OnWatch

Version 2.6.0 - Generated on July 27th, 2023

Table of Contents

Getting Started

WATCHLIST ALERTING

Welcome to OnWatch from Oosto! Detect and identify known and unknown individuals, in real-time or in historical footage, and send recognition notifications instantly to any device.

Getting Started

To get started, you'll need to do the following:

1. Activate your license.
2. Stream your live cameras within the OnWatch system.
3. Configure and adjust the OnWatch settings according to your organization's use case.
4. Create user accounts for everyone who will have access to the system.
5. Add subjects to the watch list.

OnWatch Documentation Overview

The **Documentation** tab includes the following chapters:

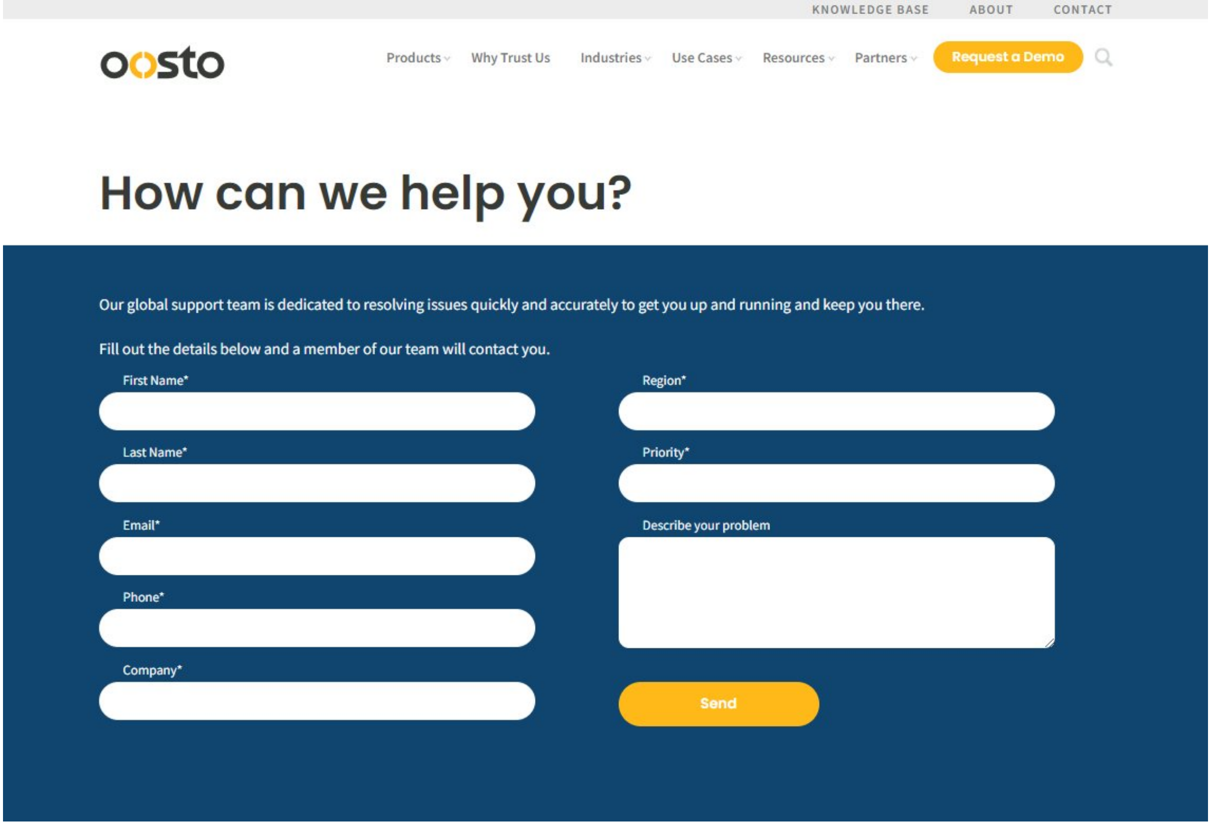
- *Settings by Super Admin* - how to configure OnWatch for your needs.
- *System Manual* - walks you through all OnWatch features in detail.
- *How To* - offers step-by-step guides on how to perform the most common actions in the system.

The **API Reference** tab provides all our API routes, as well as some sample code, in one central place.

Contact Support

How to Contact Support

You can contact Oosto Support 24/7 by filling out a case form here: https://oosto.com/support/.



How can we help you?

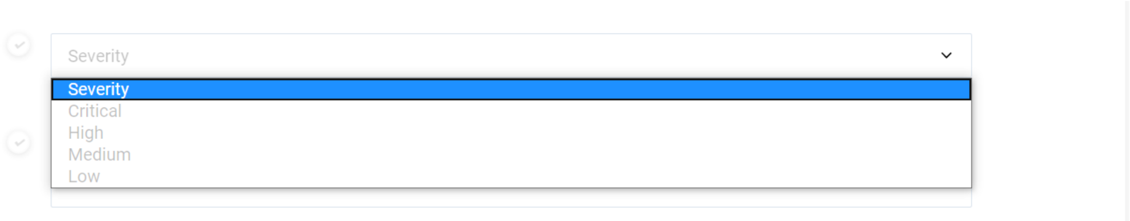
Our global support team is dedicated to resolving issues quickly and accurately to get you up and running and keep you there.

Fill out the details below and a member of our team will contact you.

Please be clear and provide correct information. Type in your:

1. First and last name
2. Company email address
3. Phone number
4. Company name
5. Region

Next, provide the severity of the case by selecting a severity level from the dropdown list of options.



To determine if your case is *Critical* or *High*, you can click on either option and a new dropdown bar will appear. Check if the problem or issue you are facing is listed in the dropdown. If not, mark the case as *Medium* or *Low* severity.

Lastly, describe - in detail - the problem you are facing. In addition, please provide the following information in the description:

- The product you are working with
- The version of the product
- Whether it is an online or offline system
- If it's an online system, please provide connection details (TeamViewer, AnyDesk, etc.)

Once you finish, click **Send**.

Environment Setup

Camera Placement Best Practices

This guide describes the best practices for camera placement and configuration to get the best results from the OnWatch system.

Terms & Concepts

What is FOV?

Each camera is positioned in a particular location and orientation in space. A camera’s Field of View (FOV) is the view of the world visible through its lens. Objects outside a camera’s FOV are not captured in a video or photograph.

Proper and strategic camera positioning improves the system's performance for capturing usable facial features in a video.

Capturing Facial Features – Mathematical Models

Facial features are represented in Oosto as a mathematical model (also called a vector).
Oosto creates a mathematical model that represents each face detected in the FOV of a camera video feed. Oosto also creates a mathematical model of all the faces that are enrolled into the Oosto system (meaning that they were added as a Person of Interest (POI) to the Oosto Watchlist).
Oosto can then recognize the appearance of a POI in a video by comparing the detected faces with the POIs in the Watchlist.
While Oosto's technology is powerful, there are some minimal requirements for video capture and camera location/positioning that are recommended to enable Oosto's artificial-intelligent, neural network to generate a high-quality mathematical model of people’s facial features.
Oosto's detector can locate faces that are as small as 45 x 45 pixels and that have been recorded in imperfect video capture conditions. However, the quality of the facial feature mathematical model is degraded when conditions are sub-optimal.

High-Quality Mathematical Models

The following sections describe various aspects for determining the optimal camera locations, angles, FOV, and other factors to get the best results from your Facial Recognition system. The best facial recognition results are achieved by providing the conditions to enable Oosto to create the highest quality facial mathematical model.

Video Face & Body Size

What Is the Optimal Face Size?

Generally, a good mathematical model can be created from faces that are represented by at least 45 x 45 Pixels Per Face (PPF). Faces of this size enable Oosto to not only detect that there is a face but also to recognize a person as being a POI (meaning someone that was added to the Oosto Watchlist).
A great performance can be achieved at 80 x 80 Pixels Per Face and up.

> 👍 OnWatch can detect the existence of a face as low as 20 x 20 Pixels Per Face. Even though recognition of a POI is not probable for such small video face sizes, these detected faces can be used for various purposes. For example, for GDPR facial blurring in video playback for privacy/confidentiality purposes.

What Is the Optimal Body Size?

When it comes to body or pedestrian recognition, a mathematical model can be created from bodies that are represented by a minimum of 20 x 20 Pixels Per Body (PPB).

Strategizing for Sufficient Size

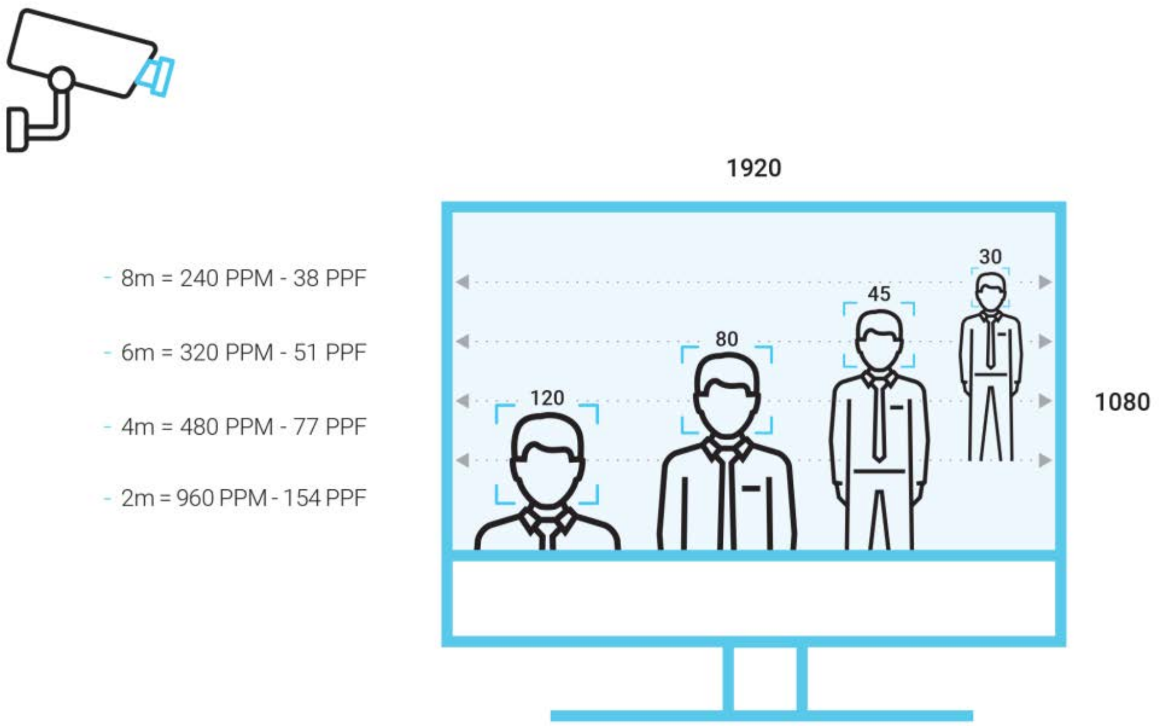
The size of the face captured in the video can also be measured by Pixels Per Meter (PPM) – the further away objects are, the fewer pixels represent them.

- The minimum PPM for face recognition is 280 PPM (equal to 45 x 45 Pixels Per Face).
- Optimum PPM for face recognition is 500 PPM (equal to 80 x 80 Pixels Per Face).
  Therefore, the first question is “How many pixels is the camera capturing per meter?”.

Taking Distance into Account

Faces that are close to the camera appear larger than those that are far away. In addition, the larger the FOV of the camera, the more bodies and faces will be detected in a single frame.

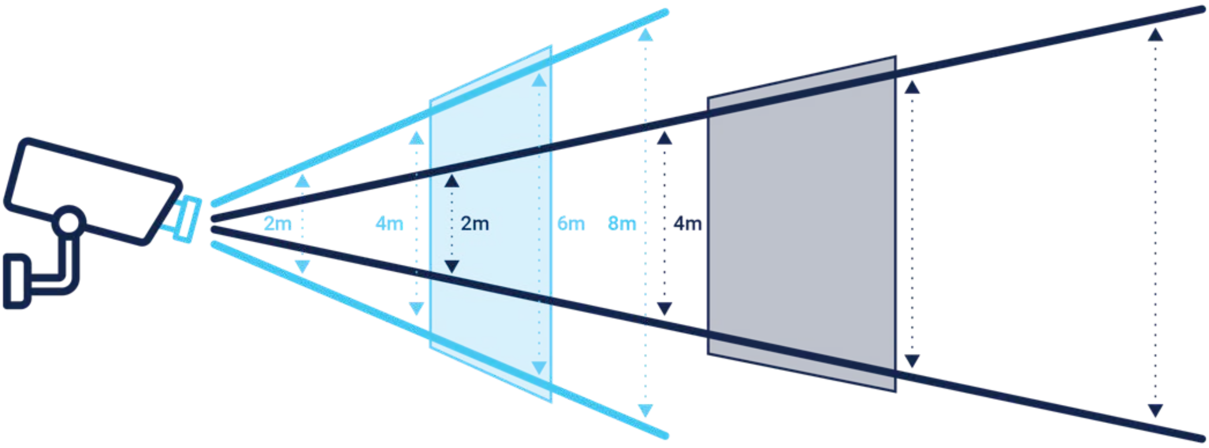
The following are some general rules of thumb regarding the number of Pixels Per Meter at varying distances from a typical Full High Definition (FHD) (2MP) camera.



Before placing the camera, assess the distance from the camera lens at which the video will capture the best frontal view. Then perform a quick calculation using the camera resolution in order to estimate the FOV width in meters in the zone of interest (where we expect to capture the faces). This measure allows us to estimate expected face or body size.

Adjusting Camera Focal Length

When using PTZ or varifocal lenses, it is possible to adjust the camera's zoom in order to capture faces and bodies in your target area. Zooming in makes the faces appear closer and larger.
The diagram below demonstrates how the distance from the camera changes, but the width of the interest zone is fixed at 6m. In this area, we capture detections with sizes ranging from a minimum of 20 x 20 for the body to 100 x 100 (3m width for FHD camera) for faces. The blue below shows a wider zoom and the red a narrower zoom –



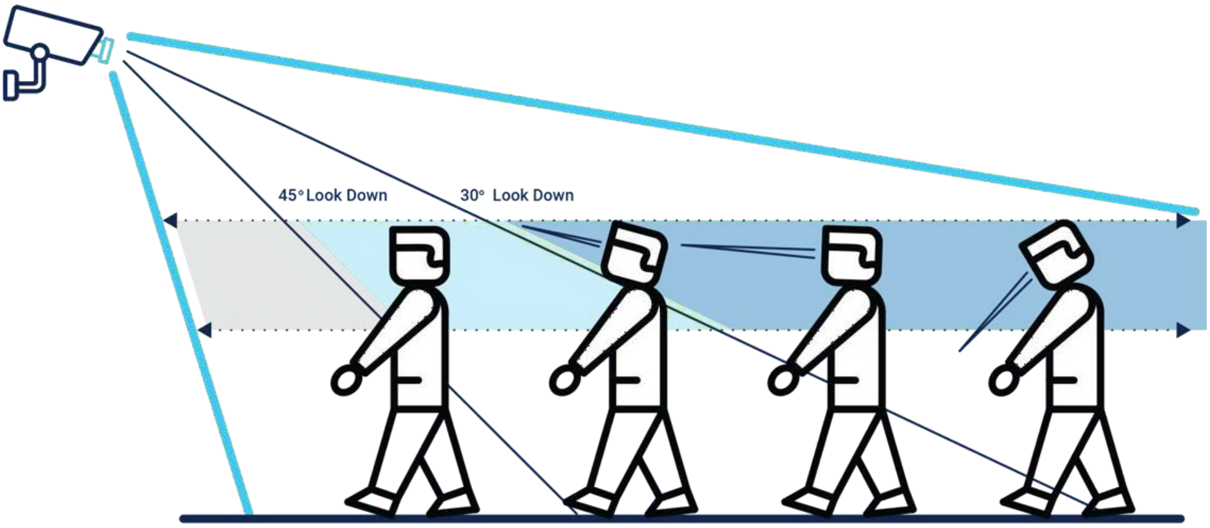
This diagram also demonstrates that the best facial recognition (the Interests Zone) is achieved closer to the camera when the zoom is wider, and further from the camera when the zoom is narrower. These numbers are only an example of the specific situation depicted in the diagram above and are not absolute.

Camera Height and Angle

OnWatch can detect faces when the angle of inclination between the face and the camera is 0-45 degrees. Optimal results occur when the camera is positioned at a 0º – 20º angle. However, reliable Face Features are achievable when the angle of inclination is up to 30º.

On the contrary, the angle of inclination for body recognition does not need to be so specific as the camera needs to capture the entire body and not a specific part, such as the face. So long as the camera is not directly on top of the body, it will be able to detect a body within the FOV.

For cameras detecting both faces and bodies, it is best to utilize an angle of inclination of 30 degrees.
It is possible to decrease the angle of inclination by moving the camera further away and using optical zoom or lenses.



The diagram above demonstrates how it is also important to consider additional factors. It is necessary to compensate for these factors by directing the angle of the camera.

Also, to ensure that people wearing caps/hats are captured with maximum performance, the camera should be placed at the shallowest angle while maintaining a clear line of sight to the capture line.
The diagram shows the optimal angle of 30° look-down as a blue area and the light-blue area of 45%, which is more challenging.

Direction of Movement

Frontal View Is Optimal

The highest quality mathematical models and recognition results are achieved when cameras are positioned to obtain a frontal view of people's faces. This is true even though the system can detect and recognize up to a 90º side view (also called full profile).

In real-world environments, people tend to turn and talk to associates, look at things in their surroundings, and so on.

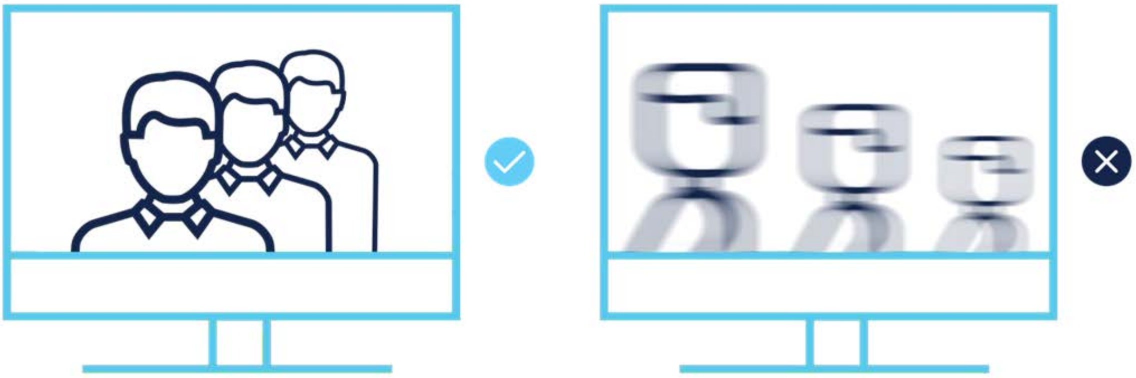
Therefore, a best practice is to place cameras so that they are pointed at and focus on areas where people are moving (walking and so on). While walking, people tend to look forward and maybe face in similar directions.

Chokepoints (where people tend to congregate) may also be applicable. However, people who are not moving, tend to congregate in a cluster and face inwards, which may block recognition angles.

Moving Towards the Camera

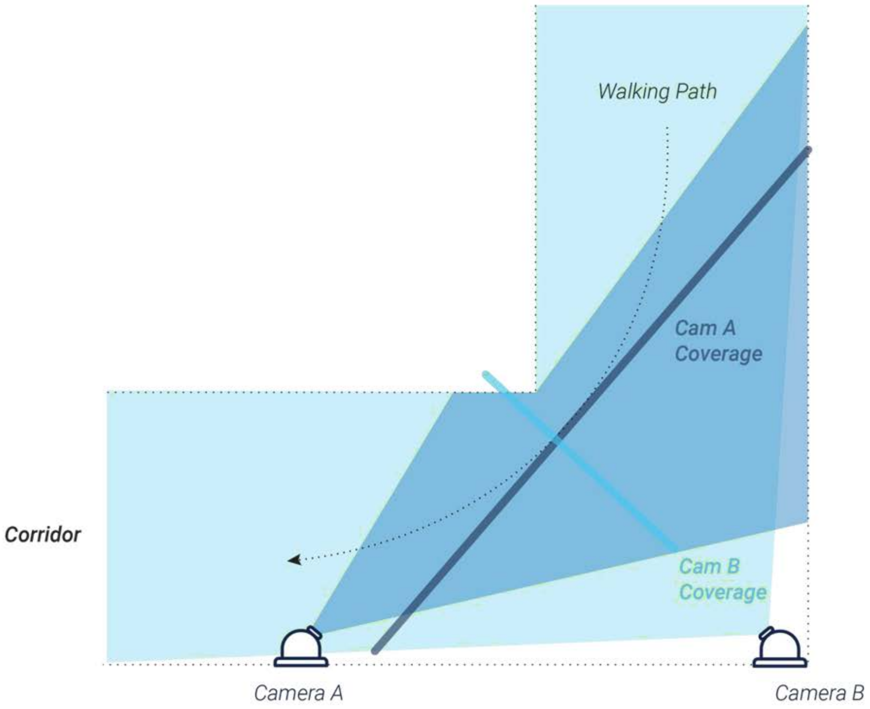
It is preferable to place cameras where people are moving towards the camera (their faces get larger as they come closer to the camera) rather than crossing the scene, as shown in the diagram below. When moving across a camera's FOV, side profiles may be captured.

In addition to the above, a slightly off-center approach opens up the surrounding area and enables other faces to be viewed. The face size will increase during the approach giving better quality, and the angle provides the greatest chance of capturing a frontal view at some point.



The angle of movement may affect video quality insofar as artefacts may appear and faces may be slightly smeared, which lowers the quality of the facial mathematical model. This typically occurs when people are crossing the scene at high speeds.

In the drawing below, Camera B is located in the corner of a corridor with a wide FOV and covers both sides. Considering typical walking paths, Camera B's faces will be detected in small size (wide-angle lens) and profile view, while Camera A's placement will typically capture faces that are looking towards the camera's direction in a higher Pixels Per Face. Therefore, Camera A's location will generate better results.



Psychological Aspects

An Interest Zone is the area at which the camera should be pointed and focused to ensure optimal capture of people’s faces (frontal view, sharp image, and so on). This might be in a specific area of a room, building entrance, hallway, or so on.

The following describes various aspects to consider when determining where to position/point the camera based on various psychological and behavioral factors.

When considering the camera’s FOV, various aspects of human psychology and behavior should be taken into account to ensure that people are not looking down at the time and place where the camera is recording them. This significantly increases the probability of achieving a high-quality mathematical model.

Focal Points Attract Attention

- When a camera is located in an area that attracts attention, such as near a TV screen or an attractive advert, it is more likely that people will look up to it.
- Sounds also attract people’s attention. For example, people tend to look towards speakers during announcements, towards crowded loud areas when passing them, and at screens with sound. This may be considered either as a focal point or a distraction, depending on camera placement.

New Areas

- People typically look down when they enter a new area, such as after going through a gate, or when they need to take special care of the next step (such as when getting on/off an escalator). In this case, the person will look down to find his/her next step and will then look up and forward immediately afterward.

Avoiding Locations with Long Walks

- In open areas where people walk long distances, many will concentrate on their mobile devices with their face pointing downwards, which makes it more difficult to get a good facial view.

Analyze your target audience's behavior to determine where to set up your interest zone. Then, place the cameras accordingly.

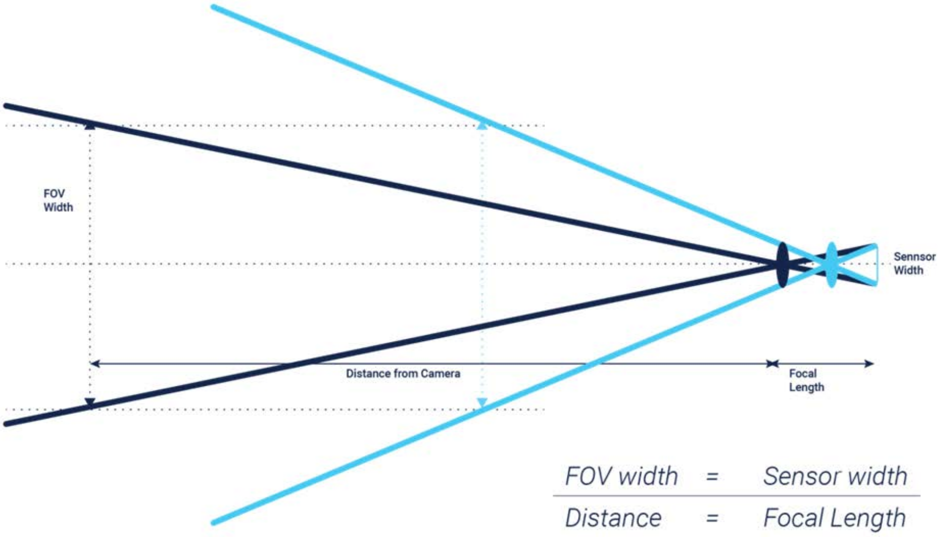
Camera Focus

In most of the CCTV camera deployments, the camera is set to Auto Focus mode. In this case, the camera algorithm will look for sharp angles in the FOV and set the focus according to that location. In many cases, this focuses the camera on patterns on the ground (such as the carpet), a picture on the wall, and so on. Usually, the camera's focus is not set up to identify a moving face or body. Because the system seeks facial or body details, it is recommended to set the camera manually so that the focus will be on the Interest Zone.

Lens Selection

When planning the Interest Zone, its distance from the camera and the expected FOV width differs according to the various types of lenses that may be used, each of which may have a different focal length.

It is important to calculate the required focal length for the scene. Using a shorter focal length widens the FOV, and the Interest Zone will be closer to the camera.

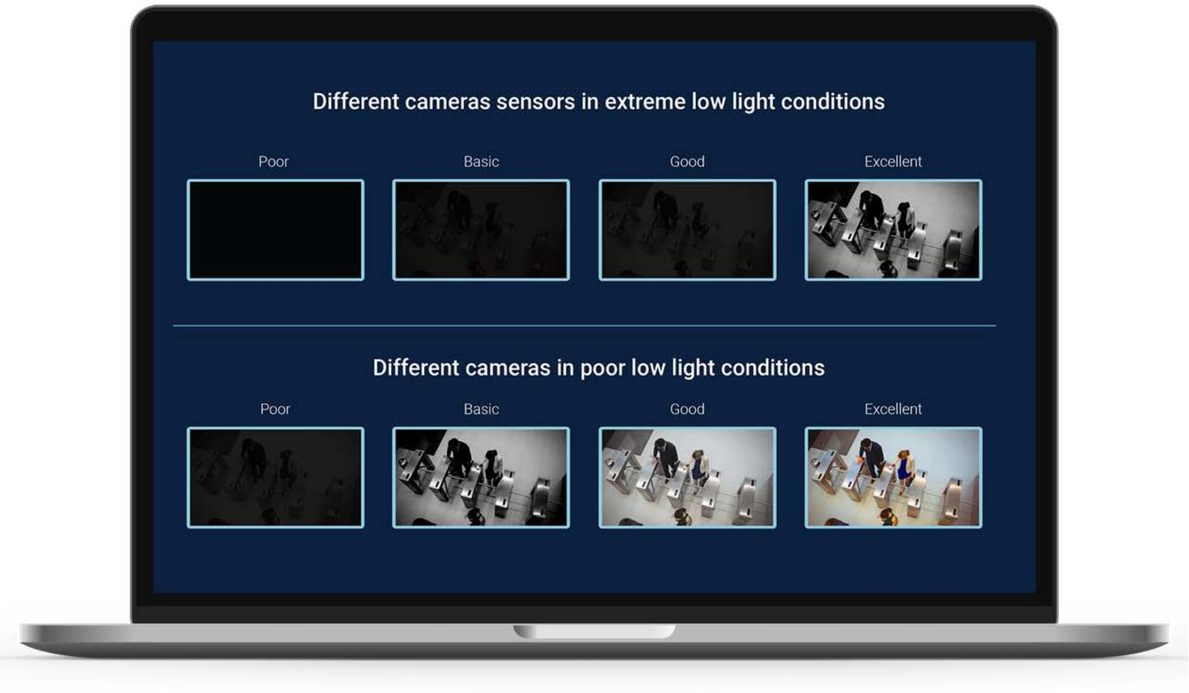


$$\frac{\text{FOV width}}{\text{Distance}} = \frac{\text{Sensor width}}{\text{Focal Length}}$$

It is not recommended to use fisheye lenses, which tend to have shorter focal lengths and wider angles. Fisheye lenses also may create a distorted view that impacts the recorded facial quality.

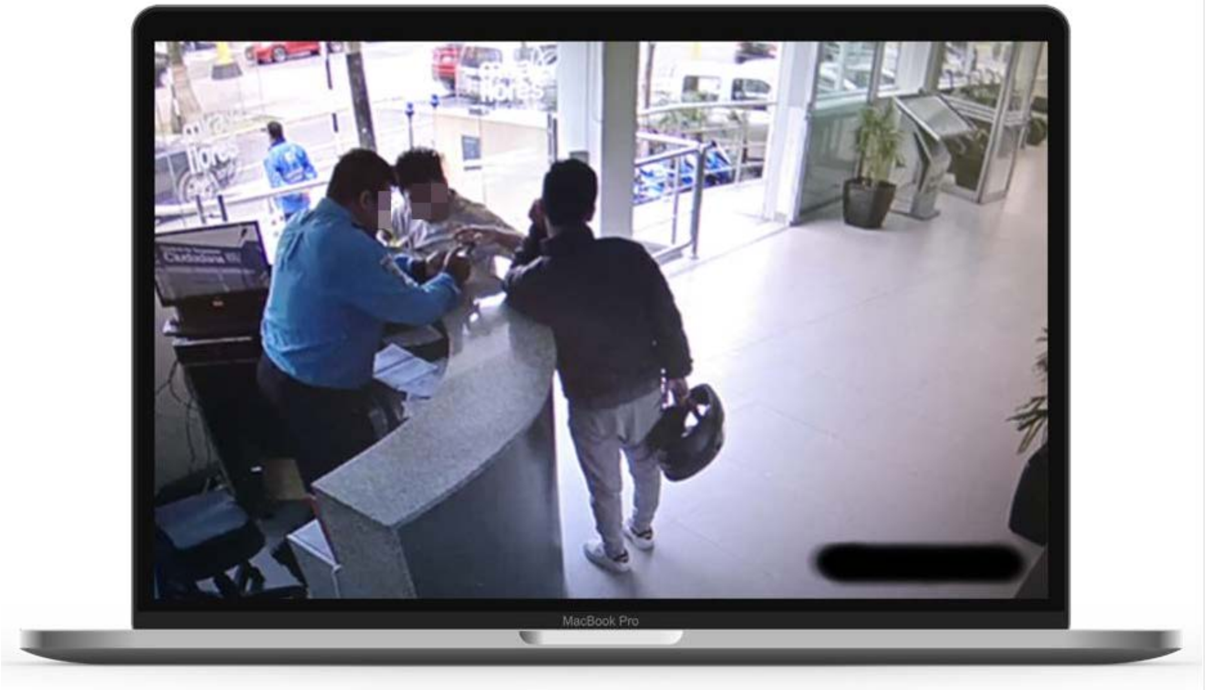
Light

Different cameras with different setups generate different image quality, and each has its fixed lux (lowlight camera performance) level, which cannot be adjusted. Therefore, it is best to select cameras that have the best possible lux.


Different cameras sensors in extreme low light conditions
Poor
Basic
Good
Excellent
Different cameras in poor low light conditions
Poor
Basic
Good
Excellent

It is best to use cameras that provide High Dynamic Range (HDR), Wide Dynamic Range (WDR), and/or Image Sensor Sensitivity (ISO) as an essential compensating measure for challenging dimmed environments.

The picture below shows a strong backlight which results in a dark face, making it difficult to distinguish facial details.



Facial and body recognition works best in areas with diffused, even lighting. Therefore, lighting should be set up so that the camera is pointing to where people’s faces will be well lit. For example, areas that are partially lit and partially dark are not optimal for body recognition.

Mirrors and marble floors may reflect light, which may influence the level of light on faces. It is recommended to mitigate or try to avoid these non-optimal lighting situations.

Bit Rate

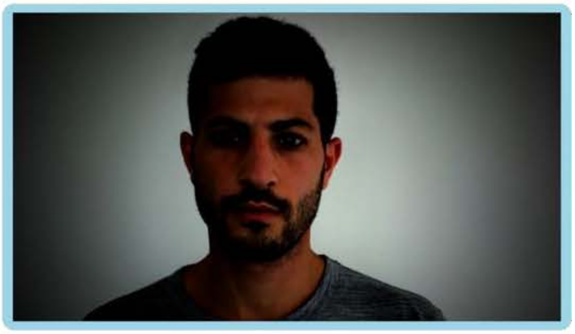
In many VMS systems, a low bit rate is used to save video storage. If a low bit rate is used, when there is a movement in the picture, there may not be enough bit rate budget to encode the video and artifacts. The resulting pixelization will generate low video quality which degrades the face’s mathematical model quality.

To ensure the best video quality when a person is in the picture, camera settings should be set to Variable Bit Rate (VBR) mode instead of Constant Bit Rate (CBR) mode.

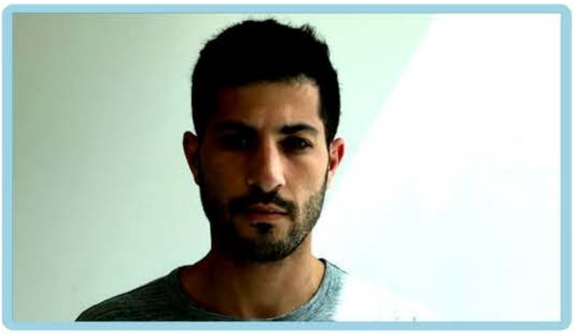
Face Enrollment

Examples of enrolled pictures

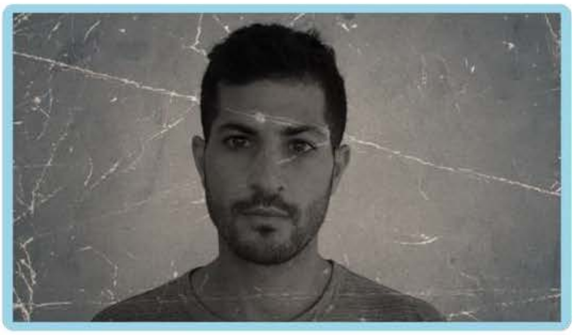
Too Dark



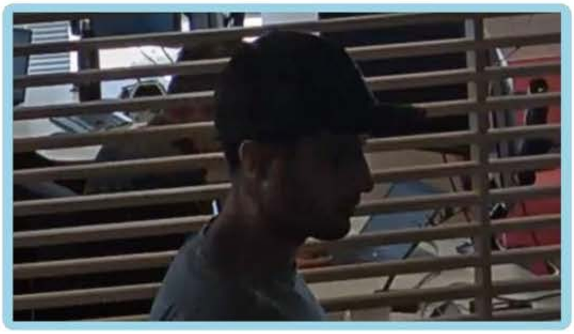
Shadows



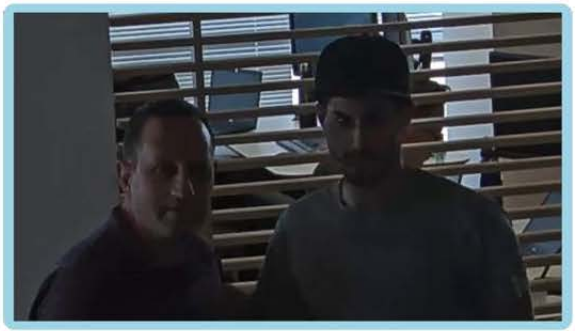
Old B&W | Water Marks



Distorted | Partially hidden



Distorted | Multiple Faces



Examples of enrolled pictures

Profile | High Angle | No Focus

Distorted

Dark Face

Reflection

Face Enrollment Best Practices

When a picture of a Person of Interest (POI) is added to the Oosto Watchlist. Oosto creates a mathematical model of that person's facial features, which is used as a reference for recognizing that person. This process is called Face Enrollment.

After a face has been enrolled, Oosto can recognize that person when they are in the Field of View (FOV) of any live or forensic video.

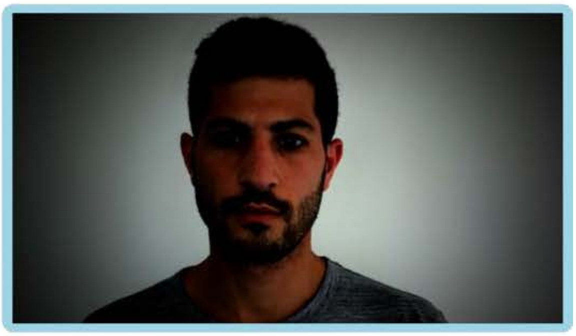
A high-quality reference picture is critical to generate the unique Facial Features data that will influence the system results. The following are the requirements for optimal face enrollment:

- Picture in JPG/BMP/PNG format
- Updated picture
- Face is in focus
- Colored photos
- Balanced light and no shadow
- Picture is not stretched or distorted
- Face size is at least 100 x 100 pixels (picture size of 200 x 200 pixels where the face is at least half of the picture)
- Facing the camera
- The entire face is visible

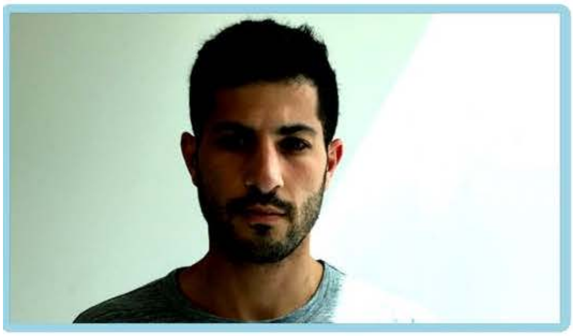
- Neutral expression and both eyes open
- Without sunglasses
- Single face in the picture

It is most preferable to enroll the highest quality picture of a POI possible into the Oosto Watchlist. When the reference picture is of lower quality, it is best to use it for manually searching for this POI and finding a better reference picture (by using the Oosto user interface or API).

