videoNEXT®

JetStreamVS

Administrative Manual

Contents

Purpose

The purpose of this document is to provide Administrators of the JetStreamVS system the information and instructions to help plan, configure, and effectively and efficiently use the system for a variety of scenarios.

Introduction

We are proud to present JetStreamVS, the cloud solution that will improve and simplify the operation and management of your security systems. Some of the system benefits are as follows:
JetStreamVS allows you to build and grow your security system.
JetStreamVS is an open, standards-based software solution that works with almost any IP camera, including HD and megapixel. JetStreamVS is a proven security technology for today and beyond. Furthermore, JetStreamVS provides the easiest and most scalable VSaaS (Video Surveillance as a Service) today. This, combined with full policy-level administration, gives you the most capable and scalable surveillance and security tool ever developed. Most importantly, the system software platform leverages a classical IT approach to video content management.

With JetStreamVS, the user can:
Capture data from an infinite quantity of cameras
Organize data into a single intelligent, workable database
Store data in the cloud storage in accordance with enterprise archival policies
Display video data in an intuitive graphical user interface to all-credentialed users via web browser or wireless device

Chapter 1: Planning your JetStreamVS System

This chapter will provide you with an introduction to the most common situations JetStreamVS Administrators will face when installing, maintaining, or troubleshooting Security System software.

After you read this chapter, you should have a conceptual understanding of how to:
- Plan your system installation
- Configure and maintain cameras
- Administer Users' Access and Permissions
- Utilize other options and services within the system
- Ensure optimal system operation

Deployment Planning Considerations

One of the most important things to keep in mind when planning your Security System deployment is to plan your installation for future growth to make sure you are effectively utilizing your initial investment as your system expands.

Please review the deployment schema.

Simple Deployment Schema

The simple setup interconnects media producers (cameras) with consumers (clients) through a network where a JetStreamVS Cloud Service provides the midpoint. JetStreamVS manages cameras, provides video-recording and media analysis, and leverages multiple camera manufacturers' specifications into a uniform user experience for Clients.

As the number of video feeds grows, this setup will easily scale by extending the network infrastructure. The total number of Clients registered in the system is not a limited amount and JetStreamVS will be able to support up to hundreds of simultaneously connected and actively working users, as long as your network infrastructure is properly sized to accommodate that level of traffic.

Still, the simple setup has two important limiting factors:
1. The number of video feeds that can be simultaneously viewed is limited by the power of the CPU and graphics card available on the client's computer.
2. Available network bandwidth from the system to the client PC should be sufficient for the sum of all video streams the client expects to see simultaneously.

Network Infrastructure

- Media streams (video/audio) are heavy on transmission and storage by definition, so your network should have sufficient capacity for proper bandwidth handling.
- Network designs should allow for growth, as experience shows that Security Systems tend to expand over time.
- Reasonable consideration should be given to reliability and network security, due to the nature of the data that will be transmitted and processed.

Data Processing

- There are two major components that rely on the processing power of your system: The number of cameras and the number of clients.
- Analytics is an add-on that provides a heavy data processing load for the system. As such, it is recommended that your Avatar have a spare CPU-core per Analytics channel you are expecting to run. For instance, if you are trying to run Analytics on three cameras, you will need at least a four-core processor.

Client Platforms

- Client requires an internet browser; Chrome is suggested.
- The number of simultaneously visualized camera feeds depends mostly on client computer CPU power and on a reasonably powerful (mid-class) video adapter.

Sizing Considerations

- The cloud solution is scaled automatically for you as you increase/decrease your subscription and includes both computing and storage.
- You are able to add as many avatars to your system as needed for your camera count and analytics processing needs.
- You can set all avatars to a single location or allocate them to several locations to allow for better connectivity to your cameras. The JetStreamVS cloud solution will consolidate muli-avatar / multi-site deployment into one operating view for you.
- Clients having local network access to avatars automatically discover this network affinity and automatically enable "local streaming", resulting in substantially less internet-connection bandwidth utilization and lower bill for the video-streaming usage, as local streaming is not counted against clients video streaming usage.

Chapter 2: Planning Your JetStream System

This section will detail how to configure the different pieces needed to get a bare-minimum installation operational. Later sections will detail specific configuration steps.

We will cover how to:
- Log into the system
- Configure the cameras - see the section called “Cameras”
- Configure the Credentials (so that your Users will use the system) - see also Chapter 3: Users, Roles and Management

Logging Into the Control Panel

The system is accessible through your internet browser.

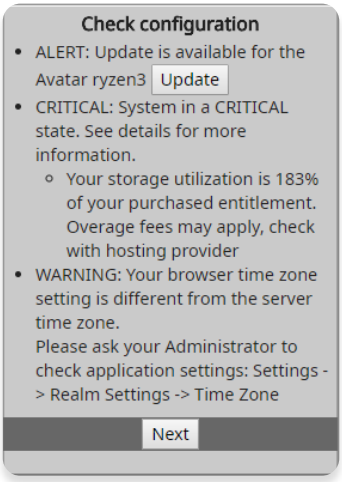
NOTE: *The primary supported browser is Google Chrome*

NOTE: *You have the option to choose a language. English is the system’s default language. Changing the language will change the character set as well as the read-direction (i.e. right-to-left versus left-to-right) for your session on the server. *This manual will assume a left-to-right reading orientation.*

Figure 1: Login Screen

The Administrator's default login name is your email address used by you during the JetStreamVS registration process. The Administrator’s password is your JetStreamVS application password chosen by you during your JetStreamVS registration process. You can change it when you finish with the system's initial configuration (see the section called “Users, Roles and Management”).

Figure 2: Check Configuration



After clicking the Login button, you will be taken to the **Check configuration** screen, which will notify you of the system status. Any system warnings, errors, or updates will show up here, so that you are notified as soon as you enter JetStreamVS. Some of the messages you will see may include: cameras in a “broken” state, time synchronization.

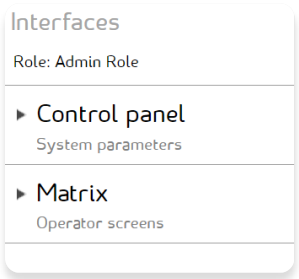
Once you have read the system warnings, click on the ‘**Next**’ button in order to be taken to the interface selector.

You may or may not receive a screen showing system warnings or errors. These would include messages about cameras being in a "broken" state, time synchronization, and software updates, if needed.

Since the Administrator by default has access to any User Interface, the next prompt will be where you select your interface. You are given the option between ‘Control Panel’ or ‘Matrix’ on the Interfaces screen, as shown in Figure 3. You will need to choose ‘**Control Panel**’ to continue with the system administration. For purposes of this manual, keep the default Role: Admin Role.

You should now be logged into the system and in the Control Panel interface.

Figure 3: Interfaces



Control Panel

This document is structured in order of appearance from the Control Panel for ease of Admin navigation. Every setting, configuration item, and any information you may need regarding your JetStreamVS system is viewable from the Control Panel.

Sets

This area in the Control Panel is where you will find your “sets” of cameras or other devices. You will read more on this under “Set Management” in Chapter 3: Users, Roles, and Management in the manual for configuration purposes.

Avatars

Where you will see the Avatars you have activated in the system. More on this under **Settings | Activate Avatar** in Chapter 3.

Video Walls

This is where you can configure the video walls. See in **Video Walls** in Chapter 5

Credentials

See more below in Chapter 3.

Chapter 3: Users, Roles, and Management

The Credentials Management system consists of four layers:
- Resources (cameras, sensors, etc.)
- Sets (resources grouped together)
- Roles (coordinated collections of Sets and Permissions)
- Users (any person participating in one or more Roles)

Resources are assigned to Sets, while Users and Sets are assigned to Roles (with privileges). A single Resource may exist in multiple Sets, and a single Set may be assigned to multiple Roles (possibly with different permissions per Role). A Role can have multiple Users assigned to it, and a User may also belong to multiple Roles.

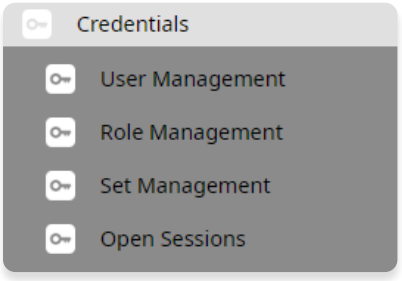
To avoid over-complicated configurations as the system grows, JetStreamVS does not allow individual Resources to be assigned directly to Users. Resources will always have to be assigned through Roles and Sets, even if a “flat” configuration is required.

NOTE: *The system automatically maintains a predefined "My Set" set and "Admin"/"Guard"/"Manager"/"Viewer" roles for convenient management of simplified (“flat”) configurations.*

Credentials (continued)

Many of your management and settings are viewable and configured here, such as User Management, Role Management, Set Management, and Open Sessions. See each of their sections within this manual for further information.

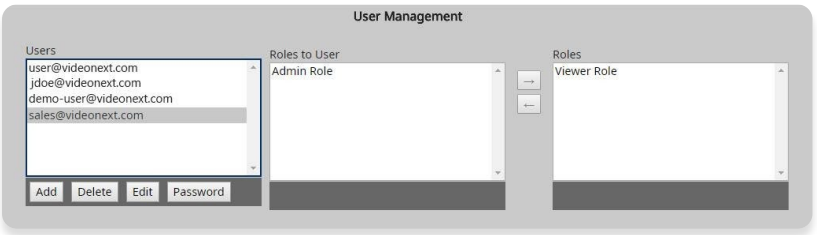
Figure 4: Credentials Layout



User Management

User Management in JetStreamVS is simplified by assigning a User to one or more Roles. It allows for easy Credential reallocation for the pool of users.

Figure 5: User Management



NOTE: *A User can only operate one Role at a time. If multiple Roles are accessible for particular Users, then the user will be allowed to select a current active Role. This is not a software limitation, but a mechanism to keep the user experience consistent among multiple Users working in concurrent environments.*
When adding or editing a User, you will be given the option to set the name, description, and password. You can also input an email account if you want events from certain devices to be sent to this user.

Role Management

Here you can manage Roles while relegating Sets to Roles and determining Credentials assignment between them.

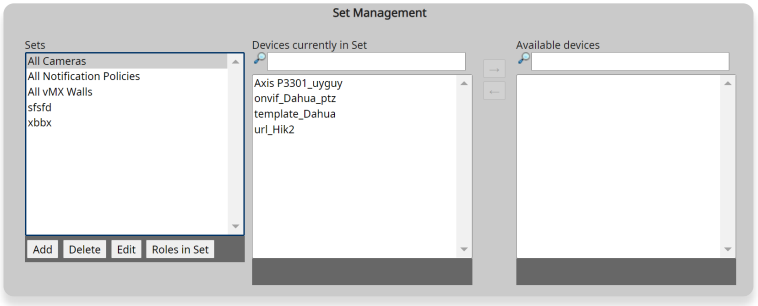
Much like with Set Management, to add or remove a Set or User to or from a Role, highlight the Set and click the left/right-arrow button(s). When a set is assigned to the Role, you can also choose the Permission level.

There are three permissions that can be assigned, and each subsequent higher permission includes the lower permissions. The lowest permission level is “View”, which only allows the user to view live video from a camera. The next level is “Control”, which enables the user to control the camera through PTZ and to view archived video. The highest permission level is “Manage”.

