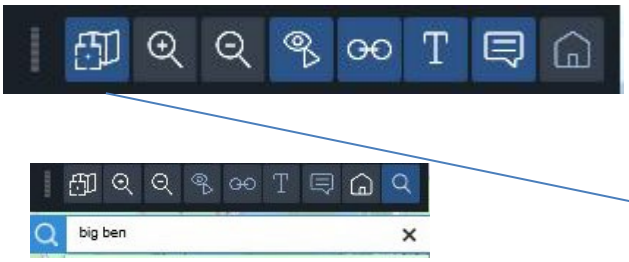
It is important to remember that this does NOT go back to current Live video.
- The video will remain in playback mode until the video is returned to Live or shut off. When it is in playback mode, a red x will display on the playback mode icon and the icon will read "To close, switch back to live;" click the icon, click the Live icon and then close playback if desired.
- To remove the timeline bar, click the Playback icon (that is currently blue) and the timeline will disappear.
- When a device is deleted from the system, existing recorded data is kept in a folder of Deleted Channels in the Resources list. These recordings from deleted devices can be played back in the same way as recordings of currently connected devices. This data will be available until the storage is filled and it is overwritten due to FIFO.

Audio

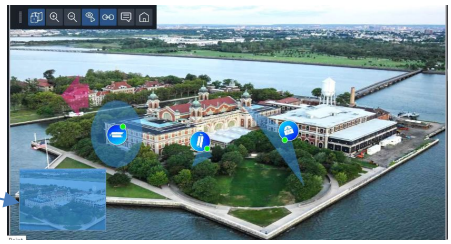
- Audio displays in a small area under the video display area, so that a tile area is not allocated.
- A timeline displays for the audio to allow playback. Playback from a time can be selected by clicking directly on the timeline. To playback from a specific date and time, click on the Play From Time clock icon; a calendar displays. Select the specific date and then enter the time, hour, minute and second. Click Apply. The audio from that specific date and time displays on the screen. The playback icons change with more options.

Maps

- Maps, both Static and GEO, are included in the Resources list. Any map can be dragged into a tile for display. The map will display as it was set for the Home position in Configuration and includes all the resources, highlights and sticky notes created there.
- The tool bar below displays for a map; this toolbar can be dragged to a different location if it is interfering with viewing the map. Using these tools, you can get the relative location after zoom, zoom in and zoom out, remove the funnel, hide linked maps, hide text on linked maps, hide sticky notes and go to Home position (if setup in Map Configuration). Additionally, on a GEO map, you can do a search to pinpoint a more specific location. Note that this toolbar will not be seen when using a screen split higher than a 4x4, due to the small size of the panes.

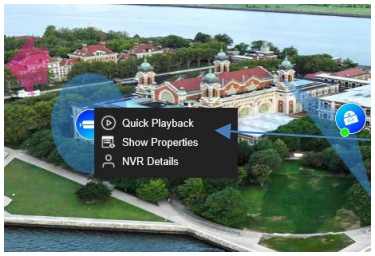


Tool bar for GEO Map with Search



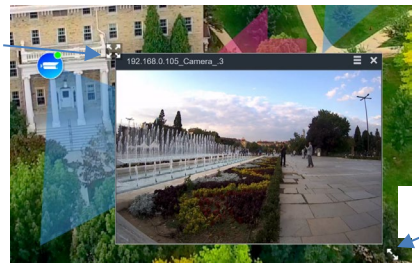
Relative location

- When viewing a map, hover over the camera icon to get a snapshot. Double clicking the icon opens the player for a complete Live view of video with all controls and information on the device available. Note that there is no PTZ control from the icon itself; open to Live view for full PTZ control. The Live view can be resized by grabbing the double arrow tool in the bottom right corner; it can be repositioned by grabbing the four-arrow icon in the top left corner. See below.
- The mouse scroll wheel can be used to zoom in and out of the map as needed and works in the same way as the plus and minus buttons on the toolbar.
- Right clicking the camera icon opens a box that offers quick playback, shows properties (camera name) and some details on the NVR the resource is on; right clicking a relay can turn it on/off.



Right click camera icon

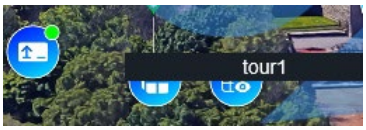
Move tool



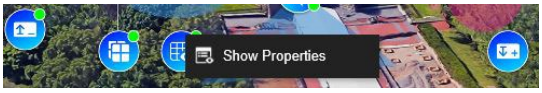
Size tool

- When resources other than a camera are on the map, including microphone, tour, view, relay output, digital input, access control door or LPR sensor, hovering over the icon/label displays the name of the resource. Right clicking allows to show the properties of the resource; right clicking on a partner resource also shows a View option, which will start the video from the camera related to the partner resource on the map. To display a view or start a tour from the map, drag the icon to an open pane on a display grid; the view or tour will display in that area. Double clicking the mic icon will open the player and allow to play audio in the same way it is done from the display area. The door icon will show the door state; right-clicking will show the actions from VAX that can be executed. The LPR label on the map can be placed near the associated camera and hovering over it will show the properties of the device.

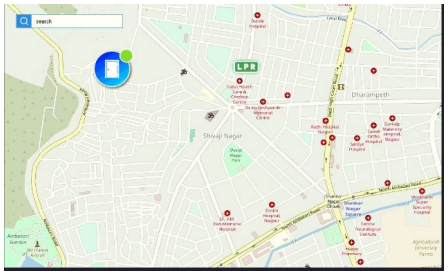
Relay, Tour, View, Digital Input icons



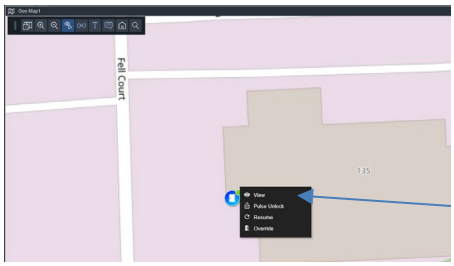
Hover for icon name



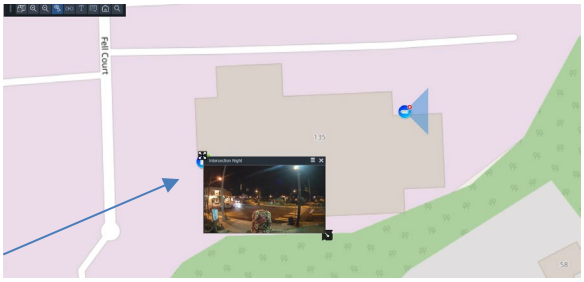
Right click icon



Door and LPR icons

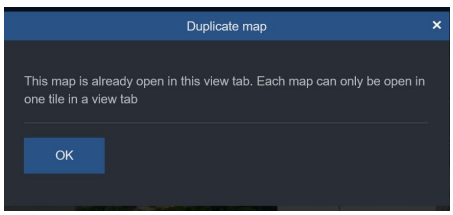


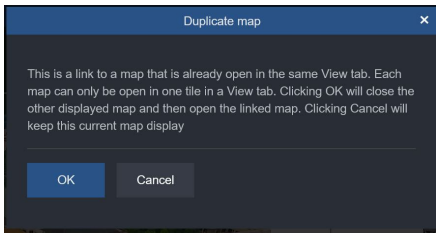
Right click icon-View



- If a highlight shape that was created with a link to another map is shown on the map, clicking the shape will navigate to that linked map and display it. Use the back arrow to return to the original map.

Important Note: There is a limitation to displaying maps. Each map can only display once in a View tab. A message will display if you try to open a map that is already open in that display. If a linked highlight is clicked that is a link to a map that is currently displaying in this same View, a message will display. Selecting OK in the message will close the map that is already displaying and then open the linked map. Clicking Cancel will maintain the current display and the link will not open.

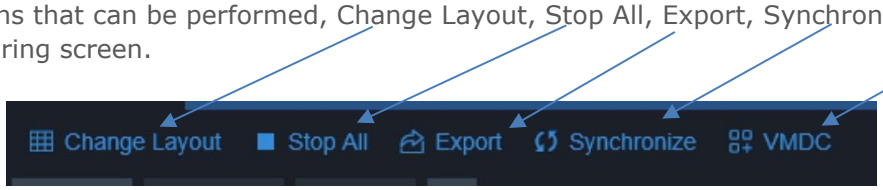




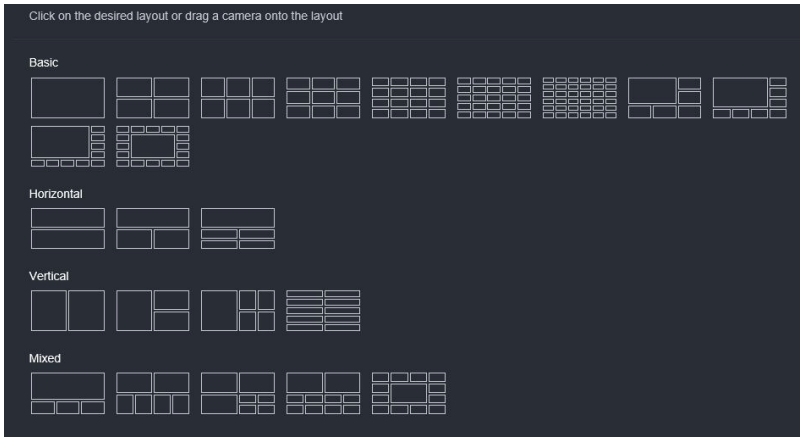
- If a highlight shape that was created without a link is shown on the map, the mouse will not change when it hovers over it and clicking will not change anything.

On Screen Controls (7)

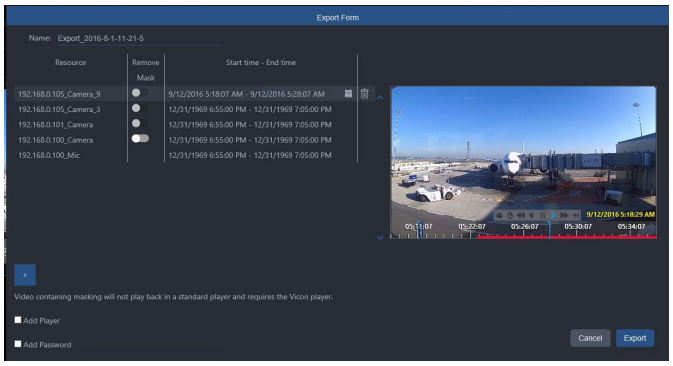
A group of icons for functions that can be performed, Change Layout, Stop All, Export, Synchronize and VMDC are at the top of the Monitoring screen.