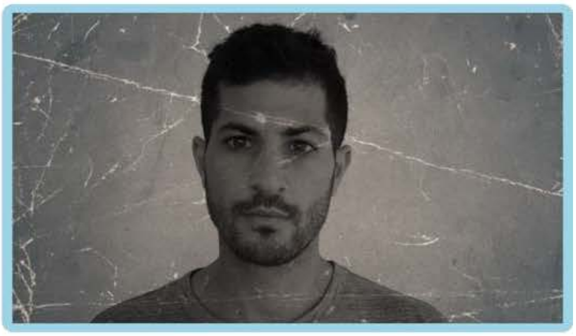
Too Dark



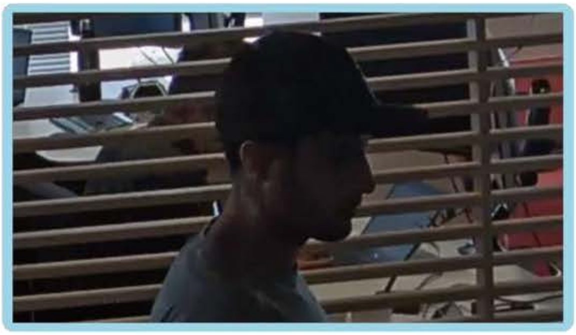
Shadows



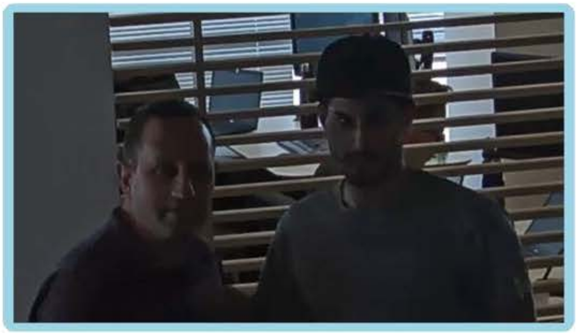
Old B&W | Water Marks



Distorted | Partially hidden



Distorted | Multiple Faces



Profile | High Angle | No Focus

Distorted

Dark Face

Reflection

Test Your API Server Connection

This guide explains how to ensure a proper connection is established between your OnWatch server and the Oosto API server.

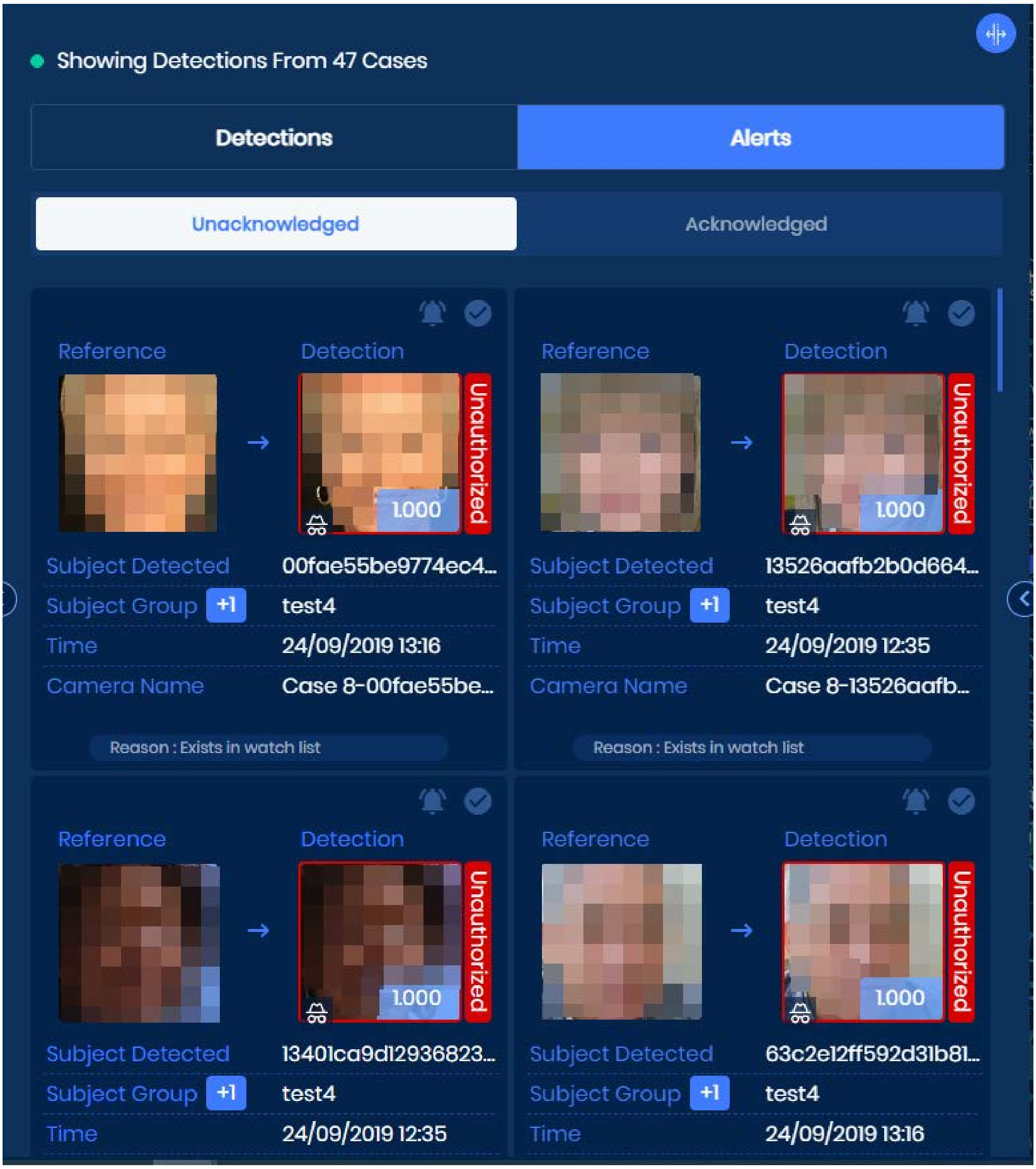
If you are interested in making API calls or receiving socket events, you will need to establish a connection between the two machines. Simply installing the OnWatch product will create the base connection but you may need to test the solution if you are experiencing technical issues.

We recommend conducting the following test before developing around our API.

> 📘 Note
>
> All sample codes are relevant for 2.6 version

Start By Checking the UI

1. Open Chrome and login to the OnWatch system.
2. Navigate to the **Live Cameras** tab and verify that you are receiving detections and alerts. If you see images on the *Live Cameras* screen, then a connection is established.



Showing Detections From 47 Cases

Subject Detected 00fae55be9774ec4...
Subject Group +1 test4
Time 24/09/2019 13:16
Camera Name Case 8-00fae55be...
Reason : Exists in watch list

Subject Detected 13526aafb2b0d664...
Subject Group +1 test4
Time 24/09/2019 12:35
Camera Name Case 8-13526aafb...
Reason : Exists in watch list

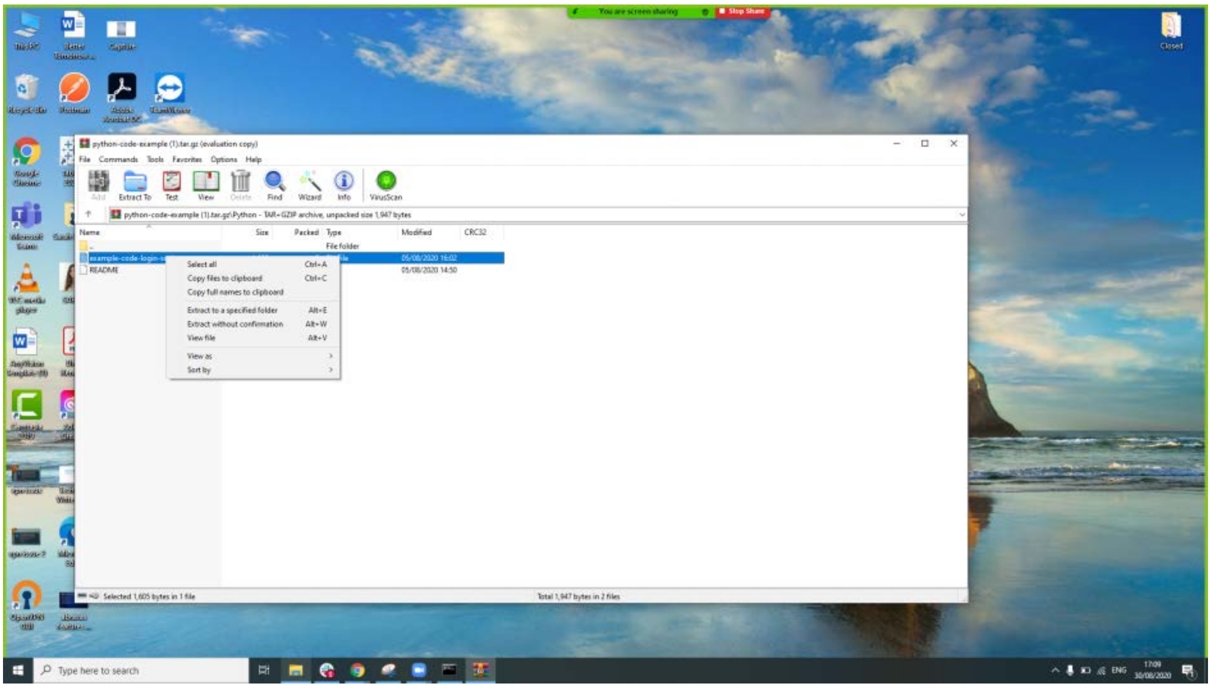
Subject Detected 13401ca9d12936823...
Subject Group +1 test4
Time 24/09/2019 12:35

Subject Detected 63c2e12ff592d31b81...
Subject Group +1 test4
Time 24/09/2019 13:16

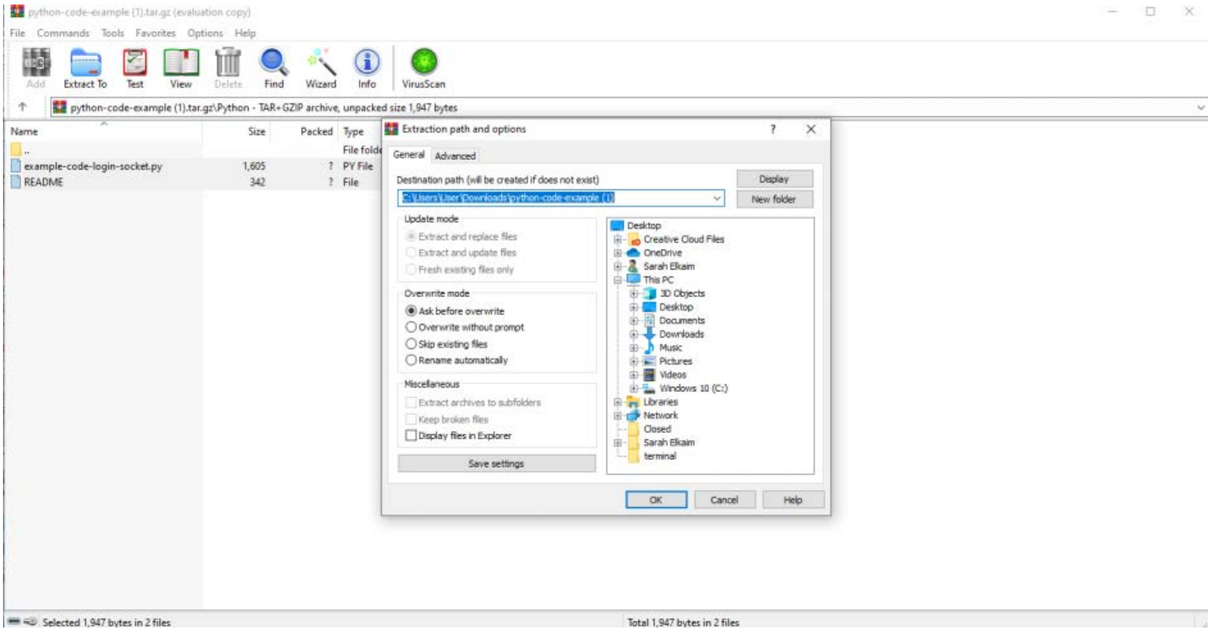
Use the Sample Code

Now that you know the system is working via the UI, run our sample code - in JavaScript or Python - to ensure the system works via API.

1. Download our API sample code in JavaScript or Python.
2. Extract the two available files by right-clicking on the downloaded .tar file and selecting **Extract to a specified folder**.


python-code-example (1).tar.gz (evaluation copy)
File Commands Tools Favorites Options Help
Add Extract To Test View Delete Find Wizard Info VirusScan
python-code-example (1).tar.gz\Python - TAR+GZIP archive, unpacked size 1,947 bytes
Name Size Packed Type Modified CRC32
File folder
example-code-login-socket.py
README
05/08/2020 16:02
05/08/2020 14:50
Select all Ctrl+A
Copy files to clipboard Ctrl+C
Copy full names to clipboard
Extract to a specified folder Alt+E
Extract without confirmation Alt+W
View file Alt+V
View as
Sort by
Selected 1,605 bytes in 1 file
Total 1,947 bytes in 2 files
Type here to search

3. Select a folder to save the new files.


python-code-example (1).tar.gz (evaluation copy)
File Commands Tools Favorites Options Help
Add Extract To Test View Delete Find Wizard Info VirusScan
python-code-example (1).tar.gz\Python - TAR+GZIP archive, unpacked size 1,947 bytes
Name Size Packed Type
File folder
Extraction path and options
General Advanced
Display
New folder
Update mode
Extract and replace files
Extract and update files
Fresh existing files only
Overwrite mode
Miscellaneous
Extract archives to subfolders
Keep broken files
Display files in Explorer
Save settings
Desktop
Creative Cloud Files
OneDrive
Sarah Elkaim
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Windows 10 (C:)
Libraries
Network
Closed
Sarah Elkaim
terminal
OK Cancel Help
Selected 1,947 bytes in 2 files
Total 1,947 bytes in 2 files

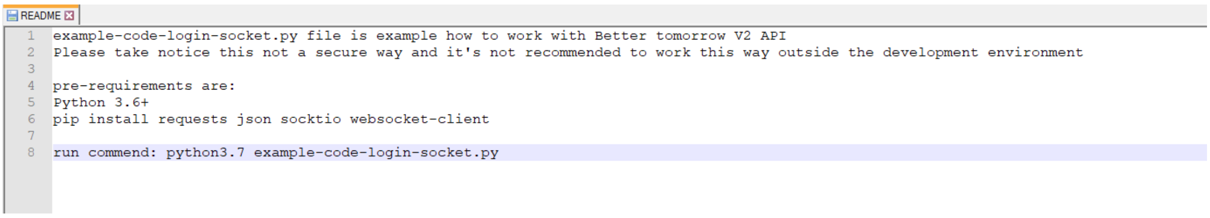
example-code-login-socket.py 1,605 ? PY File

README 342 ? File

Destination path (will be created if does not exist): C:\Users\User\Downloads\python-code-example (1)

Overwrite mode: ● Ask before overwrite ○ Overwrite without prompt ○ Skip existing files ○ Rename automatically

4. Once saved, open the README file.



```
example-code-login-socket.py file is example how to work with Better tomorrow V2 API
Please take notice this not a secure way and it's not recommended to work this way outside the development environment

pre-requirements are:
Python 3.6+
pip install requests json socktio websocket-client

run commend: python3.7 example-code-login-socket.py
```

5. Follow the instructions presented in the README file to install the necessary libraries. Make sure to include your BT username and password in the sample code as you need to log in.

6. Run the sample code in Terminal.

7. If the sample code runs successfully, you are ready to start development.

Installation

Operating Systems and Prerequisites

> 🚧 Advice
>
> Please review your proposed installation with your Oosto delivery manager who can advise you on the optimum solution for you.

Server Operating System Support

Ubuntu

- Ubuntu Server 20.04.3 (kernel 5.4.0-81) **Recommended** Guide
- Ubuntu Desktop 20.04.3 (kernel 5.11.0-27)

RHEL

- Red Hat 8.6 (Kernel 4.18.0-372.13.1.el8_6.x86_64) **Recommended** (for clean install)
- Red Hat 8.4 (Kernel 4.18.0-305.25.1.el8_4.x86_64)
- Red Hat 8.6 (Target Release date November 2022)

Deprecated (Not to be used for new installations)

- Ubuntu Server 18.04.4/5 (kernel 5.4) - Deprecating in 2.6
- Ubuntu Desktop 18.04.4/5 (kernel 5.4) - Deprecating in 2.6 Guide
- Red Hat 8.3 (Kernel 4.18.0-240.22.1.el8_86_64) - Deprecating in 2.6
- Red Hat 8.1 (kernel 4.18.0-147.el8.x86_64) - Deprecated
- RedHat 7.6 (kernel 3.10.0-957) - Deprecated

Certified Upgrade paths for RHEL and Ubuntu

- Ubuntu 18.0.4 to 20.04
- RHEL 7.x to 8.4

The system has been certified to allow the system installer to stop the OnWatch version and upgrade the full operating system. After this has been done it is important to make sure the existing OnWatch release is fully operational again before attempting the full upgrade path.

> 👍 Note:
>
> A Tips and Tricks guide can be provided for the OS upgrade. Please request this from your Oosto delivery personnel

Prerequisites

RAM - 64 GB + (may vary with each installation and architecture)
Disc OS / Disk SSD / Add storage
Hardware - described below.

Type	Designation	Size
SSD	OS	500GB+
SSD	DB	500GB (Minimum, according to system's loads)
HDD	Videos	1TB (Minimum, according to system's retention period)

Network-

Cluster requisites:
NTP server
SSH - ssh-server installed on the machine. How To check if ssh is installed:
Hostname: must be in lowercase letters

Vision AI Jetson

Oosto appliance provided via your Oosto representative is provided with a custom OS build which Ossto will provide. The appliance can be easily installed Guide

HQ

As part of HQ installation, the system requires a certificate to be installed.
Customers should provide their own corporate certificate

Ubuntu Desktop Installation

Before installing Ubuntu on your server, make sure:

- No Operating System already installed on your machine
- No important data is saved, as it will be deleted
- The server is not connected to the internet
- You have Etchersoftware (to create bootable USB Drive)

> ❗ **Existing Data will be Deleted**
>
> This procedure will delete any and all existing data already on the machine.

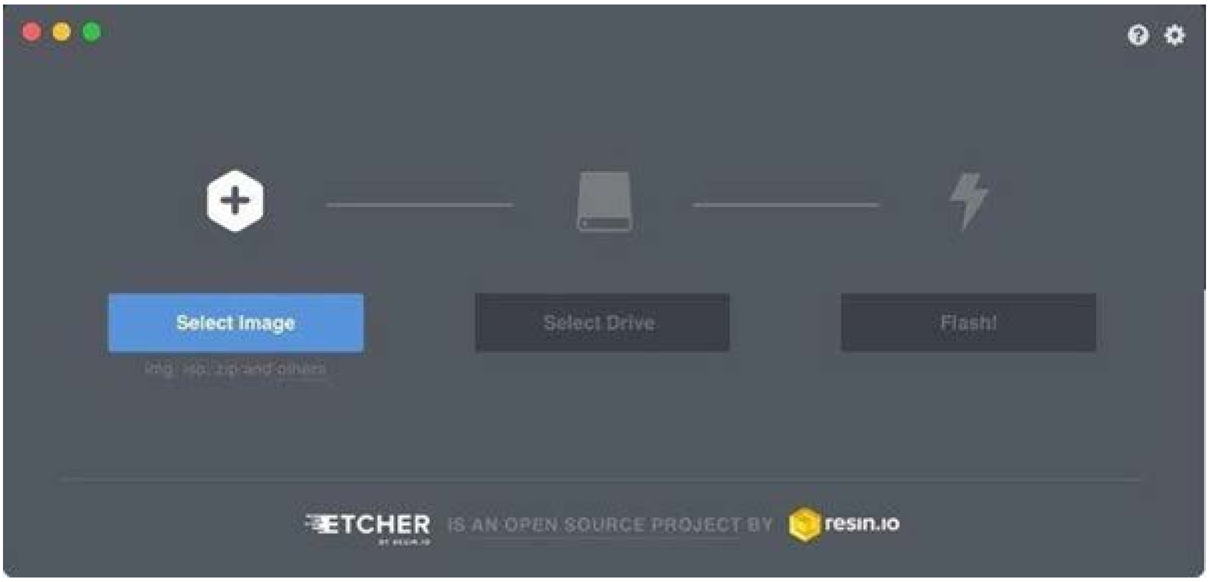
Step 1: Download the Ubuntu Image File

1. Download and install the Ubuntu Operating System.

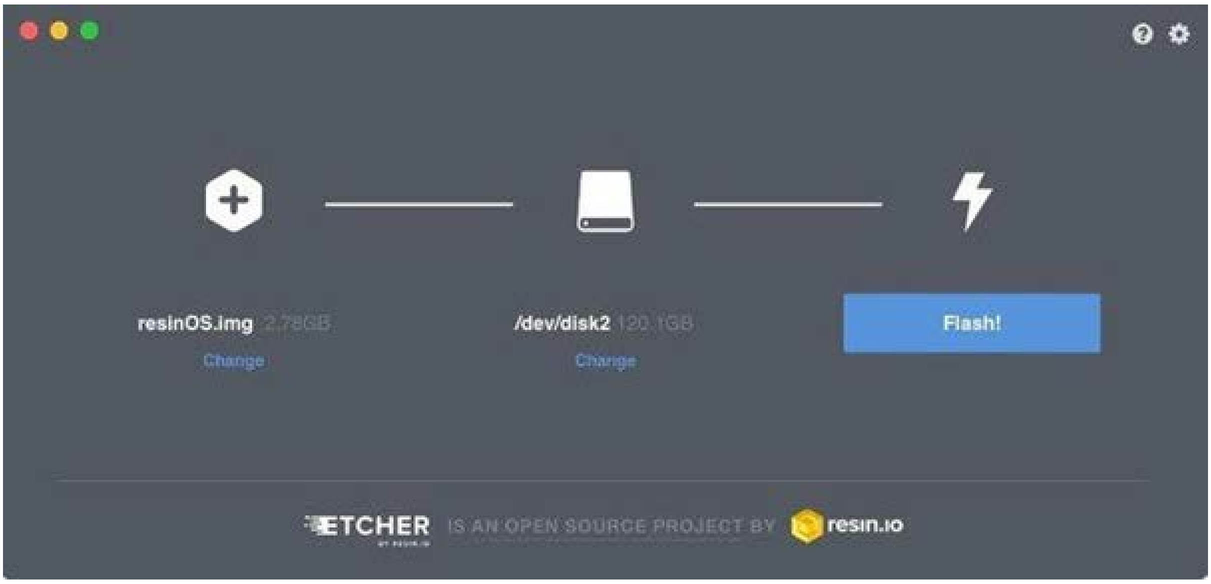
2. After the installation is complete, you will have the LiveCD image file available on your machine and can continue to create a bootable USB drive.

Step 2: Boot the System from the USB Drive

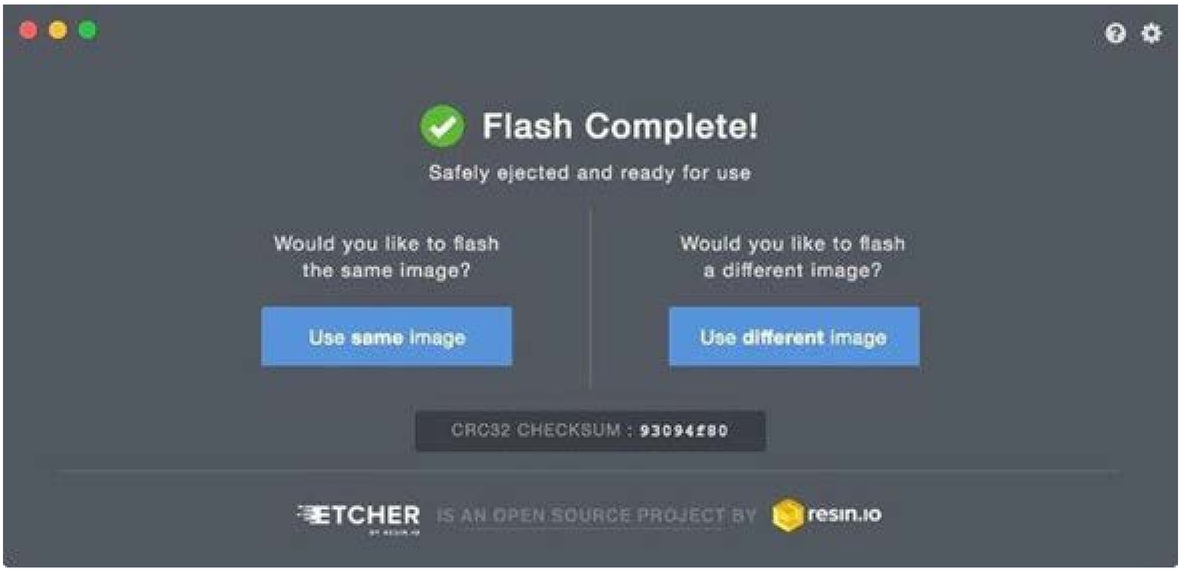
1. Open the **Etcher** application.
2. Select a **source image** by dragging and dropping one from your desktop directly to the Etcher app or by using the file selector.



3. Select the **target drive**. You may differentiate your USBs and SD cards from your hard disks so that they are not inadvertently erased.
4. Complete the process by clicking the **Flash** button.



5. After a few minutes, the USB drive will be ready for use.



Flash Complete!

Safely ejected and ready for use

Would you like to flash the same image?

Use same image

Would you like to flash a different image?

Use different image

CRC32 CHECKSUM : 93094f80

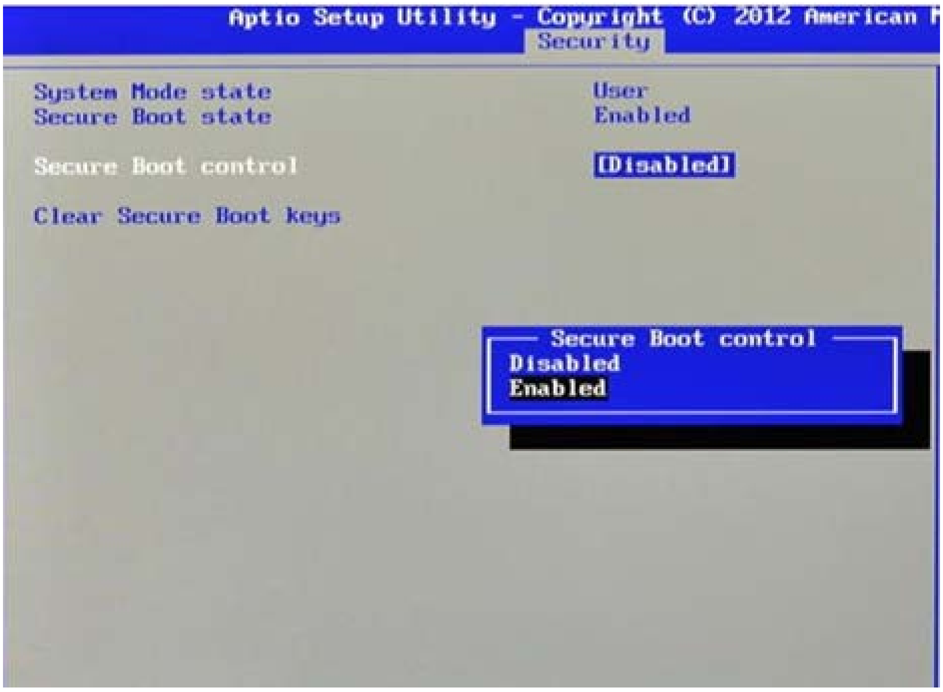
ETCHER IS AN OPEN SOURCE PROJECT BY resin.io

Step 3: Configure the BIOS

1. Plug in the USB drive that contains the Ubuntu image and boot it by pressing either the **DEL/ESC +F1/F2** keys on your keyboard.

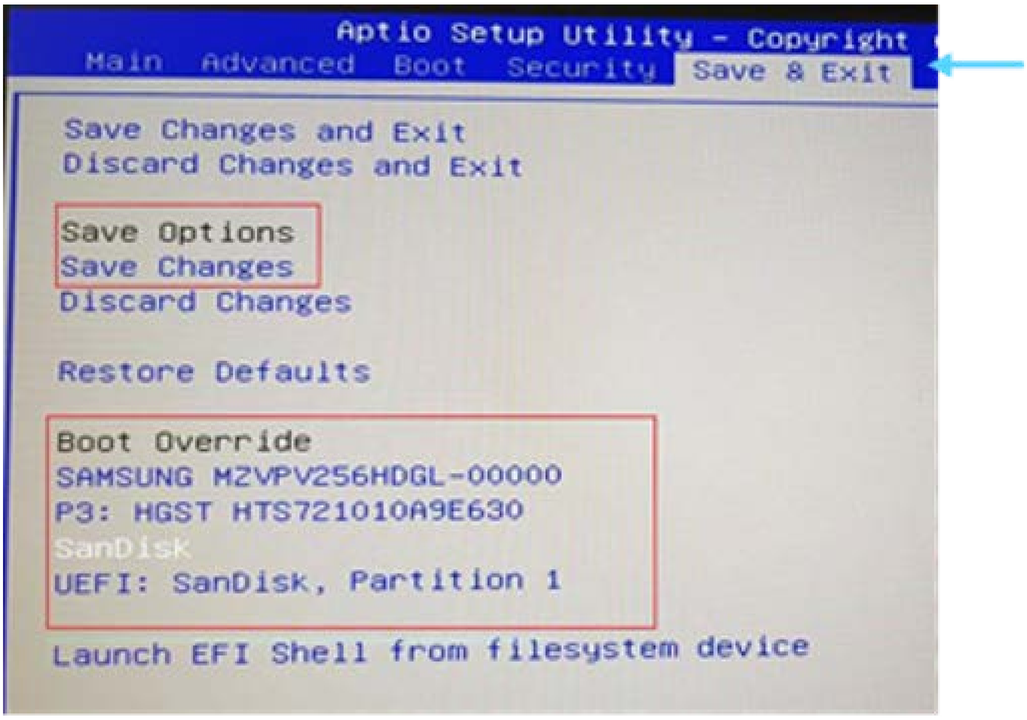
> **! Disable Network Connectivity**
>
> Disable ANY Network connectivity before proceeding to the next steps by disconnecting ethernet cable

1. In the *BIOS _menu, navigate to the _Secure Boot* menu using the arrow keys.
2. Check that the **Secure Boot** option is disabled by selecting the **Security** tab > **Secure Boot** menu.
3. Disable the **Secure Boot Control**.



```
Aptio Setup Utility - Copyright (C) 2012 American M
                                 Security

 System Mode state                    User
 Secure Boot state                    Enabled

 Secure Boot control                  [Disabled]

 Clear Secure Boot keys

                               ── Secure Boot control ──
                                Disabled
                                Enabled
```

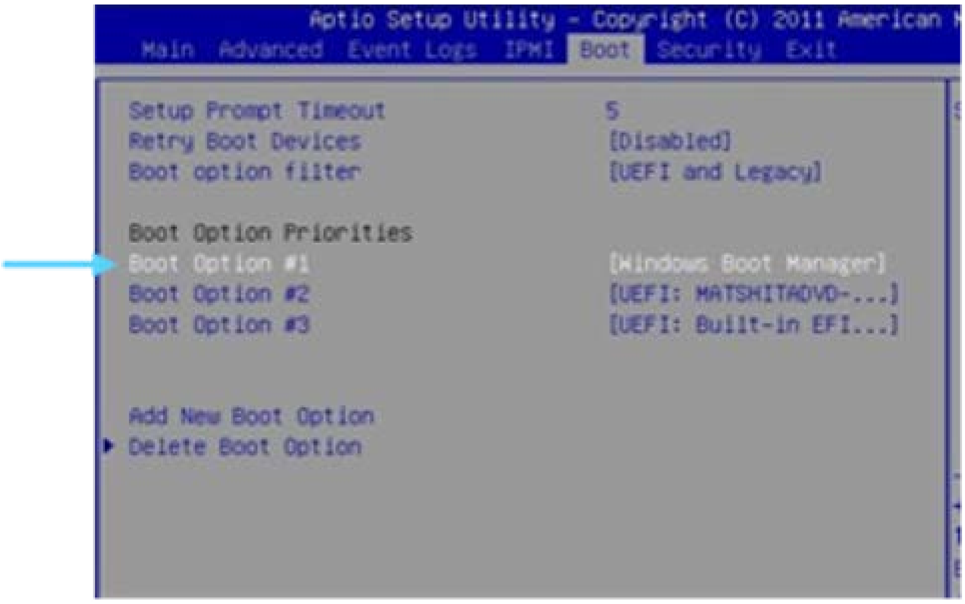
5. Select **Save & Exit** to save your changes.



```
            Aptio Setup Utility - Copyright
  Main   Advanced   Boot   Security   Save & Exit

   Save Changes and Exit
   Discard Changes and Exit

   Save Options
   Save Changes
   Discard Changes

   Restore Defaults

   Boot Override
   SAMSUNG MZVPV256HDGL-00000
   P3: HGST HTS721010A9E630
   SanDisk
   UEFI: SanDisk, Partition 1

   Launch EFI Shell from filesystem device
```

6. Select the **Boot** tab from the top menu bar.

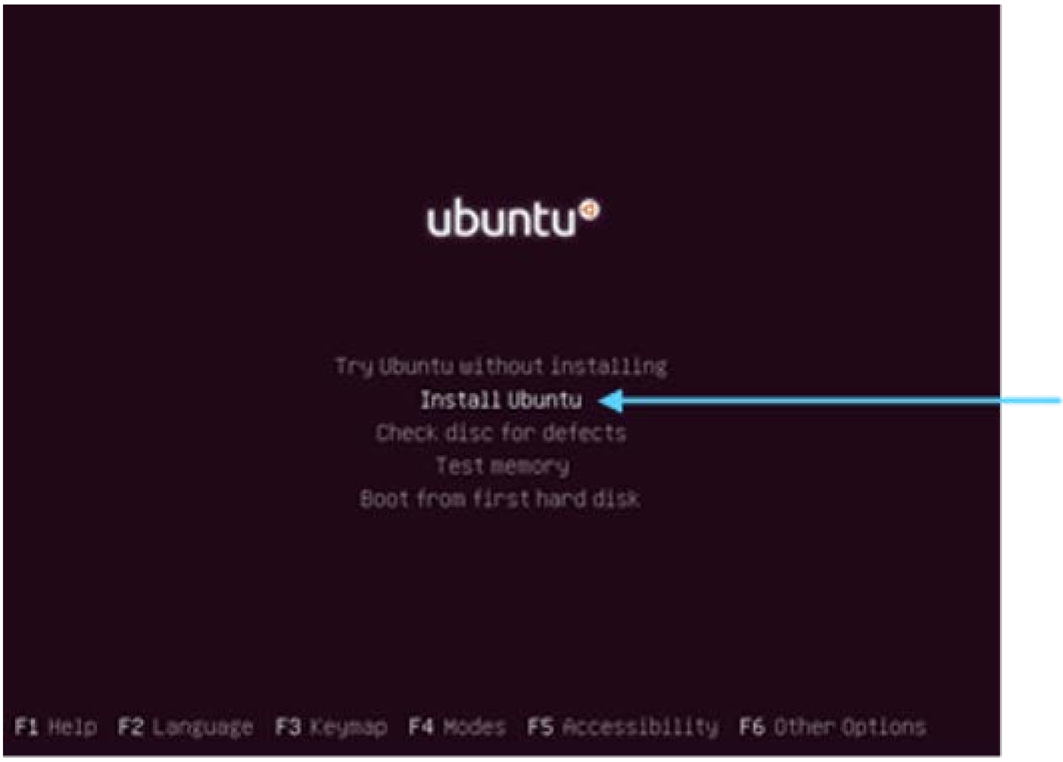
7. Select **Boot Option#1 (SanDisk)** to override the current settings and press **Enter**.