Set Management

As you have been adding the devices into JetStreamVS, they have automatically been added to one of the System Sets to keep track of them. By default, only the Admin account is able to access the System Sets, so you will need to create a few Custom Sets in order to allow other Users to access these devices.

Figure 6: Set Management



Sets (continued)

Sets play a number of roles within the JetStreamVS system. Primarily, they are a great way to keep your devices organized in a meaningful fashion. For example, you can create one Set for Indoor devices, and one for Outdoor devices. The System Sets already do this to some extent by automatically sorting all of your devices based on their type.

Additionally, Sets allow you to dictate which devices a User is able to access. As devices are grouped into Sets, and Users are grouped into Roles, you are able to assign permissions to Roles for accessing certain Sets. As mentioned above, the Admin account has access to every device in the System Sets, which contain every registered device in the system. A different User, one without access to System Sets, will be limited to the devices found within the Sets accessible to their Role. It is entirely possible to have the same device in a number of Sets.

Here, the focal point is the “Sets” list. Upon selection you will see the associated Roles and those which can be assigned to that set.

Roles and Devices

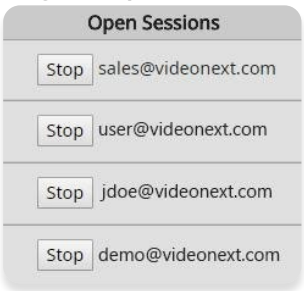
The two boxes on the far right-hand side of the screen are all Roles and Devices not currently associated with this Set. The two boxes in the center are for the Roles and Devices that are already associated with this Set. Highlighting any Role or Device will allow you to assign/unassign it to/from the currently selected Set.

- To assign or remove Devices from the Set, simply click on the device's name, then use one of the arrows located between the two boxes to move it in or out of the Set. There is also a helpful search function which will allow you to quickly find the device you are looking for by typing in its name.
- To create a new Set, click the "Add" button in the left-most box. This will open a dialogue to name the Set and provide an optional description. Once added, you will need to assign Roles that can view the Set and its associated Devices.
- To delete a Set, select it and press the "Delete" button. You can only delete "User Sets". You cannot delete System Sets (such as "All Cameras"). Deleting a Set does not alter the devices in that set. When selecting a Role in the "Role to Set" box (top-middle), you will be given the option to enable "Email-On-Event" (this is only available for user-generated Roles).

Open Sessions

This will show a view of all sessions that you have currently open. It should show any instances you are on or controlling. See example below:

Figure 7: Open Sessions

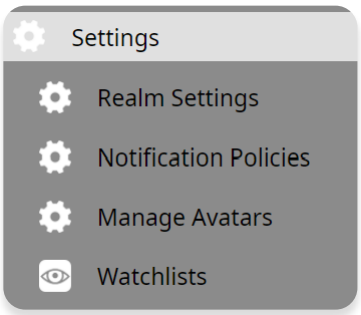


Settings

Navigate to **Settings** to edit your General System Settings:

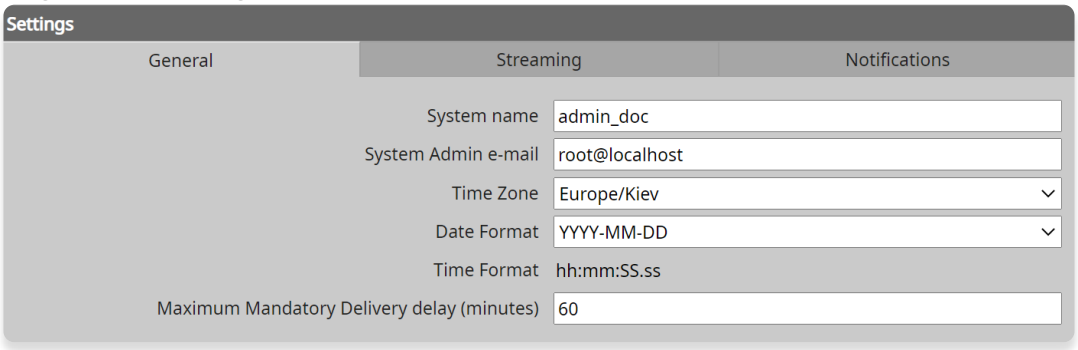
This item in the Control Panel allows you to configure many of the various settings you'll need to operate within the system. Here you will see Realm Setting, Notification Policies, Manage Avatar, and Watchlists. See each section for further information in this manual.

Figure 8: Settings



Realm General Settings

Figure 9: Realm Settings Screen

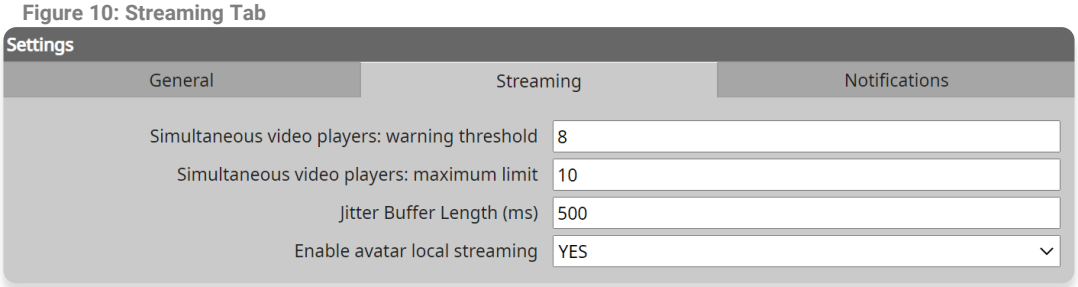


General Tab Descriptions

System Name	Use this field to describe the name of your system in the browser
System Admin E-Mail	Set your system Admin e-mail
Time Zone	Select and set your Time Zone
Date Format	Choose your Date Format
Time Format	hh:mm:SS.ss (Read only)

Streaming Settings

Figure 10: Streaming Tab



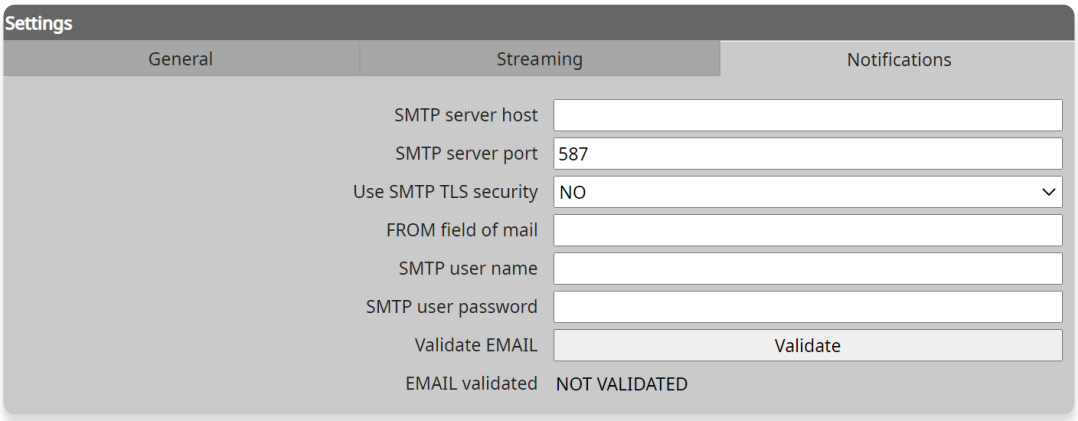
Streaming Tab Descriptions

Simultaneous Video Players: Warning Threshold	Sets the warning for high threshold of simultaneous video players accessing video in one browser session

Simultaneous Video Players: Maximum Limit	Limit the number of simultaneous players in one browser session
Jitter Buffer Length (ms)	Set Jitter Buffer in milliseconds. Setting it lower will minimize video delay but may cause jittery movements
Enable avatar local streaming	Yes/No Local avatar streaming works only during the current session if network is transparent between avatar and your workstation

Notification Settings

Figure 11: Notifications Tab

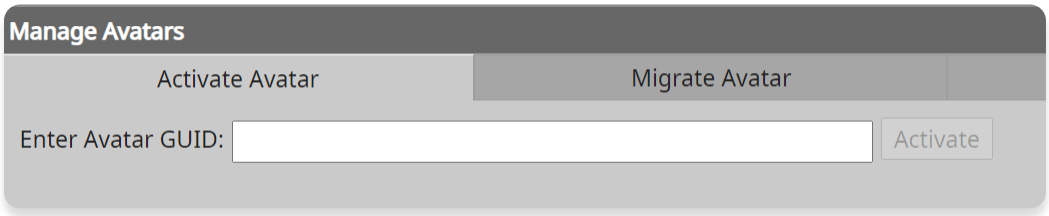


General Tab Descriptions	
SMTP server host	Host server name
SMTP server port	SMTP port number
Use SMTP TLS Security	Yes/No
FROM field of mail	From Address
SMTP user name	Username of SMTP server
SMTP user password	Password of SMTP server
Validate EMAIL	Validates if email address is active
EMAIL Validated	Email validation status (Read Only)

Activate Avatar

When you access your system at the first time, you will not see any active Avatars under the location 'Avatars', because you need to activate them for them to be known by the system.
To activate your Avatar, you need to have your Avatar's GUID number. This GUID number was created during the process of your Avatar installation. If needed, Avatar installation instructions can be read in Appendix C: Avatar Installation.
From the Control Panel, navigate to **Settings** | **Manage Avatars** and enter your GUID number. Click the '**Activate**' button.

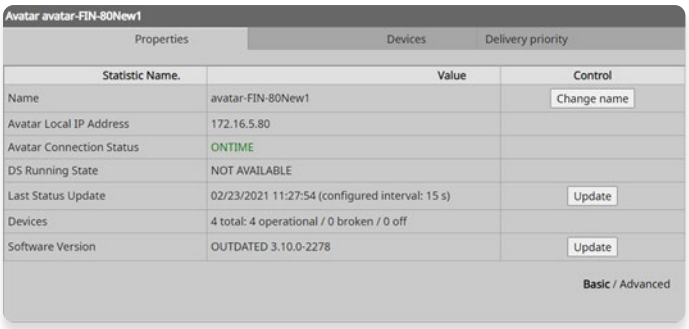
Figure 12: Activate Avatar



Avatar Configuration Panel

*This panel appears after the **Activate** button is clicked*

Figure 13: Avatar Configuration Panel



Properties

Avatar 'Properties' monitors the properties of your Avatar connection.

***NOTE:** You can also manually request an update of your properties. It will show the progress of your content delivery and turnaround time. If you see on the properties panel that the version of your Avatar is outdated you can manually request to update it. It may take from a few minutes to up to an hour for updates to be downloaded and installed. In the end of the update process, your Avatar box will restart automatically. You can continue using software as usual, the update process is executed in the background.*

Devices

Here you will find cameras registered on this particular Avatar. Allows you to add more cameras or edit camera settings.