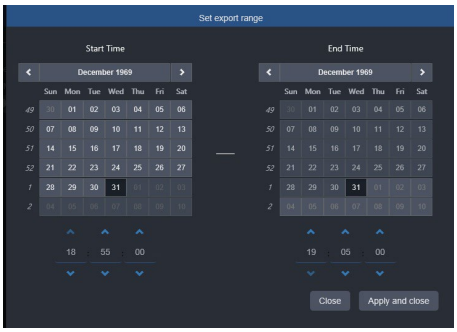


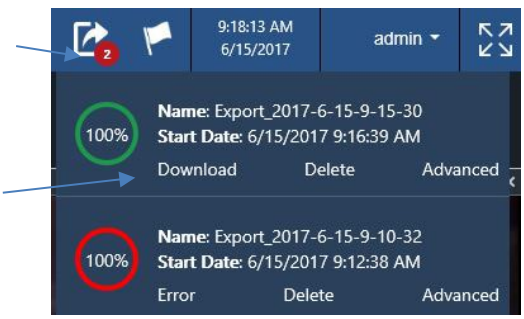
- Change Layout provides a number of video display layout options and is explained previously under Display.



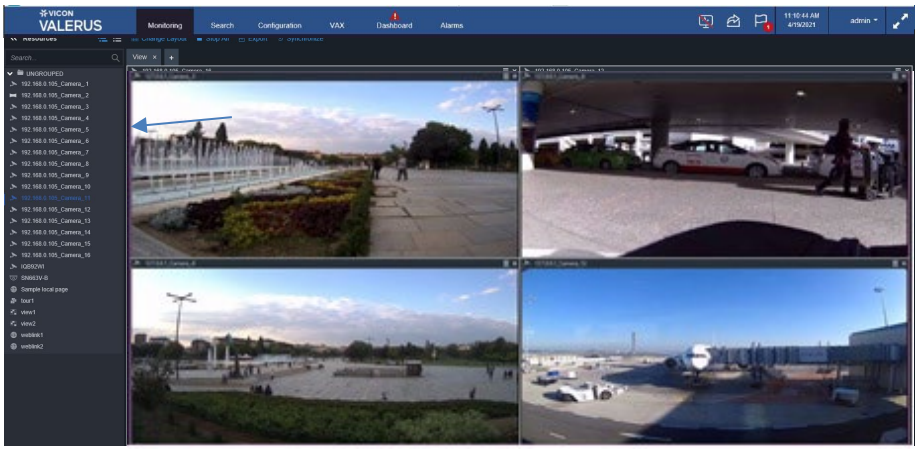
- To turn off all video display, click Stop All.
- To save a clip, select Export. A popup will display listing the Resources available to save. Select the Start and End time for the video clip by clicking on the clock icon; a popup with a calendar displays. Select the exact time and date to you want to export for each resource; when finished click Apply and close. Add another resource not in the list by clicking the plus sign; a list of resources will display. Select desired resource and click Add; if you have selected all the resources click Add and Close; click Close to close the popup without adding any resource. You can include the Player and a Password to the clip by checking those boxes; this way video can be viewed as in the VMS and is protected. Click Export to save the video on the Application Server (because the VMS is browser-based, video cannot be saved locally directly). The Export symbol will display a number that indicates that the export is in progress; click on the Export symbol for details on the progress of the export. A spinning circle indicates how the export is progressing. You can also click Abort to stop the export or Advanced for additional details. When the export reaches 100%, click download. This file can then be downloaded to a local device.





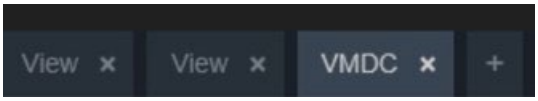


- When Synchronize is selected, the video on the display is bounded by a pink border and the playback video from all these resources are time synchronized.

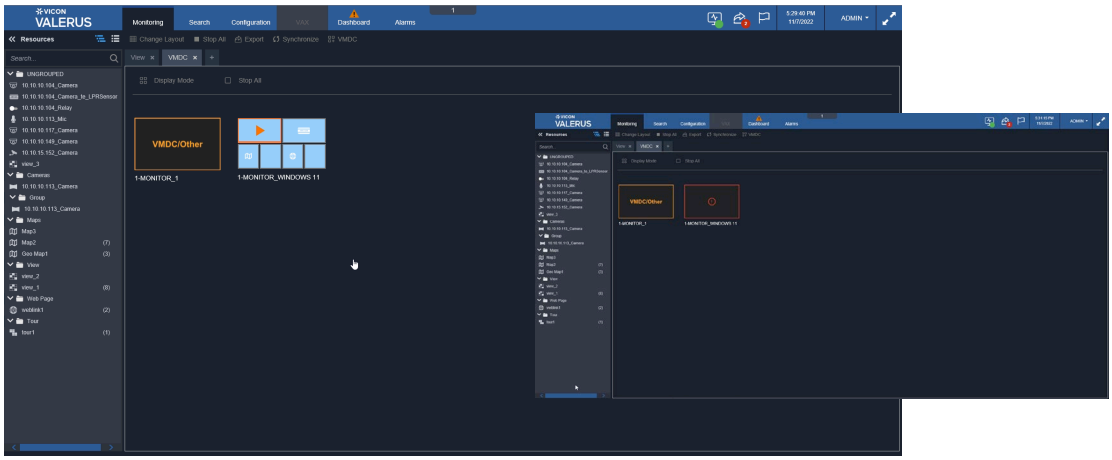


- VMDC is designed to provide users with the ability to remotely take control of any Client Workstation that is on its network (those using the same Application Server) to view/control the video displaying on those monitors. VMDC capability is enabled through User Settings, Visual (refer to User Settings for details). The monitors available to access are configured in Resources>Monitors. ***Screenshots***

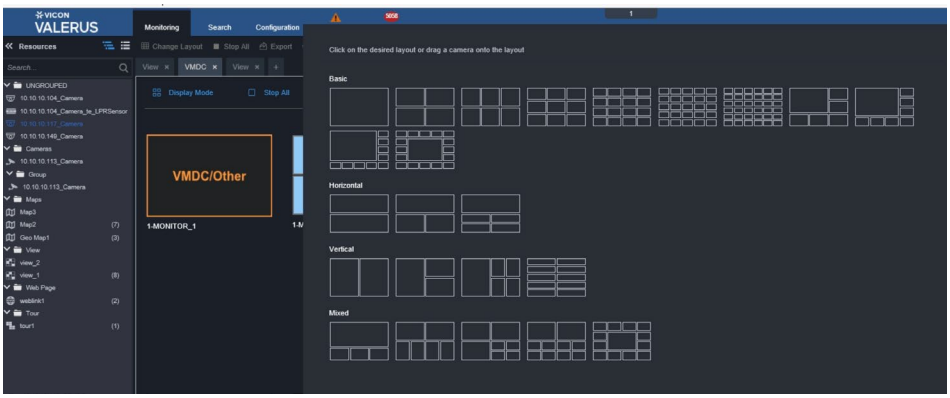
- When VMDC is clicked in the On Screen Controls, it is added as a tab next to the Views.



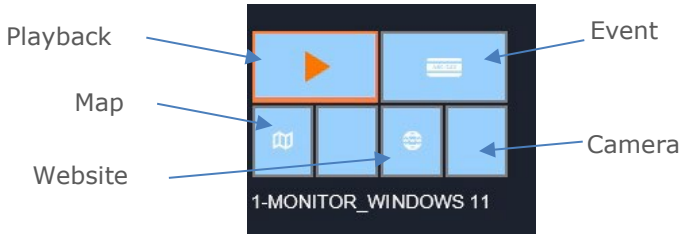
- Click the VMDC tab to display the monitors currently available. Virtual monitors have an indicator with a red border if the remote monitor has a different page open than the monitoring page, the monitor is offline, the machine is disconnected or the user is logged out. There is an orange border if the user is in a different page than monitoring page.



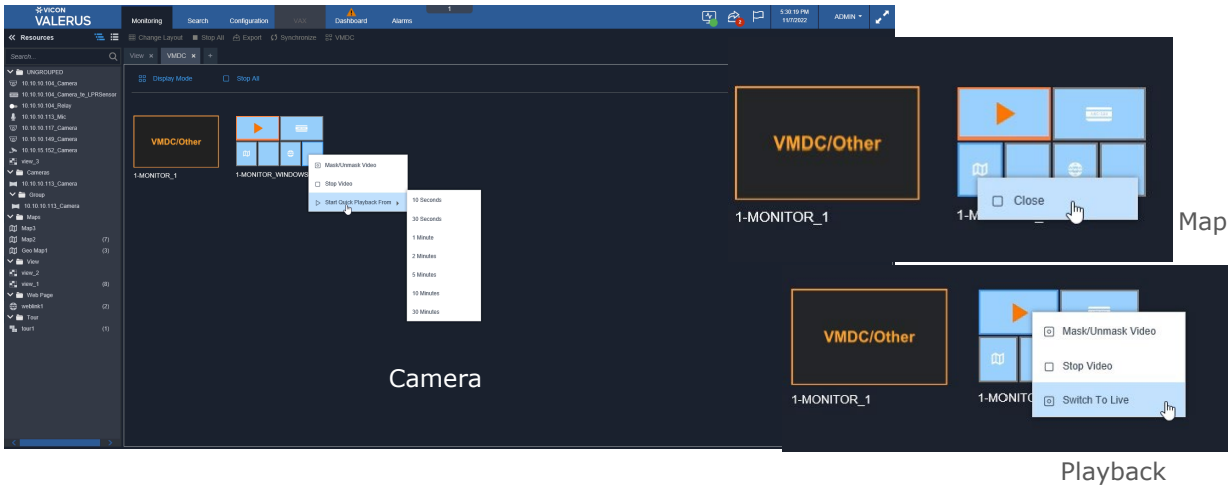
  - Select a monitor. Click Display Mode to open the layout options; select a video display layout for the monitor. Note that Display Mode is grayed out if "Alarm settings layout" has been enabled in the Monitors configuration under Resources.