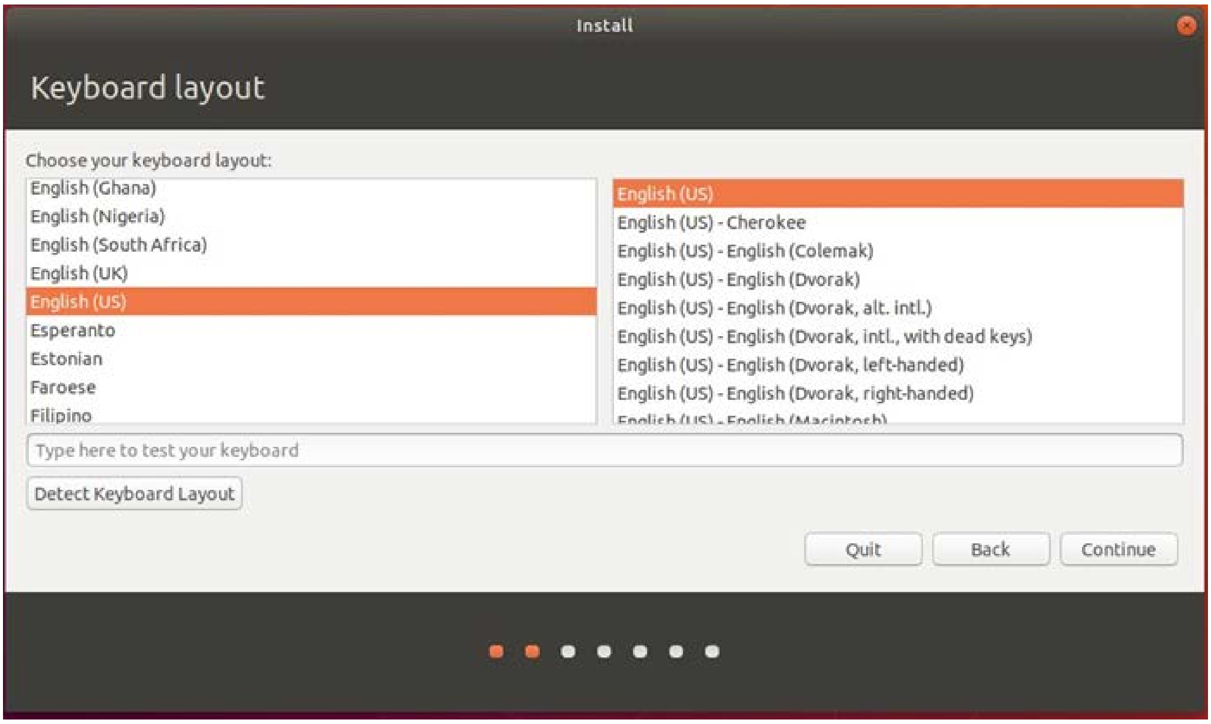
```
         Aptio Setup Utility - Copyright (C) 2011 American
  Main  Advanced  Event Logs  IPMI  Boot  Security  Exit

   Setup Prompt Timeout              5
   Retry Boot Devices                [Disabled]
   Boot option filter                [UEFI and Legacy]

   Boot Option Priorities
   Boot Option #1                    [Windows Boot Manager]
   Boot Option #2                    [UEFI: MATSHITADVD-...]
   Boot Option #3                    [UEFI: Built-in EFI...]


   Add New Boot Option
 ▶ Delete Boot Option
```

Step 4: Configure the Ubuntu Settings

1. Once Ubuntu has been installed and booted, select **Install Ubuntu**.



2. Select **English** as the default language and press **Continue**.

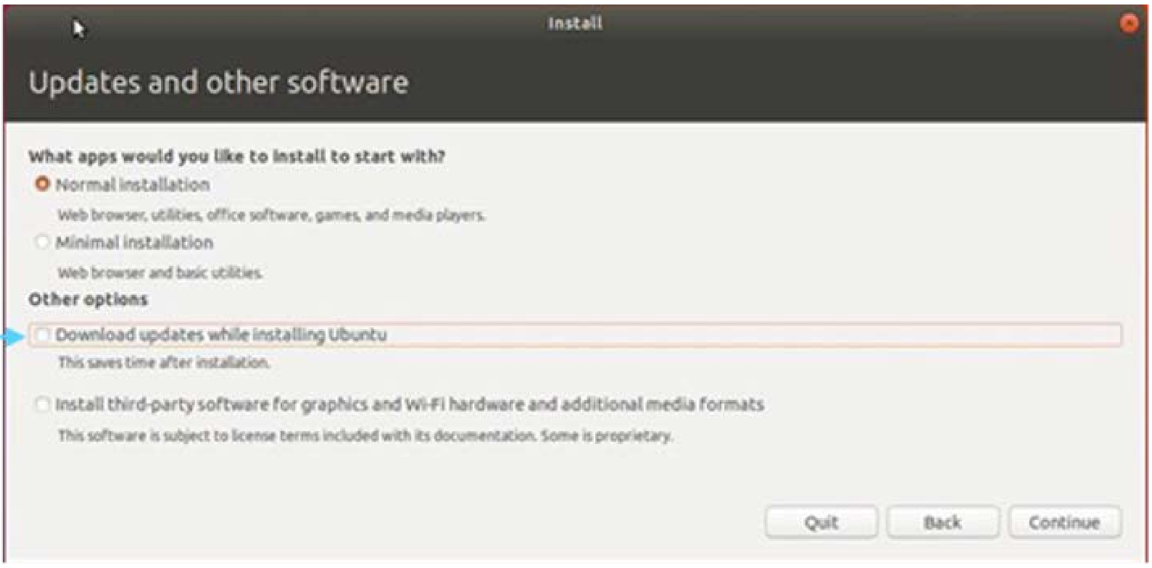

Install

Keyboard layout

Choose your keyboard layout:

English (Ghana)
English (Nigeria)
English (South Africa)
English (UK)
English (US)
Esperanto
Estonian
Faroese
Filipino
English (US)
English (US) - Cherokee
English (US) - English (Colemak)
English (US) - English (Dvorak)
English (US) - English (Dvorak, alt. intl.)
English (US) - English (Dvorak, intl., with dead keys)
English (US) - English (Dvorak, left-handed)
English (US) - English (Dvorak, right-handed)
English (US) - English (Macintosh)
Type here to test your keyboard
Detect Keyboard Layout
Quit
Back
Continue

3. Uncheck the **Download updates while installing Ubuntu** checkmark and ensure the **Normal installation checkbox** remains marked.



Updates and other software

What apps would you like to install to start with?

● Normal installation

Web browser, utilities, office software, games, and media players.

○ Minimal installation

Web browser and basic utilities.

Other options

□ Download updates while installing Ubuntu

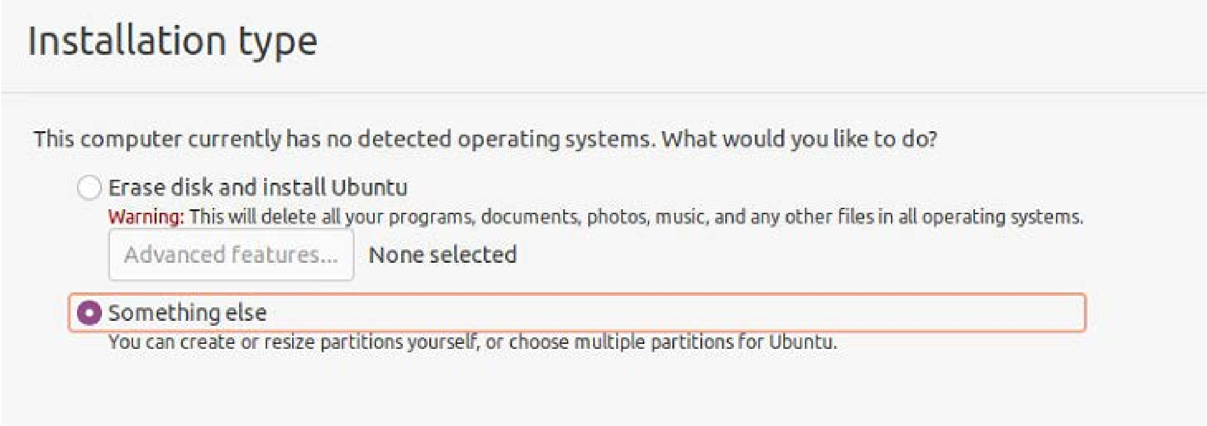
This saves time after installation.

□ Install third-party software for graphics and Wi-Fi hardware and additional media formats

This software is subject to license terms included with its documentation. Some is proprietary.

4. Click **Continue**.

5. Check the **Something Else** checkbox.



Installation type

This computer currently has no detected operating systems. What would you like to do?

○ Erase disk and install Ubuntu

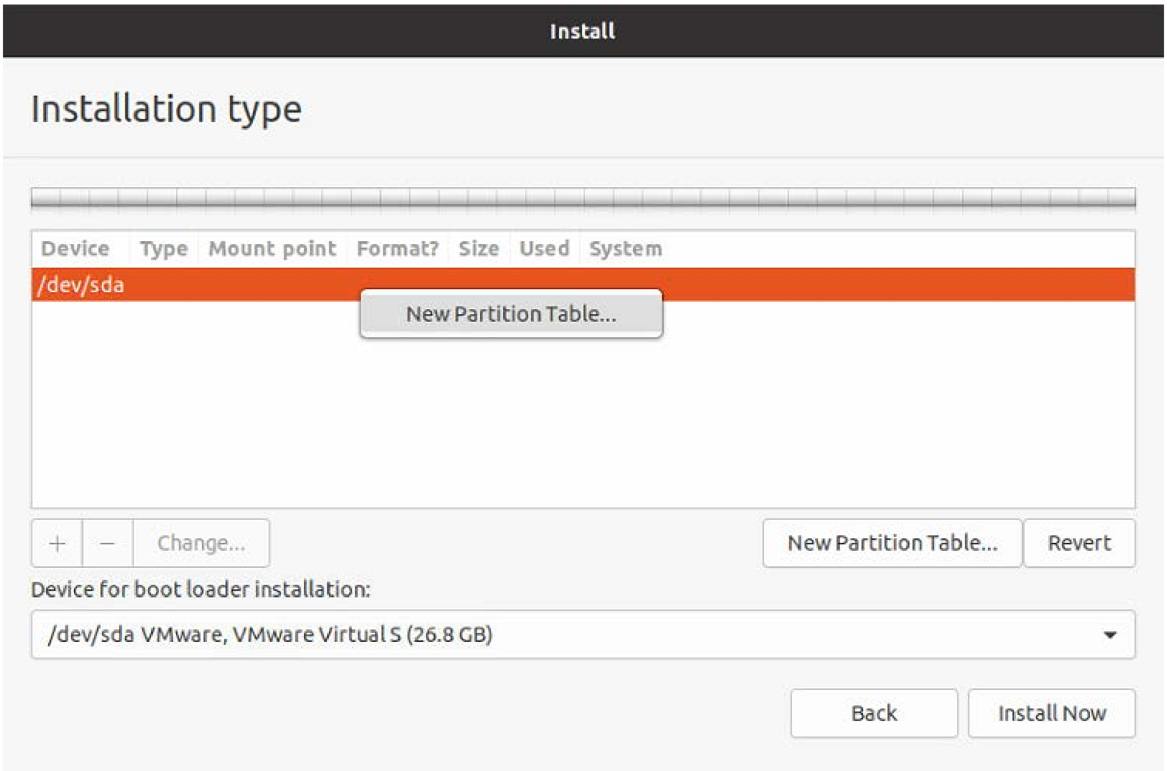
Warning: This will delete all your programs, documents, photos, music, and any other files in all operating systems.

None selected

● Something else

You can create or resize partitions yourself, or choose multiple partitions for Ubuntu.

6. Right Click on the desired disk (repeat this operation for each disk) -> New Partition table



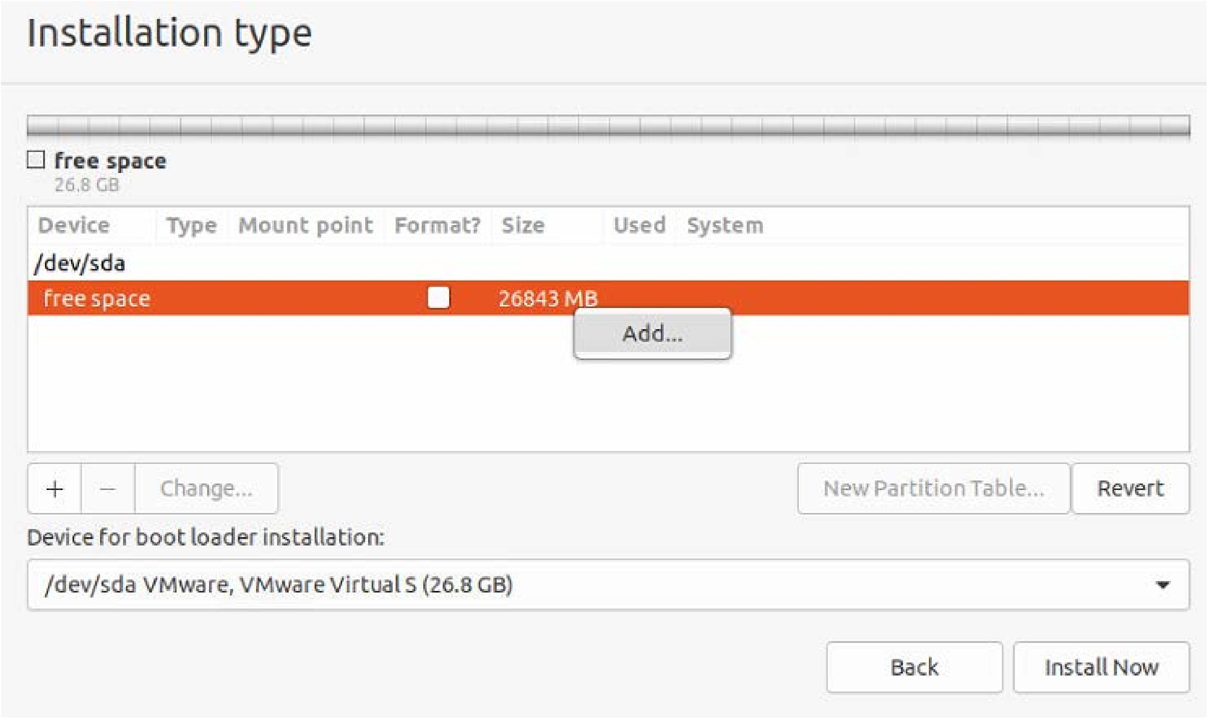
Installation type

Device	Type	Mount point	Format?	Size	Used	System
/dev/sda						

Device for boot loader installation:

/dev/sda VMware, VMware Virtual S (26.8 GB)

7. Right Click on the free space that was created, then "Add"



Installation type

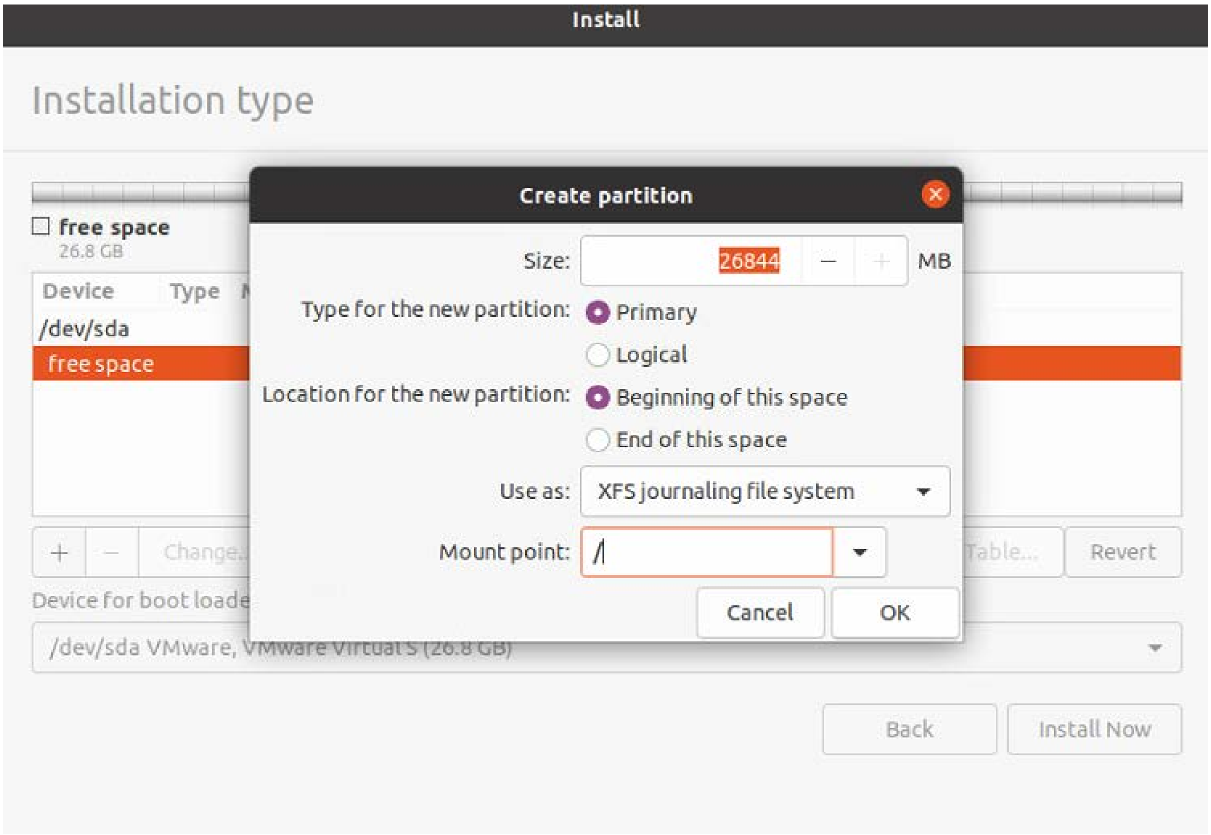
□ free space
26.8 GB

Device	Type	Mount point	Format?	Size	Used	System
/dev/sda						
free space			□	26843 MB		

Device for boot loader installation:
/dev/sda VMware, VMware Virtual S (26.8 GB)

8. Configure Disk:

Change only these options:
Use as: "XFS journaling file system"
Mount point:
For OS Disk choose: "/"
For SSD Disk choose "/ssd"
For Storage Disk type: "/storage"



Install

Installation type

Create partition

Size: 26844 MB

Type for the new partition: ● Primary ○ Logical

Location for the new partition: ● Beginning of this space ○ End of this space

Use as: XFS journaling file system

Mount point: /

! Your Disk Data will be Erased

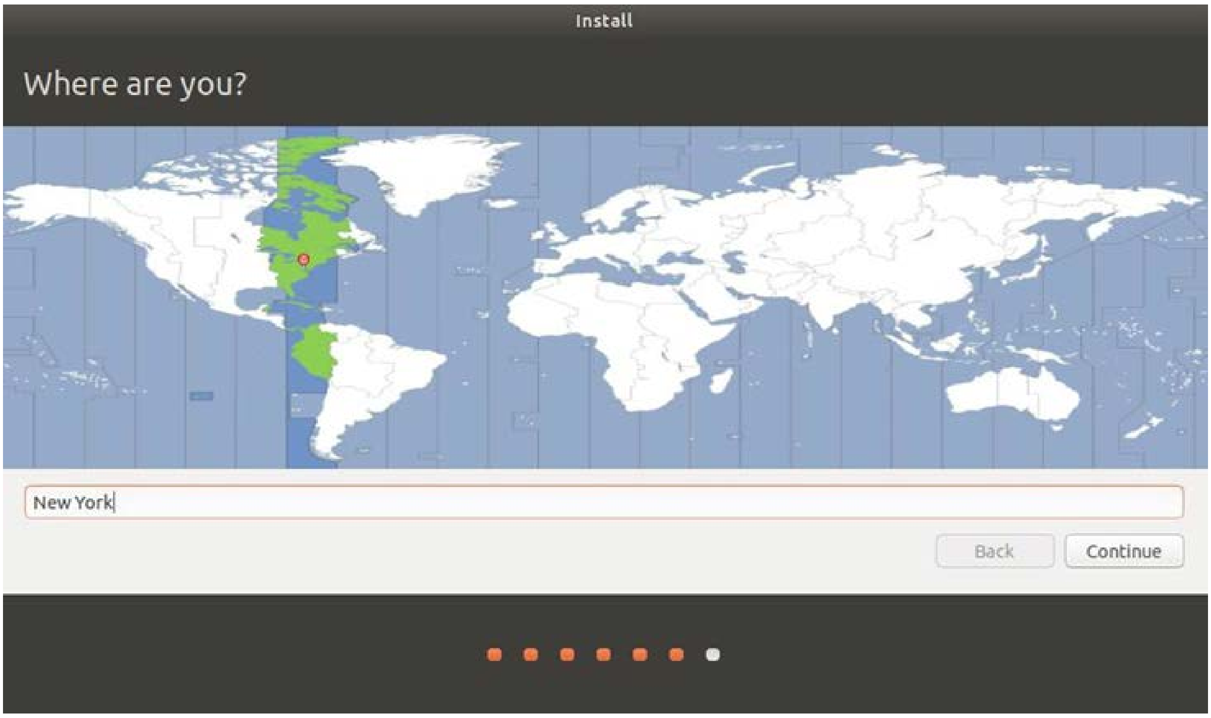
This step deletes all previous data on the drive.

6. Select your **smaller disk** in the *Select drive* dropdown menu.

7. Click **Install Now**.

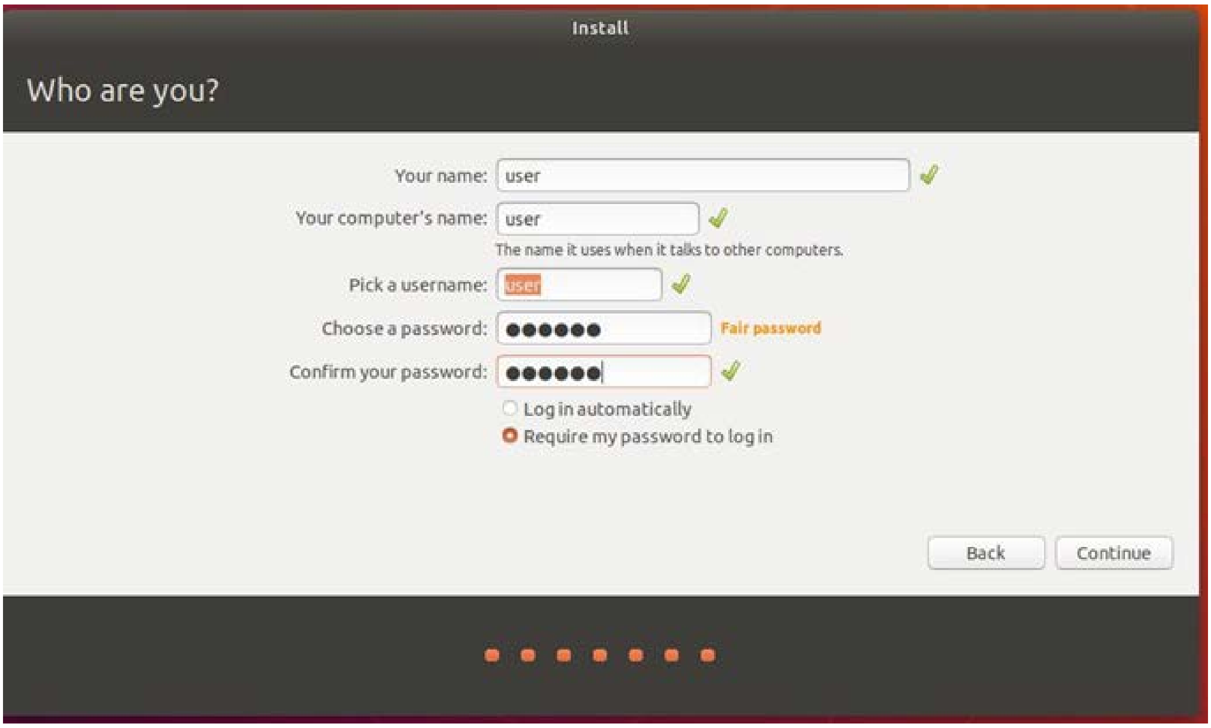
8. A popup will appear showcasing all the partitions that will be changed or deleted. Click **Continue**.

9. To specify a time zone, start typing the location (for example, New York) and watch the location sign position itself on your location. Then, click Continue.



New York

10. Enter your **username** and **computer name**.



Your name: user ✓

Your computer's name: user ✓

The name it uses when it talks to other computers.

Pick a username: user ✓

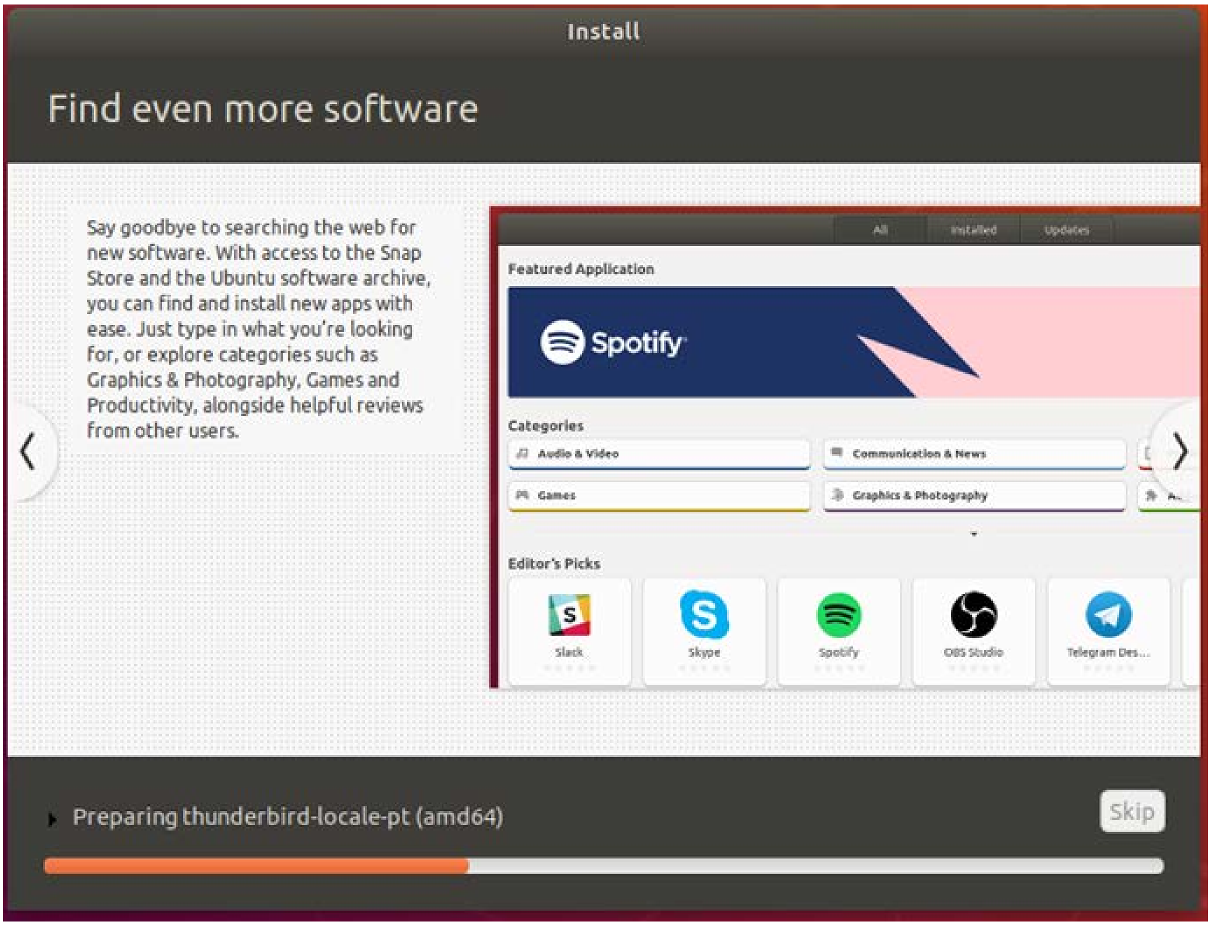
Choose a password: ●●●●●● Fair password

Confirm your password: ●●●●●● ✓

○ Log in automatically

● Require my password to log in

11. The system will take about 5 minutes to install. A progress bar will appear to showcase the status of the installation.



Install

Find even more software

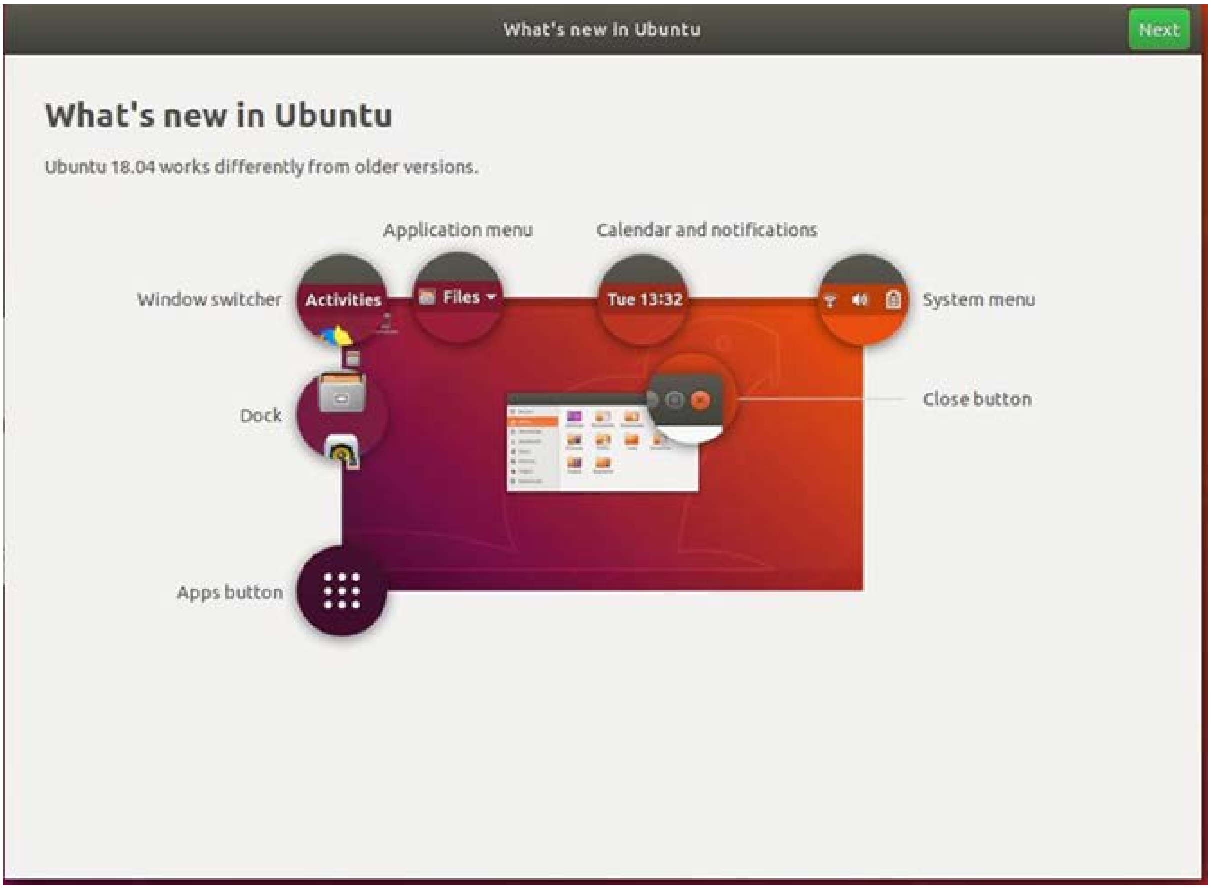
Say goodbye to searching the web for new software. With access to the Snap Store and the Ubuntu software archive, you can find and install new apps with ease. Just type in what you're looking for, or explore categories such as Graphics & Photography, Games and Productivity, alongside helpful reviews from other users.

Preparing thunderbird-locale-pt (amd64)

12. After the installation is complete, remove the USB drive and **reboot your machine**. If a black screen appears and the machine does not reboot, press **Ctrl** + **C**.

Step 5: Log in to Ubuntu

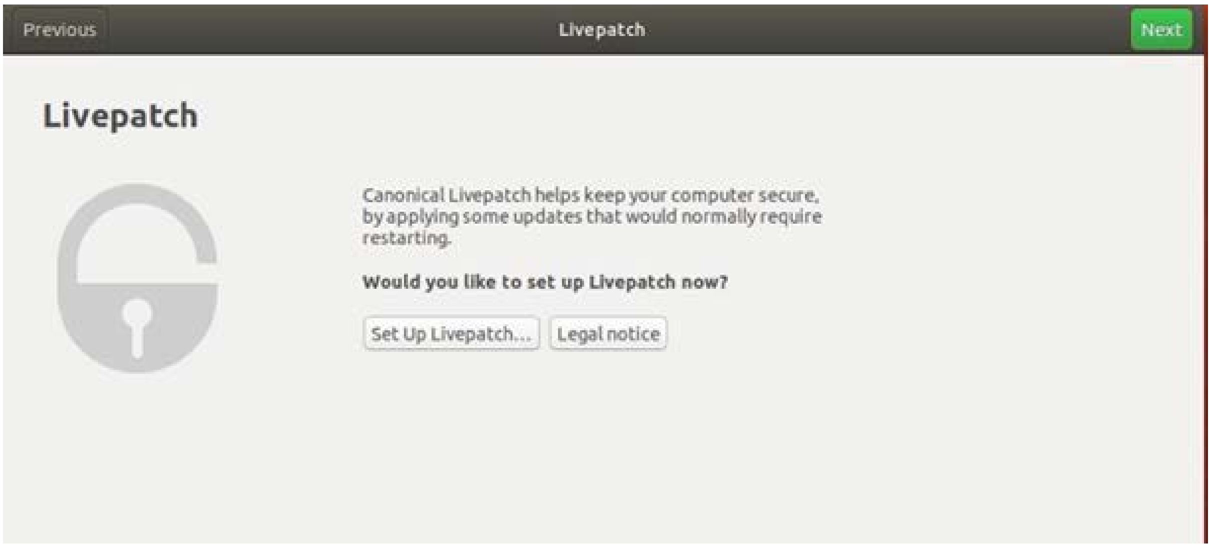
1. Open **Ubuntu** and log in.



What's new in Ubuntu

Ubuntu 18.04 works differently from older versions.

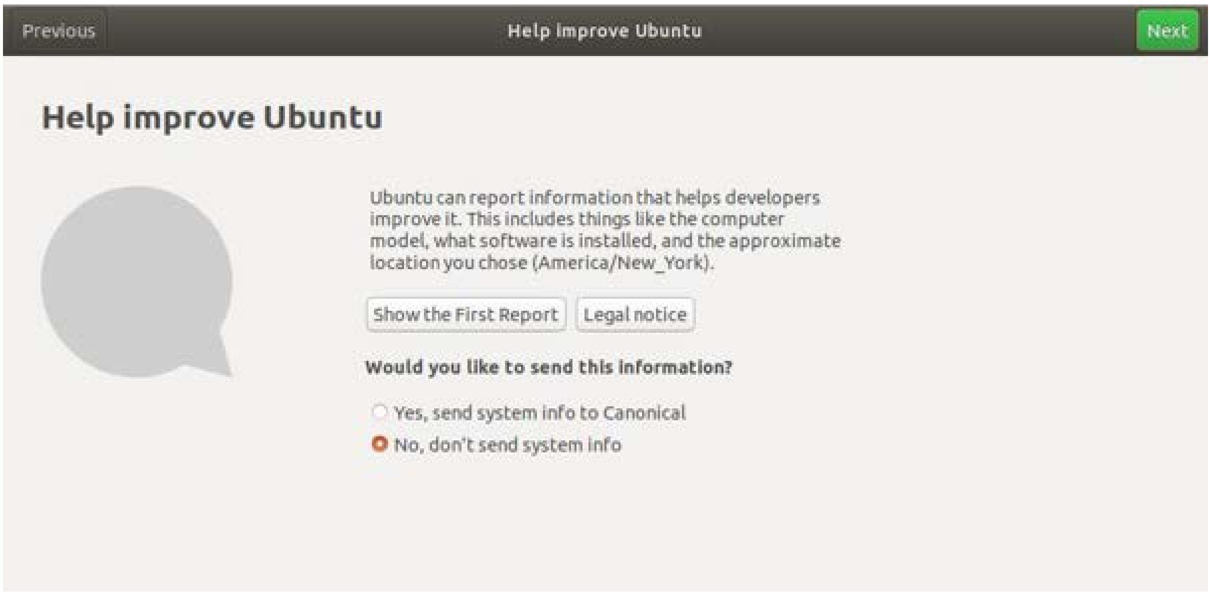
2. Click **Next** in all the following windows.



Livepatch

Canonical Livepatch helps keep your computer secure, by applying some updates that would normally require restarting.

Would you like to set up Livepatch now?

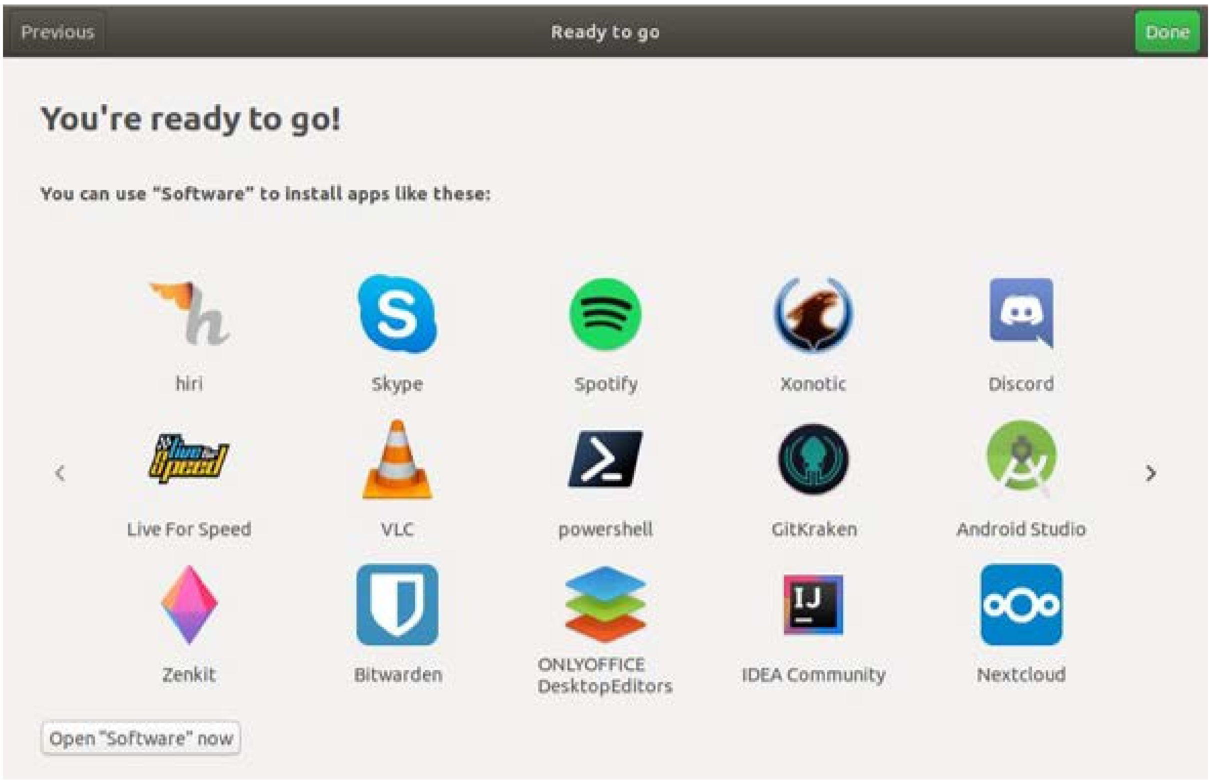


Help improve Ubuntu

Ubuntu can report information that helps developers improve it. This includes things like the computer model, what software is installed, and the approximate location you chose (America/New_York).