Delivery Priority

Sets the hierarchy for which camera delivers first

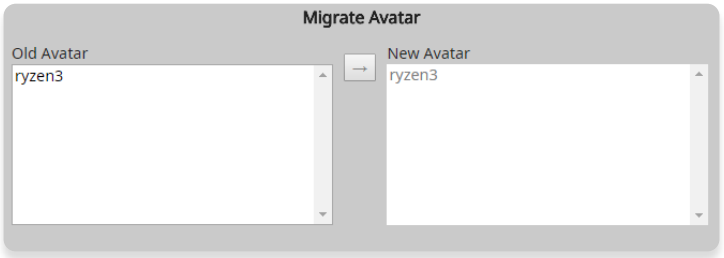
Migrate Avatar

If for some reason your Avatar box was lost, broken, or for performance purposes you need to reallocate resources, you can migrate the original settings of your Avatar to a new Avatar box using this menu. You'll need to activate your new Avatar on your system. As soon as it's activated, you will see it in the New Avatar window. Next you can select the original Avatar in the Old Avatar window, and select the New Avatar box and apply your changes. This will apply all of the settings you had on your Old Avatar box to your new Avatar including all cameras' settings.

NOTE: *Migrate Avatar is used to migrate Settings, but does not migrate archived video or video delivery queue contents. It is important to consider that, If you wish to retain any particular important data, it must be archived into the cloud before any possible loss occurs from a result of a lost or broken Avatar.*

You will need to navigate to **Settings | Migrate Avatar** to handle the above task.

Figure 14: Migrate Avatar Screen



Watchlists

Watchlists can be configured for Licence Plate Recognition (LPR) and Face Recognition. These watchlists apply to the entire system. Detected entities on devices with Watchlist functionality enabled (either license plates or people's faces) are compared against registered entries in the Watchlist. Multiple watchlists can be configured as either 'whitelists' or 'blacklists'. This changes the system behavior for non-matches and matches, respectively. For example, you might want a the system to create an alert if it sees a license plate NOT belonging to an employee; alternatively, you might want an alert when the entry-hall camera detects the face of a VIP.

In summary, activating the Watchlists feature is extremely beneficial. If Watchlists are enabled, the system can match facial recognition and/or LPR against items in the Watchlists. Watchlists are highly recommended.

Face Recognition Watchlist

Watchlists are accessible under the Settings on the navigation menu. For this case select the **Face Recognition** watchlist

To add a Face Recognition Watchlist press the **Add** button

Enter the following details in the pop-up dialog box titled **Add new watchlist**:

- **Name**: Enter a name that is easily identifiable
- **Description**: Enter a short description that explains what the list is for
- **Action**: In the dop-down menu there is the option to choose from Alert, Ignore, or Event

When to choose Alert, Ignore, or Event

Alert WL	Ignore WL	Event WL
Triggers an alert whenever the listed face is detected	When the listed face is detected the system will ignore it	Triggers an event to be recorded whenever the listed face is detected

Press **Apply** to save

Under the Operations column press the notepad icon to edit the watchlist. Press **Add entries** to add a new face. Enter the following:

- **Description**: Enter the name of the subject (ex. John Doe)
- **Expiration date**: Set and confirm an Expiration date for the photos
  Note: After the photos have reached their expiration date, they will automatically be deleted
- **Upload Picture(s)**: Press the Upload Pictures button to add pictures of the subject to the system. These pictures will be used as a reference so that the system knows what subject to fine. Adding more pictures will increase recognition accuracy

Once finished, press **Apply** to save. Your watchlist is finished.

NOTE: Add as many people desired to the watchlist by starting a new entry

License Plate Recognition Watchlist

Watchlists are accessible under the Settings on the navigation menu. For this case select the **License Plate Recognition** watchlist

To add a License Plate Recognition Watchlist press the **Add** button

Enter the following details in the pop-up dialog box titled **Add new watchlist**:

- **Name**: Enter a name that is easily identifiable
- **Description**: Enter a short description that explains what the list is for
- **Action**: In the dop-down menu there is the option to choose from Alert, Ignore, or Event

When to choose Alert, Ignore, or Event

Alert WL	Ignore WL	Event WL
Triggers an alert whenever the listed LP is detected	When the listed LP is detected the system will ignore it	Triggers an event to be recorded whenever the listed LP is detected

Press **Apply** to save

Under the Operations column press the notepad icon to edit the watchlist. Press **Add entries** to add a new license plate. Enter the following:

- **Description**: Enter a description about the license plate
- **License Plate**: Enter the exact license plate characters
- **Expiration date**: Set and confirm an Expiration date for the license plate

  Note: After the license plate has reached its expiration date, it will automatically be deleted

Once finished, press **Apply** to save. Your watchlist is finished.

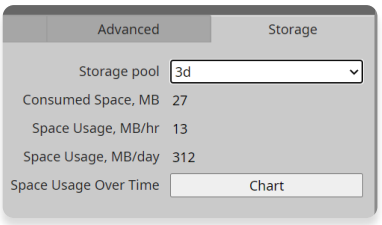
NOTE: Add as many license plates desired to the watchlist by starting a new entry

Chapter 4: Storage and Storage Management

Storage Pools

Storage Pools are created and modified as part of your subscription.

Figure 15: Storage Pool



Managing Storage Pools

The Admin Role can only view cameras added to the different Storage Pools from the menu Storage Pools.

NOTE: *Storage Pools are defined externally in the Subscription and are only referenced in the AdminUI.*

Managing Storage Consumers

Once your system is configured, you can Manage Storage Consumers. In essence, you assign your Storage Consumers (cameras) to use a particular Storage Pool.

From inside Admin UI, you must assign a camera to one Storage Pool.

Avatar storage is utilized to buffer content scheduled for delivery to the cloud storage and to serve local streaming requests and archive-on-demand requests (where originally content was not marked to be delivered by a rule engine, but rather operator explicitly requested delivery to happen).

Once the camera's number of days in storage is known, this will define the number of days content of this particular camera will be retained, both in the cloud storage and in Avatar local storage. Content is managed in FIFO manner, or “First In-First Out”.

Avatar will store as many days of video as it can, within the camera’s retention period, until it runs out of room on the storage drive. The Avatar will then begin to purge the oldest content, based on the FIFO algorithm. Avatar will attempt to retain at least 15% reserve capacity. The number of days an Avatar can retain is therefor dependent on the number of cameras it has, and the size of its storage drive.

Cameras as Storage Consumers

You can view All Cameras under: **Sets | All Cameras**

One method of storage is to load the individual camera configurations and assign the Storage Pool from the drop-down list. This method works best when you are dealing with relatively few cameras.

Chapter 5: Cameras

Individual Cameras

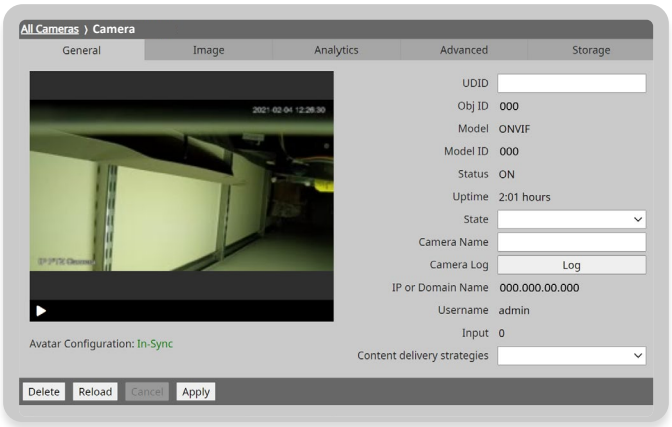
A camera's configuration page is divided into multiple tabs. On each tab there will be a box with a snapshot from the camera and a "Play" arrow to allow video to be played from that camera. The content of the tab is dependent on the make and model of the camera, but the most common attributes will be listed below.

The General Tab

Displays the state of the camera on the system. It includes information like name, model, and status.

The Configuration Menu consists of a number of tabs; each one responsible for one area of configuration. The Menu will always open on the General Tab like the one in the image to the right.

Figure 16: General Tab



Below explains the significance of each individual setting found in this tab:

General Tab Descriptions	
UDID	This represents the user-modifiable identifier. A default UDID will be generated using the Obj ID if this field is empty. It is displayed alongside the Camera Name.
Obj ID	The unique device identifier automatically assigned by the system. **Read Only**
Model	The Camera Model identified through automatic probing. **Read Only**
Model ID	The make of the camera identified through automatic probing. **Read Only**
Status	The current status of the device. The possible values are: “ON,” “OFF,” “Starting,” and “Stopping”. **Read Only**
Uptime	This lists the duration of the current network connection to the camera. If this number is routinely low, it may indicate a problem with the camera. **Read Only**

General Tab Descriptions Continued

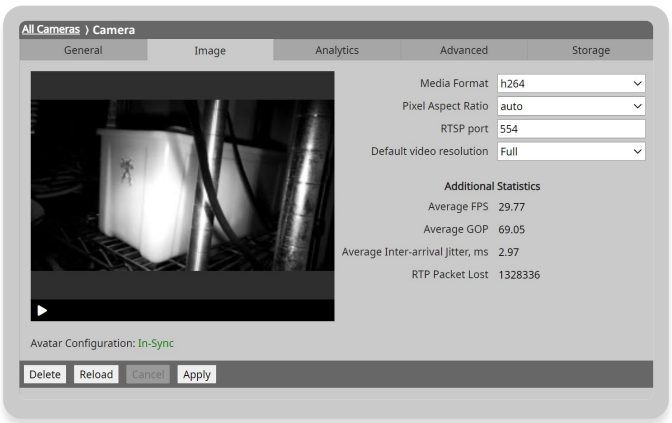
State	The control which allows you to turn the camera “ON” or “OFF”
Camera Name	Allows you to set the name of the camera. A meaningful name will allow you to easily identify the device.
Camera Log	Pressing this button will display a log of the camera's current activities. This button allows you to preview a real-time report of the internal system messages, where you might find reports on issues like wrong username/password, rejected connection, etc.

The Image Tab

The Image Tab controls what type of video should be retrieved from the camera.

The menu consists of multiple setting that are editable and some that are read only

Figure 17: Image Tab



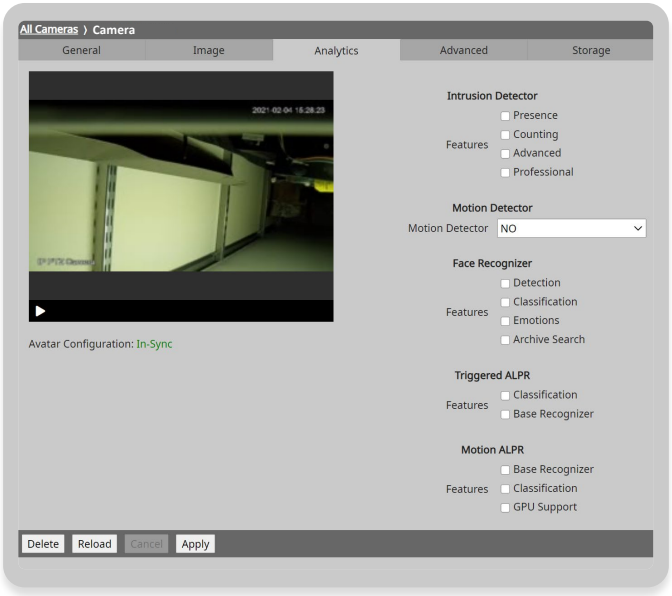
Below explains the significance of each individual setting found in this tab:

Image Tab Descriptions	
Media Format	A selection of supported video-stream formats: mjpeg, mpeg4, and h264.
Pixel Aspect Ratio	Allows you to manually set the pixel aspect ratio to be used for this camera. The default setting of “Auto” is sufficient for most use-cases.
RTSP Port **Model ID**	Allows you to set which network port to use to retrieve video. If the Retriever Protocol for the camera is HTTP, then this field will be replaced by the “HTTP port” field. The default for RTSP is port 554. The default for HTTP is port 80.
Default Video Resolution	Select Digest for standard resolution or Full for high-definition video

The Analytics Tab

The Analytics Tab allows you to select and configure Analytics that will be used with the camera. Further options will be unavailable until you turn on the base functionality, which will then expand based on your choices. JetStream offers a number of different Analytics Engines that could be used with your devices. Motion Detection comes with the JetStream system, while the other features require separate licenses in order to use them. Motion Detection does not require a separate license to run, so this feature will be covered by a later section in this Manual. You can find the steps for activating and calibrating the other Analytics Engines in their respective Manuals.