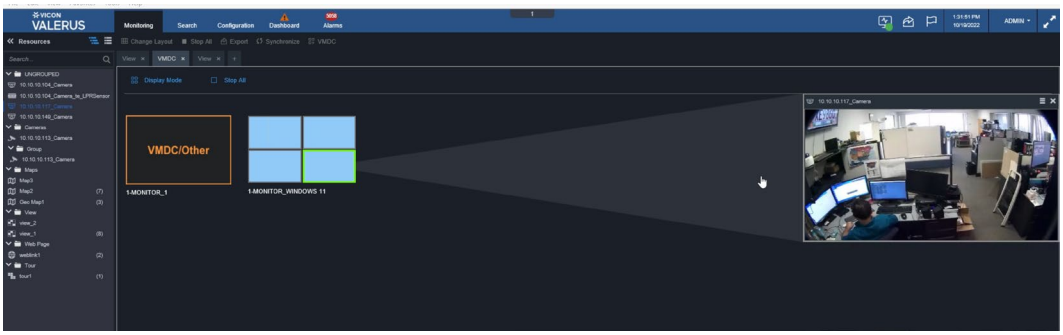
- The real-time synchronization in the virtual display synchronizes the layout status of the screens and status of the player video. Virtual monitor also indicates what type of resources are in each layout like maps, webpage, cameras, events.



- Any available Resource in the list can be added (drag-and-drop) to any of the monitors, as needed. Users can also right click the cameras resources on VMDC to mask/unmask video, stop video and do a quick playback. The functions of the right click depend on the resource type.



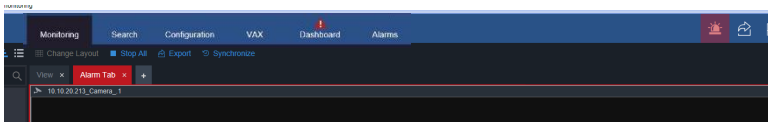
- Double click on the camera on the monitor to open a video display area; this display area can be moved anywhere on the screen for your convenience. All the controls available on the Valerus Monitoring screen are available on this video display. Only one video per monitor can viewed at a time.



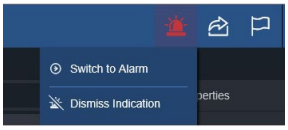
- To turn off all video display, click Stop All.

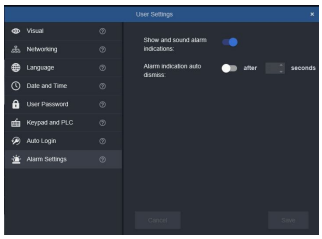
Alarms

If Events have been defined in Configuration, and an alarm event occurs, an alarm event tab, highlighted in red, will open in the tab area. No video will be overwritten, but the system will jump to open that tab. It may be convenient to dedicate the display of this tab on another monitor. All alarms will open in this tab.



In addition, an alarm icon will flash in the top toolbar and an audible alarm will sound. These alarm indications can be set on/off per user (User Settings) and can be configured to time out or require a manual shut off.

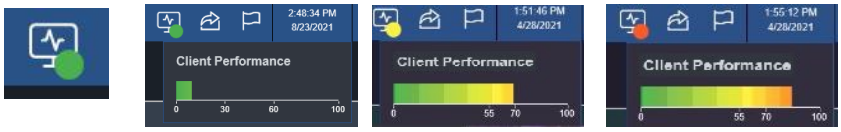




Client Monitoring

At the top of the Valerus screen there is a monitor icon. This is for an advanced monitoring application called Valerus Client Service. Adding this capability is optional.

- Hover over the icon to get a link to download this Valerus Client Service; click the link to download locally on the client. This Service does two things, generates a unique Valerus ID and allows the service to monitor client performance about the load on the local client PC. After installed, the icon changes; the Valerus ID can be found in User Settings and a colored dot appears on the monitor icon, indicating client performance. The color of this dot provides an indication of the load for all the resources on the client; green indicates good performance, yellow/orange indicates approaching an overload (50%-70%) and red means there is too much running on the client (>70%).

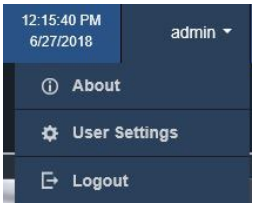


Full Screen (5)

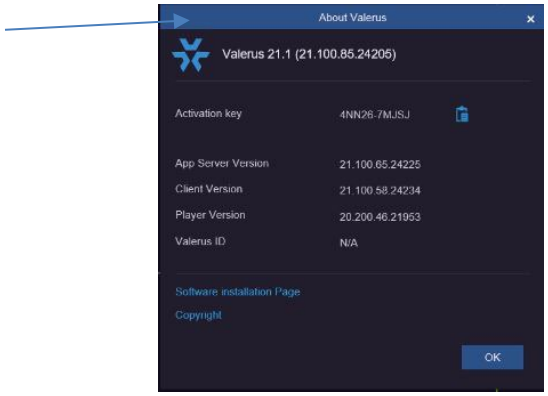
- There is a two arrow icon in the top right of the screen. This is a triple click button. When it is desirable to view the interface full screen, click on the two arrow icon. The interface will expand to fill the entire browser (similar to the F11 function). If you click it again, it will fill the entire screen with no UI. To return to standard view, press the Esc key.

Admin (6)

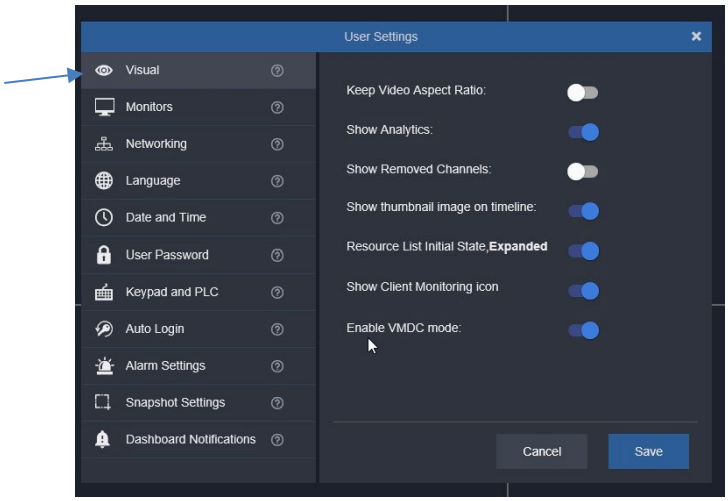
From the admin dropdown, select About, User Settings or Logout.



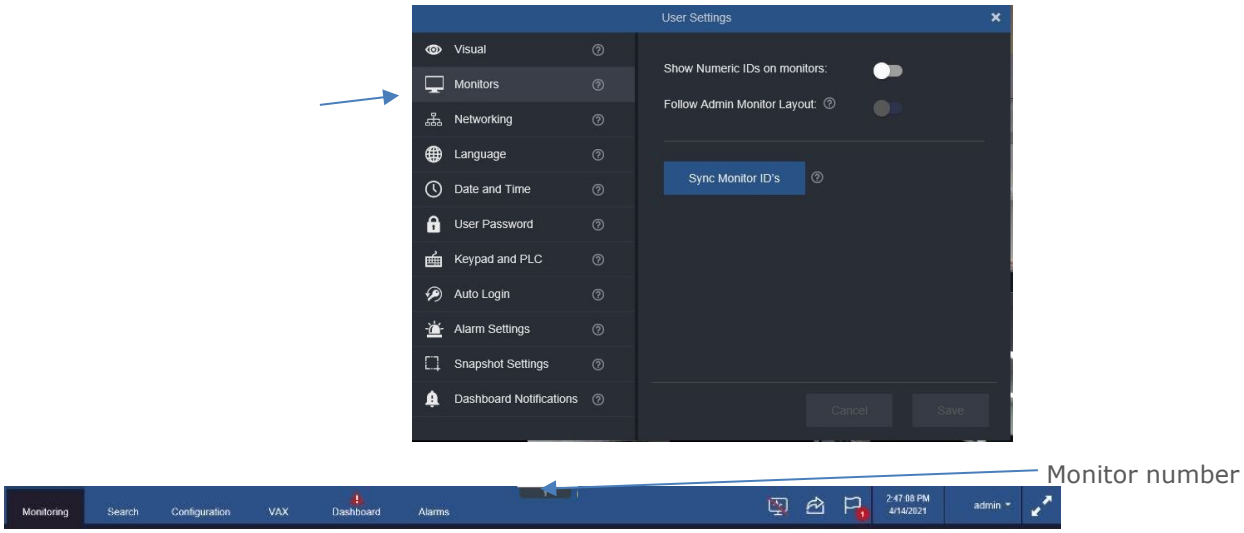
- Click About to find important details about the system. This screen provides the Activation key without having access to the Configuration screens. Your Valerus ID can also be found here if the Client Monitoring service was installed and run. It also includes a link for software installation and copyright information on open source software used in Valerus.



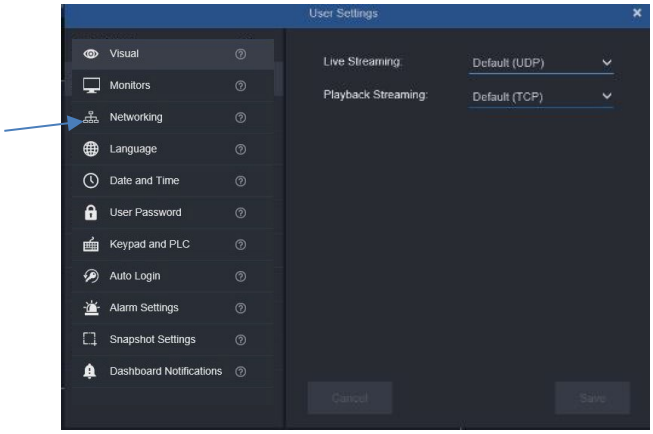
- User Settings presents an overview of the local settings of the system. These settings can be modified and saved directly from this screen. Included here are categories for Visual, Monitors, Networking, Language, Date and Time, User Password, Keypad and PLC, Auto Login, Alarm Settings, Snapshot Settings and Dashboard Notifications. Clicking each of these categories opens a list of settings.