Would you like to send this information?

○ Yes, send system info to Canonical
● No, don't send system info



You're ready to go!

You can use "Software" to install apps like these:

Step 6: Configure the Storage Drive

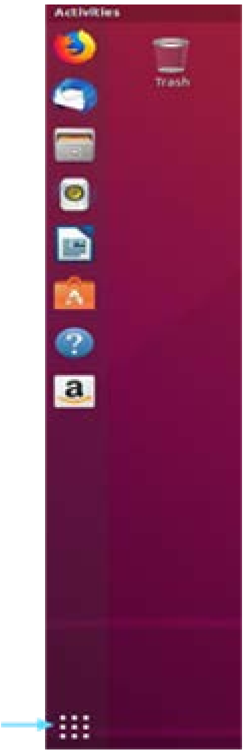
Depending on how many drives your machine has, the configuration process will differ. The system can have anywhere between one to three drives. Oosto systems allocate three partitions for storage:

- The OS itself
- /SSD
- /Storage

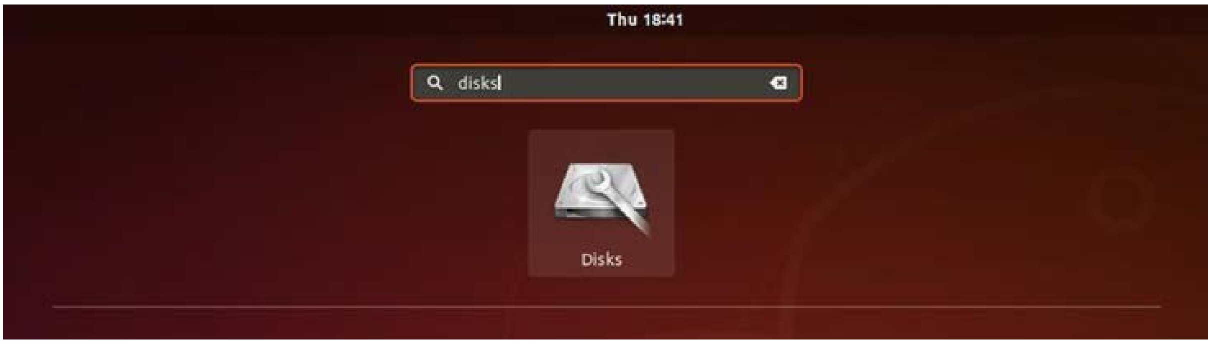
> 👍 **Continue with the remaining steps according to how many drivers your desktop has**
>
> If you have one drive, you can skip this section of the guide.
> If you have two drives, follow the process for systems with two drives.
> If you have three drives, follow the process for systems with three drives.

2 Drives

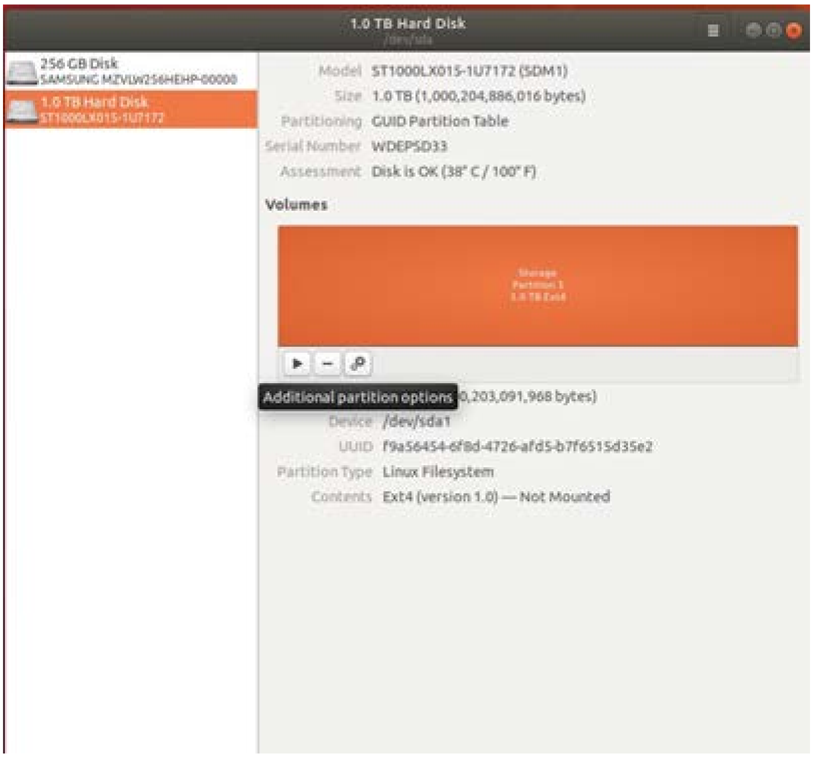
1. Click the icon at the bottom of the left window.



2. In the search field, type **disks** and then click the **Disks** icon that appears.



3. From the left side, select the **disk with the largest disk space**. (For example, in the image below, you would select the 1.0 TB disk because it is larger than the 256 GB disk.)



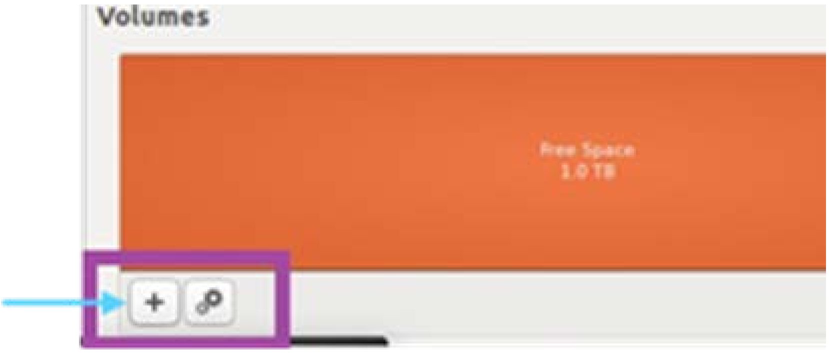
Model ST1000LX015-1U7172 (SDM1)
Size 1.0 TB (1,000,204,886,016 bytes)
Partitioning GUID Partition Table
Serial Number WDEPSD33
Assessment Disk is OK (38° C / 100° F)

0,203,091,968 bytes)
Device /dev/sda1
UUID f9a56454-6f8d-4726-afd5-b7f6515d35e2
Partition Type Linux Filesystem
Contents Ext4 (version 1.0) — Not Mounted

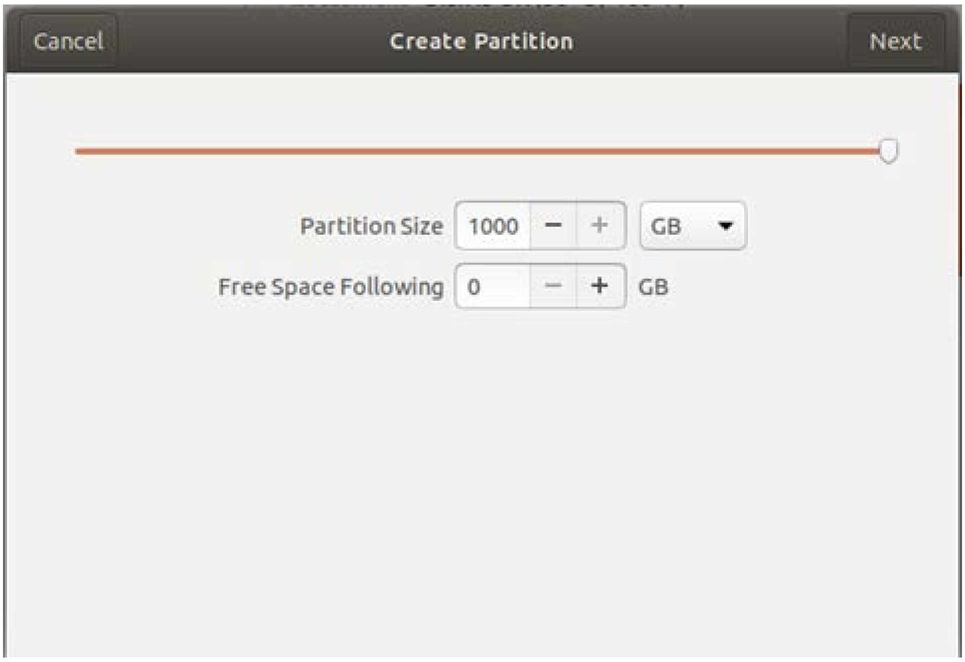
4. Look at the two small square buttons below the large orange square.

5. If there is a minus (-) symbol next to the plus (+) symbol, it means there is already data on the drive. In this case, click the **minus** button to delete the partition on the drive. After that, there should be only two buttons showing.

6. Click the **plus** button to open the Create Partition window.



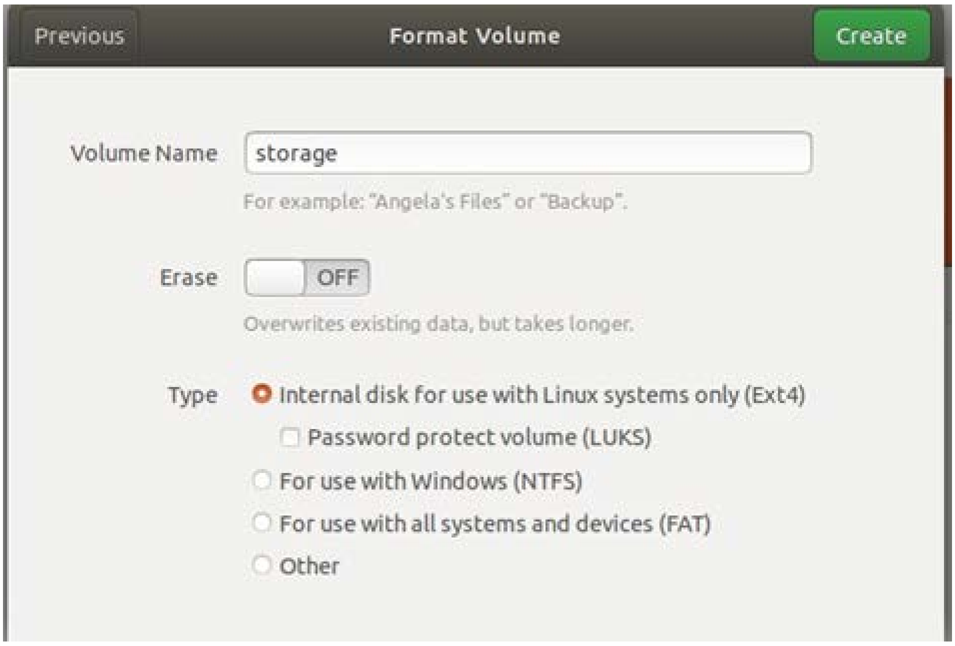
7. Make sure that the slider bar in the window is set all the way to the right and then click **Next**.



Partition Size 1000 GB

Free Space Following 0 GB

8. The Format Volume window will display. In the *Volume Name* field, enter **storage** and click the **Create** button.



Volume Name storage

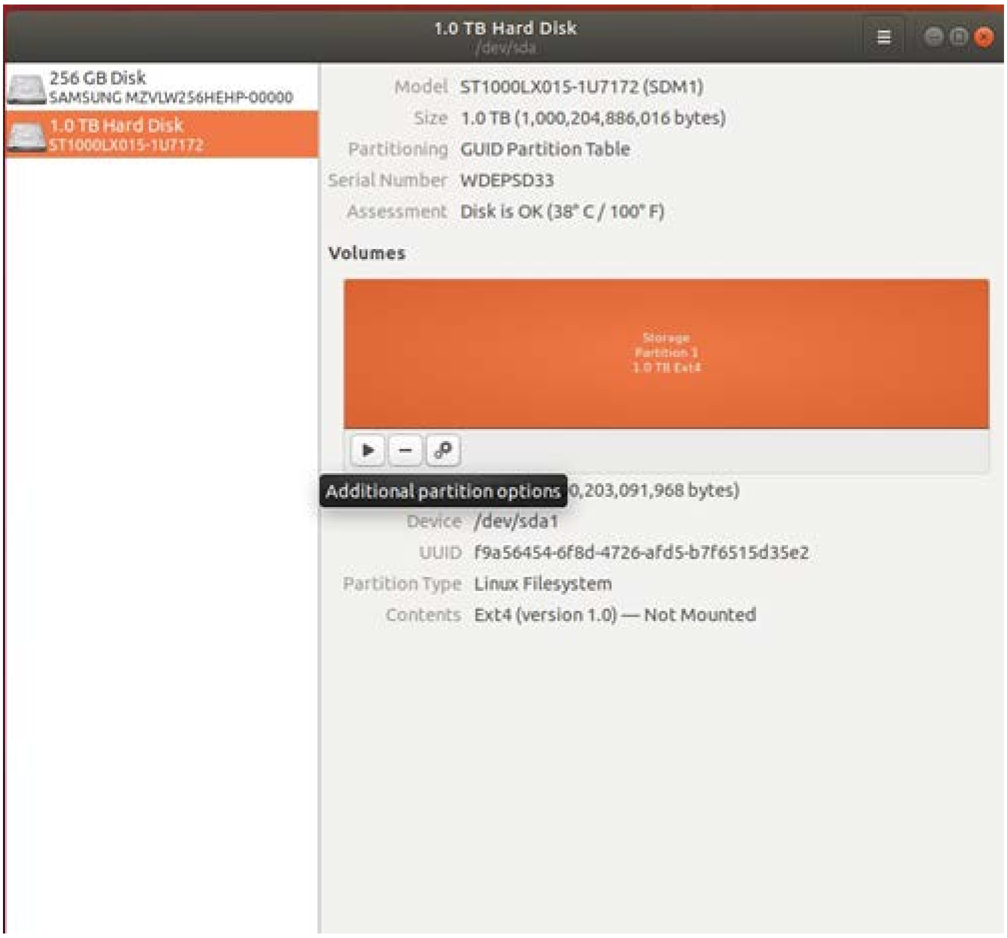
For example: "Angela's Files" or "Backup".

Erase OFF

Overwrites existing data, but takes longer.

Type
● Internal disk for use with Linux systems only (Ext4)
□ Password protect volume (LUKS)
○ For use with Windows (NTFS)
○ For use with all systems and devices (FAT)
○ Other

9. Once created, you will be directed back to the main popup, as shown below.



1.0 TB Hard Disk
/dev/sda

256 GB Disk
SAMSUNG MZVLW256HEHP-00000

1.0 TB Hard Disk
ST1000LX015-1U7172

Model ST1000LX015-1U7172 (SDM1)
Size 1.0 TB (1,000,204,886,016 bytes)
Partitioning GUID Partition Table
Serial Number WDEPSD33
Assessment Disk is OK (38° C / 100° F)

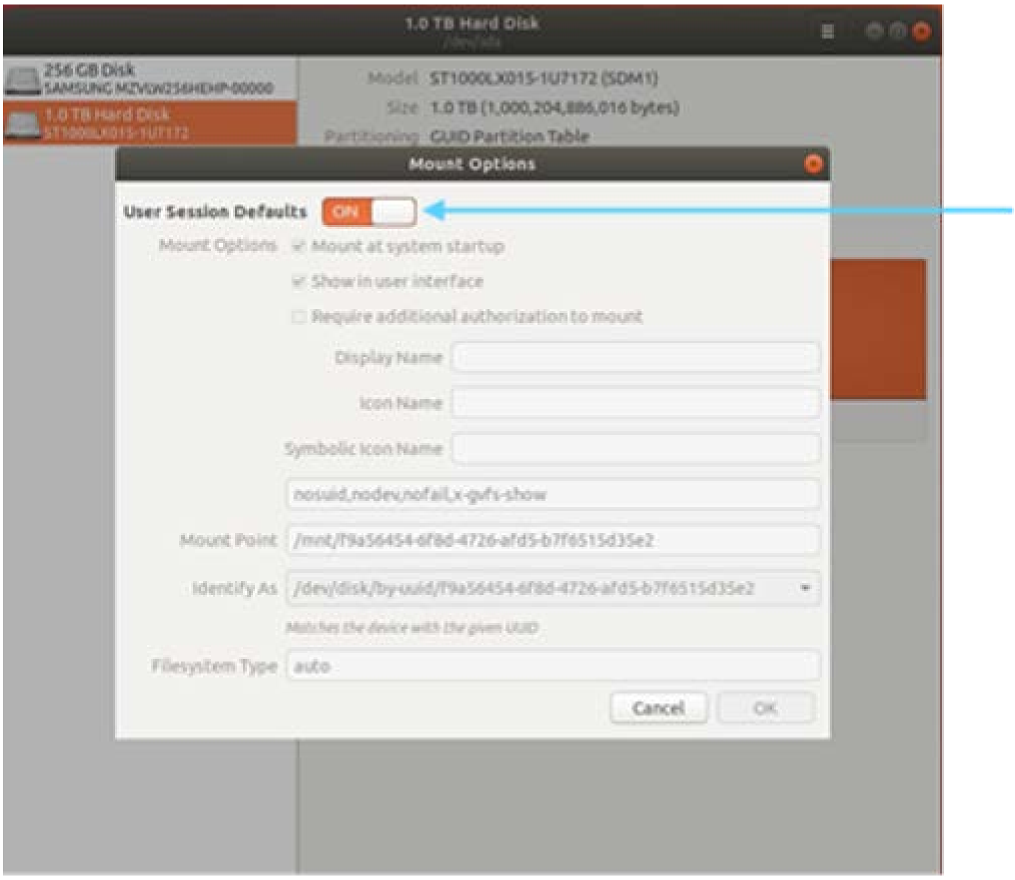
Volumes

0,203,091,968 bytes)
Device /dev/sda1
UUID f9a56454-6f8d-4726-afd5-b7f6515d35e2
Partition Type Linux Filesystem
Contents Ext4 (version 1.0) — Not Mounted

10. Chick the **Cogwheel** icon.

11. Select the **Edit Mount Options** from the dropdown.

12. In the *Mount Options* window, change the **User Session Defaults** setting to OFF by using the toggle.



Mount Options

User Session Defaults ON

Mount Options ☑ Mount at system startup
☑ Show in user interface
□ Require additional authorization to mount

Display Name

Icon Name

Symbolic Icon Name

nosuid,nodev,nofail,x-gvfs-show

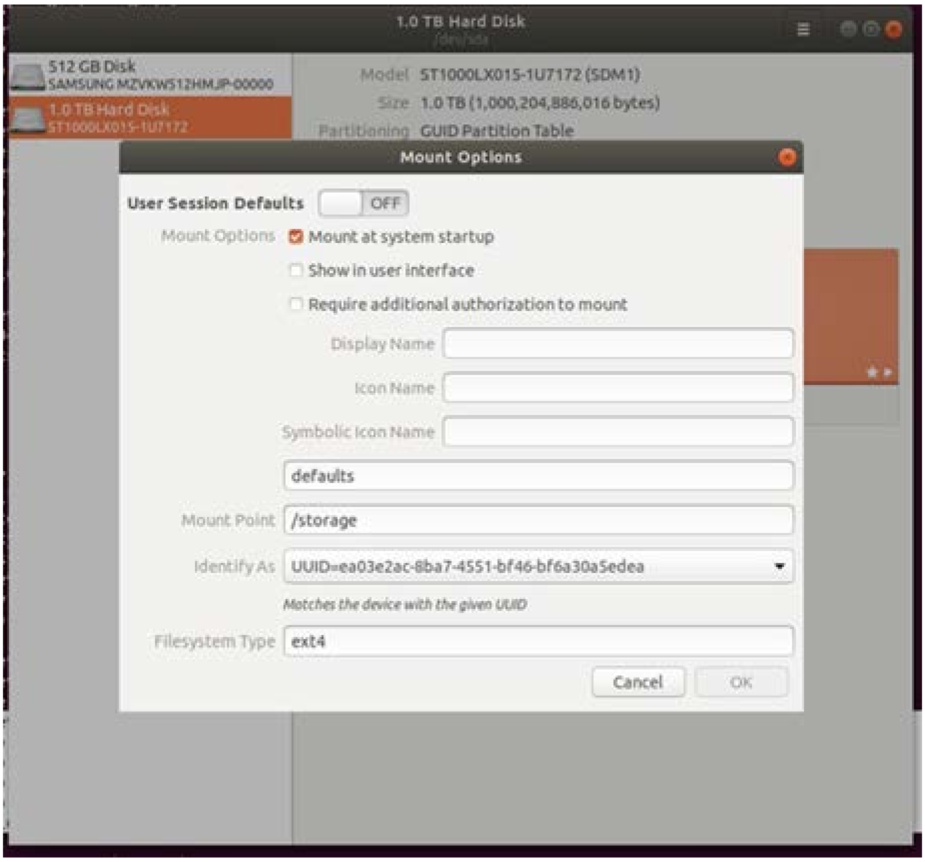
Mount Point /mnt/f9a56454-6f8d-4726-afd5-b7f6515d35e2

Identify As /dev/disk/by-uuid/f9a56454-6f8d-4726-afd5-b7f6515d35e2

Matches the device with the given UUID

Filesystem Type auto

13. In the *Mount Point* field, enter **/storage** and then click **OK**.



Model ST1000LX015-1U7172 (SDM1)

Size 1.0 TB (1,000,204,886,016 bytes)

Partitioning GUID Partition Table

Mount Options

User Session Defaults OFF

Mount Options ☑ Mount at system startup

□ Show in user interface

□ Require additional authorization to mount

Display Name

Icon Name

Symbolic Icon Name

defaults

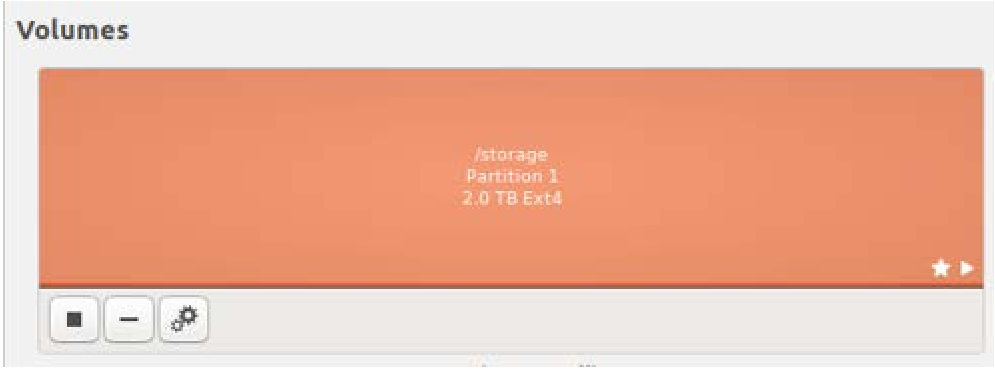
Mount Point /storage

Identify As UUID=ea03e2ac-8ba7-4551-bf46-bf6a30a5edea

Matches the device with the given UUID

Filesystem Type ext4

14. Click the **Play** button to mount the drives as the storage drive. Once pressed, the play icon will change to a square, indicating the process is running.

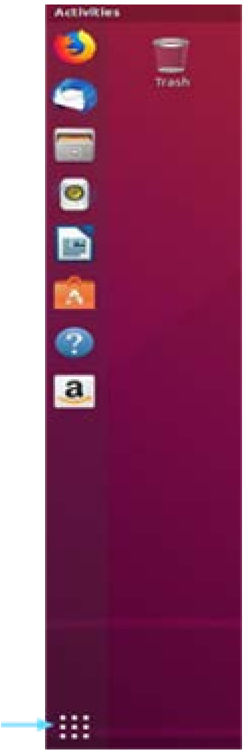


Volumes

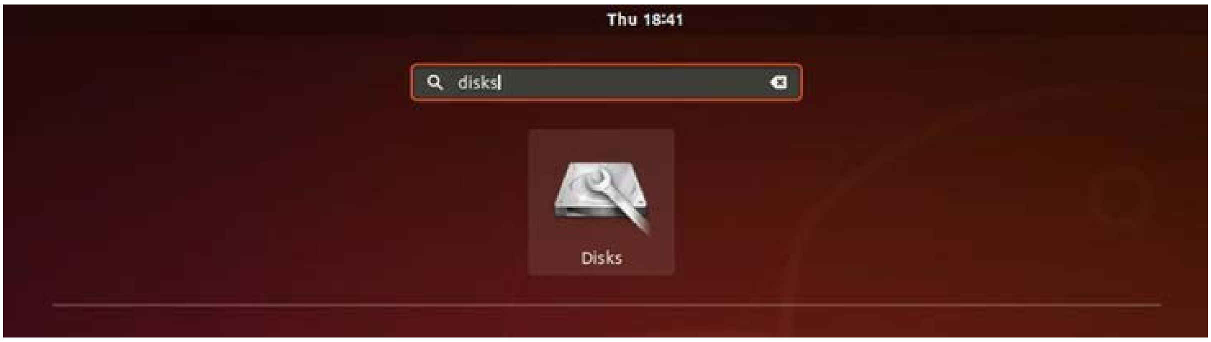
/storage
Partition 1
2.0 TB Ext4

3 Drives

1. Click the icon at the bottom of the left window.



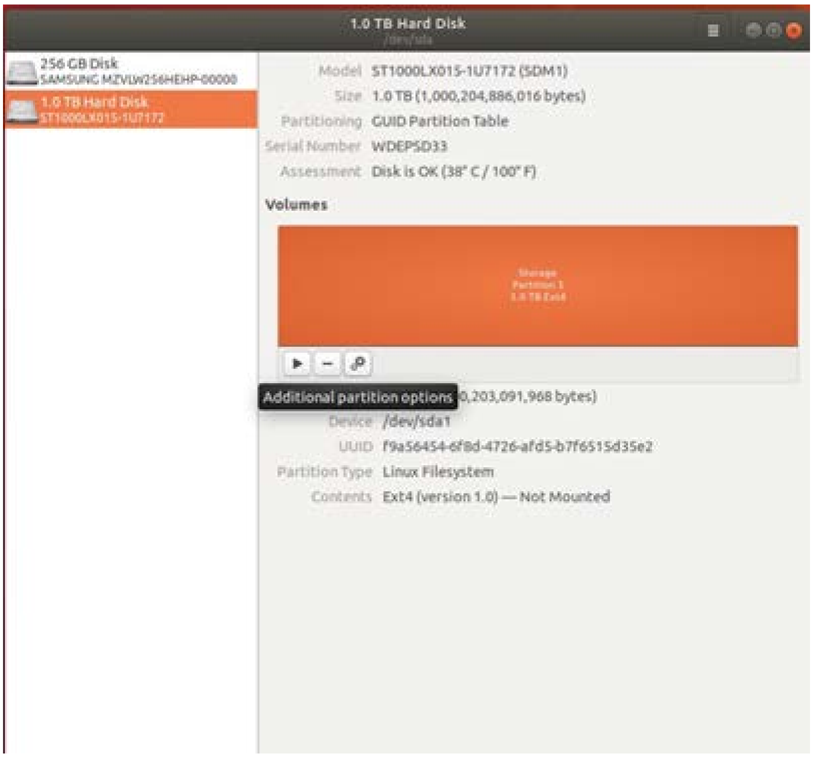
2. In the search field, type **disks** and then click the **Disks** icon that appears.



3. On the left side, you will see your three disks listed. Each disk will be responsible for each of the following partitions:
   - The OS itself
   - /Storage – mounted into the largest disk
   - /SSD – mounted into the second largest disk

/Storage Disk

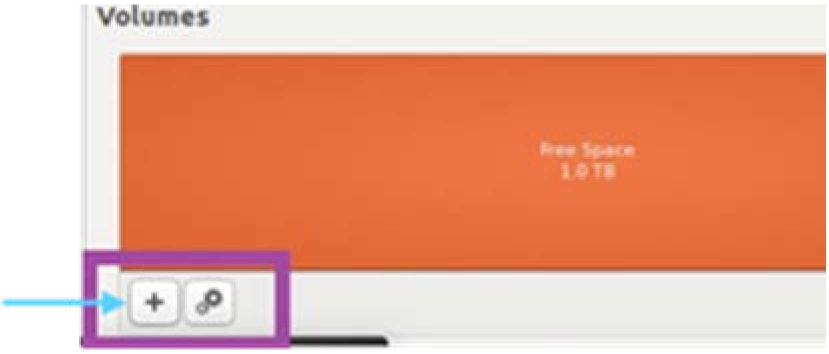
4. Select the largest disk from the left side where all your disks are listed.



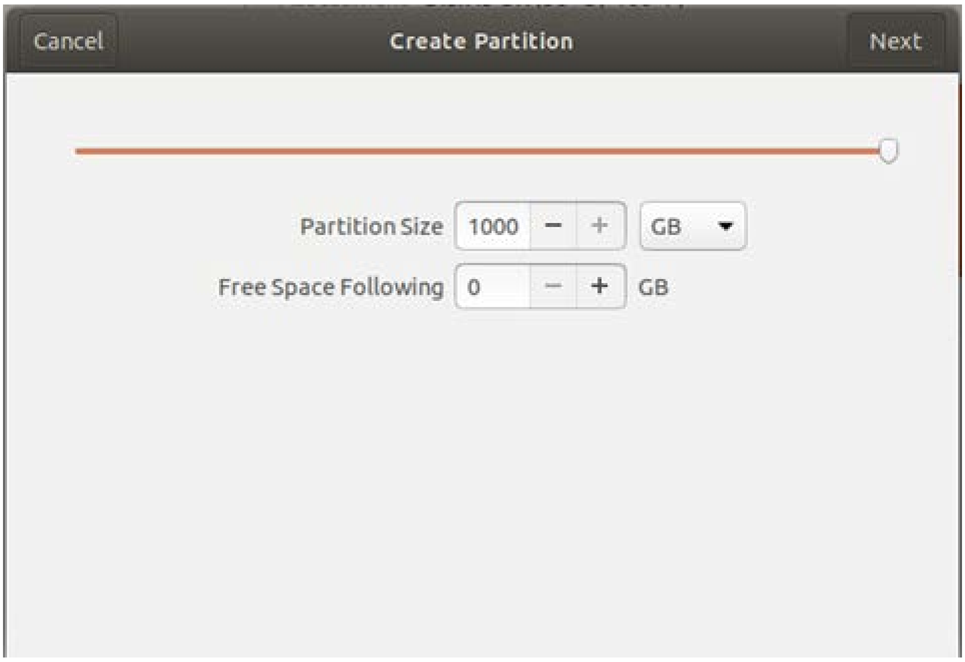
Model ST1000LX015-1U7172 (SDM1)
Size 1.0 TB (1,000,204,886,016 bytes)
Partitioning GUID Partition Table
Serial Number WDEPSD33
Assessment Disk is OK (38° C / 100° F)

0,203,091,968 bytes)
Device /dev/sda1
UUID f9a56454-6f8d-4726-afd5-b7f6515d35e2
Partition Type Linux Filesystem
Contents Ext4 (version 1.0) — Not Mounted

5. Look at the two small square buttons below the large orange square.
6. If there is a minus (-) symbol next to the plus (+) symbol, it means there is already data on the drive. In this case, click the **minus** button to delete the partition on the drive. After that, there should be only two buttons showing.
7. Click the **plus** button to open the Create Partition window.

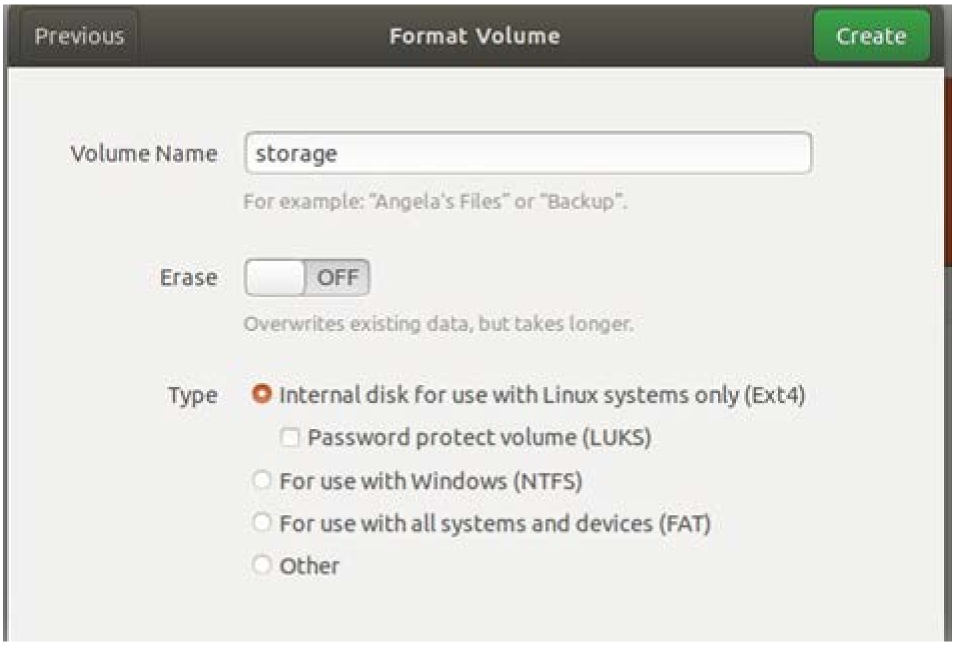


8. Make sure that the slider bar in the window is set all the way to the right and then click **Next**.



Partition Size 1000 GB
Free Space Following 0 GB

9. The Format Volume window will display. In the *Volume Name* field, enter **storage** and click the **Create** button.

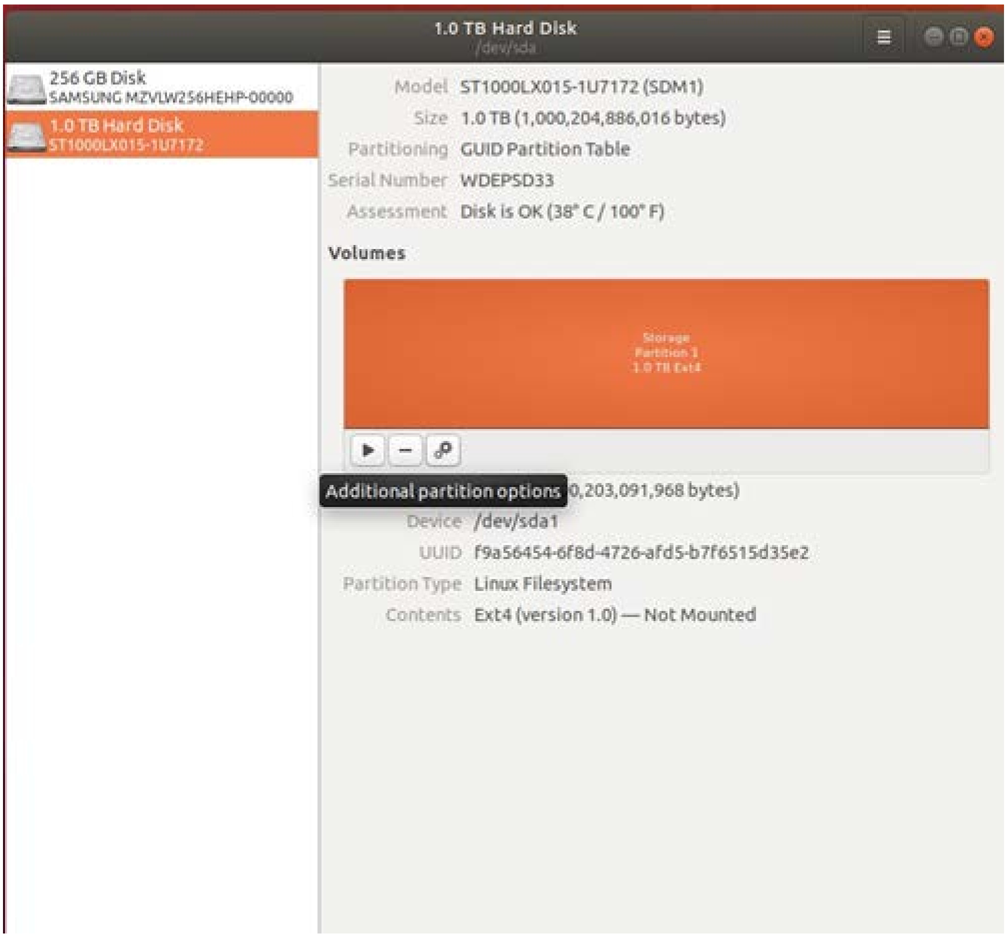


Volume Name: storage
For example: "Angela's Files" or "Backup".

Erase: OFF
Overwrites existing data, but takes longer.