Figure 18: Analytics Tab



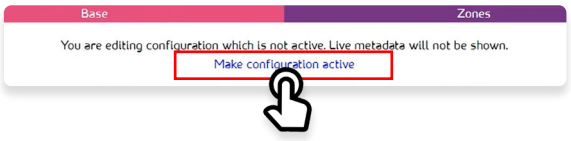
Below explains the significance of each individual setting found in this tab:

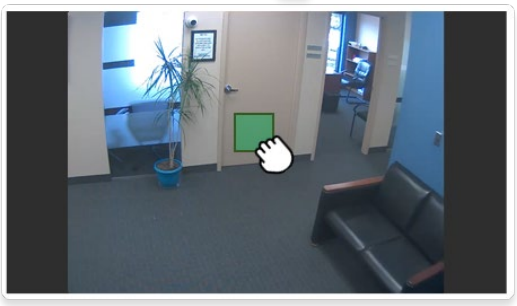
Motion Detection Analytics

To activate Motion Detection Analytics:

1. Go to the camera that needs the motion analytic. Find and select it under the **Sets** in the Navigation menu
2. Go to the **Analytics** tab
3. Under **Motion Detector** switch the drop-down menu to **YES**. Then press the **Manage configurations** button
4. Press the Add button and enter a name and description into the dialog boxes. Press Apply
5. Select the entry that was added. The Motion Detector Configurator will appear bellow
6. IMPORTANT: Start by pressing the **Make Configuration active** button. This will activate the analytic
7. Common Configurations

Figure 4.4

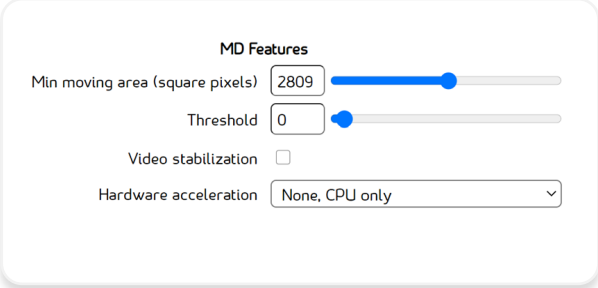




Minimum Moving Area
Configure the minimum number of moving pixels that the system will report. This will lower the amount of spammed detections that may come from birds or small objects moving

Use mouse cursor to draw the minimum size square in the snapshot view

Threshold
Set the threshold for how much an object should move before the system records a motion detection

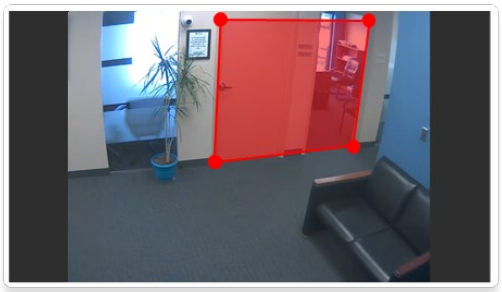


Video Stabilization
Enable this feature if the camera itself has slight movement in its feed. It prevents camera shaking from triggering a detection

Hardware Acceleration
Select if there are any graphical preferences that can speed up video processing

8. Detection Zones

Enabling a Detection Zone allows for only certain areas of the camera frame to sense motion



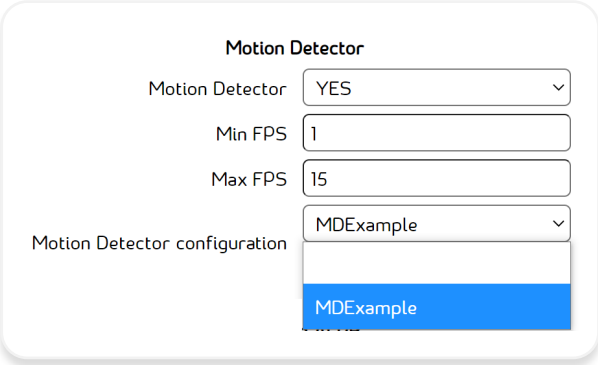
Zone Adjustments
Adjust the shape to the desired area using the colored points at each corner of the shape. Double click in the snapshot area to add more points to the shape.

Press **Add Zone**, then enter the following details:

- Enter a name that is easily identifiable
- Select a color to distinguish it from other zones
- Select whether the zone is a detect or exclude zone

9. Finalize the settings by pressing the apply button

10. Go back to the Analytics tab and go to the **Motion Detector Configuration** drop-down menu and select the newly made configuration. Press apply to save



Face Recognition Analytics

To activate Face Recognition Analytics:

1. Go to the camera that needs the motion analytic. Find and select it under the **Sets** in the Navigation menu

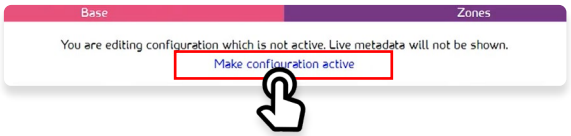
2. Go to the **Analytics** tab

3. Under **Face Recognizer** select all the features that would like to be enabled
    - Detection (Require): Enables detection of core face recognition functionality
    - Classification: Classifies the type of people that the camera sees
    - Emotions: Senses the type of emotion that the subject appears to have
    - Archive Search: Allows for search of archived subjects

4. Press the Add button and enter a name and description into the dialog boxes. Press Apply

5. Select the entry that was added. The Face Recognition Configurator will appear bellow

6. IMPORTANT: Start by pressing the Make Configuration active button. This will activate the analytic



7. Enable Core Features
   Select from multiple togglable features that will collect different types of analytics from the camera video feed
    - Age / Gender
    - Emotions
    - Quality
    - Liveliness

8. For more customization go to the **Advanced** and **Expert** tabs

9. Finalize the settings by pressing the apply button

10. Go back to the Analytics tab and go to the **Face Recognizer Configuration** drop-down menu and select the newly made configuration. Press Apply to save

Intrusion Detection Analytics

To activate Intrusion Detection Analytics:

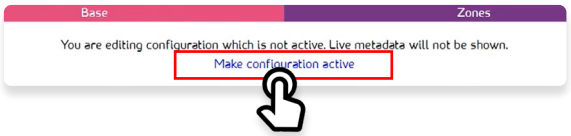
1. Go to the camera that needs the motion analytic. Find and select it under the **Sets** in the Navigation menu

2. Go to the **Analytics** tab

3. Under **Intrusion Detector** select the function type that would like to be enabled
    - Presence: Set up to detect the presence of a subject
    - Counting: Set up to count how many intrusions occur
    - Advanced: Advanced set up
    - Professional: Professional set up
4. Press the Add button and enter a name and description into the dialog boxes. Press Apply

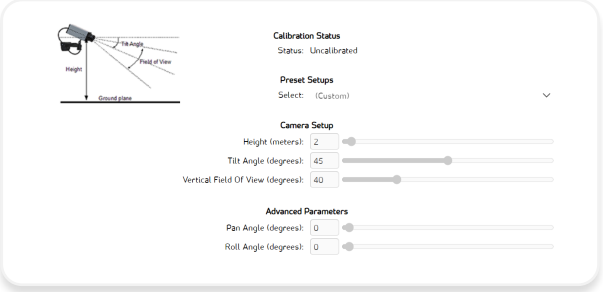
5. Select the entry that was added. The Intrusion Detector Configurator will appear bellow

6. IMPORTANT: Start by pressing the Make Configuration active button. This will activate the analytic



8. Enter any desired Counters or zones by double clicking on snapshot

9. Calibration
   Select the angle in which the camera is set to in its actual environment



10. Set the Classification, Tamper Detection, Scene Change, and Advanced Settings to the desired configuration

11. Finalize the settings by pressing the apply button

12. Go back to the Analytics tab and go to the **Intrusion Detector Configuration** drop-down menu and select the newly made configuration. Press Apply to save

Motion ALPR Analytics

To activate Motion ALPR Analytics:

1. Go to the camera that needs the motion analytic. Find and select it under the **Sets** in the Navigation menu

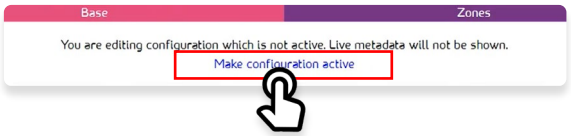
2. Go to the **Analytics** tab

3. Under **Motion ALPR** select all the features that would like to be enabled
    - Base Recognizer (Required): Enables detection of core recognition functionality
    - Classification: Classifies license plate information
    - GPU Support: Select if there are any graphical preferences that can speed up video processing

4. Press the Add button and enter a name and description into the dialog boxes. Press Apply

5. Select the entry that was added. The Motion ALPR Configurator will appear bellow

6. IMPORTANT: Start by pressing the Make Configuration active button. This will activate the analytic

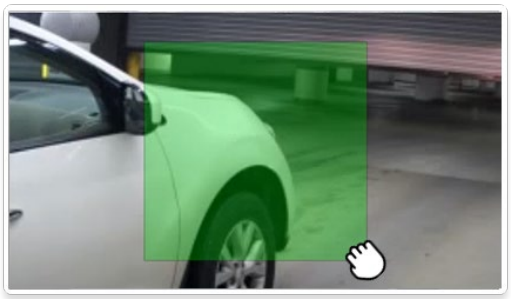


8. Enable any of the following features for core functionality
    - Detect Motion: Enables motion detection
    - Classify Vehicles: Enables classification of vehicles
    - Hardware Acceleration: Select if there are any graphical preferences that can speed up video processing

9. Set Common LP Configurations

Minimum/Maximum LP Size:
Configure the minimum/maximum License Plate size that the system should register

> Click and drag the rectangle in the snapshot viewer to adjust the size



Country & State/Territory:
Select the Country then the State/Territory so that the system may recognize license plates better

10. Detection Zones

Enabling a Detection Zone allows for only certain areas of the camera frame to sense motion

Zone Adjustments
Adjust the shape to the desired area using the colored points at each corner of the shape. Double click in the snapshot area to add more points to the shape.