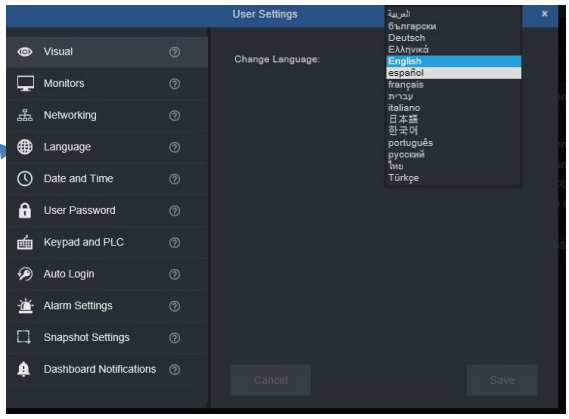
- The Visual category allows you to enable Keep Video Aspect Ratio, Show Analytics. Show Removed Channels, Show thumbnail image on timeline, determine the initial state of the Resources list, expanded or collapsed (expanded is default), Show Client Monitoring icon and Enable VMDC on Monitoring (ENTERPRISE tier only; this must be enabled here first to use this feature). Click the button to enable (blue)/disable the function.
- The Monitors category allows Show Numeric IDs on monitors (monitor number will display on a gray tab at the top of the monitor display; for use with a keypad). There is a setting that determines how the browser-based Client will open on multiple monitors. By default, each user can arrange their own monitor layout. Enabling the Follow Admin Monitor Layout option allows using the same monitor layout set by the Admin for all users, which can save time on large, multi-user sites. The Sync Monitor IDs button allows the Client to report to the Application Server what monitors it has deployed. This will be done after setting the Client and arranging the different Valerus screens on the different monitors used and will populate the information in the monitor's screen. If the Client setup is changed (for example, removing a Valerus tab from a monitor), the monitors should be synced again to reflect the change.



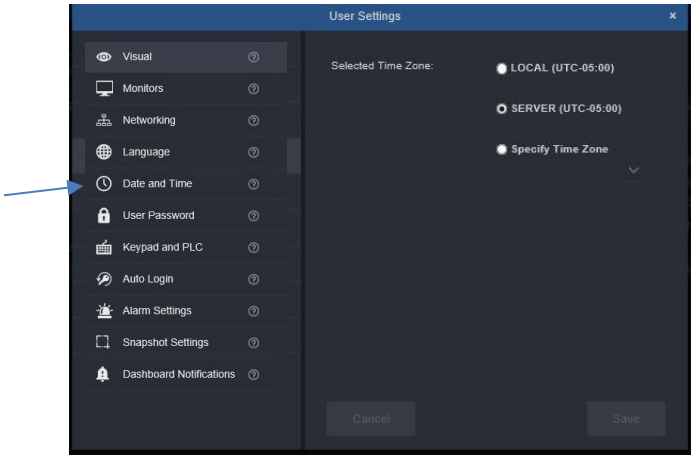
- The Networking category shows the Internet Protocol you are using for Live and Playback Streaming. These are set in Configuration, Network, but can be conveniently changed from this screen.



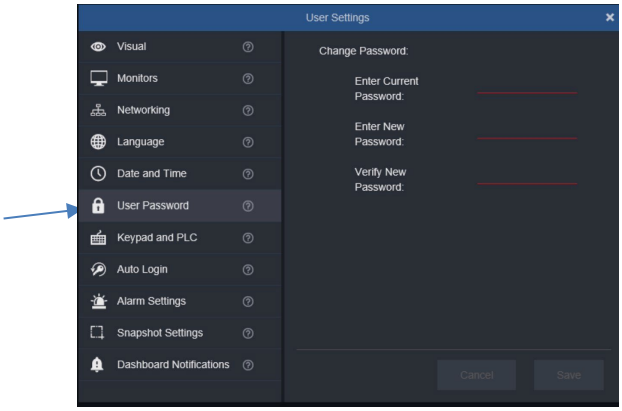
- The Language screen provides a choice of languages that the interface supports and can display in. Select the language from the dropdown list. Note that some languages appear in the list but may still display in English until the translation is complete.



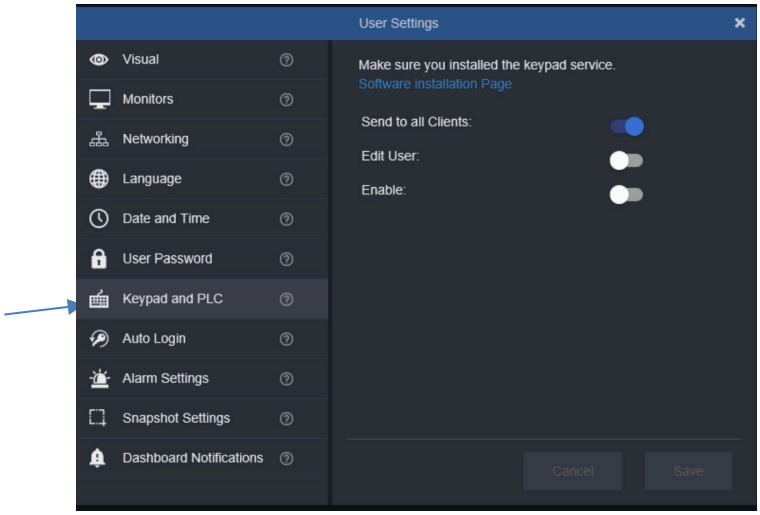
- Date and Time provides a screen to select the time zone for your system. Click the radio button for Local, Server or Specify Time Zone from the dropdown list.



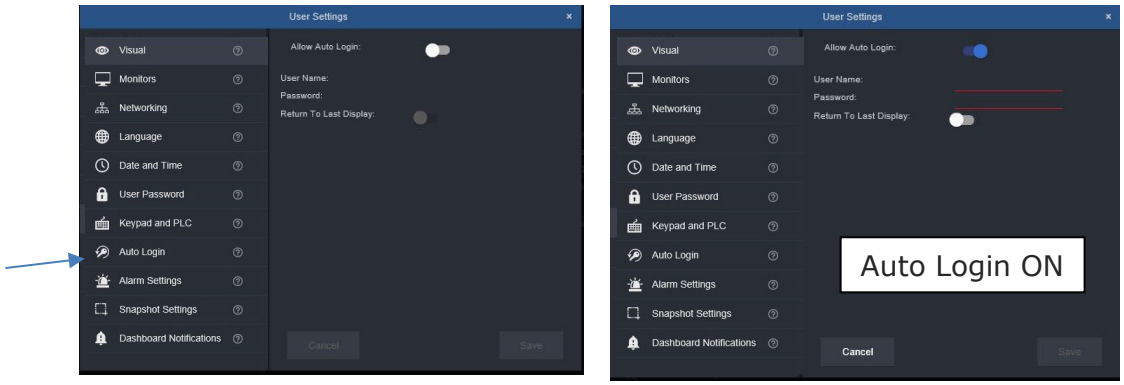
- User Password provides a screen to edit your user password without going into the Configuration screen.



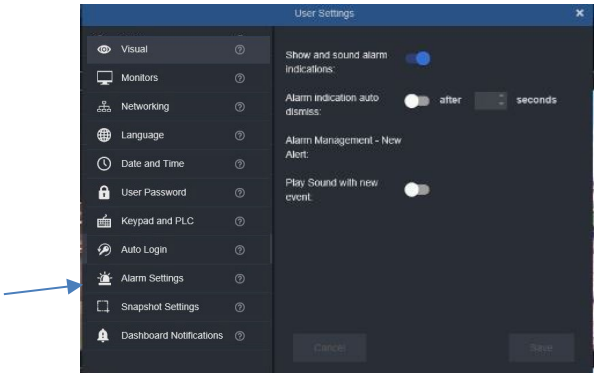
- The Keypad screen allows you to enable your keypad/controller to either the local client or to all clients (Send to all Clients is On by default) by clicking the button and then selecting the keypad/controller. When the user is enabled, a password can be entered for added security. The list will display the currently available devices; you must connect any serial device first to have it show up in the list. You must have the current software for the Vicon keypad; there is a link provided to the Valerus Software Installation page. Make sure that the current software for the keypad/controller is downloaded; if it is not, it can be downloaded directly from this screen. Remember that you must assign numeric IDs to cameras and monitors to use the keypad.



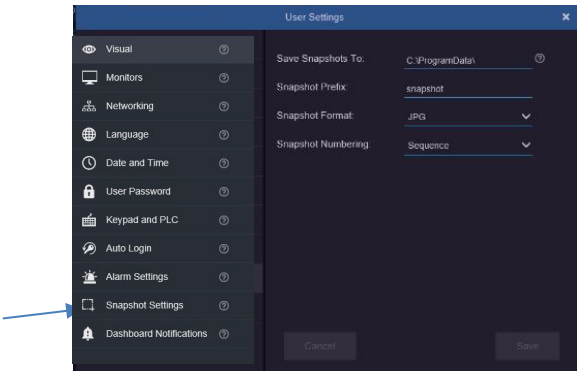
- Enable the Auto Login function by clicking the button so user can conveniently return to the last display. The Auto Login also supports the typical PLC operation.



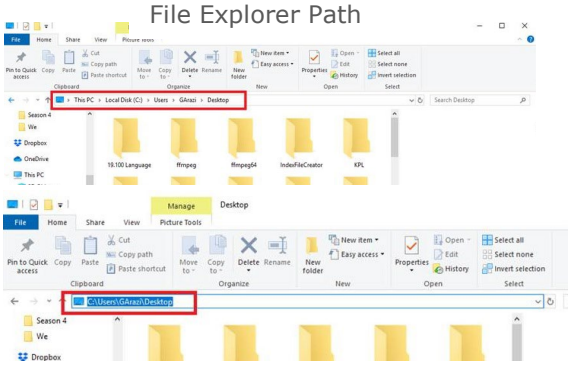
- The Alarm Settings can be configured for alarm indications per user to show an alarm icon, sound an alarm, Alarm Management-New Alert and to play a sound with a new event. The alarm indication can be set to be turned off (dismiss) after a set amount of time.



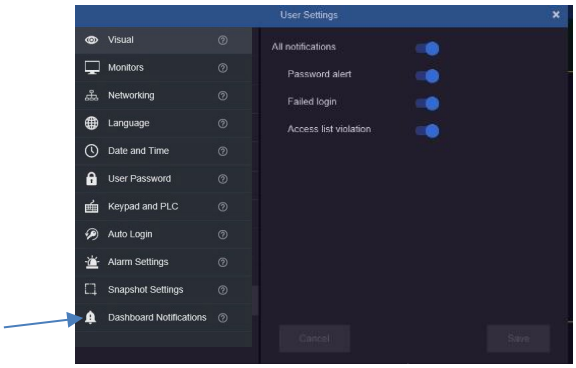
- The Snapshot Settings allows you to customize where the snapshots are saved, define a prefix for the file, select the file format (jpg, png or tiff) and determine how the snapshots are numbered, in sequence or by date/time. The default location to save snapshots is C:\ProgramData. To change this, the new path must be entered manually. The easiest way to get the path is to open File Explorer, navigate to the location where the snapshots are to be saved; click the address bar on top to show the path and then copy that path and paste it into Valerus.