Type:
● Internal disk for use with Linux systems only (Ext4)
□ Password protect volume (LUKS)
○ For use with Windows (NTFS)
○ For use with all systems and devices (FAT)
○ Other

10. Once created, you will be directed back to the main popup, as shown below.



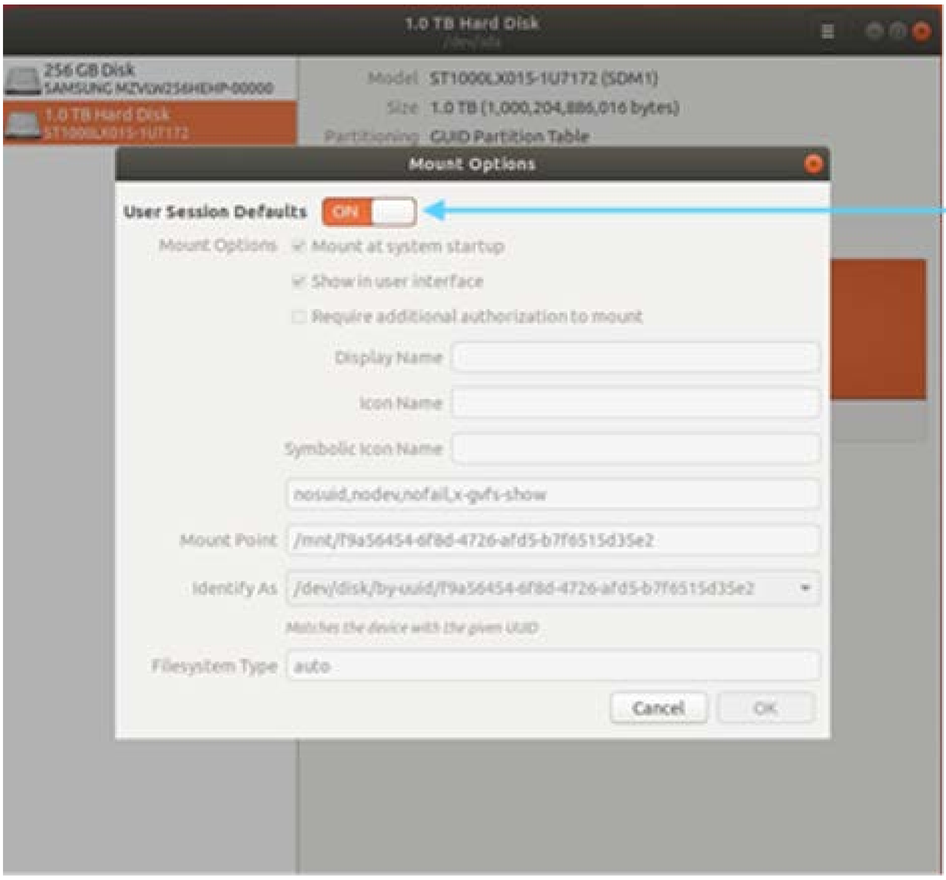
Model ST1000LX015-1U7172 (SDM1)
Size 1.0 TB (1,000,204,886,016 bytes)
Partitioning GUID Partition Table
Serial Number WDEPSD33
Assessment Disk is OK (38° C / 100° F)

0,203,091,968 bytes)
Device /dev/sda1
UUID f9a56454-6f8d-4726-afd5-b7f6515d35e2
Partition Type Linux Filesystem
Contents Ext4 (version 1.0) — Not Mounted

11. Chick the **Cogwheel** icon.

12. Select the **Edit Mount Options** from the dropdown.

13. In the *Mount Options* window, change the **User Session Defaults** setting to OFF by using the toggle.



1.0 TB Hard Disk
/dev/sda

256 GB Disk
SAMSUNG MZVLW256HEHP-00000

1.0 TB Hard Disk
ST1000LX015-1U7172

Model ST1000LX015-1U7172 (SDM1)
Size 1.0 TB (1,000,204,886,016 bytes)
Partitioning GUID Partition Table

Mount Options

User Session Defaults ON

Mount Options ☑ Mount at system startup
☑ Show in user interface
☐ Require additional authorization to mount

Display Name

Icon Name

Symbolic Icon Name

nosuid,nodev,nofail,x-gvfs-show

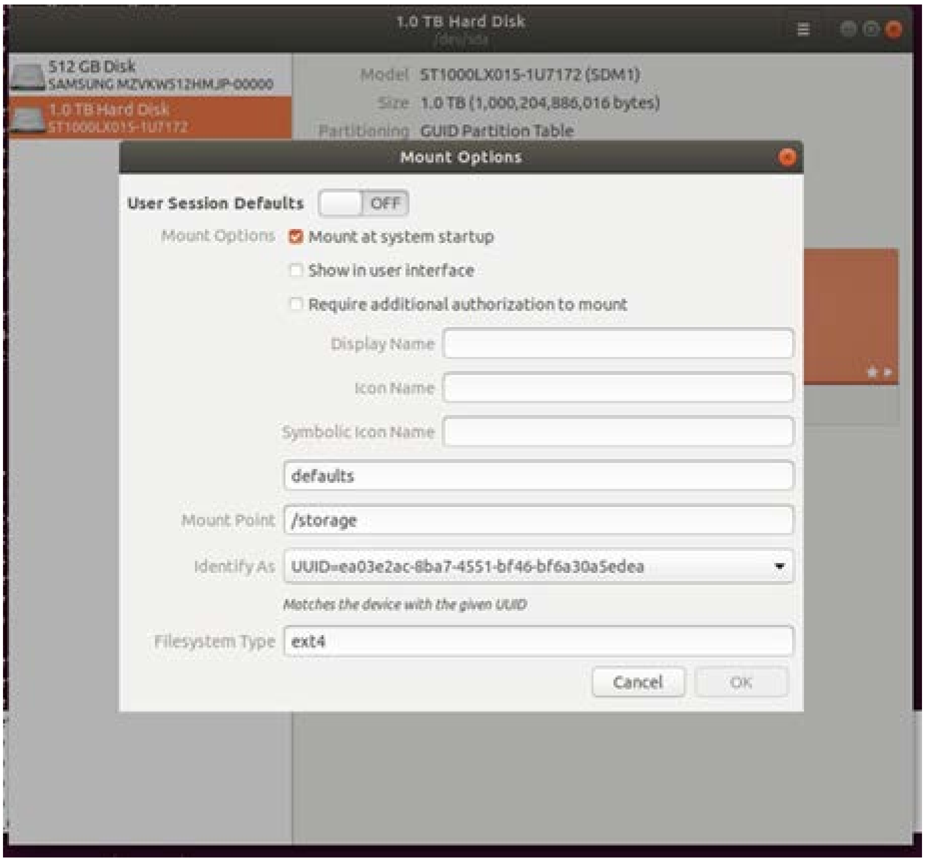
Mount Point /mnt/f9a56454-6f8d-4726-afd5-b7f6515d35e2

Identify As /dev/disk/by-uuid/f9a56454-6f8d-4726-afd5-b7f6515d35e2

Matches the device with the given UUID

Filesystem Type auto

14. In the *Mount Point* field, enter **/storage** and then click **OK**.



1.0 TB Hard Disk
/dev/sda

512 GB Disk
SAMSUNG MZVKW512HMJP-00000

1.0 TB Hard Disk
ST1000LX015-1U7172

Model ST1000LX015-1U7172 (SDM1)
Size 1.0 TB (1,000,204,886,016 bytes)
Partitioning GUID Partition Table

Mount Options

User Session Defaults OFF

Mount Options ☑ Mount at system startup
☐ Show in user interface
☐ Require additional authorization to mount

Display Name

Icon Name

Symbolic Icon Name

defaults

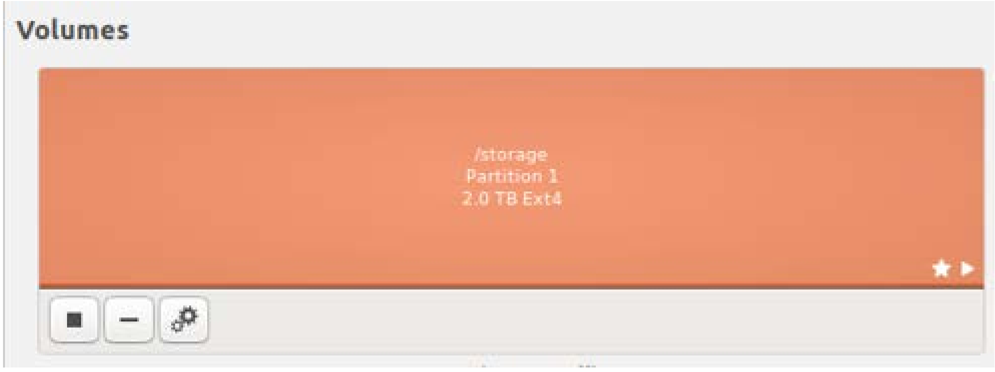
Mount Point /storage

Identify As UUID=ea03e2ac-8ba7-4551-bf46-bf6a30a5edea

Matches the device with the given UUID

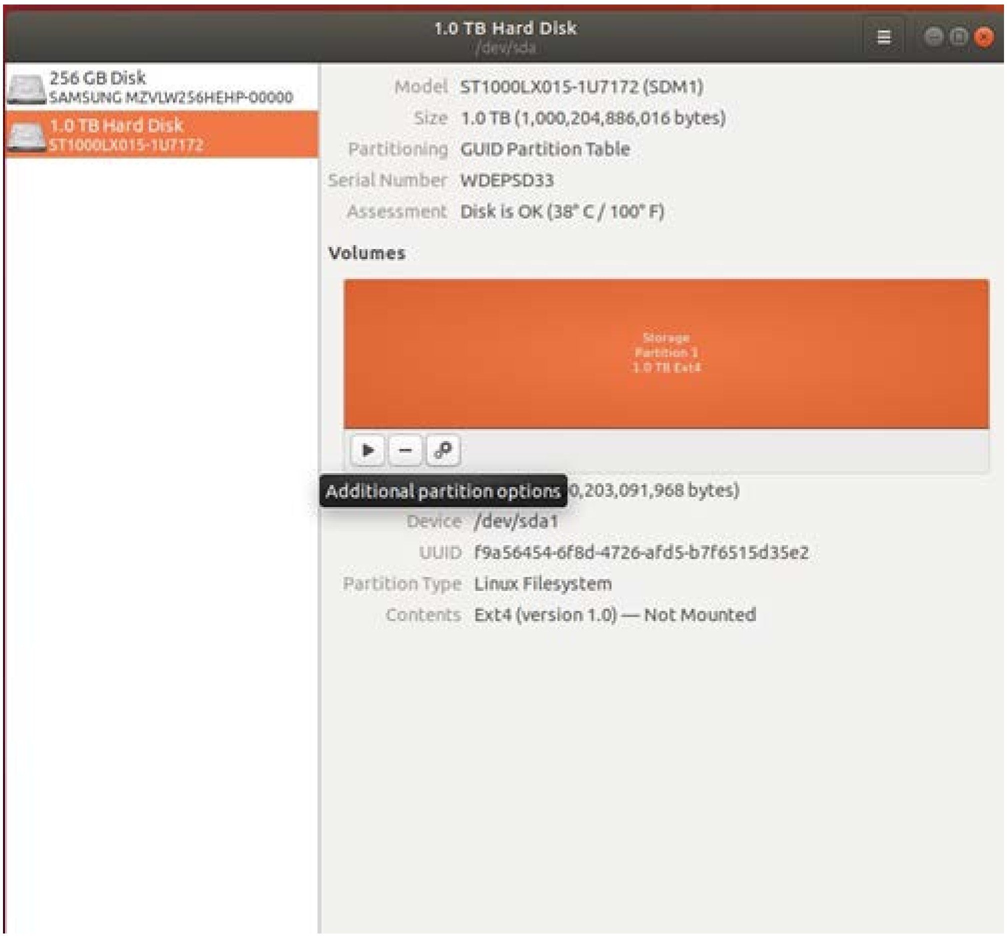
Filesystem Type ext4

15. Click the **Play** button to mount the drives as the storage drive. Once pressed, the play icon will change to a square, indicating the process is running.



/SSD Disk

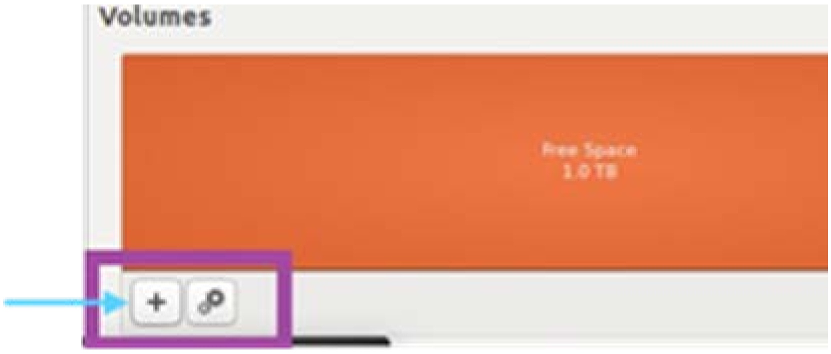
16. Select the largest disk from the left side where all your disks are listed.



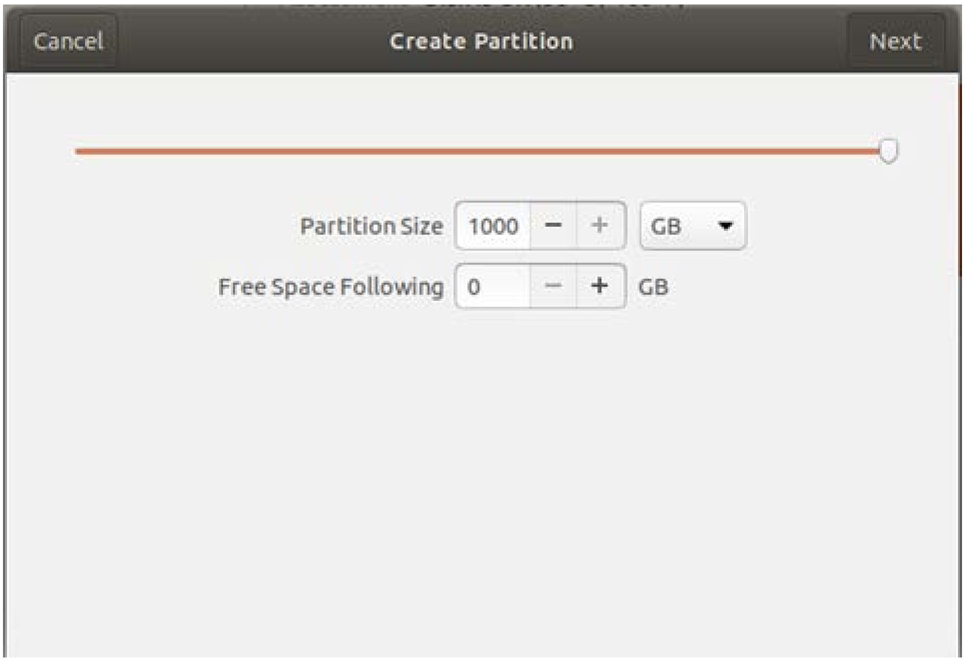
Model ST1000LX015-1U7172 (SDM1)
Size 1.0 TB (1,000,204,886,016 bytes)
Partitioning GUID Partition Table
Serial Number WDEPSD33
Assessment Disk is OK (38° C / 100° F)

0,203,091,968 bytes)
Device /dev/sda1
UUID f9a56454-6f8d-4726-afd5-b7f6515d35e2
Partition Type Linux Filesystem
Contents Ext4 (version 1.0) — Not Mounted

17. Look at the two small square buttons below the large orange square.
18. If there is a minus (-) symbol next to the plus (+) symbol, it means there is already data on the drive. In this case, click the **minus** button to delete the partition on the drive. After that, there should be only two buttons showing.
19. Click the **plus** button to open the Create Partition window.



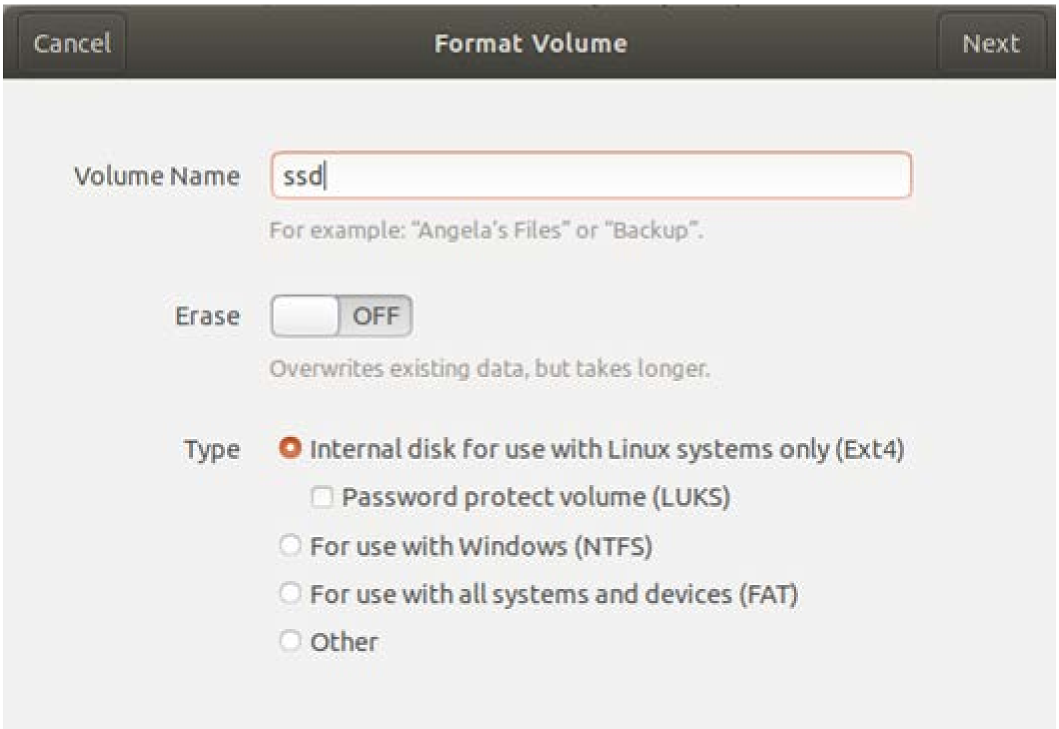
20. Make sure that the slider bar in the window is set to the right and then click **Next**.



Partition Size 1000 GB

Free Space Following 0 GB

21. The *Format Volume* window will display. In the *Volume Name* field, enter **ssd** and click the **Create** button.



Volume Name ssd

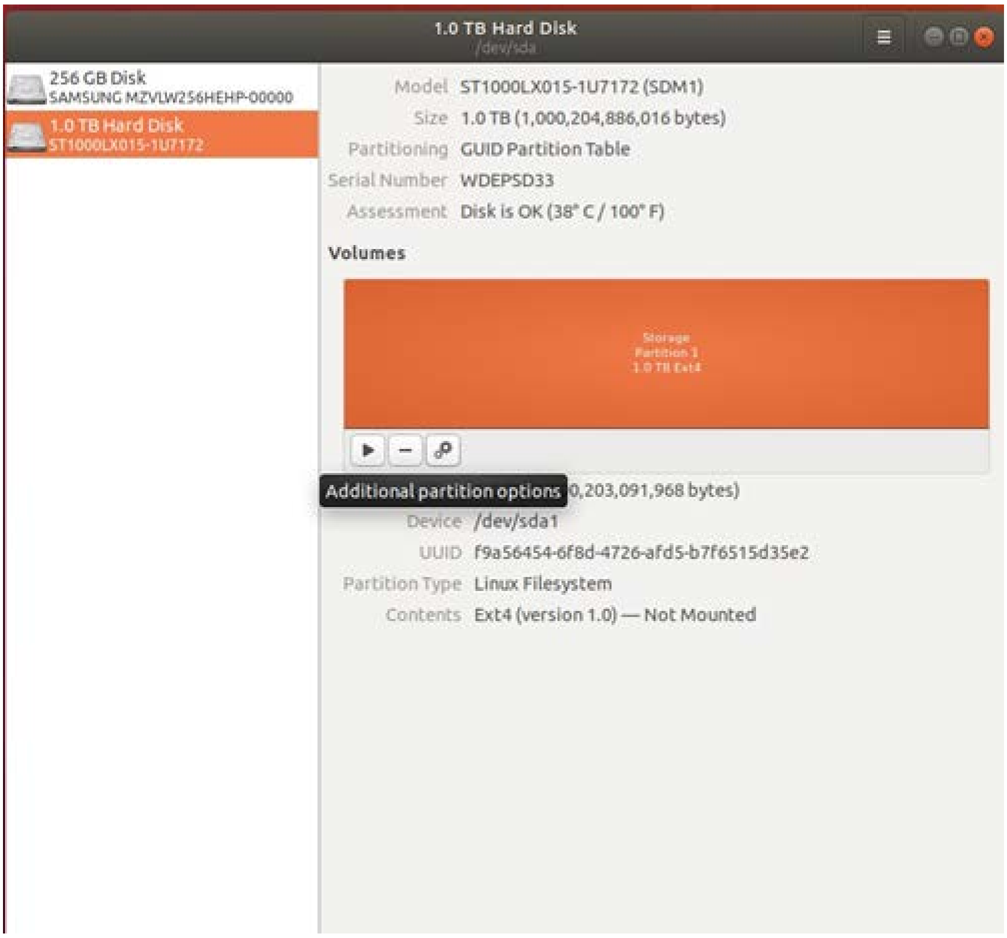
For example: "Angela's Files" or "Backup".

Erase OFF

Overwrites existing data, but takes longer.

Type
- ● Internal disk for use with Linux systems only (Ext4)
  - □ Password protect volume (LUKS)
- ○ For use with Windows (NTFS)
- ○ For use with all systems and devices (FAT)
- ○ Other

22. Once created, you will be directed back to the main popup, as shown below.



1.0 TB Hard Disk
/dev/sda

256 GB Disk
SAMSUNG MZVLW256HEHP-00000

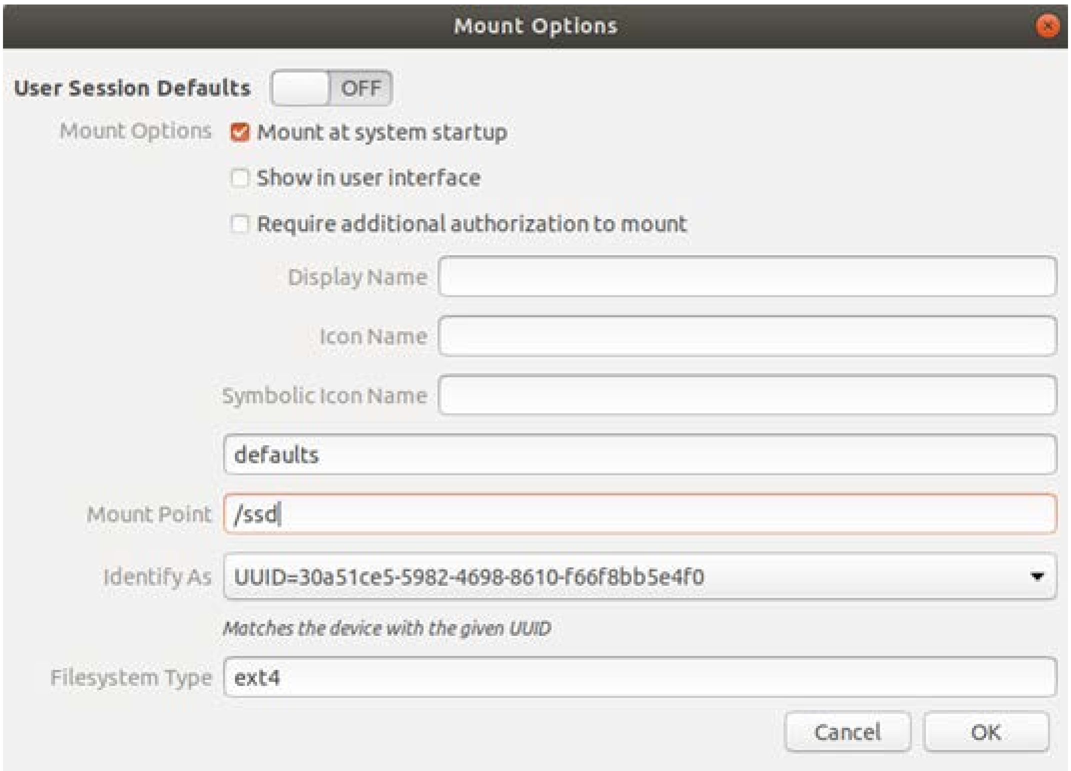
1.0 TB Hard Disk
ST1000LX015-1U7172

Model ST1000LX015-1U7172 (SDM1)
Size 1.0 TB (1,000,204,886,016 bytes)
Partitioning GUID Partition Table
Serial Number WDEPSD33
Assessment Disk is OK (38° C / 100° F)

Volumes

0,203,091,968 bytes)
Device /dev/sda1
UUID f9a56454-6f8d-4726-afd5-b7f6515d35e2
Partition Type Linux Filesystem
Contents Ext4 (version 1.0) — Not Mounted

23. Chick the **Cogwheel** icon.
24. Select the **Edit Mount Options** from the dropdown.
25. In the *Mount Options* window, change the **User Session Defaults** setting to OFF by using the toggle.



Mount Options

User Session Defaults OFF
Mount Options ☑ Mount at system startup
□ Show in user interface
□ Require additional authorization to mount
Display Name
Icon Name
Symbolic Icon Name
defaults
Mount Point /ssd
Identify As UUID=30a51ce5-5982-4698-8610-f66f8bb5e4f0
Matches the device with the given UUID
Filesystem Type ext4

26. In the *Mount Point* field, enter **/ssd** and then click **OK**.
27. Click the **Play** button to mount the drives as the /ssd drive. Once pressed, the play icon will change to a square, indicating the process is running.

Step 7: Kernel Hold Commands

1. Open Terminal.
2. Type `sudo -i` to switch to superuser then press **Enter**.
3. Type the following commands: (copy and paste the whole code block.)

Hold commands - copy and paste the whole code block

```
apt-mark hold $(uname -r);
apt remove unattended-upgrades -y;

sudo cat > /etc/apt/preferences <<EOF
Package: linux-image-*
Pin: release *
Pin-Priority: -1

Package: linux-headers-*
Pin: release *
Pin-Priority: -1
EOF
```

4. You can now connect the server to the Network.
   Your server is now ready to install an Oosto Product

5. pre-requisite - Openssh installation:

Online OS instalation | Offilne OS installation

```
apt update
apt install openssh-server -y
```

Ubuntu Server Installation

Before installing Ubuntu on your server, make sure:

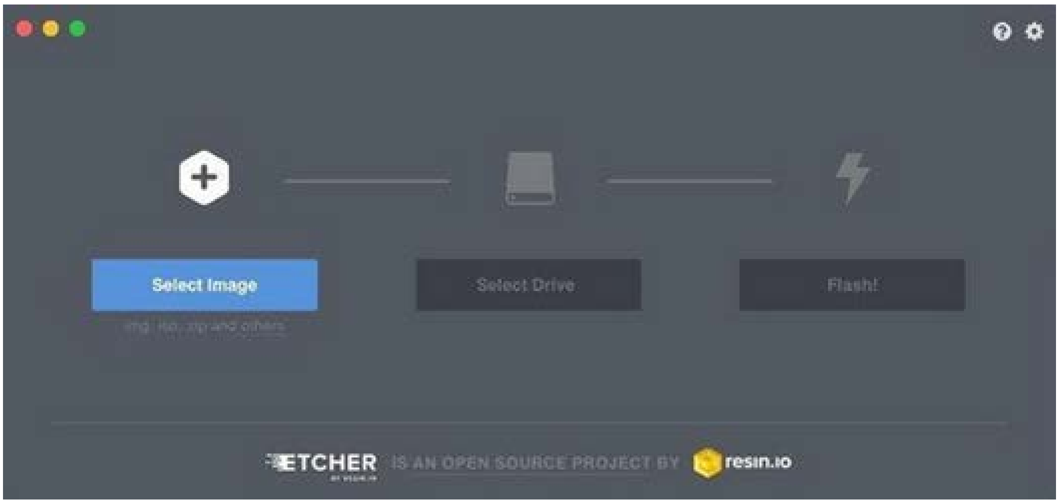
- No Operating System already installed on your machine
- No important data is saved, as it will be deleted
- You have Etcher software (to create a bootable USB Drive)
- The server is not connected to the internet

Step 1: Download the Ubuntu Image File

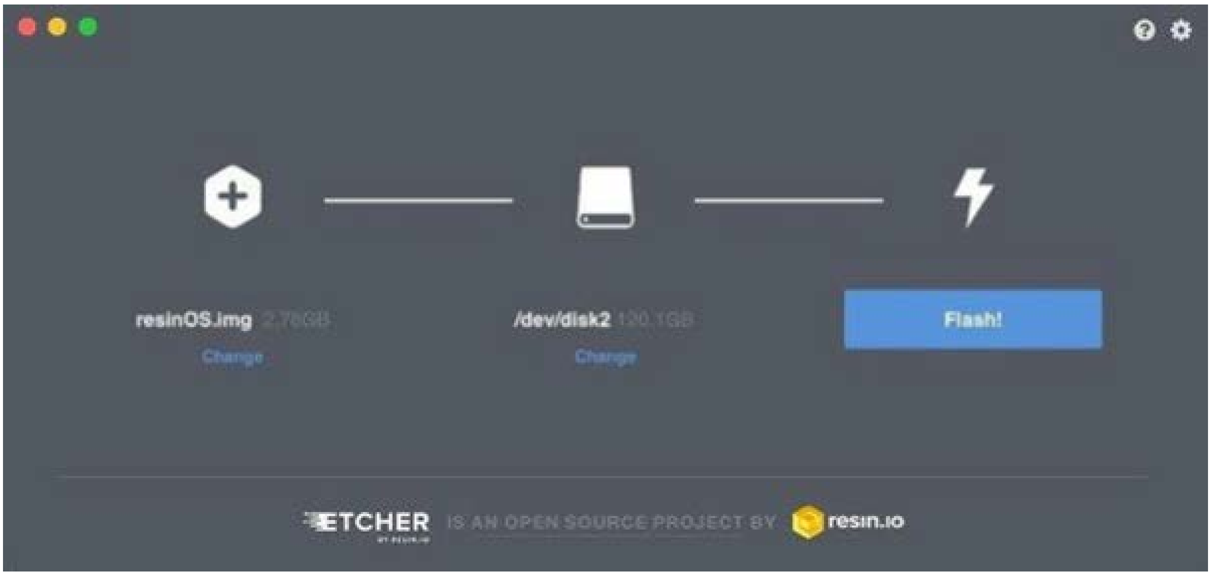
- Download the Ubuntu Server 20.04.3 Operating System from this link. https://old-releases.ubuntu.com/releases/20.04.3/ubuntu-20.04.3-live-server-amd64.iso
- After the installation is complete, you will have the LiveCD image file available on your machine and can continue to create a bootable USB drive.

Step 2: Flash a Bootable USB device

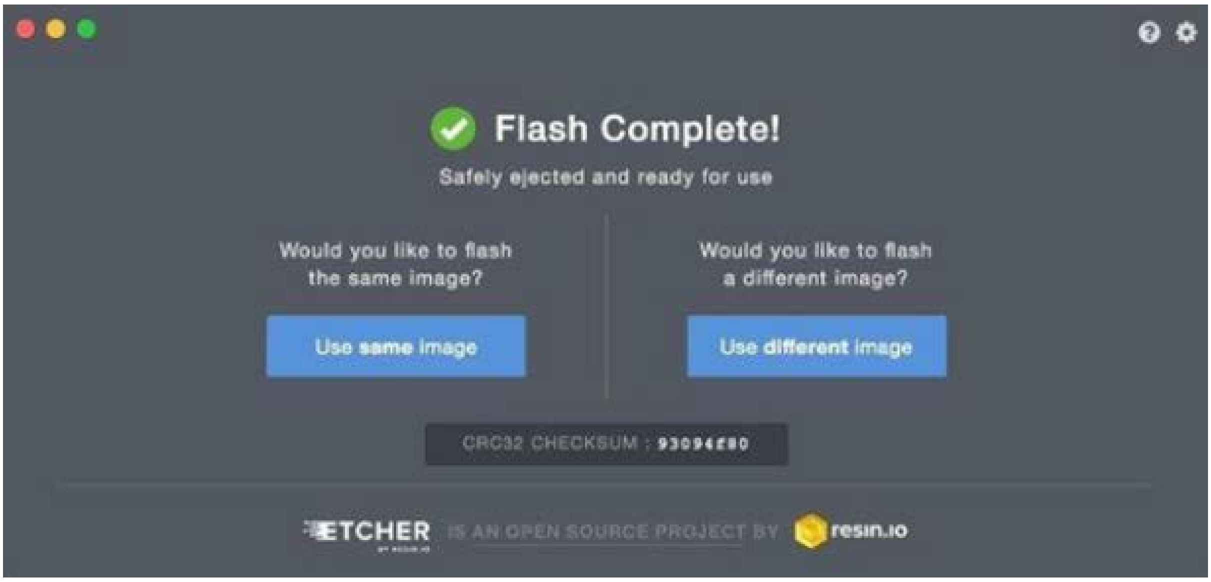
- Open the Etcher application.
- Select a source image by dragging and dropping one from your desktop directly to the Etcher app or by using the file selector.



- Select the target drive. You may differentiate your USBs and SD cards from your hard disks so that they are not inadvertently erased.
- Complete the process by clicking the Flash button.



- After a few minutes, the USB drive will be ready for use.



Flash Complete!

Safely ejected and ready for use

Would you like to flash the same image?

Would you like to flash a different image?

CRC32 CHECKSUM : 93094E80

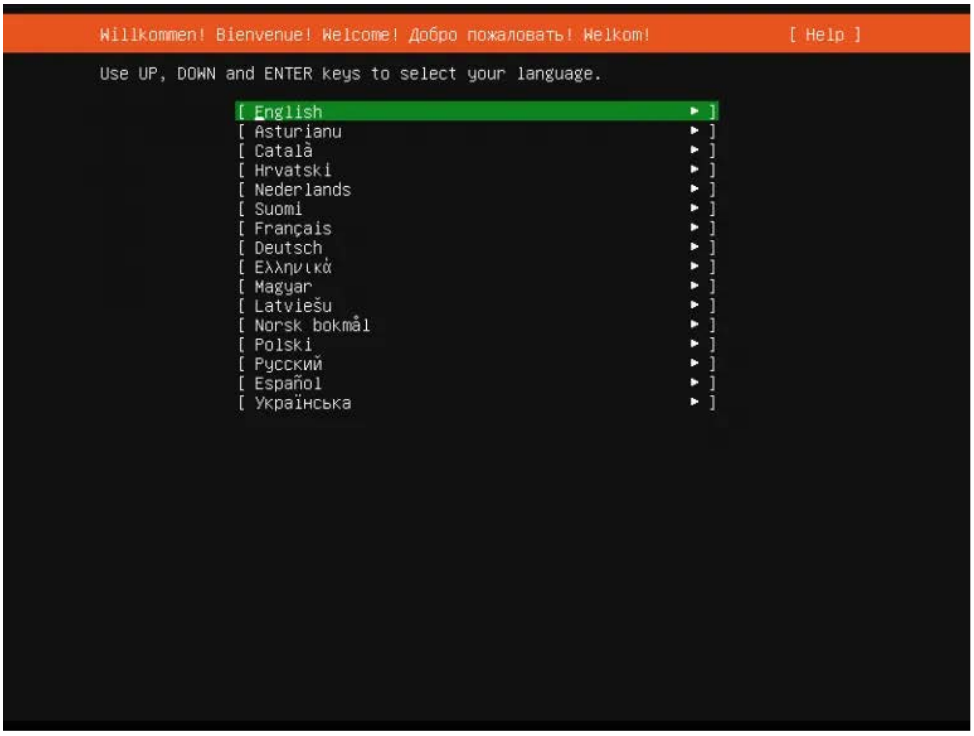
Step 3: Configure the BIOS

- Plug in the USB drive that contains the Ubuntu image and boot it by pressing either the DEL/ESC +F1/F2 keys on your keyboard.
- In the BIOS menu, navigate to the Secure Boot menu using the arrow keys.
- Check that the Secure Boot option is disabled by selecting the Security tab > Secure Boot menu.
- Disable the Secure Boot Control.
- Select Save & Exit to save your changes.
- Select the Boot tab from the top menu bar.
- Select Boot Option#1 (BootDrive Name) to override the current settings and press Enter.

Step 4: Configure the Ubuntu Settings

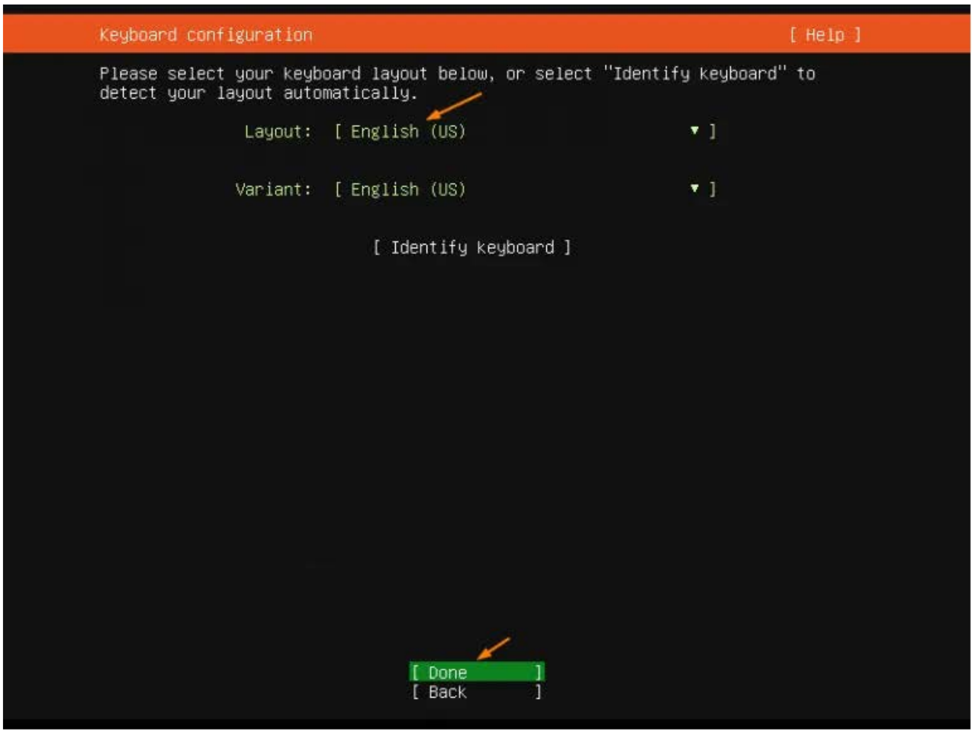
- Once you have booted from the boot drive select English as the default language and press Enter.