Press Add Zone, then enter the following details:

- Enter a name that is easily identifiable
- Select a color to distinguish it from other zones
- Select whether the zone is a detect or exclude zone

11. Set the Scene and Advanced Settings to the desired configuration. Further instructions are available in the Instructions tab

12. Finalize the settings by pressing the apply button

13. Go back to the Analytics tab and go to the **Motion ALPR Configuration** drop-down menu and select the newly made configuration. Press Apply to save

Triggered ALPR Analytics

To activate Triggered ALPR Analytics:

1. Go to the camera that needs the motion analytic. Find and select it under the **Sets** in the Navigation menu

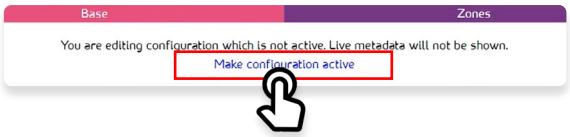
2. Go to the **Analytics** tab

3. Under **Triggered ALPR** select all the features that would like to be enabled
   - Base Recognizer (Required): Enables detection of core recognition functionality
   - Classification: Classifies license plate information

4. Press the Add button and enter a name and description into the dialog boxes. Press Apply

5. Select the entry that was added. The Triggered ALPR Configurator will appear bellow

6. IMPORTANT: Start by pressing the Make Configuration active button. This will activate the analytic

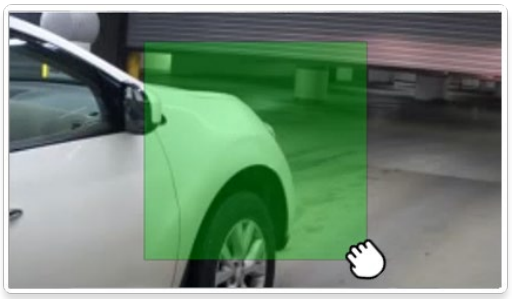


7. Set Common LP Configuration

Redaction Mode:
Used for license plate redaction. It includes more candidates during plate detection. This setting will miss fewer plates but will increase the number of false positives

Fast Mode:
The number of detection steps is set to 1. On average it gives a 30% speed-up. May result in lower accuracy when detecting small vehicles

Minimum/Maximum LP Size:
Configure the minimum/maximum License Plate size that the system should register

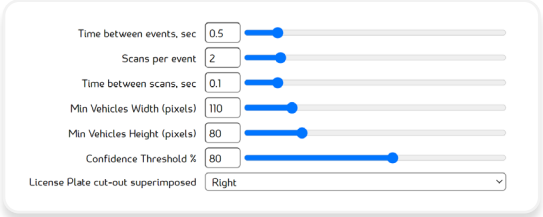


> Click and drag the rectangle in the snapshot viewer to adjust the size

Time Between Events:
Set the amount of time that goes by before the system records a new event

Scan Per Event:
Set the number of scans that the place recognizer will scan per event

Time Between Scans:
Set the amount of time that goes by before the system performs a new scan



Confidence Threshold:
This feature gives each plate that is scanned a confidence rating of what the system thinks it read. Set the minimum rating that the system should report.

8. Set the Region in the Regions tab

9. Detection Zones

Enabling a Detection Zone allows for only certain areas of the camera frame to sense motion

Zone Adjustments
Adjust the shape to the desired area using the colored points at each corner of the shape. Double click in the snapshot area to add more points to the shape.

Press Add Zone, then enter the following details:

- Enter a name that is easily identifiable
- Select a color to distinguish it from other zones
- Select whether the zone is a detect or exclude zone

10. Further instructions are available in the Instructions tab

11. Finalize the settings by pressing the apply button

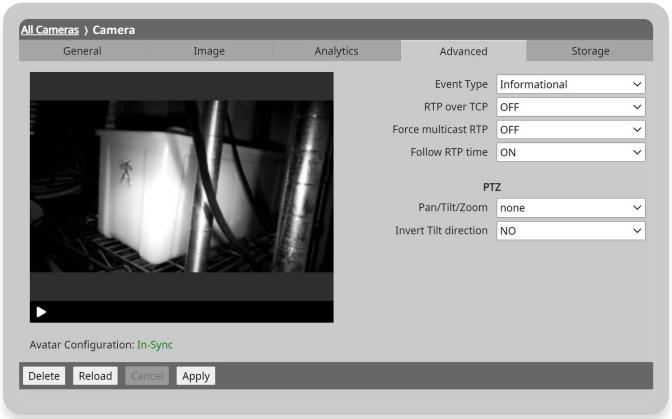
12. Go back to the Analytics tab and go to the **Triggered ALPR Configuration** drop-down menu and select the newly made configuration. Press Apply to save

The Advanced Tab

The Advanced Tab displays any advanced settings that may be related to other tabs.

This tab also contains setting about Pan, Tilt, and Zoom (PTZ) functionality.

Figure 19: Advanced Tab



Below explains the significance of each individual setting found in this tab:

Advanced Tab Descriptions

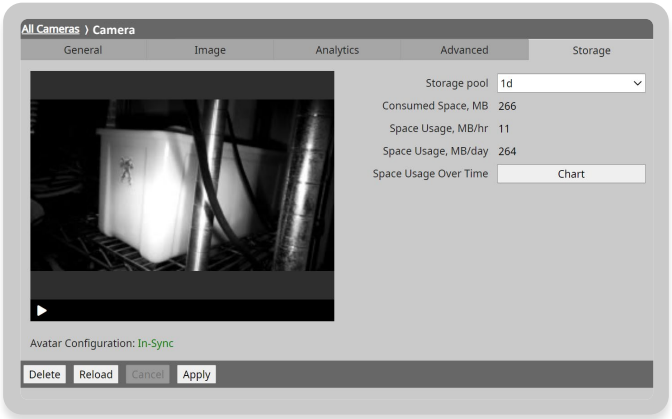
Event Type	Set the type and priority to be registered when specific events occur. The primary event types are “Informational” and “Alert.”
RTP over TCP	A choice is available to force the sending of video to the server over TCP. In some cases, setting this feature to "ON" will fix problems with receiving video at expense of higher video propagation latency. Default is set to “OFF”.
Force Multicast RTP	There is a choice to force RTP to any users receiving video over multicast.
Follow RTP Time	Allows you to enable or disable RTP time for this camera. Default value is “ON”.
Pan/Tilt/Zoom	This lists the available protocols the system will use for PTZ control. This option can be changed on encoders that support multiple PTZ protocols.
Invert Tilt Direction	Allows you to flip the control direction for the X/Y axis.

The Storage Tab

The Advanced Tab displays any storage settings and statistics.

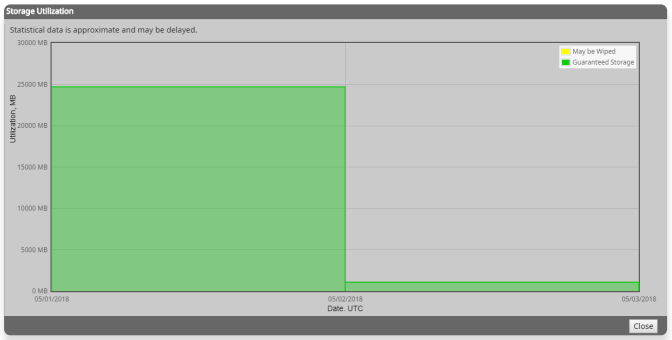
This tab also contains a function to that graphs the camera's space usage over time. To access this feature press the Chart button under Space Usage Over Time

Figure 20: Storage Tab



By clicking on the 'Chart' button, you will be able to view a chart showing storage utilization, similar to the image below:

The Storage Utilization Chart should look similar to the one seen above. As you can see, it displays the amount of drive space currently being taken up by the recordings from the device.



Below explains the significance of each individual setting found in this tab:

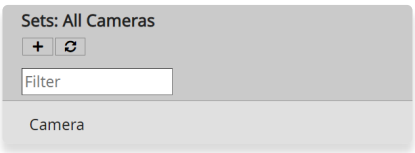
Storage Tab Descriptions	
Storage Pool	Set the type of storage pool needed for the camera. This sets how long footage is stored in the camera's archive.
Consumed Space	The total amount of storage that has been used by this camera so far in megabytes. **Read Only**
Space Usage	The total amount of storage that has been used by this camera so far in megabytes per hour/day. **Read Only**

Configuring Cameras

Please make sure your network camera is accessible over the network and you can identify basic information such as the camera model, authentication (username/password), etc…

Adding a Camera

Figure 21: Add Cameras



Start by clicking on the box with plus sign [+] to the left of the “Camera” header. Options will appear. You will now be in the Add Camera Wizard.

Next, in the Camera Add Wizard select the desired camera type. Here is a brief description of each option:

Network	URL
It simply requires the device to be broadcasting its data over the network, and JetStream is able to find it.	If a camera is not among those officially supported by JetStream, it can still be viewed through the system assuming you have the RTSP-URL of the video stream.

After Selecting a camera type continue to **URL** or **Network** Camera Configuration

URL Camera Configuration

1. Select **URL** camera type in the Camera Add Wizard
2. Enter Avatar or cloudDIRECT Camera settings with the following details:

Common Settings	
Destination	Select “**Avatar**” or “**Cloud Direct**” from the drop-down list
Name	(**Avatar Only**) Select Avatar from the list
Config via	Select **URL** if you know the RTSP URL of the cameras stream or use **Template** method to supply camera’s IP address, username and password
Camera Name	Enter camera’s display name
Storage Pool	Select desired storage pool from the drop-down list

URL	
Username	Login to access camera's video stream
Password	Password for the camera
URL	Enter camera's RTSP URL

Template	
Camera Make	Select from the list
Model/Series	Select from the list
Description	Select from the list
Camera IP/ Host	Enter IP/hostname
Port	RTSP port (optional)
Username	Login to access camera's video stream
Password	Password for the camera

ONVIF	
Destination	Select "**Avatar**" or "**Cloud Direct**" from the drop-down list
Config via	Select **ONVIF**
Camera Name	Enter camera's display name
Storage Pool	Select desired storage pool from the drop-down list
Model/Series	Select from list (Selectable after testing)
Camera IP/ Host	Enter IP/hostname
Port	Enter port
RTSP Port	Enter RTSP port
Username	Login to access camera's video stream
Password	Password for the camera
Enable PTZ	Pan, tilt, zoom feature (optional)

3. Click Test if the test is successful a camera preview will appear
4. Select a desired stream from the "Detected Stream" list and click Add

NOTE: *Some cameras might have a Username and Password associated with them which must be provided before the device can be accessed. This authentication is device specific, and you should refer to the camera's manual for specific instructions. If a password and username are required, fill out the two text fields at the bottom of the Add Camera Wizard with their respective data. When this is done, click "Next". The system will attempt to connect to the camera. If the attempt is successful, it will advance to the next screen. Otherwise, you will see a warning appear in the upper right-hand side of the screen. Possible errors could be the result of an incorrect IP address or Domain name being provided, or the password and/or username being incorrect.*

Network Camera Configuration

1. Select **Network** camera type in the Camera Add Wizard
2. Select the desired Avatar that will be utilized
3. Enter Camera IP/Domain Name or by Searching for Cameras on Network

   Option 1: Enter Camera IP or Domain Name

   a. Under Domain Name enter either the IP address or domain name of the camera
   b. Then under Camera model name enter the model name of the camera being connected
      Tip: Leave it on auto if you are unsure about the model

   Option 2: Searching for Camera on Network

   a. Press the Search cameras button to search for cameras currently available on the network
   b. Select the desired camera from the scrollable list

4. Enter the camera's **Username** and **Password**. Press Next
5. Enter required camera details:

Camera Name	Enter camera's display name
Storage Pool	Select desired storage pool from the drop-down list
Media Format	Select desired media format (h264 recommended)
Image Size	Select desired image resolution

6. Check that the camera data is correct and that a camera preview appears
7. Press Next to finalize the addition of the network camera

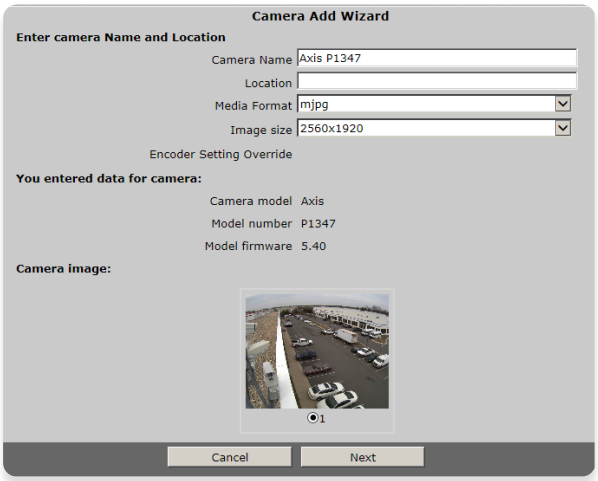
Preview

Here you can give a name and location, as well as choose the resolution and media format to be used by the selected cameras.