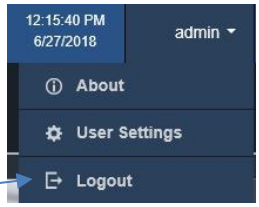
File Explorer Path

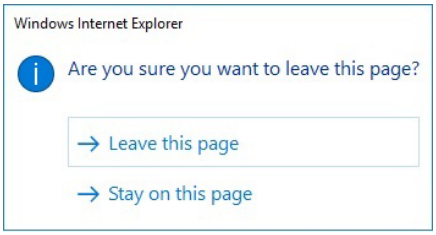


- Dashboard Notifications are typically set to show all notifications received in the Dashboard. Some notifications that may be repetitive in nature and not of interest can be switched off. Those are: enabling the default Password alert, Failed login and Access list violation.



- To exit the application, click Logout and Leave this page. Click Stay on this page to keep the program open.

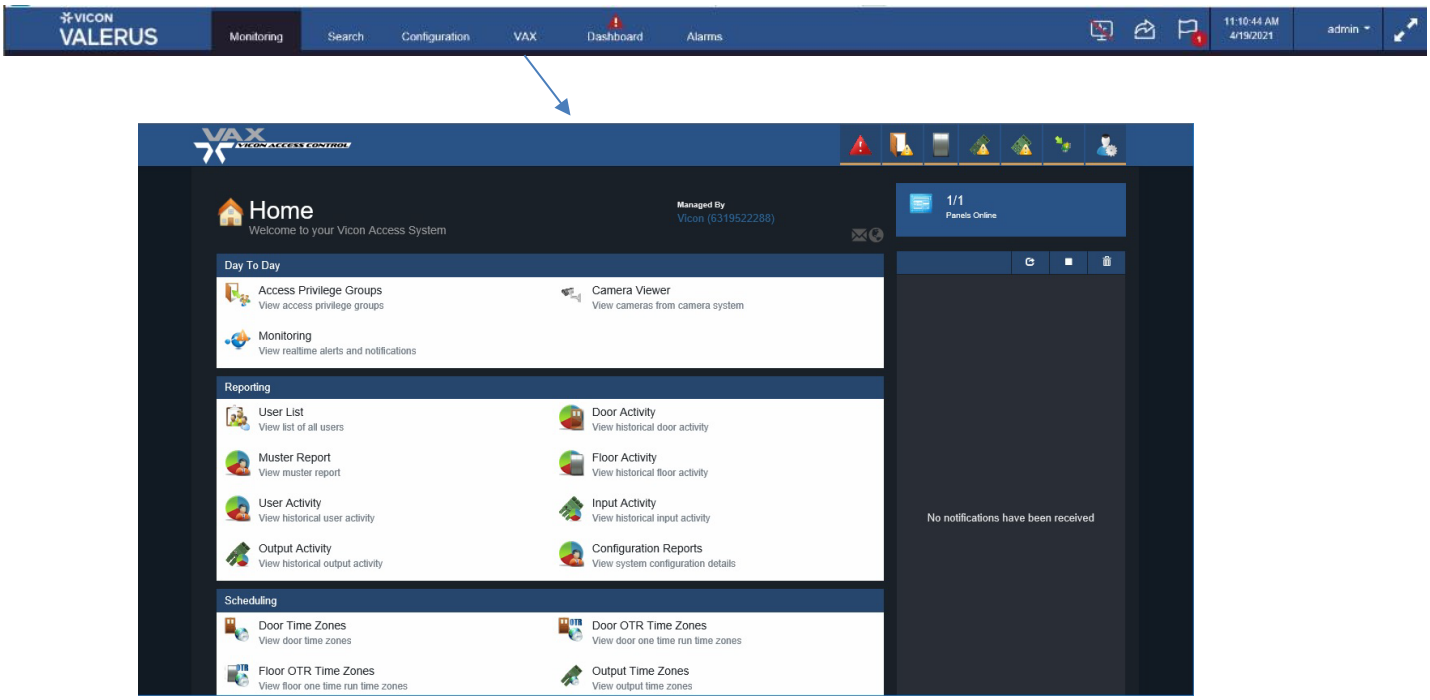




- The VMS closes all video display and returns to the Login screen. From this Login, there is an option to return to the last display page. This can be turned on or off by clicking it. The option is on (blue) by default.

VAX

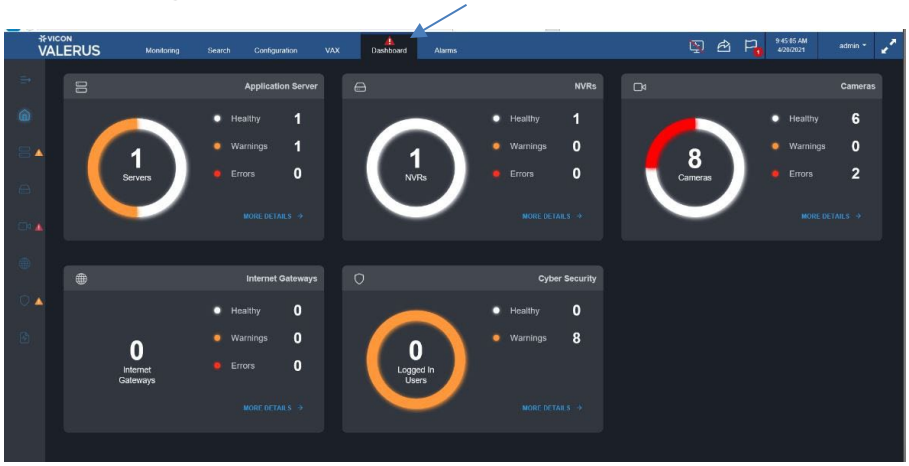
The VMS easily integrates the VAX access control system and offers the ability to control VAX directly from Valerus. Before VAX can be accessed from the tab, it must be enabled from the Configuration, System, Networking screen. Refer to that section in the manual for details. Click on the VAX tab; a popup screen will open the integrated VAX system. This screen can then be moved to any monitor in the system, so Valerus and VAX can be viewed simultaneously. Refer to the VAX documentation to operate the access control system.



It may occasionally be required to refresh VAX. When working with VAX in IE11, use the F5 button to refresh the page.

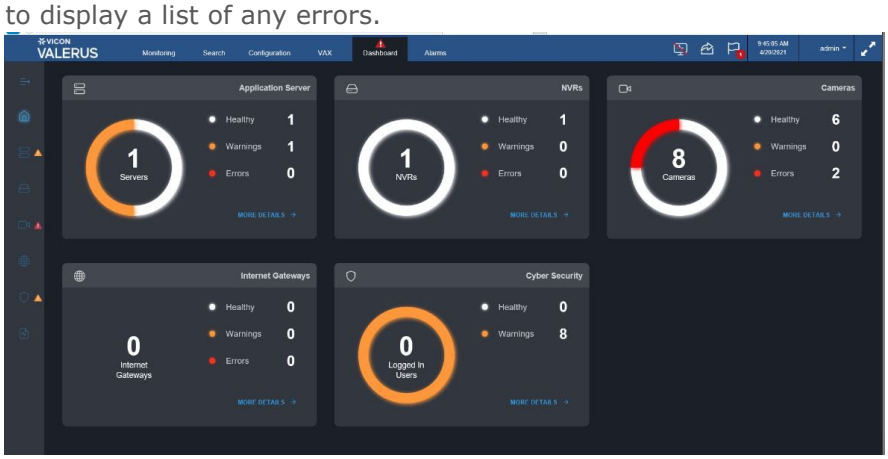
Dashboard

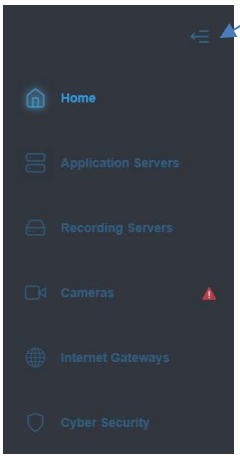
The VMS provides a Dashboard that presents the system's health status. If there are any errors or warnings, this is indicated on the Dashboard tab with either an orange or red triangle; a table of error messages is at the end of this chapter. Click on the Dashboard tab to open the system Dashboard. It is expected that in an average system all indications will be green and healthy. You can also access Statistics about your devices (Application Server, Recording Servers/NVRs and Cameras/Devices) from this screen to view; pie charts and graphs present information about camera distribution, storage, bandwidth, etc. There are tabs at the top to select Health Monitoring or Statistics.



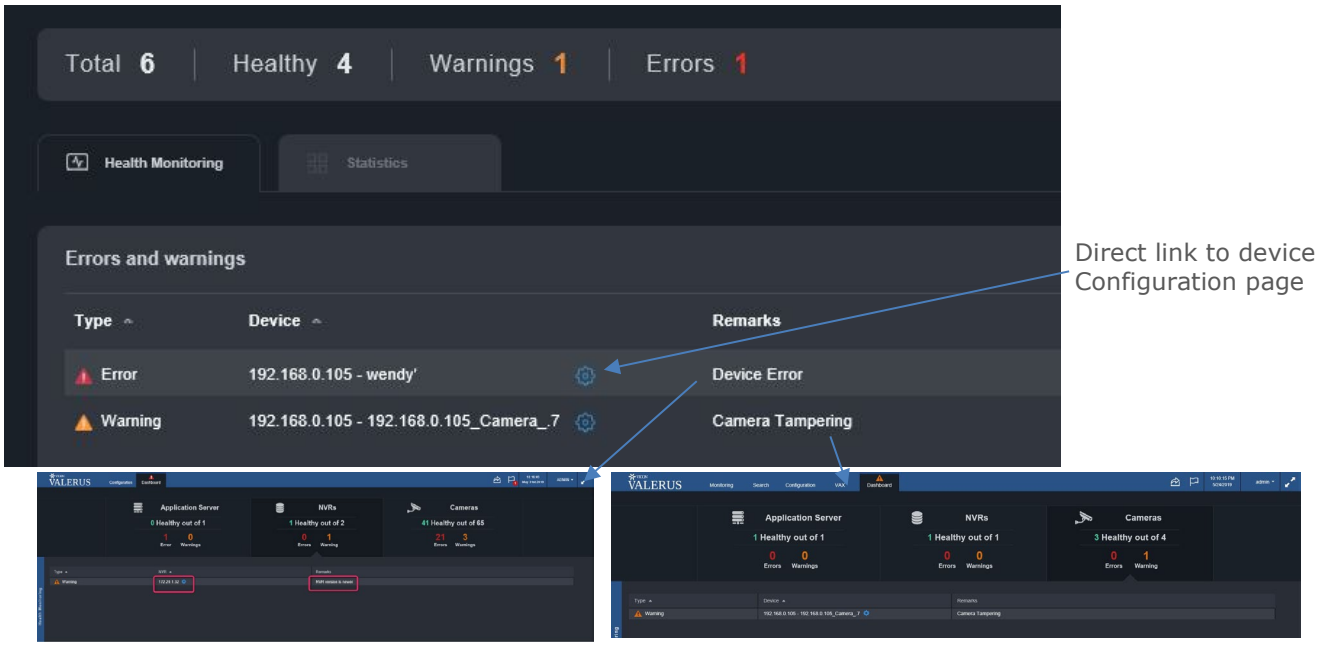
Health Monitoring

The total number of devices is indicated for Application Server, NVRs, Cameras, etc. Below the device categories are the indications for the health of the devices. The screen below shows a system of 1 Application Server, 1 NVR and 5 Cameras. Along the left side, there are icons indicating Home, Application Server, Recording Server, Internet Gateway and Cyber Security; clicking the expansion icon at the top will enlarge this and clicking again will collapse it. Click an icon or on More Details for the Application Server, NVR or Camera section to display a list of any errors.