> **! Disable Network Connectivity**
>
> Disable ANY Network connectivity before proceeding to the next steps
> by disconnecting ethernet cable



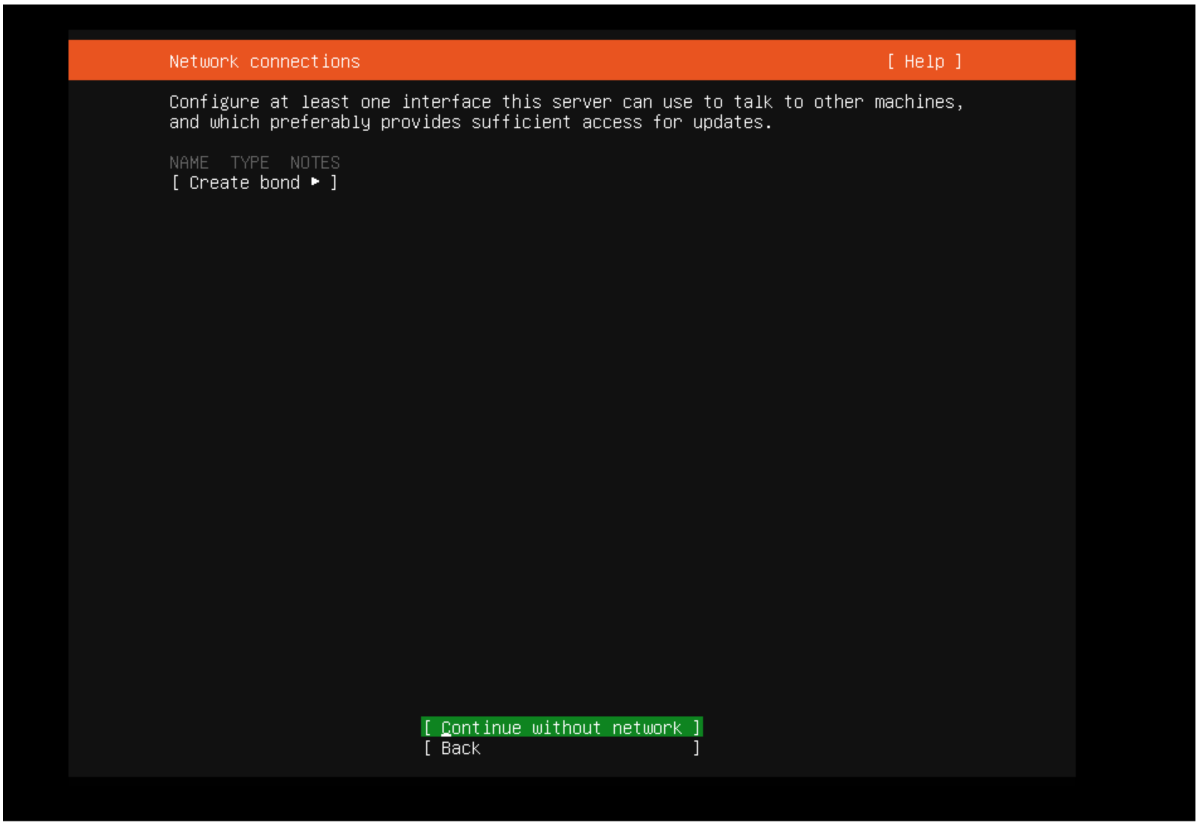
```
Willkommen! Bienvenue! Welcome! Добро пожаловать! Welkom!        [ Help ]

Use UP, DOWN and ENTER keys to select your language.

             [ English                                  ▸ ]
             [ Asturianu                                ▸ ]
             [ Català                                   ▸ ]
             [ Hrvatski                                 ▸ ]
             [ Nederlands                               ▸ ]
             [ Suomi                                    ▸ ]
             [ Français                                 ▸ ]
             [ Deutsch                                  ▸ ]
             [ Ελληνικά                                 ▸ ]
             [ Magyar                                   ▸ ]
             [ Latviešu                                 ▸ ]
             [ Norsk bokmål                             ▸ ]
             [ Polski                                   ▸ ]
             [ Русский                                  ▸ ]
             [ Español                                  ▸ ]
             [ Українська                               ▸ ]
```

*Choose your preferred keyboard layout for your Ubuntu 20.04 server and then choose the “Done” option and hit enter.



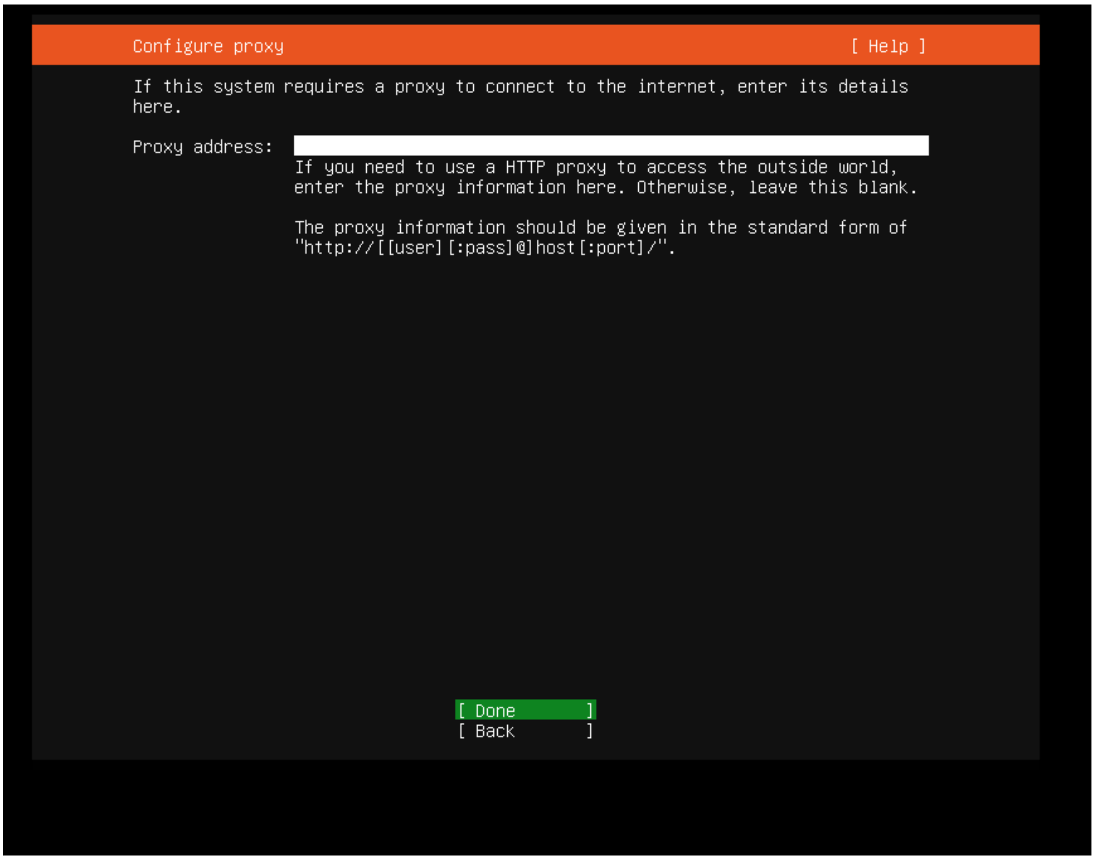
```
Keyboard configuration                                           [ Help ]

Please select your keyboard layout below, or select "Identify keyboard" to
detect your layout automatically.

              Layout:  [ English (US)                      ▾ ]

             Variant:  [ English (US)                      ▾ ]

                         [ Identify keyboard ]




                                [ Done      ]
                                [ Back      ]
```

If your system is connected to the network make sure to disable it and unplug the network cable, make sure you select "Continue Without network" afterward



```
Network connections                                             [ Help ]

Configure at least one interface this server can use to talk to other machines,
and which preferably provides sufficient access for updates.

NAME  TYPE  NOTES
[ Create bond ▸ ]
```

On the "Configure proxy" menu, select "Done".



```
Configure proxy                                                 [ Help ]

If this system requires a proxy to connect to the internet, enter its details
here.

Proxy address:
               If you need to use a HTTP proxy to access the outside world,
               enter the proxy information here. Otherwise, leave this blank.

               The proxy information should be given in the standard form of
               "http://[[user][:pass]@]host[:port]/".
```

On the "Configure Ubuntu archive mirror" menu, also select "Done"

Disks configuration:

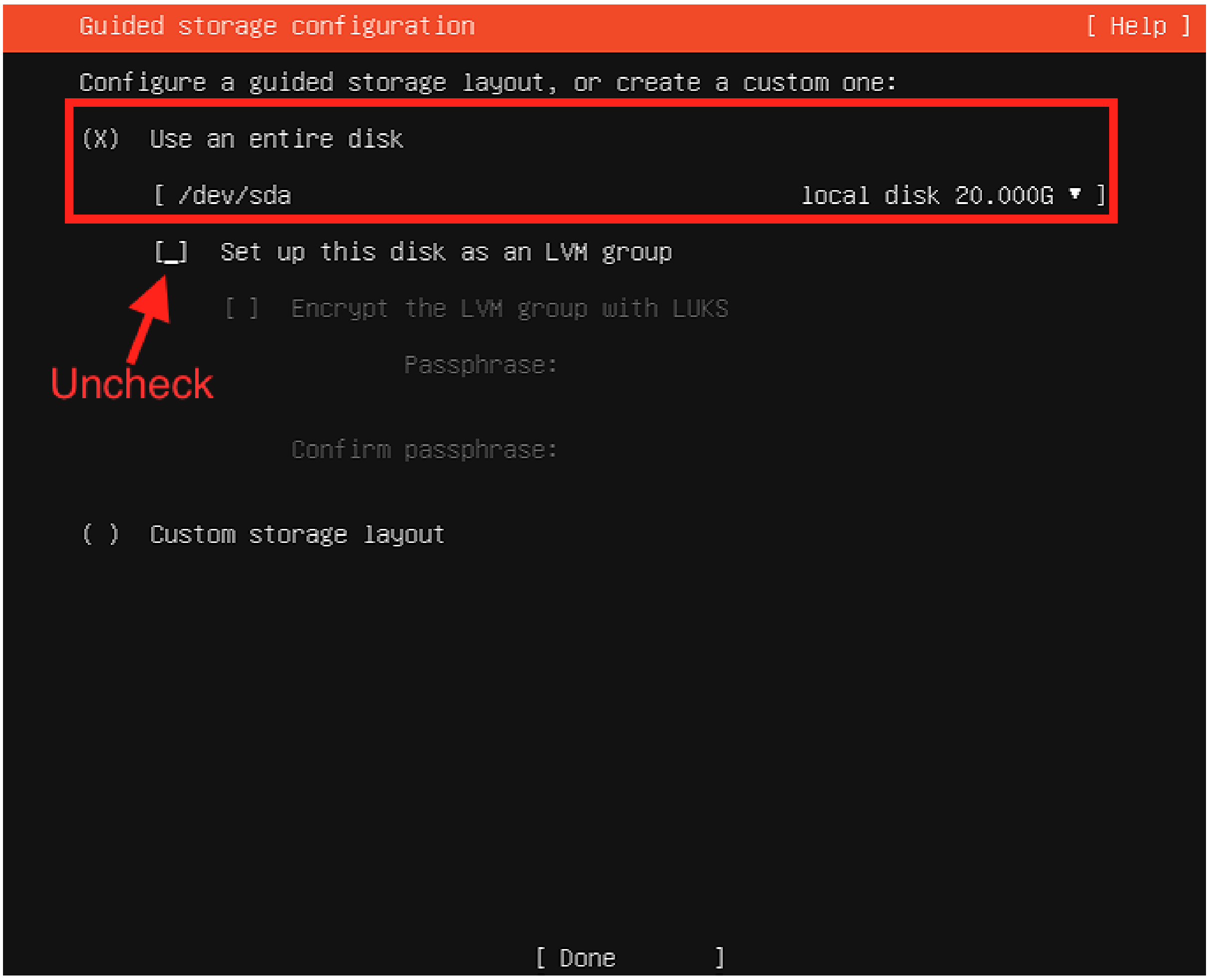
Please make sure that the proper storage devices (type & size) are attached,

Contact your Account manager if you have any questions regarding Disks configuration setup

Oosto products allocate three partitions for data, minimum 3 disks:

- "The OS itself and /": minimum size 500GB SSD/NVME
- "/SSD": minimum size - 500GB SSD (SSD -)
- "/Storage": minimum 1000GB HDD(depending on retentions)

OS Disk:
1.Disable the "Set up this disk as an LVM group" Box,
2.Check "Use an entire disk" while choosing the matching Disk

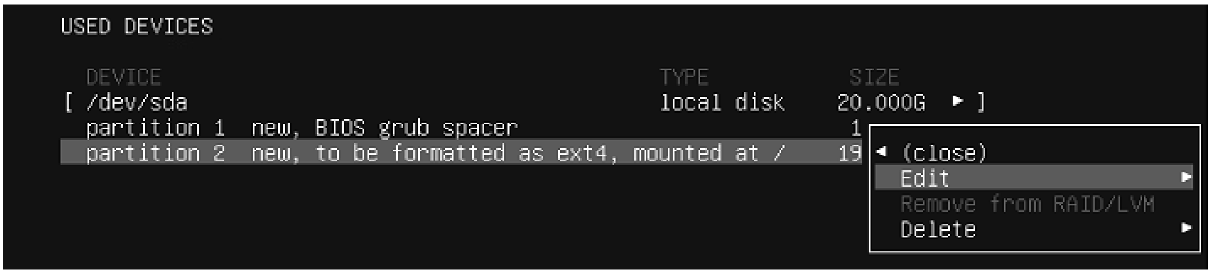


```
  Guided storage configuration                                      [ Help ]
  Configure a guided storage layout, or create a custom one:
  (X)  Use an entire disk

       [ /dev/sda                                    local disk 20.000G ▾ ]

       [ ]  Set up this disk as an LVM group

            [ ]  Encrypt the LVM group with LUKS

                           Passphrase:

                   Confirm passphrase:

  ( )  Custom storage layout

                              [ Done       ]
```

3. Press Done.

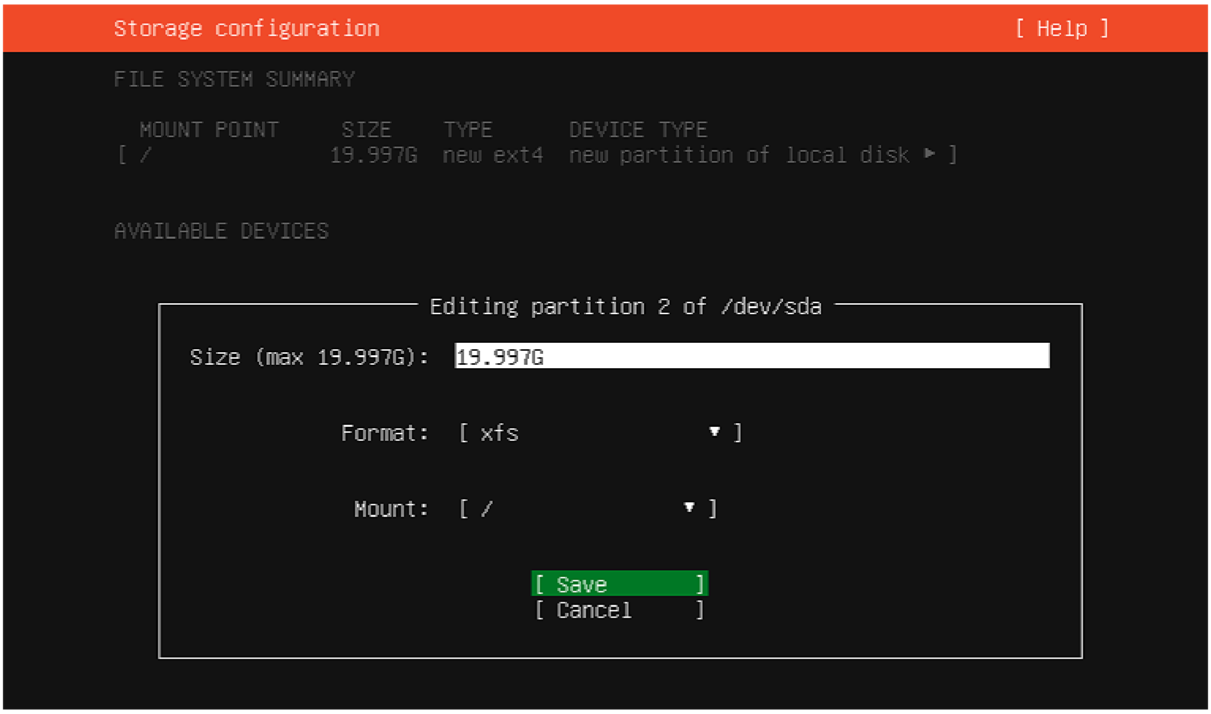
4. Change the Filesystem type of the / partition from ext4 to xfs

Choose the / partition only (at the bottom part of the screen), press enter then choose Edit.



```
 USED DEVICES

   DEVICE                                          TYPE           SIZE
 [ /dev/sda                                        local disk   20.000G  ▸ ]
   partition 1  new, BIOS grub spacer                                1
   partition 2  new, to be formatted as ext4, mounted at /          19  ◂ (close)
                                                                       Edit              ▸
                                                                       Remove from RAID/LVM
                                                                       Delete            ▸
```

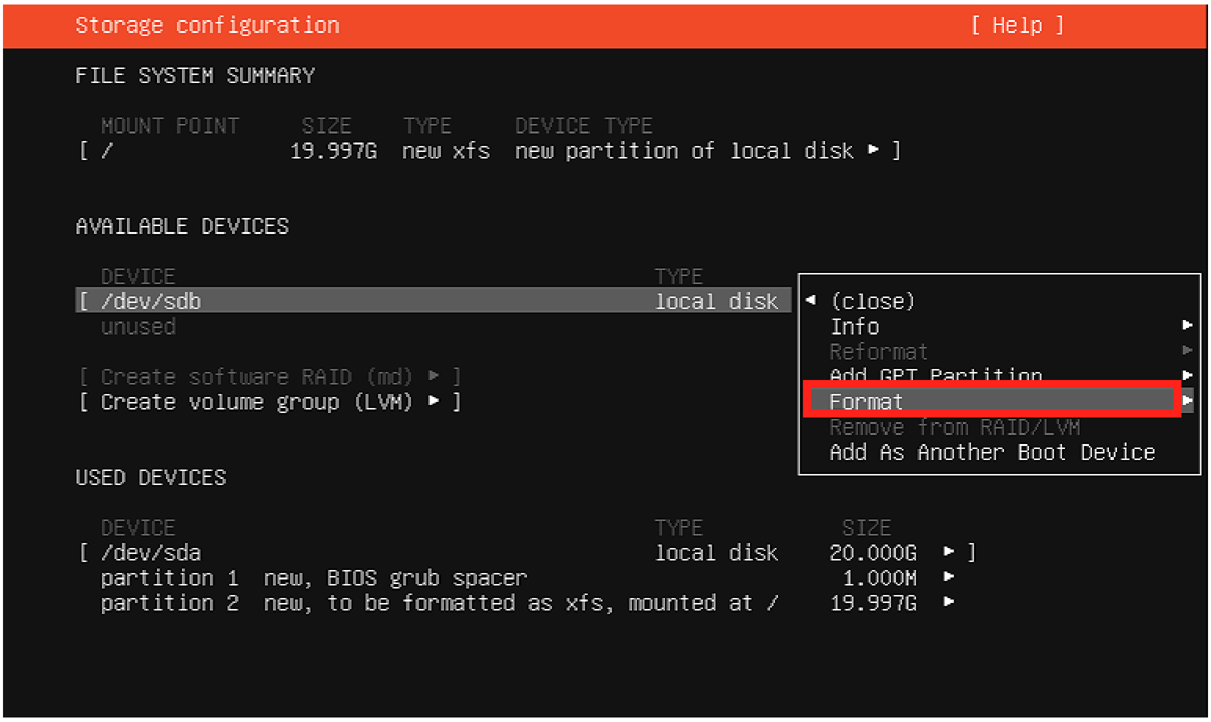
Change the format to XFS, then save.



```
    Storage configuration                                        [ Help ]
    FILE SYSTEM SUMMARY

      MOUNT POINT      SIZE    TYPE      DEVICE TYPE
    [ /               19.997G  new ext4  new partition of local disk ► ]

    AVAILABLE DEVICES

          Editing partition 2 of /dev/sda

      Size (max 19.997G):  19.997G

                  Format:  [ xfs              ▾ ]

                   Mount:  [ /              ▾ ]

                              [ Save      ]
                              [ Cancel    ]
```

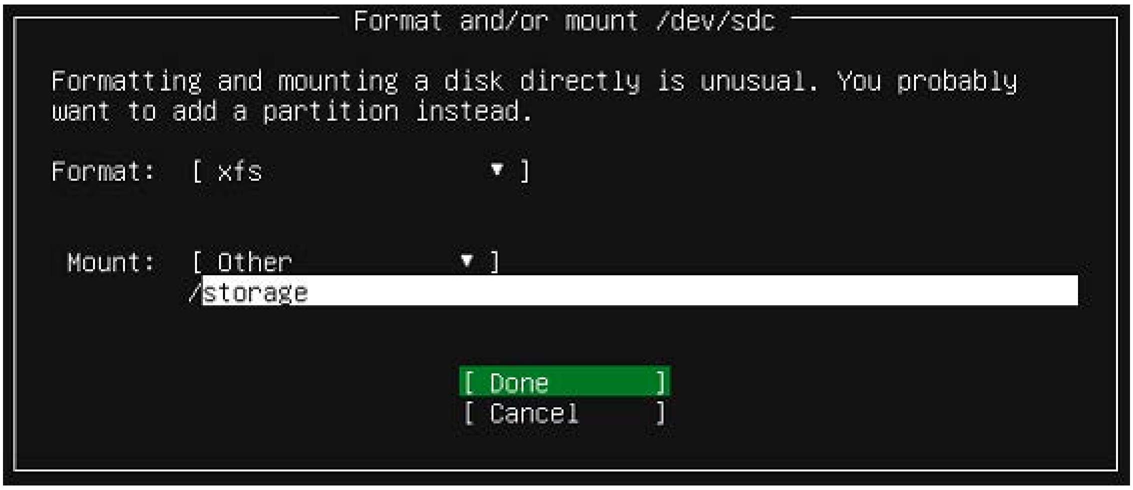
SSD/Storage Disks:

First, Format the matching storage device:
if there is an reformat option, procced with reformat and then format again with the FS type



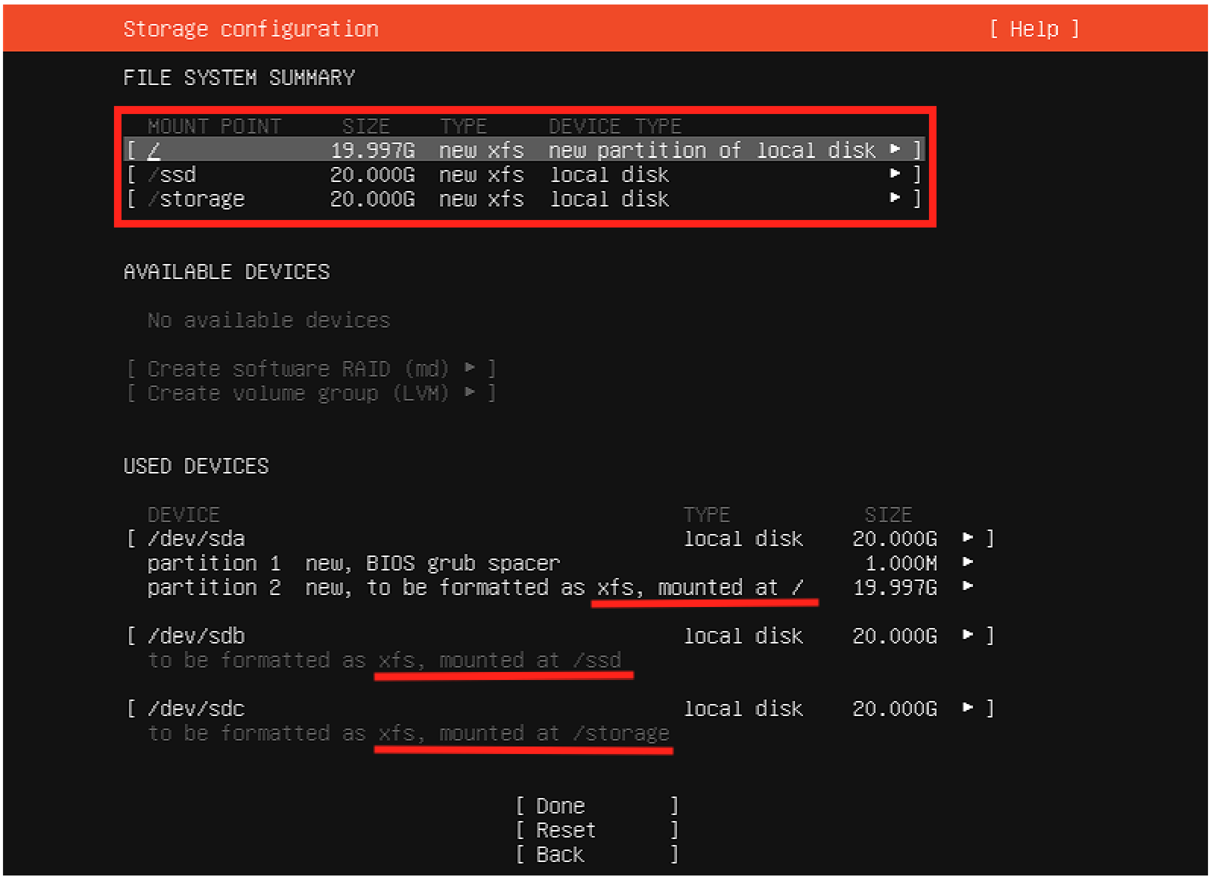
```
    Storage configuration                                        [ Help ]
    FILE SYSTEM SUMMARY

      MOUNT POINT      SIZE    TYPE      DEVICE TYPE
    [ /               19.997G  new xfs   new partition of local disk ► ]

    AVAILABLE DEVICES

      DEVICE                                   TYPE
    [ /dev/sdb                                 local disk   ◂ (close)
      unused                                                  Info                    ►
                                                              Reformat                ►
    [ Create software RAID (md) ► ]                           Add GPT Partition       ►
    [ Create volume group (LVM) ► ]                           Format                  ►
                                                              Remove from RAID/LVM
                                                              Add As Another Boot Device
    USED DEVICES

      DEVICE                                   TYPE          SIZE
    [ /dev/sda                                 local disk    20.000G  ► ]
      partition 1  new, BIOS grub spacer                      1.000M  ►
      partition 2  new, to be formatted as xfs, mounted at /  19.997G  ►
```

Change the format to XFS, Then change the mount to "Other", write /ssd or /storage



```
Format and/or mount /dev/sdc

Formatting and mounting a disk directly is unusual. You probably
want to add a partition instead.

Format:  [ xfs                ▼ ]

 Mount:  [ Other            ▼ ]
         /storage

                    [ Done      ]
                    [ Cancel    ]
```

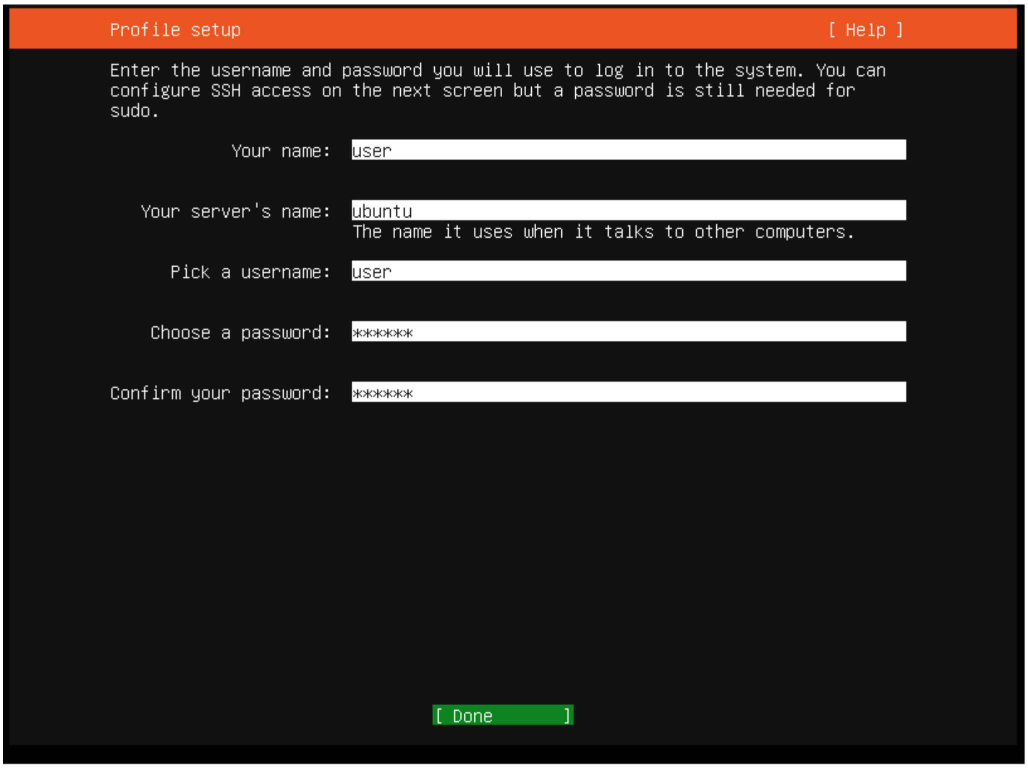
OS Disk Filesystem type change & final validation, the Expected result should look like this:



```
Storage configuration                                              [ Help ]
FILE SYSTEM SUMMARY

  MOUNT POINT     SIZE    TYPE     DEVICE TYPE
[ /             19.997G  new xfs  new partition of local disk ► ]
[ /ssd          20.000G  new xfs  local disk                  ► ]
[ /storage      20.000G  new xfs  local disk                  ► ]

AVAILABLE DEVICES

  No available devices

[ Create software RAID (md) ► ]
[ Create volume group (LVM) ► ]

USED DEVICES

  DEVICE                                      TYPE        SIZE
[ /dev/sda                                    local disk  20.000G  ► ]
  partition 1  new, BIOS grub spacer                       1.000M  ►
  partition 2  new, to be formatted as xfs, mounted at /  19.997G  ►

[ /dev/sdb                                    local disk  20.000G  ► ]
  to be formatted as xfs, mounted at /ssd

[ /dev/sdc                                    local disk  20.000G  ► ]
  to be formatted as xfs, mounted at /storage

                         [ Done      ]
                         [ Reset     ]
                         [ Back      ]
```

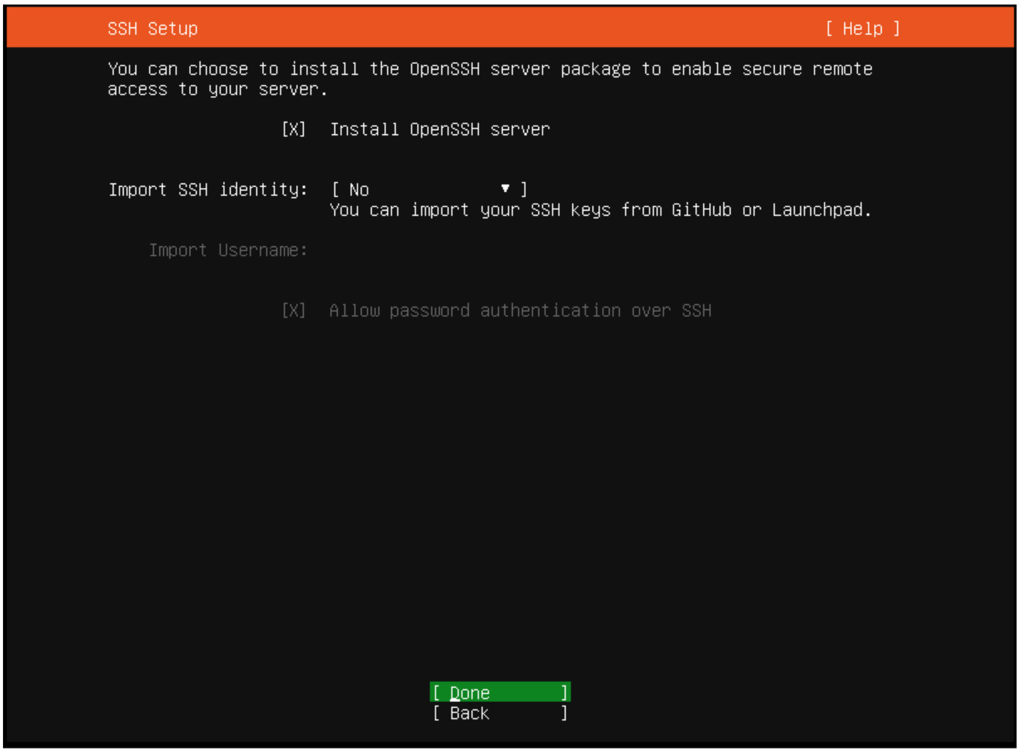
On This step:

- Choose your name (user)
- Choose Your server's name (default is "ubuntu")
- Choose your Username (user)
- Choose and verify your Password (user1!)
  Choose "Done", when done.



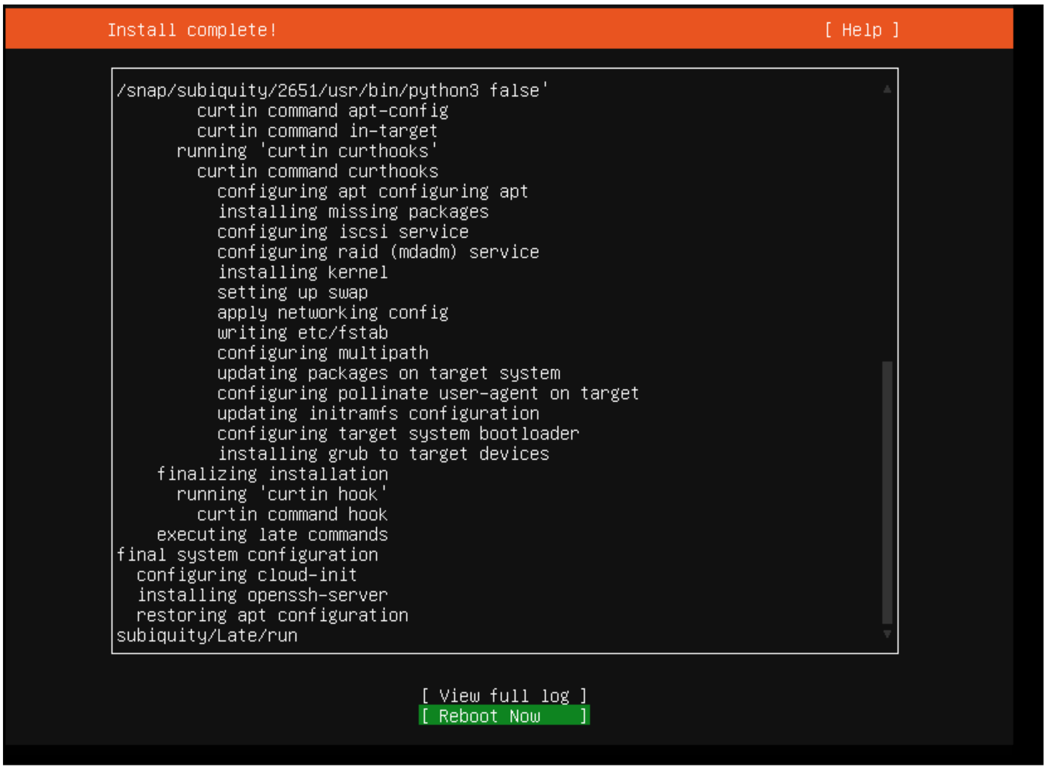
```
Profile setup                                                      [ Help ]

Enter the username and password you will use to log in to the system. You can
configure SSH access on the next screen but a password is still needed for
sudo.

            Your name:  user

     Your server's name:  ubuntu
                          The name it uses when it talks to other computers.

      Pick a username:  user

     Choose a password:  ******

   Confirm your password:  ******

                                 [ Done       ]
```

On this "SSH Setup" step, choose the box to "Install OpenSSH server" , and Choose "Done"

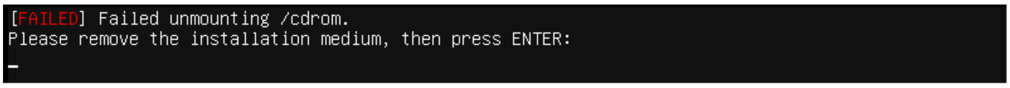


```
SSH Setup                                                          [ Help ]

You can choose to install the OpenSSH server package to enable secure remote
access to your server.

                 [X]  Install OpenSSH server

Import SSH identity:  [ No               ▼ ]
                      You can import your SSH keys from GitHub or Launchpad.

    Import Username:

                 [X]  Allow password authentication over SSH

                                 [ Done       ]
                                 [ Back       ]
```

- The system will take about 5 minutes to install.
- When it finishes, you will be able to choose " Reboot now". choose it. after reboot, you will be required to remove the USB drive and click "Enter".



```
/snap/subiquity/2651/usr/bin/python3 false'
        curtin command apt-config
        curtin command in-target
      running 'curtin curthooks'
        curtin command curthooks
          configuring apt configuring apt
          installing missing packages
          configuring iscsi service
          configuring raid (mdadm) service
          installing kernel
          setting up swap
          apply networking config
          writing etc/fstab
          configuring multipath
          updating packages on target system
          configuring pollinate user-agent on target
          updating initramfs configuration
          configuring target system bootloader
          installing grub to target devices
    finalizing installation
      running 'curtin hook'
        curtin command hook
    executing late commands
final system configuration
  configuring cloud-init
  installing openssh-server
  restoring apt configuration
subiquity/Late/run
```



```
[FAILED] Failed unmounting /cdrom.
Please remove the installation medium, then press ENTER:
_
```

Once we have logged in we will run the following commands:

Text

```
apt-mark hold $(uname -r)
apt remove unattended-upgrades -y

sudo cat > /etc/apt/preferences <<EOF
Package: linux-image-*
Pin: release *
Pin-Priority: -1

Package: linux-headers-*
Pin: release *
Pin-Priority: -1
EOF
```

Now the server could be connected to the network.
For configuring and enabling the network by Netplan follow this guide:
guide

Your server is now ready to install an Oosto Product

Vision AI Jetson Firmware Installation

VMware installation & JetsonInstaller Machine import

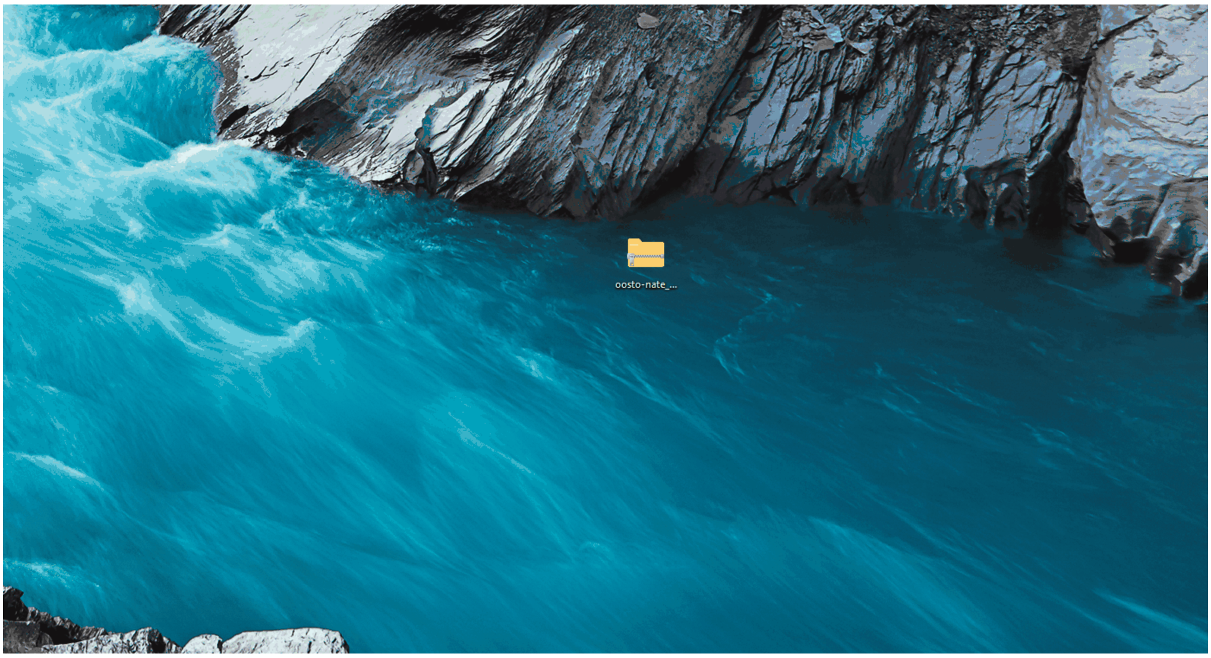
VMware player installation:

Please download Vmware from this link: Download link, choose Windows / Linux on VMware site.