A snapshot of the camera will be displayed. If the camera that you added has multiple video feeds available (such as with a multi-port encoder) each video feed will have a snapshot and you can choose which feed to use.

If you are using a multi-node system, you can also choose which node to place the camera on. The system will attempt to place the camera on the system with the fewest cameras by round-robin.

Figure 22: Preview



Press Next

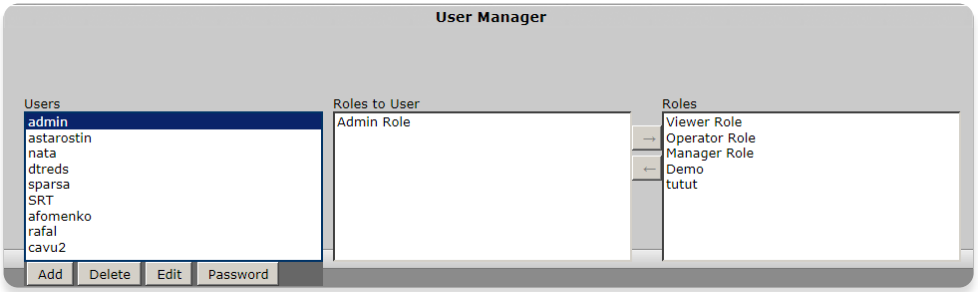
Your system should now have minimal functionality. Please see Chapter 4, Advanced System Configuration for more configuration options

Changing Your Password

The final step towards a complete basic setup of the system is to change the password for the “admin” account from the default to something a bit more secure. The passwords for every user in the system are managed through the JetStream Control Panel interface. JetStream offers two ways to modify a password: changing it or resetting it. Changing a password requires the user to provide the old password in addition to the new one. The reset option allows the user to set a temporary password that overrides the old one, but must be changed after first use. These procedures can be done by anyone who has access to an account with Administrative privileges, so it is important to keep your account information safe.

From the JetStream Control Panel, navigate to Settings>Credentials>User Manager in the left-hand menu. This will open a screen similar to the one portrayed below

Figure 23: User Management



From this screen it is possible to add, delete, or modify user accounts for JetStream. For now though, we will be focusing on changing the passwords. Select the “admin” account by clicking on it and hit the “Password” button. This will bring up a pop-up menu like the one seen in the image below.

When changing the password of a user with an Admin role only the “Change password” option will be available. Selecting a with a Viewer role will only give the option “Set password (will be marked as expired).”

The two options visible here are the ones described in the opening paragraph of this section. Clicking on them expands a relevant menu, allowing you to enter the new password and provide the old one if necessary.

Figure 24: Password Changer (Admin Role)

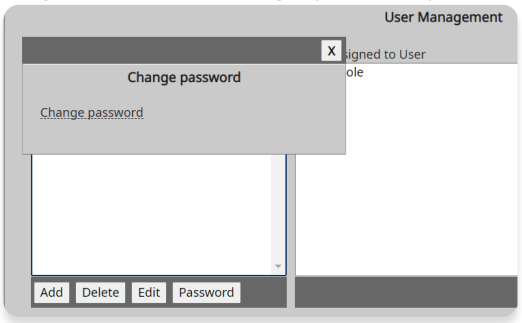
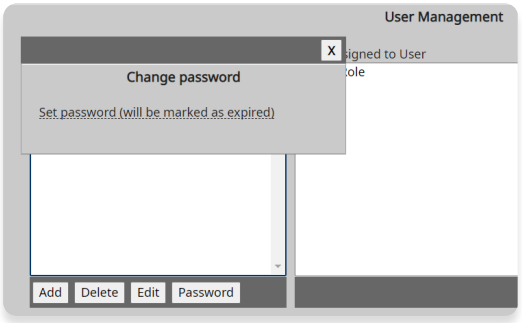


Figure 25: Password Changer (Viewer Role)



Since we know the current password for the “admin” account, click on the “Change Password” option. In the text boxes that appear, enter “topse” as the old password, and a new password that will satisfy the security requirements of JetStream passwords.

In order to comply with security standards, JetStream imposes the following requirements on any passwords being created:

- At least 6 characters long
- At least 1 uppercase letter
- At least 1 lowercase letter
- At least 1 number
- At least 1 symbol

Only one password change is allowed every 24 hours Sufficient diversity of the password (not one repeating letter) is required.

Once you have entered a valid password, click “Save” to complete the action. If there is an issue with the password, a warning message will appear at the top-right corner.

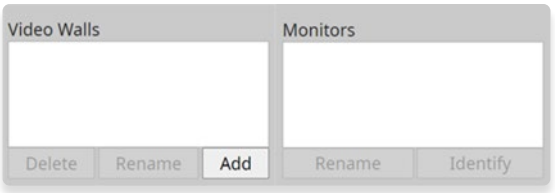
With these steps, the basic system setup is complete. The system can now be used to access the video being recorded by the camera, in both Live and Archive mode. In the next chapter we will cover the features and settings available in JetStream which allow you to customize your system to suit your needs.

Video Walls

Before adding a Video Wall into make sure to add monitors through display server via SSH in PuTTY

Configuration

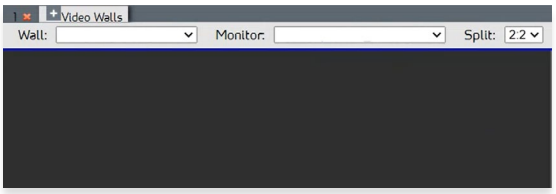
Figure 26: Video Walls



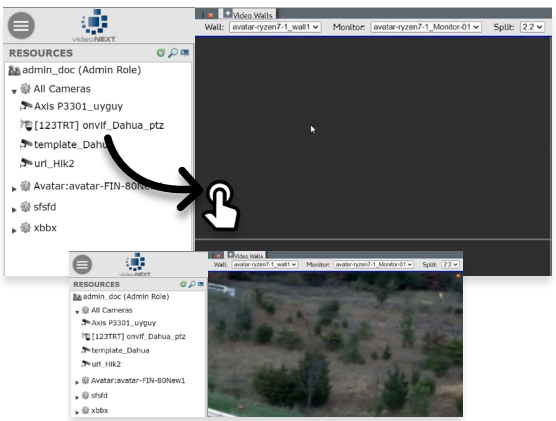
On the navigation menu press **Video Walls**. Then press Add to add a new Video Wall. The Name should correspond with the name entered in SSH. Once added the assigned monitors should appear under the Monitor box

Video Walls In Matrix

On the navigation menu press **Matrix.** The Matrix will open. On the top of page there will be a tab titled VideoWalls. Click on the tab. The window will give three drop-down lists. Select the active Wall and Monitor then select the type of split desired



Once the grid is set drag and drop the desired cameras into the empty spaces. The cameras will populate the area. The split setting can be changed at anytime to add more cameras to the wall.



Only Avatar cameras can be used in the Video Wall. CloudDIRECT is not Compatible

Notification Policies

Setting up Notification policies makes it easy to keep up with what is going on with the system. By setting up this feature the system will actively send emails to administrators about any selected actions that are going on in the system, such as logins, media exports, device health, etc.

Precondition Requirements:

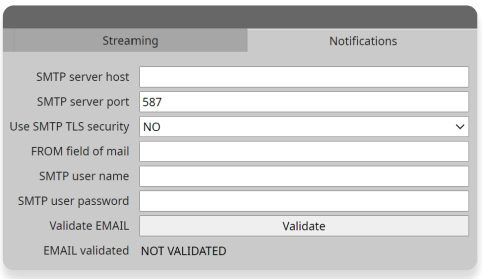
- A work-related Gmail mailbox with a confirmed phone number
  NOTE: The email must have a confirmed phone number or Google will block further steps
- In the Gmail account, open Settings -> Security and Login -> Unsafe applications are allowed -> **ENABLE**

Notification Policies Setup

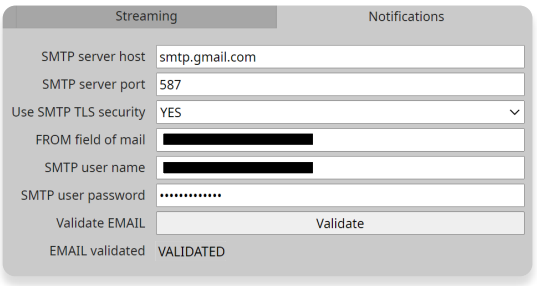
Open JetStream and go to Settings on the navigation menu -> Realm Setting -> Notifications Tab

Enter the following:

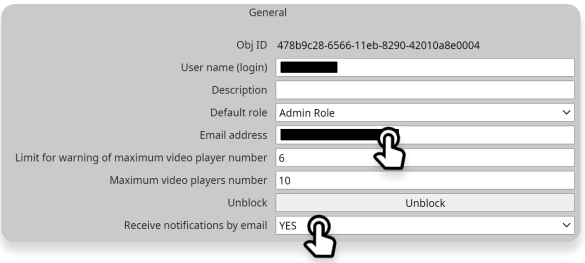
- **SMTP Server Host**: smtp.gmail.com
- **SMTP Server Port**: 465
- **Use SMTP TLC Security**: YES
- **FROM Field of Mail**: (work related Gmail address)
- **SMTP Username**: (work related Gmail address)
- **SMTP User Password**: (work related Gmail address account password)



Press the Validate Email button. This will send a validation email to the prior enter address. Open your email inbox. There will be a validation email with a clickable link, pressing it will take you back to JetStream with a confirmation message saying that the email has been validated. Go back to JetStream and enter the Notifications Tab again. The Email Validated section should read VALIDATED



Go to Credentials on the navigation menu -> User Management -> Users and select the admin user then press **Edit**. In the General Menu enter the work rated Gmail address into the Email address field and in the Receive notifications by email drop-down menu select YES. Press Apply to save settings



Creating Notification Policies

1. Start by going to Setting in the navigation menu -> Notification Policies. Press [+] to add a new policy

2. In the General field enter the following settings:
   - **Policy Name**: Enter a name that is easily identifiable
   - **Role Name**: Select the role that corresponds to the notification type
   - **Channel**: Email
   - **Timeout**: Select a timeout
   - **Message Entity**: Select Notifications Count Only or Include Notification Details
     NOTE: Picking Notifications count only will give just the how many notifications have occurred in the email message. Picking Include Notification Details will give details about each notification in the email message.
   - **Notifications Limit** (IND only): Set a limit to how many notifications per email
   - **Policy Type**: Select Audit Policy or Event Log Policy

Choosing Audit or Event Log Policy

Audit	Event Log
Will give notifications about system related occurrences such as: • User Security • User Actions • Object Management • Device Health	Will give notifications about events that have occurred on in front of the cameras

3. Choose anything listed in the check boxed list that would like to be included in the email notifications

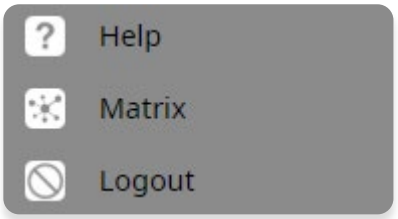
4. Press **Apply** to save the policy

5. Go **Notification Policies** to overview all the active Notification Policies

6. Check that your work-related Gmail inbox is actively receiving notification emails

Chapter 6: Remaining Control Panel Features

Figure 27: Remaining Controls



Help

The Help sections are informative, non-instructional

About
Shows your system version number, Acknowledgements, and End User License Agreement.