A Warning (orange) indicates that the device is not working properly. An Error (red) indicates a more serious problem, like a camera is completely not working. There can be multiple warnings or errors per device. Clicking the icon next to the device dashboard error is a direct link to that device's configuration page, as long as user has permission. Below, 5 cameras have 2 warnings and 1 error. Clicking on the errors or warnings will display the problem in a table under the Dashboard, indicating the IP of the device and the problem. A Warning will also be sent when the license is due to expire in less than 14 days. A newer version available alert will be sent as needed.



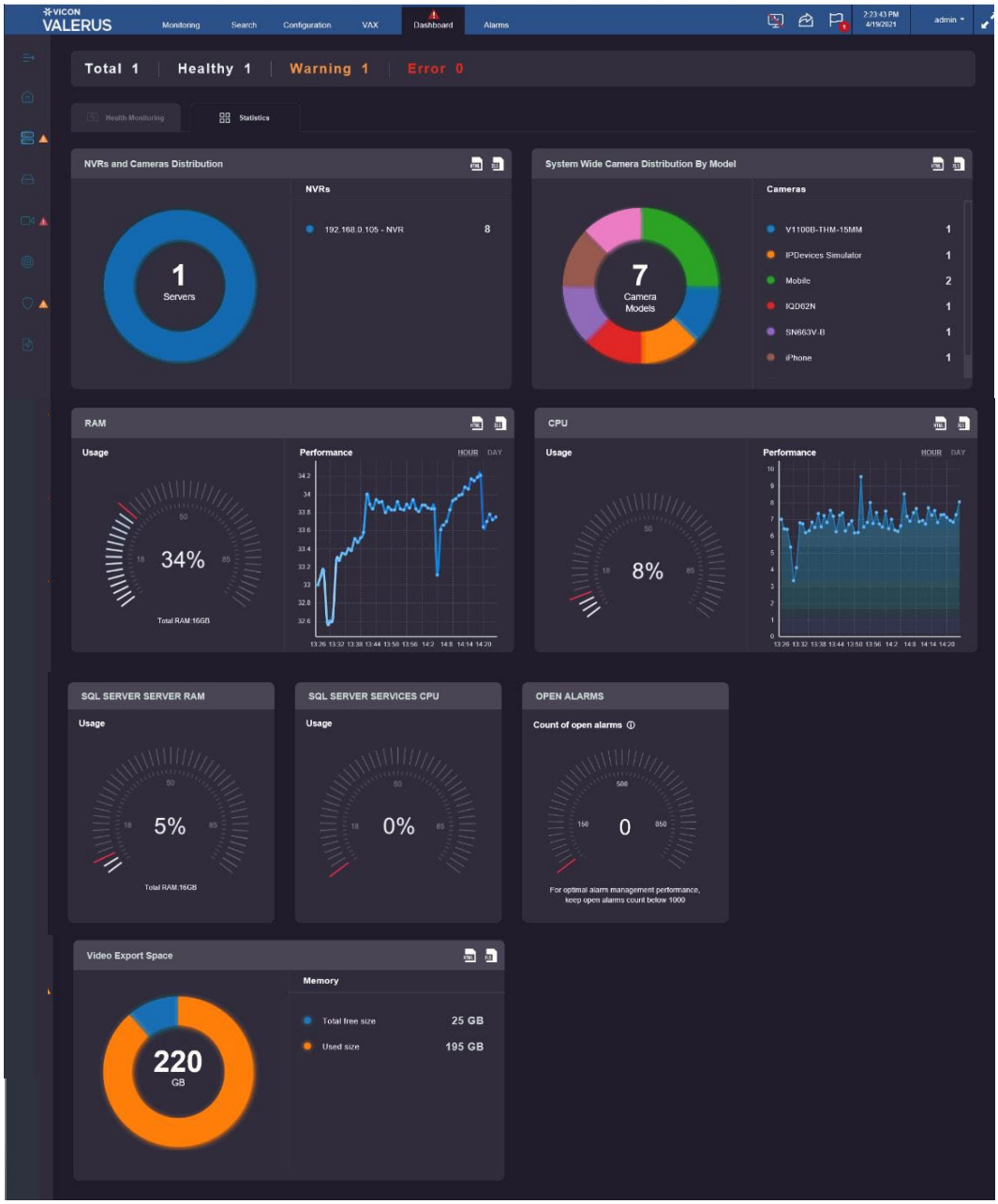
A table of error notifications, what they mean and a troubleshooting method to fix it is outlined at the end of this chapter.

Statistics

After selecting the Application Server, NVR or Cameras, you can click the Statistics tab on the top to view valuable statistics about your system. This information is very useful in analyzing system performance or to troubleshoot any problems you may be encountering.

Application Server Statistics

The charts and graphs present the system NVRs and how many cameras are being recorded on each. Additionally, see how many cameras from each model are connected to the system and RAM and CPU usage; also view the RAM/CPU usage from the SQL Server. In the rare instance that emails are not being sent, a message is sent stating sending email failed. This message will only display if you remain logged in to the system; the message can be cleared. A gauge of Open Alarms displays a count of alarms that are new and have not been assigned to any user or closed. If too many alarms remain open, this may impact the database as well as impact on Alarms Management performance (cause slower response time); a message will be sent if this number goes above 1000. To avoid this problem, either close the alarms or set the alarms to auto close (expire) after a certain period of time; refer to the manual for Alarms Management for details. A graph of Video Export space is also provided. This shows the amount of free space and used space on the drive that is designated for storing exported video; this is important especially if that drive is used for storing other data. A report can be created for each of these charts and graphs, in Excel or HTML format by clicking the icon in the right corner or the screen.

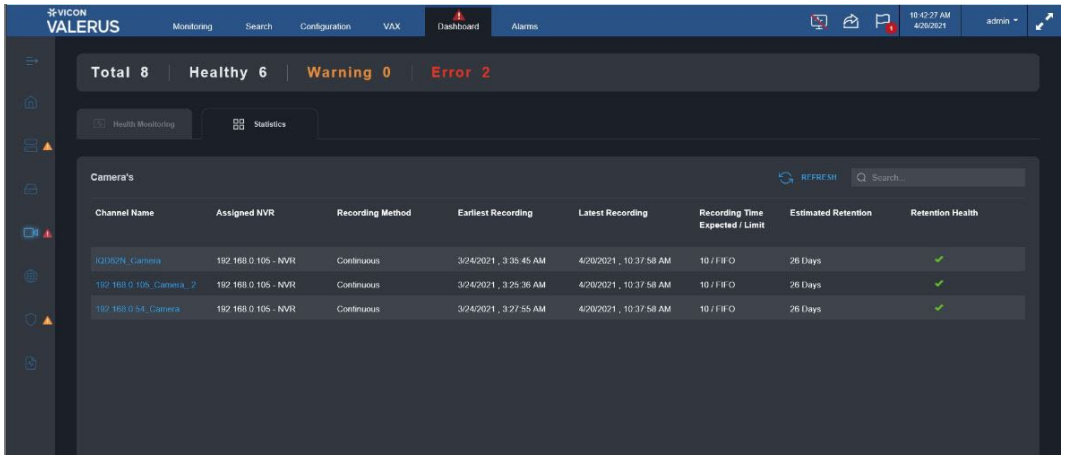

VICON
VALERUS
Monitoring
Search
Configuration
VAX
Dashboard
Alarms
admin
Total 1
Healthy 1
Warning 1
Error 0
Health Monitoring
Statistics
NVRs and Cameras Distribution
NVRs
192.168.0.105 - NVR 8
1
Servers
System Wide Camera Distribution By Model
Cameras
V1100B-THM-15MM 1
IPDevices Simulator 1
Mobile 2
IQD62N 1
SN663V-B 1
iPhone 1
7
Camera Models
RAM
Usage
34%
Total RAM:16GB
Performance
HOUR DAY
CPU
Usage
8%
Performance
HOUR DAY
SQL SERVER SERVER RAM
Usage
5%
Total RAM:16GB
SQL SERVER SERVICES CPU
Usage
0%
OPEN ALARMS
Count of open alarms
0
For optimal alarm management performance, keep open alarms count below 1000
Video Export Space
Memory
Total free size 25 GB
Used size 195 GB
220
GB

Recording Servers (NVRs) Statistics

Click the NVR. Charts and graphs show a summary for all NVRs in the system. Charts show cameras connected to the NVR by their model and how much storage is used by the different channels. Also see the average recording bandwidth, daily and weekly, standard/RAID system bandwidth utilization, RAM and CPU usage, NVR latency (connection speed) and Recording HDD SMART Status (if your system has Self-Monitoring Analysis and Reporting Technology -SMART- Valerus communicates with it and reports back so preventative measures can be taken). A report can be created for each of these charts and graphs, in Excel or HTML format by clicking the icon in the right corner or the screen.