Please follow this guide for installing VMware player: VMware Installation Guide (2 minutes guide)

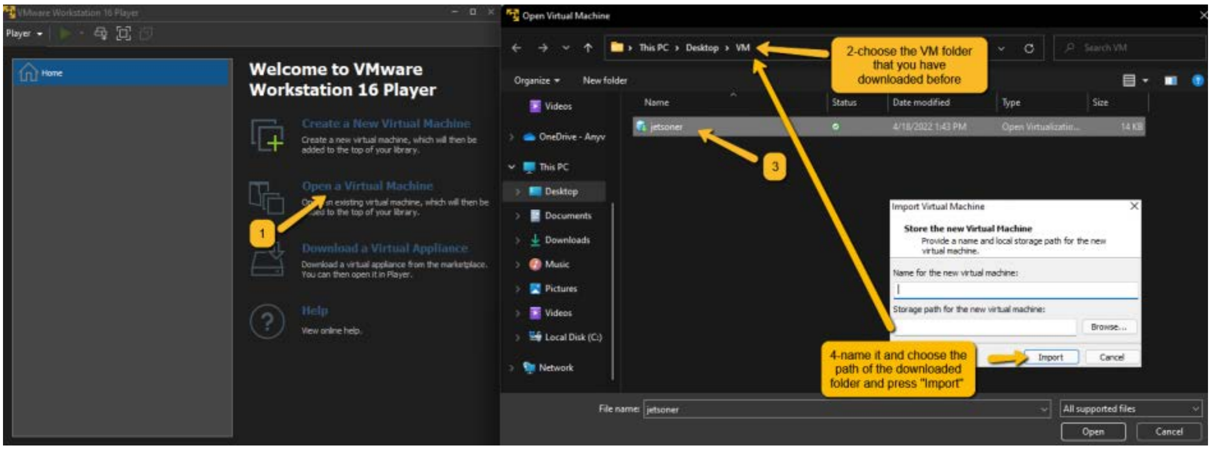
Machine image download: Download link , password: Oosto1!

Copy the content of the zipped file as shown below, after that the zip file can be deleted.



The next step is importing the machine and powering it up, lunch VMware workstation player 16, and follow the next image:

** in case of having issues launching VMware workstation player 16 please contact IT Support - itsupport@oosto.com



1

2-choose the VM folder that you have downloaded before

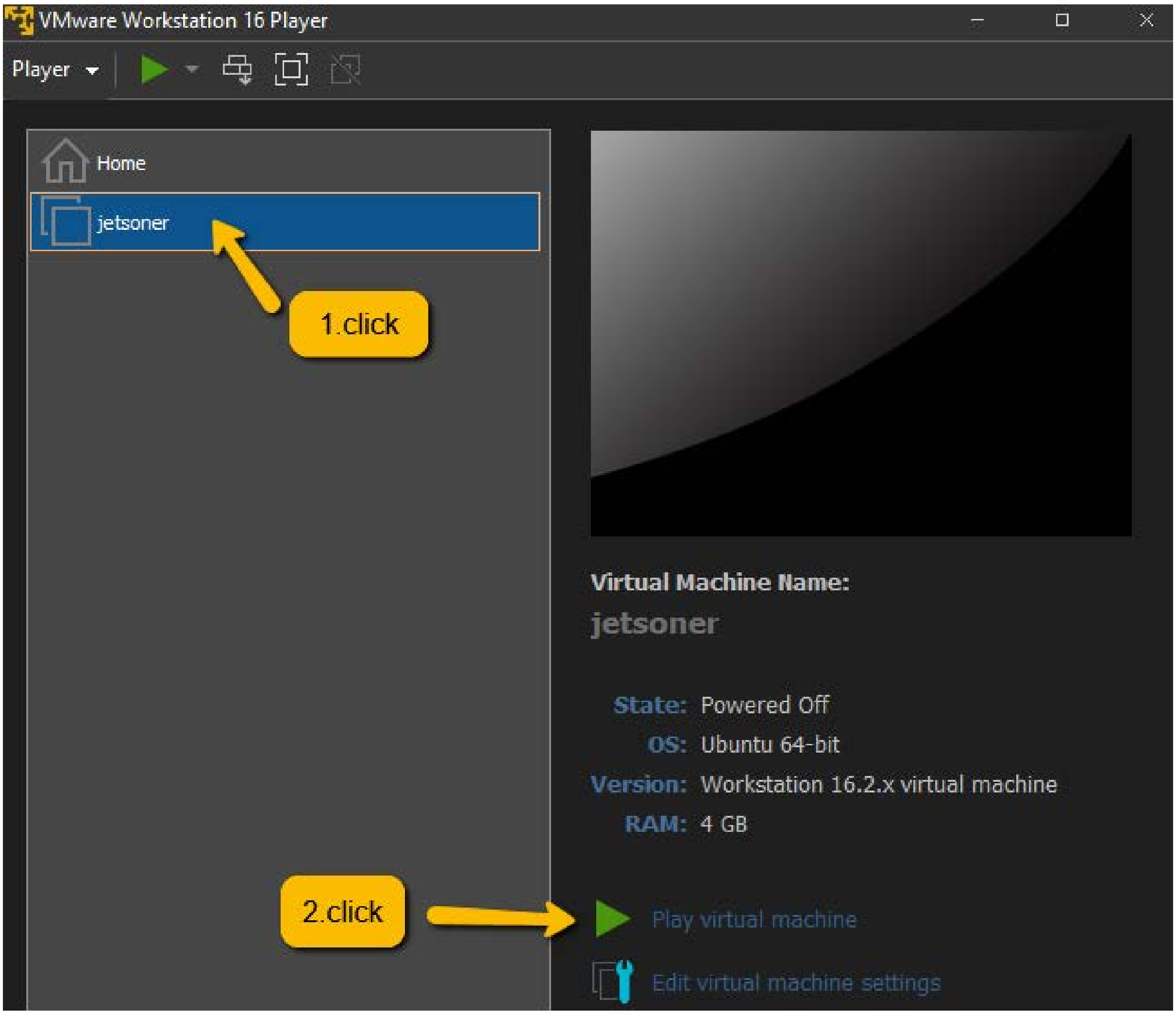
3

4-name it and choose the path of the downloaded folder and press "Import"

** Name it as you wish.

**Changing the path is optional.

Power up the machine:



1.click

2.click

Virtual Machine Name: jetsoner

State: Powered Off

OS: Ubuntu 64-bit

Version: Workstation 16.2.x virtual machine

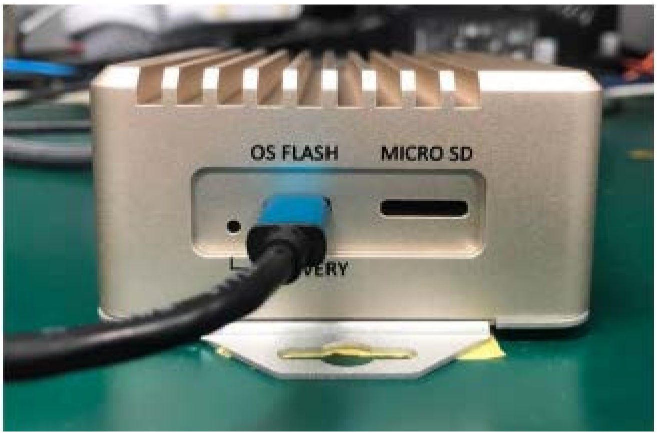
RAM: 4 GB

Enter Jetson in recovery mode

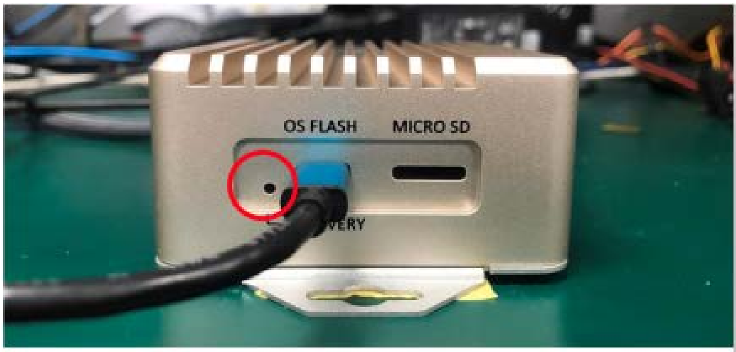
We need to boot the target Jetson device in recovery mode, for the AAEON BOXER-8251AI :

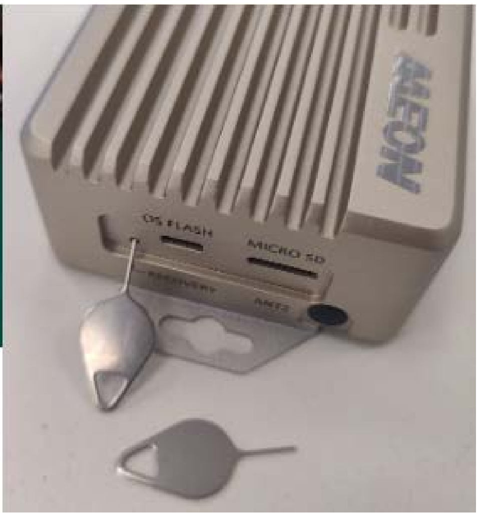
Connect the USB cable to the Jetson on the OS FLASH Port on the BOXER-8251AI and the other end to an available USB port on the host PC.

Please make sure you are using a High-speed micro USB data cable !!!

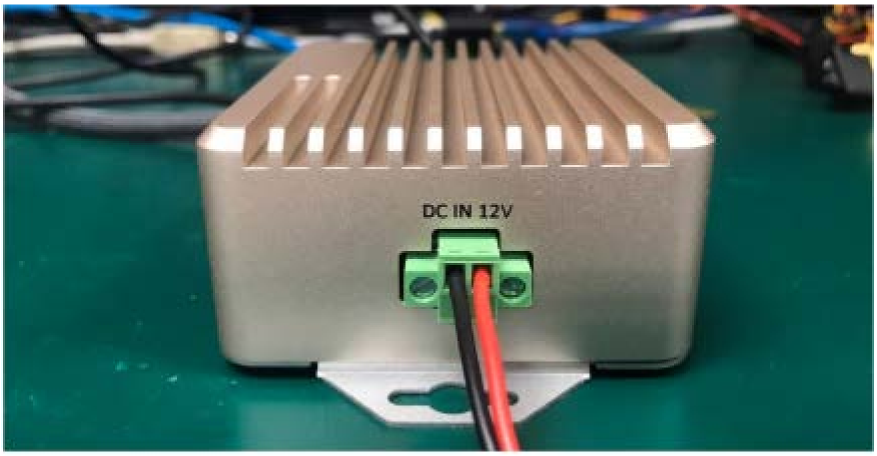


Press and hold the FORCE RECOVERY button. FORCE RECOVERY button is highlighted in the following image:

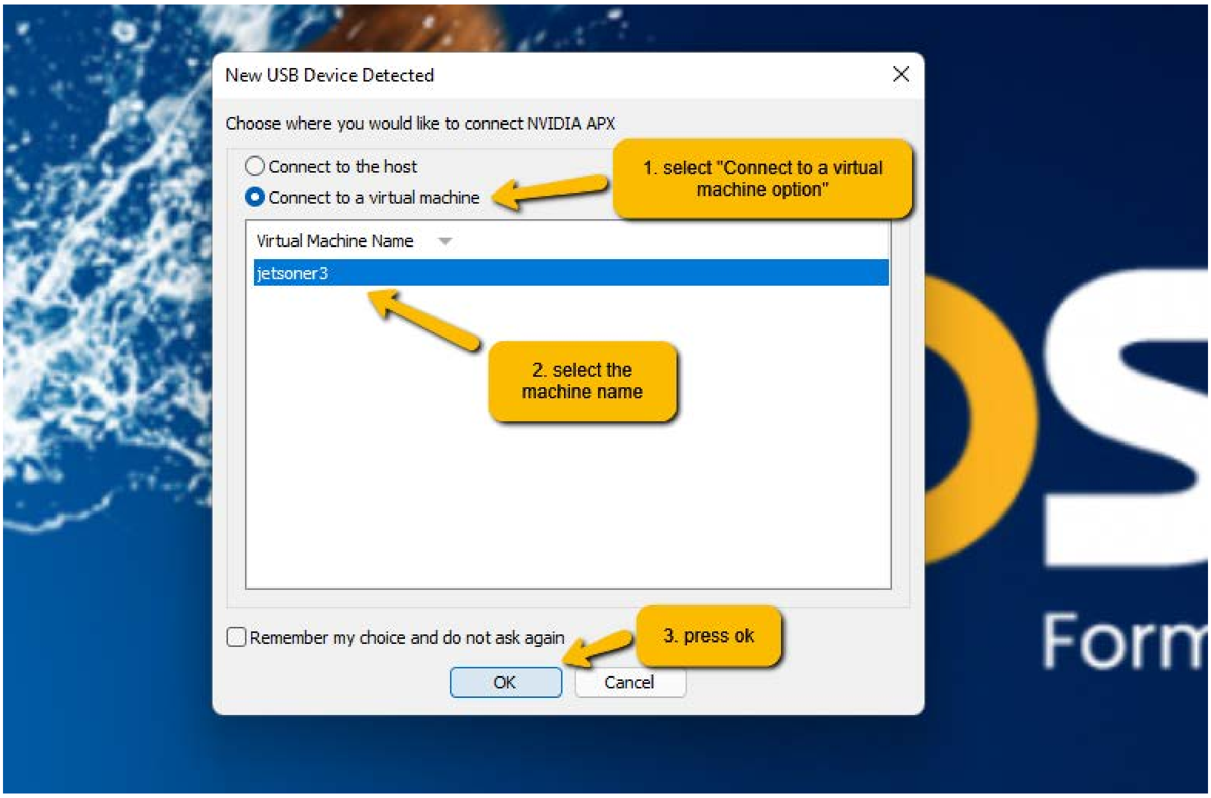




While holding the FORCE RECOVERY button, connect the power adapter. Continue to hold the FORCE RECOVERY button for two seconds, then release.



The following message will appear on your machine, Don't select “Remember my choice ….“



New USB Device Detected

Choose where you would like to connect NVIDIA APX

○ Connect to the host

● Connect to a virtual machine

1. select "Connect to a virtual machine option"

Virtual Machine Name

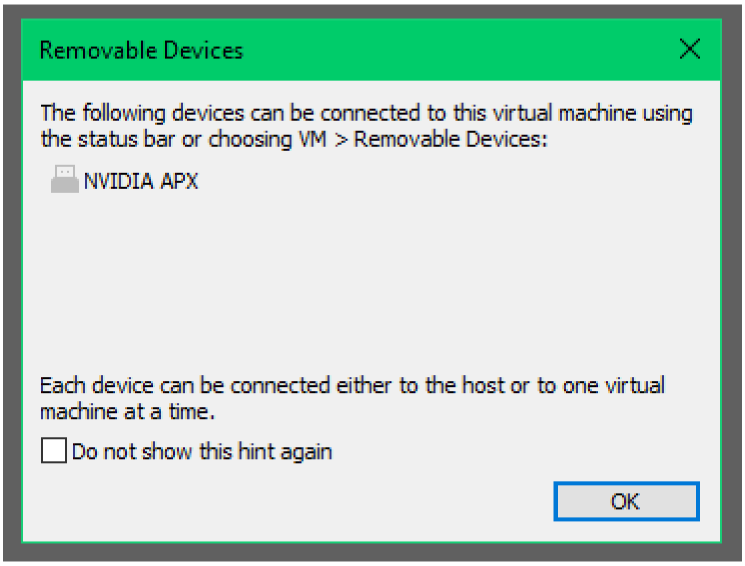
jetsoner3

2. select the machine name

□ Remember my choice and do not ask again

3. press ok

This message will appear.



Removable Devices

The following devices can be connected to this virtual machine using the status bar or choosing VM > Removable Devices:

NVIDIA APX

Each device can be connected either to the host or to one virtual machine at a time.

□ Do not show this hint again

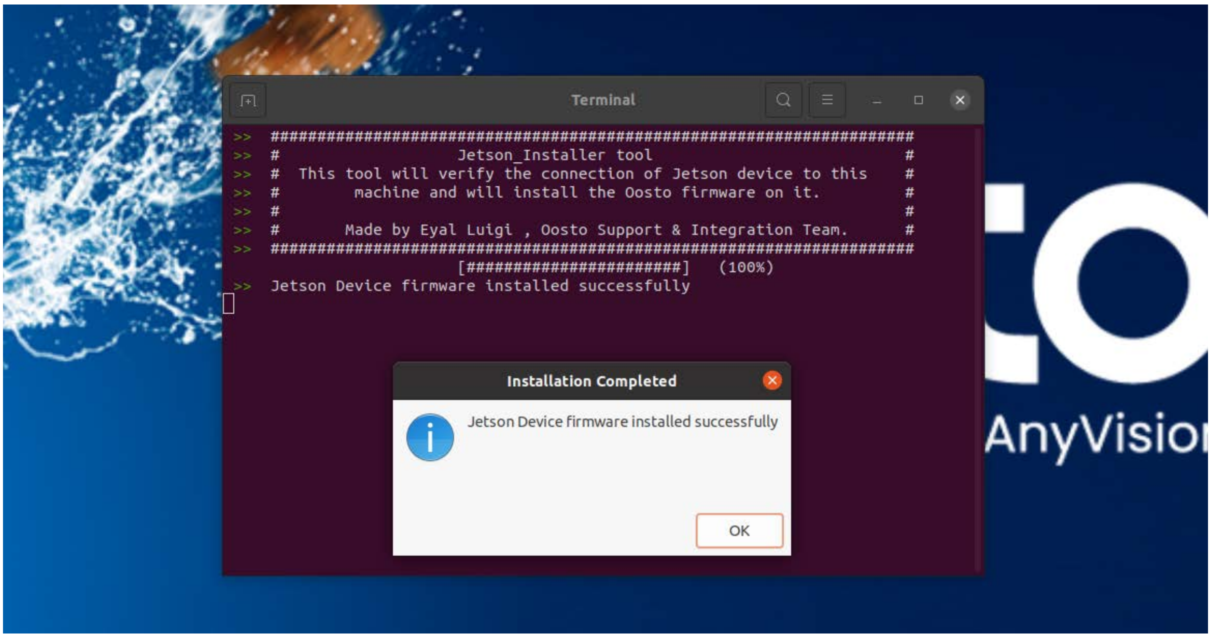
Jetson Flashing step:

A. Double Click on the Oosto folder,

B. Then Double click on the Jetson.sh and select “run it in the terminal”

C. Read the message, press OK and the installer will start.

Expected successful installation result:



```
>>  ######################################################################
>>  #                     Jetson_Installer tool                          #
>>  #  This tool will verify the connection of Jetson device to this     #
>>  #        machine and will install the Oosto firmware on it.          #
>>  #                                                                    #
>>  #       Made by Eyal Luigi , Oosto Support & Integration Team.       #
>>  ######################################################################
                        [########################]   (100%)
>>  Jetson Device firmware installed successfully
```

Installation Completed

Jetson Device firmware installed successfully

OK

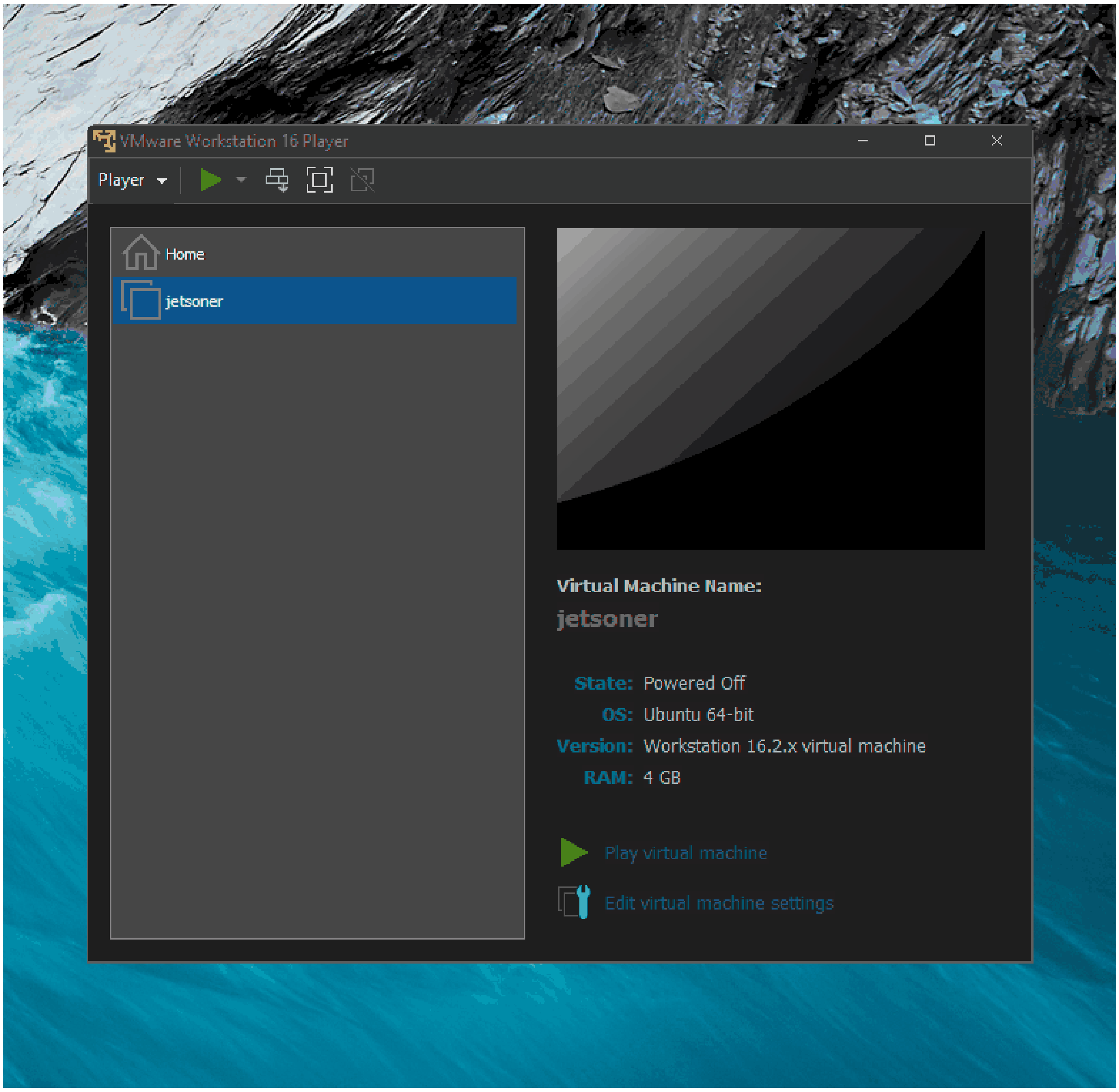
Notice that the screen will enter sleep mode after a while, it won't effect the installer

After that, you can unplug the Jetson from the power adapter and it is ready for use, please continue the installation process with the wizard install guide

Please provide Teamviewer / Anydesk Connection Details for getting assistance from the Support Team.

Avahi-Discovery utility (Also built in the Wizard-installer)

Please Enable network connection for this machine, follow those steps



Virtual Machine Name:
jetsoner

State: Powered Off
OS: Ubuntu 64-bit
Version: Workstation 16.2.x virtual machine
RAM: 4 GB

Then connect your Jetson device via Network cable to the Ethernet.

Make sure your Jetson and PC are on the same network and that you have DHCP activated on your network.

Next, Press on the Avahi-Discovery tool icon, look for oosto / Linux device, click on it and the IP that is assigned for this jetson will appear

In order to login to your Jetson device, you must use an ssh keypair which can be built-in Jenkins: http://anv-jenkins.anyvision.co/job/devops-core/job/devops-core-services/job/jetson-sshkey-generator/

Make sure the keys are with the correct permissions:

```Text
chmod 400 customer_id_rsa_signed.pub customer_id_rsa
```

And then use the following command with these flags:

```Text
ssh -i customer_id_rsa_signed.pub -i customer_id_rsa oosto@ipAddress
```

On Watch - Installation Guides

! Note

Please speak to your Oosto delivery manager to discuss the correct installation for your program and obtain the downloading link

Clean Installation using CLI interface [Fixed IP]

- All In One - Online and Offline installation
- Adding a Node to an existing cluster
- Add Jetson to the cluster
- HQ (Speak to oosto representative)

Installation using the Application Wizard Installer

- Clean install Cluster
- Adding a node to an existing cluster
- Add Jetson to the cluster

Online 2.6 All In One - CLI Installation

> 🚧 Note
>
> When installing Offline, you will need to run this step in a machine that is connected to the internet and copy the downloaded files to the machine you wish to install on

1. Prerequisites

What You'll Need

- Supported OS Ubuntu or Red Hat see release notes for exact versions
- Chrome web browser (to access the Dashboard)
- User with Root privileges required

> 🚧 An Installation Key is Required
>
> Before you can begin the installation process, please contact your Oosto Representative or Project Manager to receive an installation key (Key.txt) for the installation procedure.

2. Download Ansible Installer Files

> 🚧 Make sure the key.txt file is located in the same directory from which you’re running the command

Text

```
wget -qO- https://oosto-public-scripts.s3.eu-central-1.amazonaws.com/ansible-downloader/1.2.4-8/ansible-
```

> 👍 The Ansible files will be downloaded into /opt/ansible-installer-

3. Configuring Your Inventory.ini File

Change your working directory to the ansible-installer directory:

Text

```
cd /opt/ansible-installer-<VERSION>
```

Inside the inventory directory, edit the inventory.ini file and set the following configurations:

ansible_ssh_user=<YOUR_USERNAME>
ansible_ssh_pass=<YOUR_PASSWORD>
ansible_sudo_pass=<YOUR_SUDO_PASSWORD>

Make sure your inventory.ini looks like the example below:

Username & Password

```
[all:vars]
#ansible_user=<YOUR_USERNAME>
#ansible_ssh_private_key_file=inventory/<YOUR_PRIVATE_KEY>.pem
product_version="onwatch-2.6.5-2"
auto_install=true

##### To use username@password for ssh connection #####
ansible_ssh_user=<YOUR_USERNAME>
ansible_ssh_pass=<YOUR_PASSWORD>
ansible_sudo_pass=<YOUR_SUDO_PASSWORD>
```

- Set your Operating System Distribution using one of the options shown in the comments, for example, for Ubuntu 20.04:

Text

```
##### Use "target_os_dist" to select the hosts OS distro for offline / online. Options:
##### ubuntu1804 | ubuntu2004 | rhel7 | rhel8
target_os_dist="ubuntu2004"
```

- Remove the comment from the line that starts with **master1** under ***[main_master]***
- Set the Internal IP (Could be found with "ip r" command)
- Advertise_ip - will be used for AIO only!
  This option will preserve access to OW via specified ip even if the server's IP has changed.
  it will disable any option to expand the usage of the system to a cluster
  make sure that the chosen advertise IP does not collide with other IP
  This could be checked by the ping command.
  Once you know the IP, add variable named "advertise_ip" right after the "ansible_hosts"'s IP
  As in the below example.

without advertise_ip Advertise_ip

```
master1 ansible_host=<SERVER'S INTERNAL IP>

Example:
master1 ansible_host=192.168.1.22
```

4. Start the Ansible Installation

> 🚧 After you’ve downloaded the ansible-installer files, replace VERSION with the ansible installer version you downloaded

Text

```
cd /opt/ansible-installer-VERSION
./ansible-dep-installer.sh
./run-playbook.sh -i inventory/inventory.ini install-k3s.yml -t online
```

Optional: Backup / Restore steps: (after installation completion)

Text

```
sudo su -
kubectl get configmap backup-wl-restore-configmap -o yaml | sed 's|registry:30000//|registry:30000/|g' |
kubectl set image cronjob/backup-wl-cron backup-wl-cron=registry:30000/anyvision-training/watch-list-bac
kubectl get job | grep backup-wl | awk {'print $1'} | xargs kubectl delete job
```

Offline 2.6 All In One - CLI Installation

In offline mode, Oosto's system will be installed in a stand-alone configuration without any connectivity to Oosto's server. In order to support full installation, the installer should be fully prepared with the SW stack on-prem.

1. Prerequisites

What You'll Need

- Supported OS Ubuntu or Red Hat see release notes for exact versions
- Chrome web browser (to access the Dashboard)
- User with Root privileges required

> 🚧 **An Installation Key is Required**
>
> Before you can begin the installation process, please contact your Oosto Representative or Project Manager to receive an installation key (Key.txt) for the installation procedure.

2. Download Ansible Installer Files

> 🚧 Make sure the key.txt file is located in the same directory you're running the oneliner from *

Text

```
wget -qO- https://oosto-public-scripts.s3.eu-central-1.amazonaws.com/ansible-downloader/1.2.4-8/ansible-
```

*** If your key.txt is located in another path, use --cred-path KEY_PATH, example:**

Text

```
wget -qO- https://oosto-public-scripts.s3.eu-central-1.amazonaws.com/ansible-downloader/1.2.4-8/ansible-
```

> 👍 Ansible files will be downloaded into /opt/ansible-installer-

3. Configuring Your Inventory.ini File

Edit the inventory/inventory.ini file with the following:

- First, change your working directory to the ansible-installer directory:

Text

```
cd /opt/ansible-installer-<VERSION>
```

- Edit the inventory/inventory.ini file using your preferred editor (Vim, nano, etc.)
- Set username and password in ansible_ssh_user, ansible_ssh_pass and and ansible_sudo_pass OR ansible_user and ansible_ssh_private_key_file for ssh using <YOUR_PRIVATE_KEY>.pem file (located in the inventory file), example:

> ❗ Make sure you keep only one user data section commented out, while the other is commented. using both sections will end up with failed installation!

Private key (PEM file) Username & Password

```
[all:vars]
ansible_user=<YOUR_USERNAME>
ansible_ssh_private_key_file=inventory/<YOUR_PRIVATE_KEY>.pem
product_version="onwatch-2.6.5-2"
auto_install=true

##### To use username@password for ssh connection #####
#ansible_ssh_user=<YOUR_USERNAME>
#ansible_ssh_pass=<YOUR_PASSWORD>
#ansible_sudo_pass=<YOUR_SUDO_PASSWORD>
```

- Set your Operating System Distribution using one of the options below, for example, ubuntu 20.04:

Text

```
##### Use "target_os_dist" to select the hosts OS distro for offline / online. Options:
##### ubuntu1804 | ubuntu2004 | rhel7 | rhel8
target_os_dist="ubuntu2004"
```

> **NOTE: If you are using a private_key.pem file, make sure you put it in the inventory/ directory and that it has the right file permissions (400).**
>
> If not, execute - chmod 400 inventory/YOUR_PRIVATE_KEY.pem

Download Files##

On your online machine download the files and packages

- Set ONLY in the [download_machine] section the machine name and keep the localhost parameters as below

Text

```
[download_machine]
download1 ansible_host=localhost ansible_connection=local
```

- Run the download file using

Text

```
./run-playbook.sh -i inventory/inventory.ini install-k3s.yml -t download
```

After the download playbook will be done successfully, copy “/opt/ansible-installer-" to your airgap environment.

Configure Node Groups##

On the offline machine, edit again the inventory.ini file

- Comment the download machine in [download_machine] section
- Comment out the master line under [main_master] set your machine name and his **internal IP**
  Example: replace this line

Text

```
# master1 ansible_host=[ENTER_IP]
```

With this one (11.11.11.79 is an example only, make sure to sue an IP that has no conflict in the local network)

Advertise-IP Without Advertise-IP

```
master1 ansible_host=10.1.20.20 advertise_ip=11.11.11.79
```

> ### ! Advertise-IP
>
> Use Advertise-IP in case you **don't have plans** to extend this master into cluster (add nodes in the future). Otherwise, use the example without Advertise-IP

OPTIONAL - Configure extra Servers:

If you wish to add more servers to your cluster, just add them under the relevant Node group, expand the list below to determine where to place them.

Variable	Purpose
main_master	The server from which you run the install files is used to store the install files, logs, and cluster management.
gpu_node	Pipe nodes
data_node	memsql nodes
k3s_master	extra k3s masters

Example:

Text

```
[main_master]
master1 ansible_host=10.20.11.34

[k3s_master]
#master2 ansible_host=[ENTER_IP]

[data_node]
data1 ansible_host=10.20.11.35

[gpu_node]
gpu1 ansible_host=10.20.11.36
```

4. Start the Ansible Installation

> 🚧 After you’ve downloaded the ansible-installer files, replace VERSION with the ansible installer version you downloaded

Text

```
cd /opt/ansible-installer-VERSION
./ansible-dep-installer.sh
./run-playbook.sh -i inventory/inventory.ini install-k3s.yml -t airgap
```

Backup / Restore steps: (after installation completion)

Text

```
sudo su -
kubectl get configmap backup-wl-restore-configmap -o yaml | sed 's|registry:30000//|registry:30000/|g' |
kubectl set image cronjob/backup-wl-cron backup-wl-cron=registry:30000/anyvision-training/watch-list-bac
kubectl get job | grep backup-wl | awk {'print $1'} | xargs kubectl delete job
```

5. Clean your environment(for deleting the system, not part of the installation)

To clean your entire environment, you can use the *clean.yml* file provided with all the files of the ansible-installer, at */opt/ansible-installer-VERSION* path.

> ❗ Caution:
>
> Running clean.yml is a non-interactive process, which can **delete your entire environment including your data** if not used properly with the exact tags you intended to use.