Subscription
Your specific Subscription information. See example below:

Figure 27: Subscription

Subscription

Category	Subscribed Option	Currently Used	Subscription Limit
Base Subscription	Expiration date	2018-05-03	
	Avatars	1	5
	License Plate Recognizer: Base Recognizer	1	5
	License Plate Recognizer: Classification	1	5
	License Plate Recognizer: Real-Time Watchlists	1	5
	License Plate Recognizer: GPU Support	1	5
	3DiVi Face Recognizer: Detection	1	5
	3DiVi Face Recognizer: Real-Time Watchlist	1	5
	3DiVi Face Recognizer: Archive Search	0	5
	Intrusion Detector: Presence	0	5
	Intrusion Detector: Advanced	0	5
	Intrusion Detector: Professional	1	5
	3DiVi Face Recognizer: Classification	1	0
	Storage GB	186.13	100
	Stream GB	6.73	2 000
Storage pool: Pool 1	Video stored	5 days	
	Cameras	6	20

Quick Start
The following is the default text you will see when clicking on this item:

Matrix

Matrix is the Operator view and will show Operator settings. Information on the Matrix view can be found in the Operator Manual.

Logout

Clicking ‘Logout’ will log you out of your current session.

Chapter 7: Troubleshooting

Resolving common JetStream issues:

Issue	Solution 1	Solution 2	Solution 3
Avatar offline	Check the power of avatar	Check the connectivity	Network card hang
Recording issue	Check the delivery content		
Cannot view the history or recorded video	Check the set of permission for the viewer account	In case if you are using the viewer account: make sure to enable the permissions of set in Role management to Manage or control	
Camera view slow	Check the avatar load	Check the FPS	Check the upload speed
Cameras not added under the account	Check the Role Management and make sure it's under the require account		
Camera broken	Check if its pinging or not	Check the connection cable	Check camera status ON/Off
Account password expire or need to reset	Password reset from User management if it’s a viewer account	Reset the password from Realm admin if it’s an admin	
Avatar not working after power restoration Automatically	Need to enable the feature from BIOS		
Video wall has empty message	Re-select the camera on Matrix-Video wall	Reset the services	
Video wall not working	Check the service has been enable or not	Reset the services	
Cameras removed from Video wall	Re-select the camera on Matrix-Video wall		
Add new account with permission	Create a new account and set the role and set management		
Date and time not correct	Enable the NTP server at camera	Need to enable the feature from camera	

Issue	Solution 1	Solution 2	Solution 3
Zoom in Zoom out not working	Enable the feature from matrix-setting-enable zoom	Enable the zoom feature from camera setup>advanced (Pan/Tilt/Zoom)	
Mobile app not working	Make sure to install the latest release from official app store		
Camera not streaming in mobile app	Make sure to install the latest release from official app store	Sign out and sign in again	
Live stream not working	Check avatar delivery queue if any data pending	Check the speed test	Check the camera Resolution and bitrate
Rename camera label	Change the camera name from the camera	Rename the camera from Raqib	

Raqib check list and Service Assurance Process

Connectivity

1. Verify the connectivity status
2. Verify the link type: MRS, Awal, 4G, Fiber or other

Basic Troubleshooting

1. Make sure the subscription valid
2. Restart the modem
3. Make sure the Ethernet port working and blinking

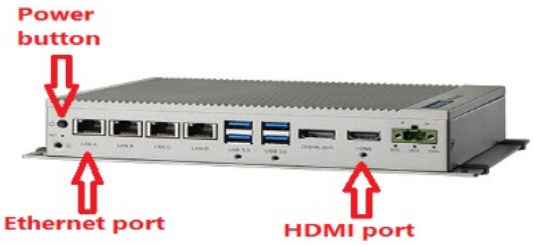
Avatar

1. Verify Avatar powered-check power indicator
2. Verify the network switch
3. Verify the network port on Avatar
4. Verify if there is errors/Alarms shown on the Avatar

Basic Troubleshooting

1. Make sure the power is on
2. Restart the Avatar
3. Re-plug the Ethernet cable

Advantech Avatar



Front Side

Back Side

User Interface

1. Verify if the user can log in to RAQIB portal
2. Verify if there is any issue with internet connectivity

Video wall / Matrix

1. Verify the Video wall
2. Record any messages shown in Video Wall tiles
3. Verify if the camera has been added under the user
4. Verify if the user using the supported browsers (chrome or Firefox only)
5. Verify the video wall cable connection

Note

1. In case if Password expired or wrong password message, reset the user password from Raqib portal
2. Make sure the user using the supported browsers – Google chrome or Firefox on

Basic Troubleshooting

1. Make sure the HDMI cable connected
2. Make sure the user using the supported browsers – Google chrome or Firefox only

Camera

1. Verify the Cameras Status
2. Verify any errors/Alarms shown
3. Check the port of the camera blinking on the switch or not
4. Verify if you able to ping the cameras or not
5. What is the camera status
6. Capture Camera Log, mention the error shown

Basic Troubleshooting

1. Ping the camera from Avatar OS
2. Re-plug/Reboot the camera cable from switch side

Mobile application

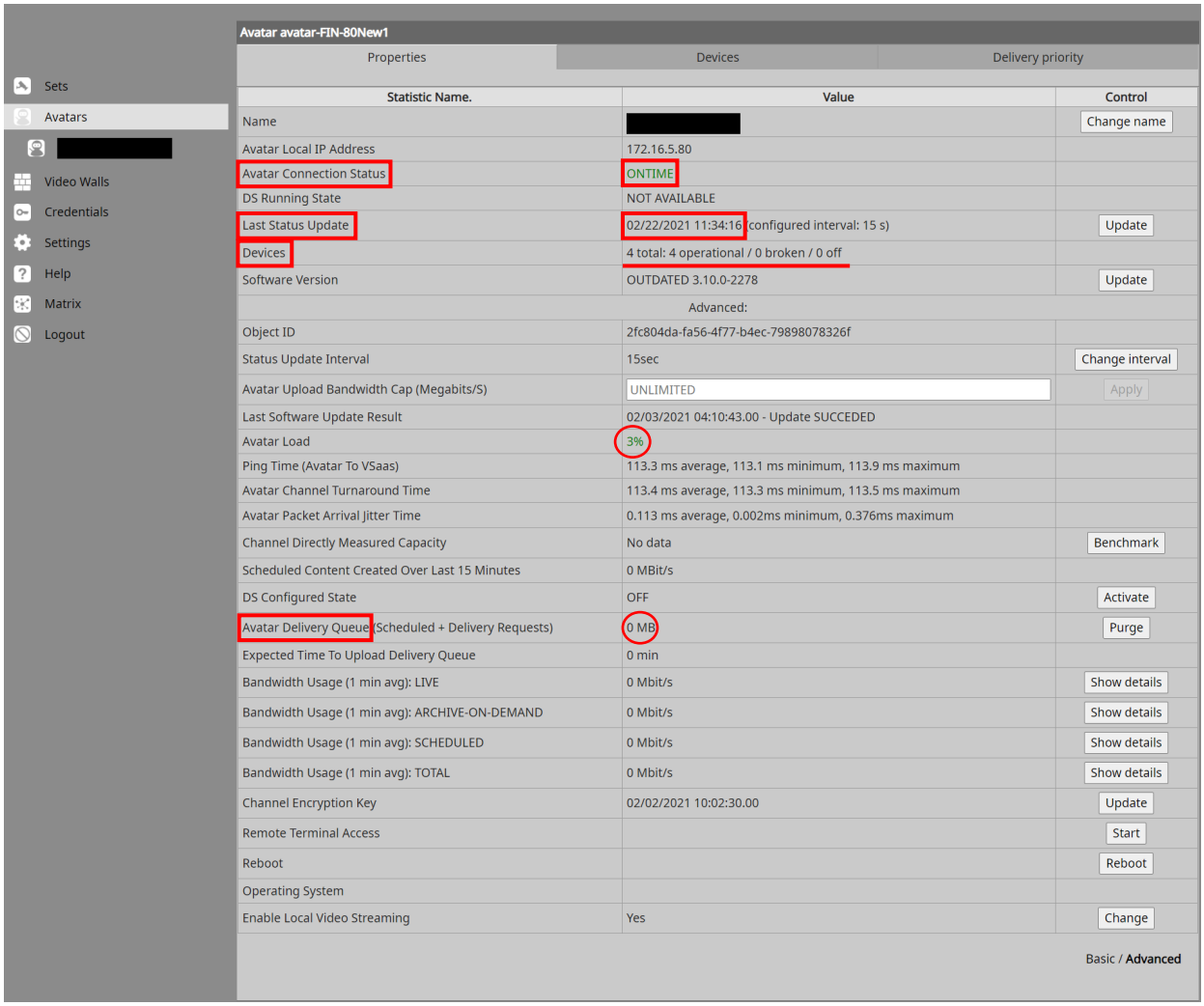
1. Verify if the customer has internet on his phone or tablet
2. Verify if he has the correct login credentials (username & password)