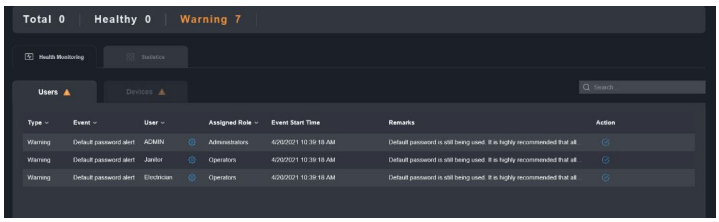
Cameras (Device) Statistics

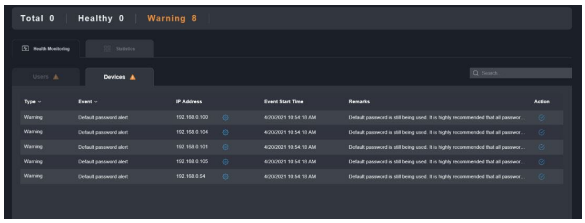
A table displays showing a summary for all devices in the system. When a device is clicked, a graph displays showing the expected recording days versus the projected recording at the current time. There is also a graph showing the bandwidth pulled from a camera to an NVR and the recorded bandwidth. Note that incoming can be both camera streams while recorded is a single stream at a time. You can also receive a message if you have a recording issue, where the camera is connected to the system but is not recording. A report can be created for each of these charts and graphs, in Excel or HTML format, by clicking the icon in the right corner or the screen.



Internet Gateways and Cyber Security

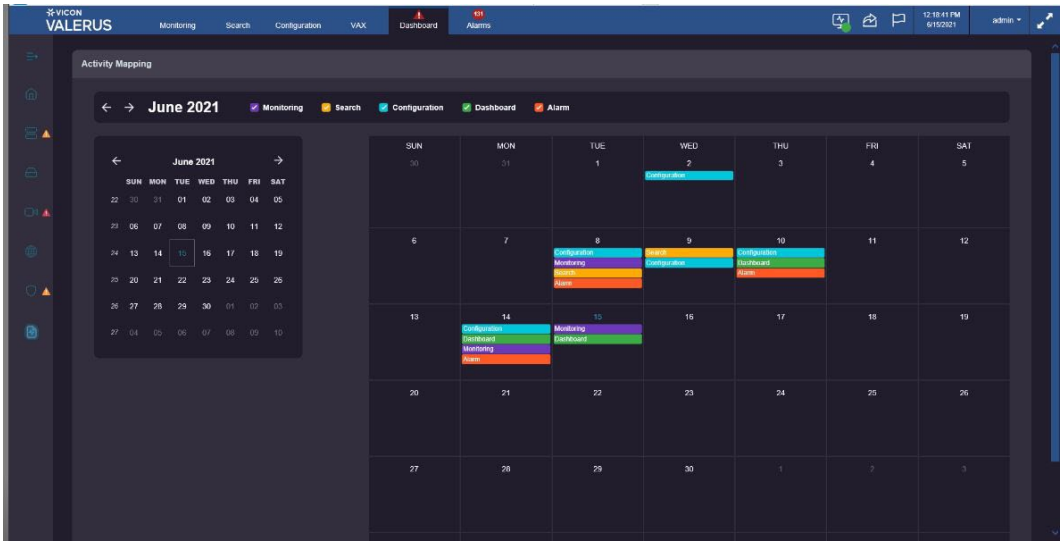
The Internet Gateways Health Monitoring screen indicates if the system is disconnected or offline. The Cyber Security displays information on Users and Devices. It shows who is logged in on the system and from where. A user can be removed if necessary. It will also display such issues as the same user logs in from two different units; in this case a duplicate user warning is sent and one of the users can be removed. Additionally, it reminds if a user is still using the default password and if any user is trying to login from an IP address that is not on the Access List.





Activity Mapping

Activity Mapping shows a calendar view and color-coded markings highlighting where there have been audits. This provides a high-level view, as opposed to a textual report, with the ability to access those entries.



- At the top of the screen there is a color key indicating the color identification of the screen where there has been activity:

  Monitoring: Purple
  Search: Yellow
  Configuration: Blue
  Dashboard: Green
  Alarm: Orange

- Select a date from the calendar. Clicking an entry will bring you to the Audit Log for the entry that has been filtered by the category and time of the activity.

Error Type	Error Message	Message Means	Error Fix
Error	Communication Failure: shown with client IP/Name	Connection between client and Application Server is down	Make sure the Application Server is running and check network connection between the client PC and the Application Server.
Warning	NTP Failure: shown with application server IP/Name)	Network Time Protocol Service is not running on the Application Server	On the Application Server go to Windows services and verify the "Network Time Protocol" service is running.
Warning	SNMP Service Failure	SNMP service is not running on the Application Server	On the Application Server go to Windows services and verify the "VII SNMP" service is running.
Error	License has expired	License evaluation period has ended (30 days from installation)	Under settings – System – Licensing, activate the system using a valid license key purchased from Vicon or as a free TRY system.
Warning	License will expire in ***#*** days	License evaluation period is going to end in the indicated number of days	This is a pre-expiration message, allowing time to obtain and activate a permanent system license.
Warning	UPP has expired. Contact your sales representative to renew	UPP (Upgrade Protection Plan) for your system has expired	Contact your Vicon representative to renew the UPP. You will need your system activation key to order.
Warning	UPP is about to expire on ***Date*** in ***#*** days. Contact your sales representative to renew.	UPP (Upgrade Protection Plan) for your system will expire in the indicated number of days	This is a pre-expiration message allowing time to renew you UPP and re-activate your license.
Warning	Last backup completed over 10 days ago	Last system backup was done over 10 days ago	This message is for informational purpose only. Vicon recommends setting the system to automatically backup every week.
Warning	Application server drive ***#:/*** has only ***#*** GB of free space available. Download and clear all exports from the server.	The Application Server O.S drive (typically C:/) is low on disk space and needs attention	This issue might be a result of multiple video exports that have not been removed from the Application Server. Make sure you download all exports to your PC and delete those exports (see exporting video for details). If this issue persists there maybe files, not related to Valerus, using too much space
Warning	Recording stream failure	NVR failed to record the stream it was set for	Check the stream settings for your camera and recording setting.
Warning	Camera tampering	Camera sent "Tamper" event	This event is generated by cameras that are covered or moved. Check the camera view for obstructions.
Warning	PTZ low pressure	A pressurized dome sent "Low Pressure" event	Check the PTZ camera internal pressure.

Warning	Device is not recording	Failed to record the device to the NVR	In configuration – Devices – Cameras and Devices tab, check the device status; if the status is OK, make sure the NVR is online (green check mark). This will also appear if a device recording is set to OFF.
Error	Storage failure	Storage failure - cannot record at all	Make sure that the NVR is online (green check mark) and the drives allocated for recording are accessible for writing and not blocked by a Windows permission issue.
Error	Could not connect to Local Drives	Problem connecting to a recording drive when the system is being initialized	Allow the drives some time to connect (for example, in an attached RAID this may take longer than the NVR to boot up) and if the problem persists, check the drives' connectivity.
Warning	No storage settings	Storage has not been set for this NVR	In configuration – Devices – NVRs, select the specific NVR and in storage definitions add drives for recording.
Warning	NTP Service failure: shown with NVR IP/Name	Network Time Protocol Service is not running on the NVR	On the NVR go to Windows services and verify the "Network Time Protocol" service is running.
Warning	SNMP service failure: shown with NVR IP/Name	SNMP Service is not running on the NVR	On the Application Server go to Windows services and verify the "VII SNMP" service is running
Error	Communication failure: shown with NVR IP/Name	Communication failure between the NVR and Application Server	Verify the Application Server is running. Verify the NVR is running. Check network communication between NVR and Application Server.
Error	Communication Failure: shown with Internet gateway IP/Name	Communication failure between the Internet gateway and Application Server	Verify the Internet Gateway is installed and properly configured.
Error	Server ID was not found	A device recorded in the database is pointing to a different Application Server than the current one	Delete the device from the NVR and then add it again.
Warning	Event subscription failure	Failed to register to receive events from the device (either pull point or base notification)	The NVR will continue to try and register for the events.
Error	Device not connected	Device that was previously connected is now showing status "offline"	Check device connectivity and IP address until it shows online (green check mark).
Error	Device error	There is a communication problem between NVR and camera/device	Check that the device status if online (green check mark) and that it can communicate (ping); try restarting the device

Error	Device not authorized	Device cannot communicate with the NVR due to a credentials issue	Verify that the credentials for the device (user and password) are set correctly.
Warning	MAC address changed	The device MAC address has been changed (different than the one the device was added with)	Delete the device from the NVR and then add it again.
Warning	NVR device database mismatch	One of the parameters set in the camera does not match the settings in Valerus	This is a situation where a certain setting in Valerus (example, resolution) does not match what the camera reports as set. Valerus will attempt to correct this issue, but if it persists contact Vicon Technical Support.
Error	NVR mismatch	NVR internal ID does not match its ID on the Application Server	Make sure NVR was not replaced with a new one and that the NVR database was not copied from another NVR. If the problem persists contact Vicon Technical Support.
Error	Server unauthorized	Credential error between Application Server and the NVR	Verify the NVR credentials are correct.
Error	Recording Problem	Camera is connected but not recording	Check camera recording settings Check the time line to confirm it is really not recording. Try to reboot the camera.

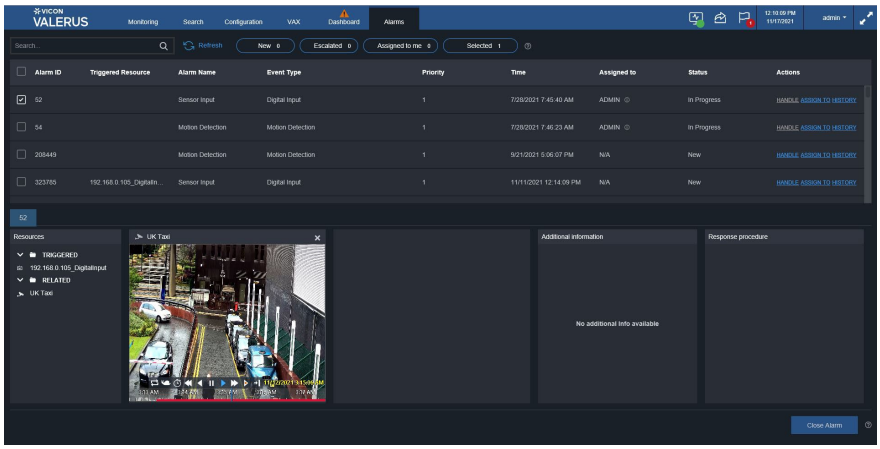
Alarms

The Alarms screen is dedicated for Alarms Management and shows the alarms along with their status; these are the events that have been elevated to alarm status set in the Advanced, Alarms screen in Configuration. From this screen, the operator can work to review and categorize the alarms. This tab can be moved to another monitor for ease of use. ***Refer to the Alarms Management Guide for a more detailed understanding on how to manage alarms.***

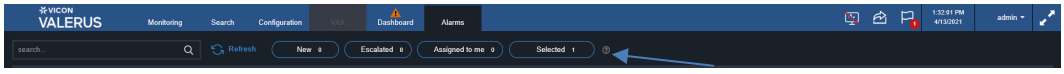
Alarms is a main tab on the top of the Valerus interface.

When this alarm screen is not in focus, a number will display on top of the tab showing the number of **new** alarms added since it was last closed. There is also an audible "ping" sound when a new alarm comes in; this can be turned off in User Settings if necessary.

- The alarm will show for the users that have been defined in the configuration phase; therefore, different users may get and work on different alarms, while others (Admin, for example) will see them all.

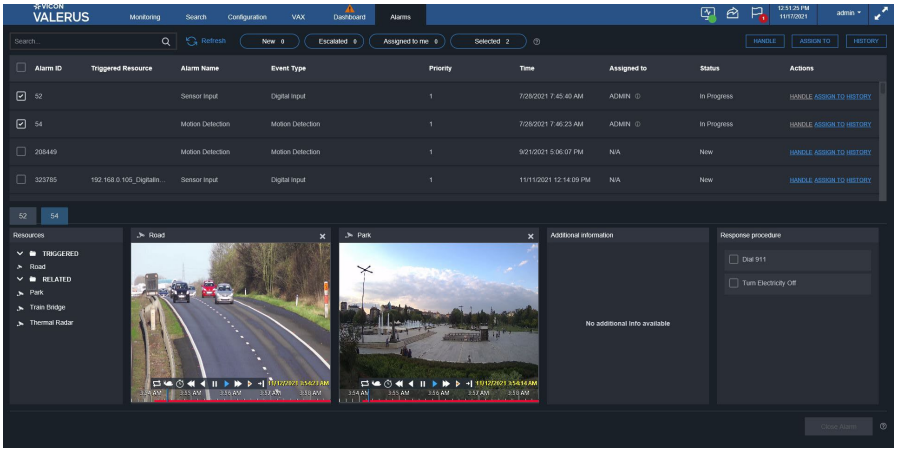


- The columns on the alarm list allow sorting the list in an order that is relevant to a specific user.
- On the top of the alarm page, there are several filtering options meant to simplify the selection of the alarms the operator needs to view and work on. They sort the alarms in whatever sense of urgency works best for the operator. The filtering buttons will turn blue when selected. These include a Search field for entering Alarm ID, Name or type or alarm, a New filter that will show only alarms with a status of new, an Escalated filter that will show alarms with an escalated status, an Assigned to me that will show alarms that are assigned to the currently user and a Selected filter that shows only the alarms that are currently selected from the list by this operator (multi-selection of alarms). This page refreshes every 15-30 seconds but can be manually refreshed by clicking the Refresh button.



After the alarms have been sorted, each open alarm can be addressed. An open alarm is an alarm that came into the system, is on the list but has not been assigned to anyone or has not been selected to handle by anyone. The ultimate goal is closing the alarms, which can only be done after handling of the alarm based on its life cycle settings.

Additionally, after selecting and playing an alarm, a Snapshot, Bookmark and Export (video and audio) can be created and is supported by the player.



- For each alarm in the list, there is an ID, Triggered Resource, Name, Event, Priority, Time, Assigned to, Status and Actions. In the Actions column, the alarm can be selected to handle by the current user or assigned to a user.
- Click on the alarm to display its information as it was configured at the bottom of the screen. Multiple alarms can be selected.
- Clicking History displays a list of time when this specific alarm has triggered in the past, providing information on a repetitive alarm.

Shipping Instructions

Use the following procedure when returning a unit to the factory:

1. Call or write Vicon for a Return Authorization (R.A.) at one of the locations listed below. Record the name of the Vicon employee who issued the R.A.

   Vicon Industries Inc.
   135 Fell Court
   Hauppauge, NY 11788
   Phone: 631-952-2288; Toll-Free: 1-800-645-9116; Fax: 631-951-2288

   For service or returns from countries in Europe, contact:

   Vicon Industries Ltd
   Unit 4, Nelson Industrial Park,
   Hedge End, Southampton
   SO30 2JH, United Kingdom
   Phone: +44 (0)1489/566300; Fax: +44 (0)1489/566322

2. Attach a sheet of paper to the unit with the following information:

   a. Name and address of the company returning the unit
   b. Name of the Vicon employee who issued the R.A.
   c. R. A. number
   d. Brief description of the installation
   e. Complete description of the problem and circumstances under which it occurs
   f. Unit's original date of purchase, if still under warranty

3. Pack the unit carefully. Use the original shipping carton or its equivalent for maximum protection.
4. Mark the R.A. number on the outside of the carton on the shipping label.

Vicon Standard Equipment Warranty

Vicon Industries Inc. (the "Company") warrants your equipment to be free from defects in material and workmanship under Normal Use from the date of original retail purchase for a period of three years, with the following exceptions:

1. Valerus Shadow Elite Servers, Recorders and Client Workstations: Five years from original retail purchase.
2. Vicon IP Cameras: Five years from original retail purchase.
3. Access Control System Components: Two year from date of original retail purchase. Some credentials have a lifetime warranty; refer to VAX warranty document for details.
4. Thermal Sensor VTR-3XXX/VTR-6XXX: One year from date of original retail purchase.
5. For PTZ cameras, "Normal Use" excludes prolonged use of lens and pan-and-tilt motors, gear heads, and gears due to continuous use of "autopan" or "tour" modes of operation. Such continuous operation is outside the scope of this warranty.
6. Any product sold as "special" or not listed in Vicon's commercial price list: One year from date of original retail purchase.

NOTE:

- If the product is to be used outdoors or in dusty, humid, or other hostile environments, it must be suitably protected.
- Camera products must be protected, whether in use or not, from exposure to direct sunlight or halogen light as the light may damage the camera image sensor. This applies to both indoor and outdoor use of the cameras.
- Failure to comply with any of the aforementioned requirements will invalidate this Limited Hardware Warranty.

Date of retail purchase is the date original end-user takes possession of the equipment, or, at the sole discretion of the Company, the date the equipment first becomes operational by the original end-user.

The sole remedy under this Warranty is that defective equipment be repaired or (at the Company's option) replaced, at Company repair centers, provided the equipment has been authorized for return by the Company, and the return shipment is prepaid in accordance with policy. Repaired or replacement hardware will be warranted for the remainder of the original Warranty Period or ninety (90) days, whichever is longer. When a product or part is exchanged the replacement hardware becomes the property of the original purchaser and all hardware or part thereof that is replaced shall become the property of Vicon.

The warranty does not apply (a) to faulty and improper installation, maintenance, service, repair and/or alteration in any way that is not contemplated in the documentation for the product or carried out with Vicon consent in writing, operation adjustments covered in the operating manual for the product or normal maintenance, (b) to cosmetic damages, (c) if the product is modified or tampered with, (d) if the product is damaged by acts of God, misuse, abuse, negligence, accident, normal wear and tear and deterioration, improper environmental conditions (including, but not limited to, electrical surges, water damage, chemical exposure, an/or heat/cold exposure) or lack of responsible care, (e) if the product has had the model or serial number altered, defaced or removed, (f) to consumables (such as storage media or batteries) (g) to products that have been purchased "as is" and Vicon the seller or the liquidator expressly disclaim their warranty obligation pertaining to the product, (h) to any non-Vicon hardware product or any software (irrespective of packaged or sold with Vicon hardware product) and Vicon products purchased from an unauthorized distributor/reseller, (i) to damage that occurs in shipment or (j) to damages by any other causes not related to defective design, workmanship and/or materials.

The warranty for the products shall run from Vicon to End User customers only (including product purchased through authorized partners and resellers). Vicon is not obligated under any circumstances to honor warranties on product(s) purchases from internet auction sites including eBay, uBid or from any other unauthorized resellers. Except as explicitly provided herein, Vicon disclaims all other warranties, including the implied warranties of fitness for a particular purpose and merchantability.

Software supplied either separately or in hardware is furnished on an "As Is" basis. Vicon does not warrant that such software shall be error (bug) free. Software support via telephone, if provided at no cost, may be discontinued at any time without notice at Vicon's sole discretion. Vicon reserves the right to make changes to its software in any of its products at any time and without notice.

The Warranty and remedies provided above are exclusive and in lieu of all other express or implied warranties including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. Certain jurisdictions do not allow the exclusion of implied warranties. If laws under such jurisdictions apply, then all express and implied warranties are limited to the warranty period identified above. Unless provided herein, any statements or representations made by any other person or firm are void. Except as provided in this written warranty and to the extent permitted by law, neither Vicon nor any affiliated shall be liable for any loss, (including loss of data and information), inconvenience, or damage, including, but not limited to, direct, special, incidental or consequential damages, resulting from the use or inability to use the Vicon product, whether resulting from breach of warranty or any other legal theory. Notwithstanding the foregoing, Vicon total liability for all claims under this warranty shall not exceed the price paid for the product. These limitations on potential liabilities have been an essential condition in setting the product.

No one is authorized to assume any liability on behalf of the Company, or impose any obligations on it in connection with the sale of any Goods, other than that which is specified above. In no event will the Company be liable for indirect, special, incidental, consequential, or other damages, whether arising from interrupted equipment operation, loss of data, replacement of equipment or software, costs or repairs undertaken by the Purchaser, or other causes.

This warranty applies to all sales made by the Company or its dealers and shall be governed by the laws of New York State without regard to its conflict of laws principles. This Warranty shall be enforceable against the Company only in the courts located in the State of New York.

The form of this Warranty is effective May 1, 2021.

THE TERMS OF THIS WARRANTY APPLY ONLY TO SALES MADE WHILE THIS WARRANTY IS IN EFFECT. THIS WARRANTY SHALL BE OF NO EFFECT IF AT THE TIME OF SALE A DIFFERENT WARRANTY IS POSTED ON THE COMPANY'S WEBSITE, *WWW.VICON-SECURITY.COM*. IN THAT EVENT, THE TERMS OF THE POSTED WARRANTY SHALL APPLY EXCLUSIVELY.

VICON INDUSTRIES INC.

For office locations, visit the website: vicon-security.com