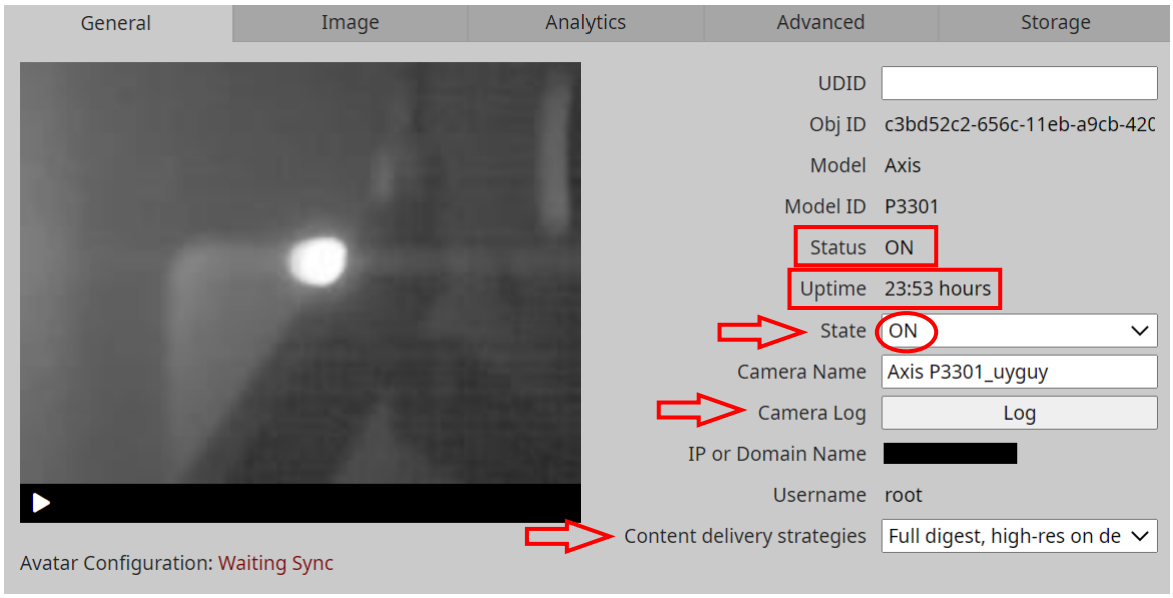
Basic Troubleshooting

1. Make sure the client using the correct version of Raqib app

Before open ticket-Individual Items

1. Login to the admin account
2. What is the Avatar Connection Status, on time, offline or ...
3. What is the Last Status Update (should be no older than ~10 mins ago)
4. What is the Avatar Load (should not exceed 80%)
5. What is the Avatar Delivery Queue (should be no more than 100MB)





Camera Log

Filter:

Update

Date Time	Severity	Message
01/10/2020 05:14:07	ERROR	MultiFramedRTPSource.cpp 517 RTP packet loss detected. Expected: 43332, but got: 43333
01/08/2020 15:51:00	ERROR	MultiFramedRTPSource.cpp 517 RTP packet loss detected. Expected: 31825, but got: 31826
01/07/2020 21:04:54	ERROR	MultiFramedRTPSource.cpp 517 RTP packet loss detected. Expected: 39637, but got: 39638
01/07/2020 17:27:26	ERROR	MultiFramedRTPSource.cpp 517 RTP packet loss detected. Expected: 27522, but got: 27523
01/07/2020 17:06:53	ERROR	MultiFramedRTPSource.cpp 517 RTP packet loss detected. Expected: 23824, but got: 23825
01/07/2020 11:33:25	ERROR	MultiFramedRTPSource.cpp 517 RTP packet loss detected. Expected: 15000, but got: 15001
01/05/2020 01:07:10	INFO	Decoder.cpp 61 using MMXEXT
01/05/2020 01:07:10	INFO	bilinear scaler, from yuv420p to yuv420p
01/05/2020 01:07:10	WARN	deprecated pixel format used, make sure you did set range correctly
01/05/2020 01:07:10	INFO	snapshot_writer.cpp 224 Downsampled width: 256, height: 144
01/05/2020 01:07:10	WARN	deprecated pixel format used, make sure you did set range correctly
01/05/2020 01:07:10	INFO	RTSPMediaProducerImpl.cpp 546 Entering to loop to receive stream...
01/05/2020 01:07:10	INFO	RTSPMediaProducerImpl.cpp 520 Setup "video/H264" subsession (transport: UDP, client ports: 50632-50633)
01/05/2020 01:07:08	INFO	Retriever.cpp 776 DEVURL exist. Use it!
01/05/2020 01:05:49	WARN	CompositeModule.cpp 128 Invalid argument
01/05/2020 01:05:48	INFO	Retriever.cpp 1028 Done!
01/03/2020 09:38:03	INFO	Decoder.cpp 61 using MMXEXT
01/03/2020 09:38:03	INFO	bilinear scaler, from yuv420p to yuv420p
01/03/2020 09:38:03	WARN	deprecated pixel format used, make sure you did set range correctly
01/03/2020 09:38:03	INFO	snapshot_writer.cpp 224 Downsampled width: 256, height: 144
01/03/2020 09:38:03	WARN	deprecated pixel format used, make sure you did set range correctly
01/03/2020 09:38:03	INFO	RTSPMediaProducerImpl.cpp 546 Entering to loop to receive stream...
01/03/2020 09:38:02	INFO	RTSPMediaProducerImpl.cpp 520 Setup "video/H264" subsession (transport: UDP, client ports: 42564-42565)

Appendix A: System Requirements

This section is for various suggestions and metrics used in deciding hardware, network, and storage capacity required.

Recommendations on Client Station Platforms

PC/Windows platform, minimum requirements:

- **Screen Resolution:** At least 1920 x 1080
- **Processor:** Intel Core i5, 1.6 – 2.11 GHz (or equivalent and higher)
- **RAM:** 8 GB
- **Video Card:** NVIDIA GEFORCE 1 - 2 GB (or similar and higher)
- **Hard Drive:** 500 GB
- **System Type:** 64-bit operating system
- **Recommended Browser:** Google Chrome

Appendix B: Installation Instructions

What you will need

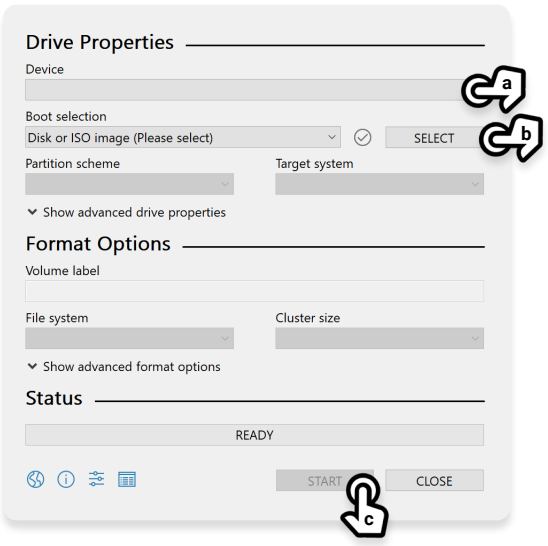
- USB Flash Drive (2Gb Minimum)
- Link to a disk image with ISO (for example, FTP)
- A program for creating a bootable USB flash drive (for example, Rufus)
- A client program for connecting to SSH (for example, PuTTY)
- Monitor, Keyboard, Internet connection for Avatar Device

Installing an Avatar

1. ISO Download
Download the latest 3.10 codebase ISO disk image from the link (CentOS7 + Avatar):
https://ftp.videonext.net/private/AVATAR-RELEASES/isos/

2. Create Bootable Flash Drive
Using the program "Rufus" - create a bootable USB flash drive with the downloaded ISO

a. Select USB Device
b. Select ISO file from file explorer
c. Once READY, press START to begin transfer to USB Flash Drive



3. Booting the ISO onto the Avatar

a. Getting the device ready

Make sure the device is powered off before starting. While still powered off insert the flash drive with this ISO file. Power on the device and immediately enter the device's BIOS.

Note: Different devices have varying ways of getting into the BIOS. Consult manufacture instructions

a. Configure device BIOS

Once in the BIOS, set it so that the device can boot from a USB flash drive

c. Booting the ISO

Once booted the screen will display a CentOS 7 prompt. Using the arrows on the keyboard select **`Install Avatar`** and press ENTER to execute. The software will take a moment to install

When the Installation Summary screen appears, go through the steps marked with an alert icon ⚠️ and press Begin Installation. The software will take a few minutes to install

Figure C Example

4. Configuring the Avatar

a. Login

Login as user **sos**
Default password: **s.o.s.**

The 'sos' user will be prompted to change the password to a new one. Change the password for 'sos' to a new password

Once the new line staring with [sos@avatar ~] appears

Figure A Example

```
Avatar login: sos
Password: PW WILL BE INVISIBLE
You are required to change your password
Changing password for sos.
(current) UNIX password: PW WILL BE INVISIBLE
New password: PW WILL BE INVISIBLE
[sos@avatar ~]$
```

b. Escalate permissions to the user 'sos'

Enter the command: **sudo -i**
Re-enter the newly set sos password

Figure B Example

```
[sos@avatar ~]$ sudo -i
[sudo] password for sos: PW WILL BE INVISIBLE
[root@AV-000 ~]#
```

c. Changing root password

Change to user: **[root@avatar ~]#**
Enter the command '**passwd**' to change the password to a new one for the user 'root'
Enter new password and retype it. The system should update successfully

Figure C Example

```
[root@avatar ~]# passwd
Changing password for user root.
New password: PW WILL BE INVISIBLE
Retype new password: PW WILL BE INVISIBLE
passwd: all authentication tokens updated
successfully
[root@avatar ~]#
```

d. Finding Avatar IP

Enter the command '**ifconfig**' to find the IP of the avatar

Scroll down to the **eth0** line and find the IP next to the **inet** line

Figure D Example

```
[root@avatar ~]# ifconfig


eth0: flags=0000<UP,BROADCAST,RUNNING,MULTICAST>
      inet 000.000.00.00 netmask 000.000.000.0
      inet 6 0000::0000:0000:0000:0000 prefixlen
      ether 00:00:00:00:00:00 txquelen 0000…
```

IMPORTANT: Copy the IP address for reference

5. Activating the Avatar

Activate the avatar via the /etc/avatar-pre-conf file (Pre-configuration file for Avatar)

a. Opening and Editing Pre-Conf File:

Enter '**`cd /etc/`**' into the console, this will define the ETC directory
Then enter '**`vi avatar-pre-conf`**' into the console, this will open the Pre-Configuration file

To edit the file, press the INSERT key

In the avatar-pre-conf file, enter the following:

- dst=<VaaS-Address>

  Note: Enter "#" before the realm address to disable the realm's access to the Avatar
- ntp=<NTP-Server-Address>
- hostname=<Avatar-Hostname>

Exit editing mode by pressing the ESC key
Save and exit the file by entering the command '**`:wq`**'

Enter '**`cd /root/`**' to return to the root directory

b. Activation

In the console activate the Avatar. It may take a moment to establish a connection between the Avatar and realm

Once the GUID code appears under the last line of the console the Avatar activation has been finished

IMPORTANT: Copy the GUID for reference

Figure A Example

```
[root@avatar ~]# cd /etc/
[root@avatar etc]# vi avatar-pre-conf
```

```
# Pre-configuration file for Avatar
# Bellow are listed parameters…

#dst=test1.video.net
dst=test2.video.net

ntp=0.pool.ntp.org

hostname=AV-000
~
~
~
```

```
~
~
:wq
```

```
[root@avatar etc]# cd /root/
[root@avatar ~]#
```

Figure B Example

```
[root@avatar ~]# activate
Using VSaaS: dst=test2.video.net
Generating SSH keys
Configuring logrotate
Set hostname=AV-000
Stop avatar engines if any running
Net.ipv4.ping_group_range = 0 0000000000
Our GUID: 00000000-0000-0000-0000-000000000000
```

Adding an Avatar to Devices

1. On the Navigation Menu go to **Settings**, then **Manage Avatars**
2. Go to the Activate Avatar tab
3. Obtain your GUID that was generated previously in PuTTY (i.e. `cc0aaf19-9b3f-4976-8129-eb00820aba10`)
4. Enter GUID into the dialog box
5. Click Activate to activate your Avatar. The Avatar has been added to the system

videoNEXT