The clean process will use the same *inventory.ini* file you used in your installation process.
First, make sure your */opt/ansible-installer-VERSION/inventory/inventory.ini* file is updated with all the relevant hosts you wish to clean the installation from. Example:

Text

```
[main master]
master1 ansible_host=10.1.20.20
```

> 📘 The example above will run the clean process on each node from the list (master1-3,edge1-2)

Now you can run the *clean.yml* with your *inventory.ini*, replace YOUR_TAGS with the relevant tags you wish to use from the table below, separated by " , "

Text

```
./run-playbook.sh -i inventory/inventory.ini clean.yml -t YOUR_TAGS
```

Example :

Text

```
./run-playbook.sh -i inventory/inventory.ini clean.yml -t nvidia,k3s
```

Tag	Purpose	Comments
k3s	Remove all k3s dependencies and delete the k3s cluster from your machines.	A reboot is required after using this tag.
k8s	Remove all Kubernetes (Gravity) previous versions and Docker service from your machines.	1. A reboot is required after using this tag. 2. Do not use this tag while having the k3s environment running.
nvidia	Remove all Nvidia-related packages from your machines.	1. Remove all Nvidia-related packages from your machines. 2. A reboot is required after using this tag.
data	Remove */SSD* and */storage* directories.	1. Remove */SSD* and */storage* directories. 2. **This tag will delete your entire data!**

Appendixes

Configuring Cluster Variables

Variable	Purpose	Comment
ansible_user *ansible_ssh_private_key_file*	**SSH key usage (no user: pass needed)** - These variables set the SSH user for the installer to use, and the private key relative path - the key must be under *inventory/* directory.	You must u section or *ansible_ss* *ansible_ss* *ansible_su*
ansible_ssh_useransible_ssh_passansible_sudo_pass	These 3 keys must be combined. These variables set the SSH user, password, and sudo password for the installer to use globally (unless defined in a particular node section). The user must have *sudo* permissions to run *root-* related commands.	You must u section or *ansible_ss* section.
auto_install	Whether to automatically install your product layers (defined at */inventory/product-versions/PRODUCT_VERSION.yml*) or only load them into your local chartmuseum to be installed by rancher UI. the default value is *true*.	
product_version	The product configuration file name, which presents the product version you're about to install. This is a YAML file exists under */inventory/product-versions/* directory	
target_os_dist	This variable defines the operating system you're about to install. This variable **must be configured** before offline installations to determine the Nvidia-driver files and the dependencies packages.The value options are: *ubuntu2004* - target OS is Ubuntu20.04*ubuntu1804*- target OS is Ubuntu18.04*rhel8* - target OS is RHEL8.3/8.4*rhel7* - target OS is RHEL 7.7 - **deprecated**The default variable is *ubuntu2004*	

Configuring Host Variables

To assign environment variables to hosts during the Ansible installation, set them under the host entry in the [main_master], [k3s_masters],[data_node],[gpu_node],[edge] sections. For example:

Text

```
hq_mongo_ip=["10.1.10.33","10.1.10.81","10.1.10.92"]

[main_master]
master1 ansible_host=10.20.11.34 advertise_ip=172.168.10.25 override_system_hostname=false
```

Variables	Purpose	Comments
hq_mongo_ip	This variable is only relevant for *site_hq* plugin installation. The default value is *["127.0.0.1","127.0.0.2","127.0.0.3"]* .	You should add this value under Product Config (Just uncomment it and use your relevant value)
advertise_ip	This variable defines the IP address that apiserver uses to advertise itself.This variable must not be presented unless you wish to install only one master which will be used as an All-In-One installation (A Cluster with *advertise_ip* variable will not function!).	This variable should be used only under the [main_master] section.
override_system_hostname	This variable defines whether or not to automatically override the system hostname for this specific host.The default variable is *true*.	All the hosts in the inventory.ini must be the same as their corresponding server's current hostname if this variable is set to *false*.
ansible_host	The IP/name of the target host to use instead of *inventory_hostname*.Use this variable only with *-t* _download _option.	
ansible_connection	The connection plugin is used for the task on the target host.Use this variable only with -t download option.	
gpu_usage	For each host with a GPU, we can optionally select the “gpu*usage” variable:The value options are:_gpu_usage=engine* Selecting “engine” will stipulate running PipeNG on x86 host and G-Streamer on ARM host.*gpu_usage=reid* - Selecting “reid” will stipulate running ReID with FAISS on the host x86 & ARM.*gpu_usage=engine-reid* - Selecting “engine-reid” will run PipeNG and ReID with FAISS on the host (x86 Only when version is newest then v2.5.0).	The default choice will be “engine”

Add Node to OnWatch Cluster Via CLI

Installation - Cluster Node (Add a New Server to Cluster)

When adding a new node to the cluster, please follow the pre-requirements and make sure you have a cleaned environment.

**If there is already an ansible, please skip to step 3.

1. Get or Generate S3 Credentials

Get a key.txt token to be able to download the latest ansible-repo into your host.
Generate key credentials from Jenkins

Text

```
cat >> key.txt << 'END'
[default]
aws_access_key_id = [key_id]
aws_secret_access_key = [access_key]
END
```

2. Download Ansible Installer Files

Make sure the key.txt file is located in the same directory you're running the oneliner from *

Text

```
wget -qO- https://oosto-public-scripts.s3.eu-central-1.amazonaws.com/ansible-downloader/1.2.4-0/ansible-
```

- If your key.txt is located in another path, use --cred-path KEY_PATH, example:

Text

```
wget -qO- https://oosto-public-scripts.s3.eu-central-1.amazonaws.com/ansible-downloader/1.2.4-0/ansible-
```

Ansible files will be downloaded into /opt/ansible-installer-

3. Configuring Your Inventory.ini File

Edit the inventory/inventory.ini file with the following:

- First, change your working directory to the ansible-installer directory:

Text

```
cd /opt/ansible-installer-<VERSION>
```

- Edit the inventory/inventory.ini file using your preferred editor (vim, nano, etc.)
- Set username and password in ansible_ssh_user, ansible_ssh_pass and and ansible_sudo_pass OR ansible_user and ansible_ssh_private_key_file for ssh using <YOUR_PRIVATE_KEY>.pem file (located in the inventory file), example:

> 🚧 Note
>
> Make sure you keep only one user data section commented out, while the other is commented.
>
> using both sections will end up with failed installation!

Text

```
[all:vars]
ansible_user=<YOUR_USERNAME>
ansible_ssh_private_key_file=inventory/<YOUR_PRIVATE_KEY>.pem
product_version="onwatch-2.6.2-1"
auto_install=true

##### To use username@password for ssh connection #####
#ansible_ssh_user=<YOUR_USERNAME>
#ansible_ssh_pass=<YOUR_PASSWORD>
#ansible_sudo_pass=<YOUR_SUDO_PASSWORD>
```

Set your Operating System Distribution using one of the options below, for example, ubuntu 20.04:

Text

```
##### Use "target_os_dist" to select the hosts OS distro for offline / online. Options:
##### ubuntu1804 | ubuntu2004 | rhel7 | rhel8
target_os_dist="ubuntu2004"
```

> 🚧 Note
>
> if you are using a private_key.pem file, make sure you put it in the inventory/ directory and that it has the right file permissions (400).
> If not, execute - chmod 400 inventory/YOUR_PRIVATE_KEY.pem
>
> - In case you need to generate yourself a .pem key:
>
> ssh-keygen -t rsa -f $HOME/.ssh/id_rsa -P "" && cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys
> Then you can copy the id_rsa and id_rsa.pub files to the inventory/ directory, and change the ansible_ssh_private_key_file accordingly (no need for the .pem suffix at this case).

Set Nodes To Be Added To Your Cluster

First, make sure your current inventory file is valid and the node names and IP addresses are correct, example:

Text

```
[main_master]
master1 ansible_host=10.20.11.34

[k3s_master]
master2 ansible_host=10.20.11.31

[data_node]
data1 ansible_host=10.20.11.35

[gpu_node]
gpu1 ansible_host=10.20.11.36
```

Then, add the relevant node you want to join to the cluster under the right section (see Node Groups), for example, if you want to add a data node, your inventory.ini should look like this:

Text

```
[main_master]
master1 ansible_host=10.20.11.34

[k3s_master]
master2 ansible_host=10.20.11.31

[data_node]
data1 ansible_host=10.20.11.35
data2 ansible_host=10.20.11.41 # -----------> additional node to join the cluster
[gpu_node]
gpu1 ansible_host=10.20.11.36
```

Node Groups

If you wish to add more servers to your cluster, just add them under the relevant Node group, expand the list below to determine where to place them.

Variable	Purpose
main_master	The server from which you run the install files is used to store the install files, logs, and cluster management.*You must use “main_master”, and it must be only 1.
k3s_master	extra k3s masters
data_node	memsql nodes
gpu_node	Pipe nodes

Example:

Text

```
[main_master]
master1 ansible_host=10.20.11.34

[k3s_master]
#master2 ansible_host=[ENTER_IP]

[data_node]
data1 ansible_host=10.20.11.35

[gpu_node]
gpu1 ansible_host=10.20.11.36
```

Configuring Host Variables

> 📘 Use this section only if you wish to add nodes with GPU cards, in order to obtain their role (gpu_usage is the value you should use).

To assign environment variables to hosts during the Ansible installation, set them under the host entry in the [main_master], [k3s_masters],[data_node],[gpu_node],[edge] sections. For example:

Text

```
hq_mongo_ip=["10.1.10.33","10.1.10.81","10.1.10.92"]

[main_master]
master1 ansible_host=10.20.11.34 advertise_ip=172.168.10.25 override_system_hostname=false
```

Variable	Purpose
hq_mongo_ip	This variable is only relevant for site_hq plugin installation. The default value is ["127.0.0.1","127.0.0.2","127.0.0.3"] . *You should add this value under Product Config (Just uncomment it and use your relevant value)
advertise_ip	This variable defines the IP address that apiserver uses to advertise itself. This variable must not be presented unless you wish to install only one master which will be used as an All-In-One installation (A Cluster with advertise_ip variable will not function!). *This variable should be used only under the [main_master] section.
override_system_hostname	This variable defines whether or not to automatically override the system hostname for this specific host. The default variable is true. *All the hosts in the inventory.ini must be the same as their corresponding server's current hostname if this variable is set to false.
ansible_host	The IP/name of the target host to use instead of inventory_hostname. Use this variable only with -t download option.
ansible_connection	The connection plugin is used for the task on the target host. Use this variable only with -t download option.
gpu_usage	For each host with a GPU, we can optionally select the “gpu_usage” variable: The value options are: • gpu_usage=engine Selecting “engine” will stipulate running PipeNG on x86 host and G-Streamer on ARM host. • gpu_usage=reid - Selecting “reid” will stipulate running ReID with FAISS on the host x86 & ARM. • gpu_usage=engine-reid - Selecting “engine-reid” will run PipeNG and ReID with FAISS on the host (x86 Only in v2.5.0). *The default choice will be “engine”

4. Run the Join Node Playbook

Text

```
./run-playbook.sh -i inventory/inventory.ini join-node-k3s.yml
```

After the playbook is finished successfully, run the following command and make sure your new node is in the list:

Text

```
kubectl get nodes
```

old

------------------Old

When adding a new node to the cluster, please follow the pre-requirements and make sure you have a cleaned environment.

1. Login to the Cluster

Open your browser and replace the <master_ip> with the Master Node server IP
https://<master_ip>:32009

Log in using these credentials:

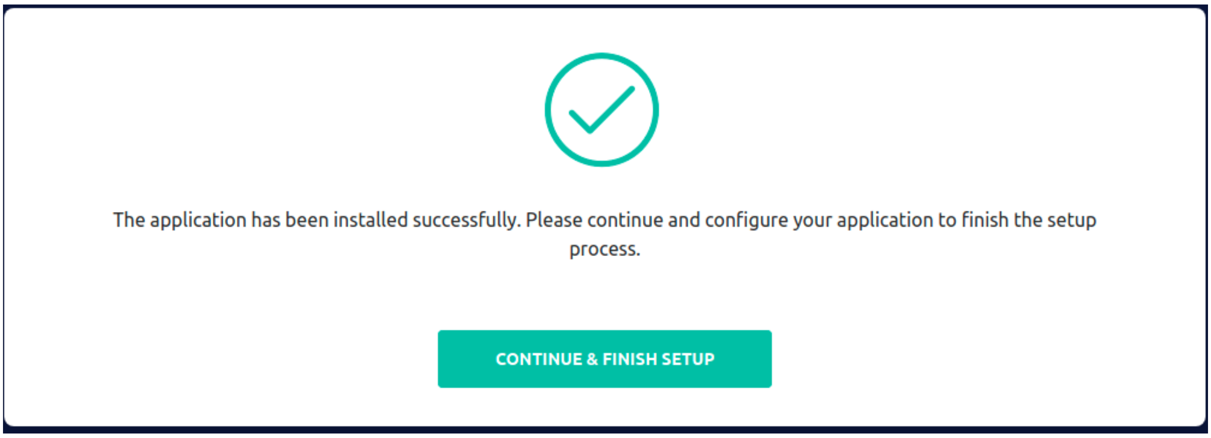
- Username: admin
- Password:

Run this command to get gravity password (on your terminal):

Text

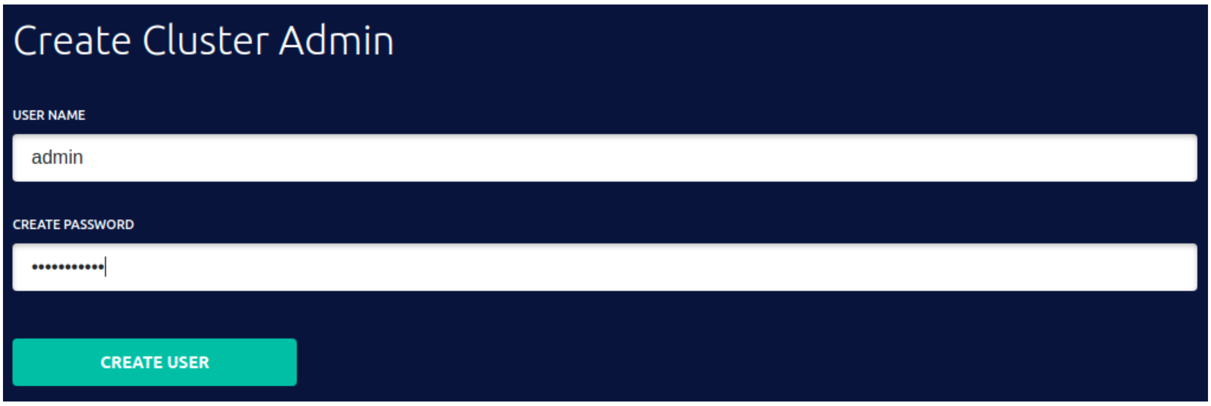
```
kubectl -n kube-system get secret gravity-secret -o=jsonpath='{.data.password}' | base64 --decode ; echo
```

Click on CONTINUE & FINISH SETUP



The application has been installed successfully. Please continue and configure your application to finish the setup process.

Now use the same credentials again:



Create Cluster Admin

USER NAME

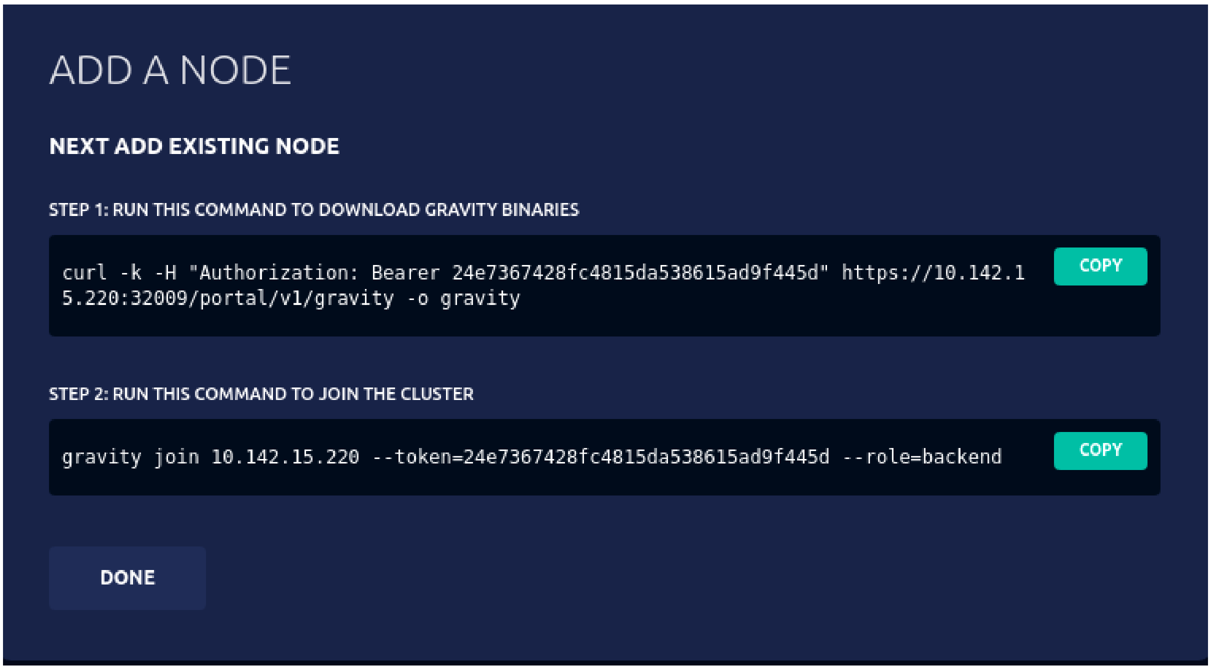
admin

CREATE PASSWORD

•••••••••••

2. Generate CLI to Add the Node to the Cluster

Go to the "Nodes" tab, and click on "ADD NODE"
Choose “node", then "CONTINUE".



ADD A NODE

NEXT ADD EXISTING NODE

STEP 1: RUN THIS COMMAND TO DOWNLOAD GRAVITY BINARIES

```
curl -k -H "Authorization: Bearer 24e7367428fc4815da538615ad9f445d" https://10.142.15.220:32009/portal/v1/gravity -o gravity
```

STEP 2: RUN THIS COMMAND TO JOIN THE CLUSTER

```
gravity join 10.142.15.220 --token=24e7367428fc4815da538615ad9f445d --role=backend
```

3. Add the Node to the Cluster

Press "COPY" on the first command

On the Node Machine

```
sudo su -
PASTE and RUN first command
# Move gravity executable to $PATH
mv gravity /usr/local/bin
chmod +x /usr/local/bin/gravity

PASTE and RUN second command
```

For example

Text

```
sudo su -
curl -k -H "Authorization: Bearer 24e7367428fc4815da538615ad9f445d" https://10.142.15.220:32009/portal/v
# Move gravity executable to $PATH
mv gravity /usr/local/bin
chmod +x /usr/local/bin/gravity

gravity join 10.142.15.220 --token=24e7367428fc4815da538615ad9f445d --role=node
```

4. Validate the Node joined the Cluster

On the Master Machine

Execute this command:

Text

```
kubectl get node
```

Now make sure you see the newly added node, Copy the new node name and replace NODE_NAME with it:

Master Extra-Master edge reid

```
#Disable memsql from running on this server
kubectl label node NODE_NAME memsql-

#Disable pipe from running on this server
kubectl label node NODE_NAME pipe-
kubectl delete pod $(kubectl get pods | grep pipeng-0 | awk '{print $1}')
```

4. Scale Up Pipeng

On the Master Machine

> ❗ **Master pipe shutdown**
>
> If you don’t want pipe to run on your master node
> kubectl label node NODE_NAME pipe-
>
> For this use case the Pipeng scaling calculation will be diffrent:
> (N * Nodes) - Nodes that will run pipe.

Run this command to scale the number of PipeNG instances to the number of available nodes (N * Nodes + Master)
For example:
Master with 2 nodes set replicas to “3”
Master with only one node set replicas to “2”

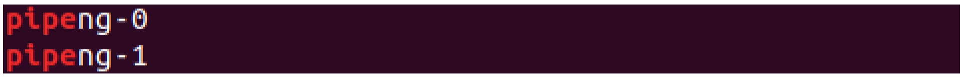
example

```
exmaple:
kubectl scale statefulset pipeng --replicas=2
```

Make sure the new Pipeng pod is ready after a while.

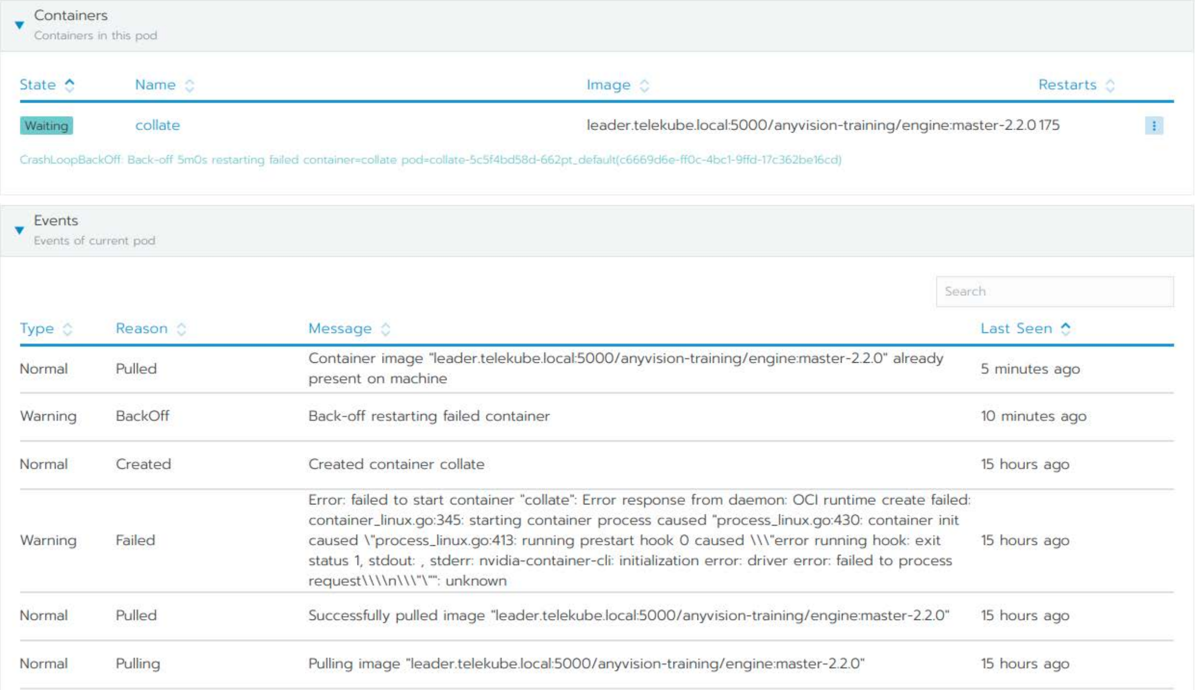
Text

```
kubectl get pod | grep pipeng
```



```
pipeng-0
pipeng-1
```

*If your collate / pipe is down (red bar) (Rancher)
you need to reboot your machine to apply your nvidia driver installation .



Containers
Containers in this pod

State	Name	Image	Restarts
Waiting	collate	leader.telekube.local:5000/anyvision-training/engine:master-2.2.0	175

CrashLoopBackOff: Back-off 5m0s restarting failed container=collate pod=collate-5c5f4bd58d-662pt_default(c6669d6e-ff0c-4bc1-9ffd-17c362be16cd)

Events
Events of current pod

Type	Reason	Message	Last Seen
Normal	Pulled	Container image "leader.telekube.local:5000/anyvision-training/engine:master-2.2.0" already present on machine	5 minutes ago
Warning	BackOff	Back-off restarting failed container	10 minutes ago
Normal	Created	Created container collate	15 hours ago
Warning	Failed	Error: failed to start container "collate": Error response from daemon: OCI runtime create failed: container_linux.go:345: starting container process caused "process_linux.go:430: container init caused \"process_linux.go:413: running prestart hook 0 caused \\\"error running hook: exit status 1, stdout: , stderr: nvidia-container-cli: initialization error: driver error: failed to process request\\\\n\\\"\"": unknown	15 hours ago
Normal	Pulled	Successfully pulled image "leader.telekube.local:5000/anyvision-training/engine:master-2.2.0"	15 hours ago
Normal	Pulling	Pulling image "leader.telekube.local:5000/anyvision-training/engine:master-2.2.0"	15 hours ago

5. Scale API Services

2 Replicas per Pipeng service.

Text

```
kubectl scale --replicas=6 deployment/subjects-service
kubectl scale --replicas=6 deployment/tracks-consumer-producer
```

You’re all set!

Remove a Node from cluster

1. Login to the Cluster

Open your browser and replace the <master_ip> with the Master Node server IP
https://<master_ip>:32009

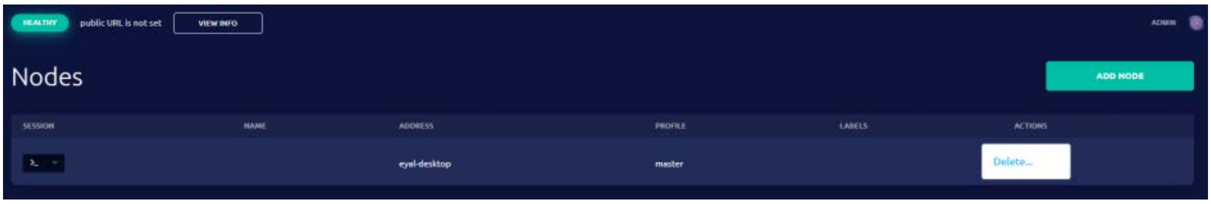
- Log in using these credentials:
  Username: admin
  Password:
  run this command to get gravity password (on your terminal):

Text

```
kubectl -n kube-system get secret gravity-secret -o=jsonpath='{.data.password}' | base64 --decode ; echo
```

2. Remove Node from UI

Navigate to Nodes, Then Press on *** (three dots button) > DELETE



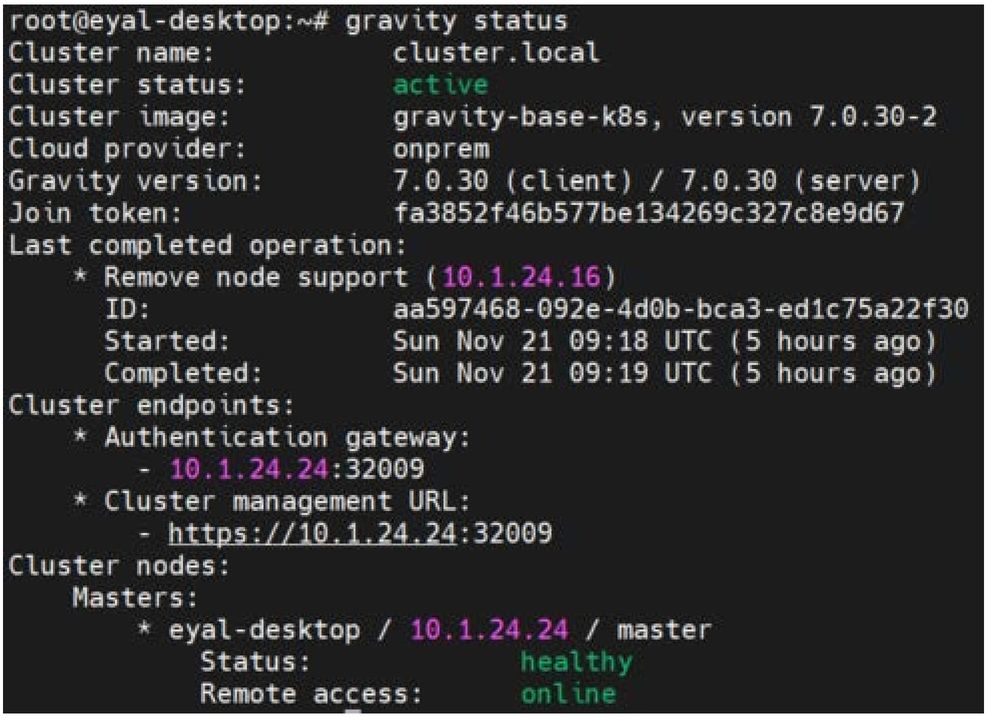
The node will be removed from the cluster.

for validating the removal run this command **On the Master Machine**

Text

```
gravity status
```

correct output should look like this (in this case 10.1.24.16 was removed)



```
root@eyal-desktop:~# gravity status
Cluster name:           cluster.local
Cluster status:         active
Cluster image:          gravity-base-k8s, version 7.0.30-2
Cloud provider:         onprem
Gravity version:        7.0.30 (client) / 7.0.30 (server)
Join token:             fa3852f46b577be134269c327c8e9d67
Last completed operation:
    * Remove node support (10.1.24.16)
      ID:               aa597468-092e-4d0b-bca3-ed1c75a22f30
      Started:          Sun Nov 21 09:18 UTC (5 hours ago)
      Completed:        Sun Nov 21 09:19 UTC (5 hours ago)
Cluster endpoints:
    * Authentication gateway:
        - 10.1.24.24:32009
    * Cluster management URL:
        - https://10.1.24.24:32009
Cluster nodes:
    Masters:
        * eyal-desktop / 10.1.24.24 / master
            Status:             healthy
            Remote access:      online
```

3. Scale Down PipeNG

On the Master Machine

Run this command to scale the number of PipeNG instances to the number of available nodes (N * Nodes + Master)
For example:
Master with 2 nodes set replicas to “3”
Master with only one node set replicas to “2”

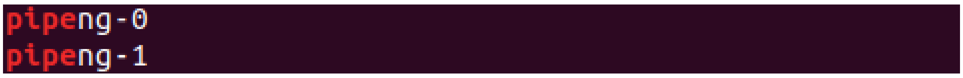
Text

```
kubectl scale statefulset pipeng --replicas=2
```

Make sure the new PipeNG pod amount is correct considering your systems cluster size

Text

```
kubectl get pod | grep pipeng
```



```
pipeng-0
pipeng-1
```

4. Clean Node - Optional

On the Node Machine

use **./clean -k** script for cleaning any Gravity / Kubernetes leftovers and clean storage leftovers
clean.sh can be copied from the master via SCP command

Text

```
scp clean.sh user@10.10.10.10:/clean.sh/path

example:

scp clean.sh user@10.1.24.24:/home/user
cd /home/user
./clean -k
reboot
rm -rf /storage/* /ssd/*
```

Add Jetson to existing Cluster via CLI

> ❗ You Cannot add a jetson to cluster installed with Advertise IP!

1 Generate a dedicated ssh keypair for the specific customer:

Access the Jenkins job → Set CUSTOMER_NAME as the name of the customer you're creating the keys for → Press “Build”.

The job output will include a .tar file which includes three files in it:
oosto_CUSTOMER_NAME_id_rsa
oosto_CUSTOMER_NAME_id_rsa.pub
oosto_CUSTOMER_NAME_id_rsa_signed.pub

2 Extract the .zip file you've got

unzip the file to the inventory directory using this command:

Text

```
unzip ZIP_FILE_NAME.tar -d inventory/
```

3 Under the [edge] section, add the relevant Oosto jetsons information

example:

Text

```
[edge]
edge1 ansible_host=10.1.20.1
edge2 ansible_host=10.1.20.2
```

4 Adding SSH Files

Under [edge:vars] comment out the # and replace [PRIVATE_KEY_PATH] and [PUBLIC_SIGNED_KEY_PATH] with the files you copied at stage #3, example:

Text

```
[edge:vars]
ansible_ssh_private_key_file=inventory/oosto_CUSTOMER_NAME_id_rsa
ansible_ssh_extra_args="-i inventory/oosto_CUSTOMER_NAME_id_rsa_signed.pub"
```

> 📘 **The keys you created are valid only for seven days; to recreate keys, start the process over from stage 1.**

5 Add the jetson to the Cluster

Text

```
cd /opt/ansible-installer-<Version>
./run-playbook.sh -i inventory/inventory.ini join-node-k3s.yml
```

For offline system run the command with "-t airgap" option

Text

```
cd /opt/ansible-installer-<Version>
./run-playbook.sh -i inventory/inventory.ini join-node-k3s.yml -t airgap
```

After the playbook is finished successfully, run the following command and make sure your new node is in the list:

Text

```
kubectl get nodes
```

Installation Wizard - Using the Vision AI Jetson

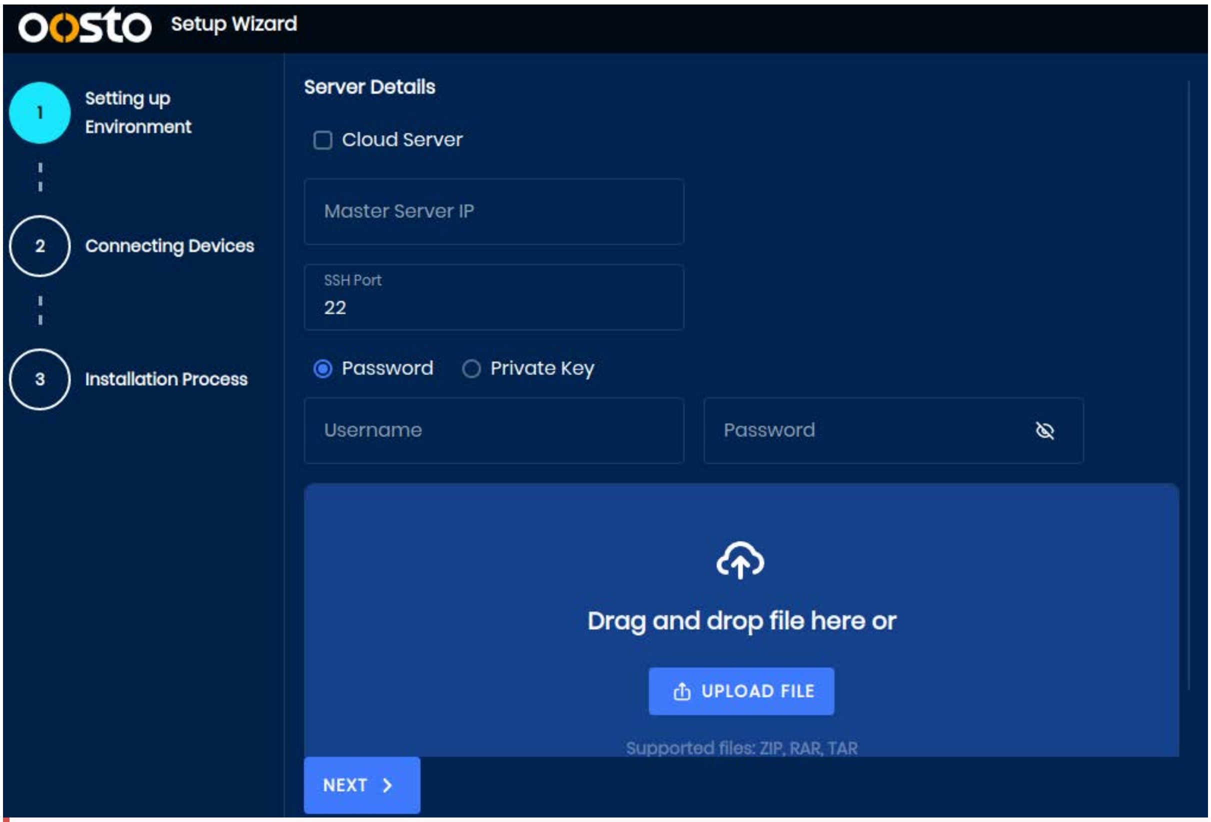
General and Prerequisites

Installation wizard provides a user to construct a cluster and install the edge devices in a relatively simple and straight forward way.
The Wizard enables to define both Jetson and non Jetson Edge appliances, associate them to a cluster and proceed to an installation of a pre-defined configured SW package.

> The following procedure is relevant for the quick installation process. The installer will be supplied by your Oosto delivery manager
> Please refer to the **Offline / Online installation** page if an advanced installation is required.

Step 1 - Setting up Environment

Define a master server, and click Next
For selecting a file on this step follow the instructions of Step 3



oosto Setup Wizard

1 Setting up Environment

2 Connecting Devices

3 Installation Process

Server Details

□ Cloud Server

Master Server IP

SSH Port: 22

● Password ○ Private Key

Username

Password

Drag and drop file here or

UPLOAD FILE

Supported files: ZIP, RAR, TAR

NEXT >

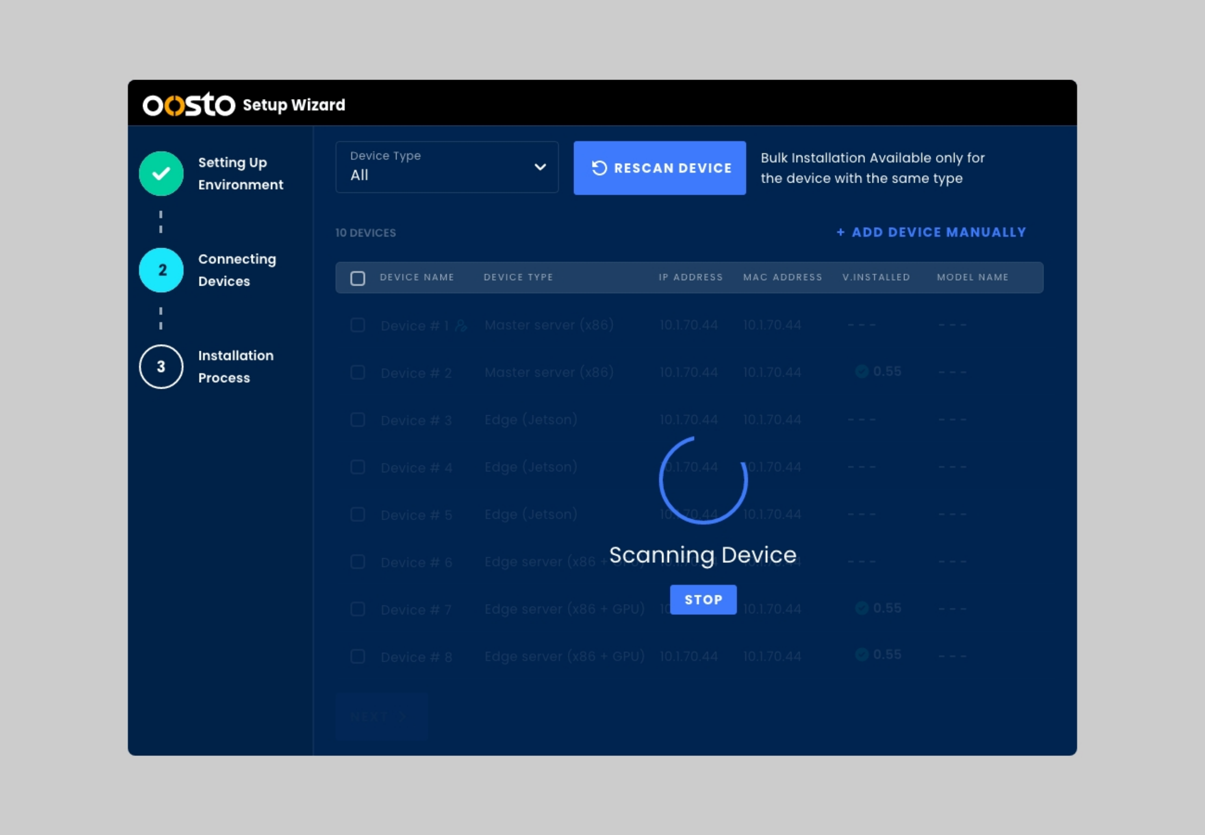
> ❗ **Prerequisites**
>
> Available master Server with credentials - and SSH installed
> Assigned IP address
> Available Username & Password / Private Key

Step 2 - Connecting Devices (Cluster Construction)

Automatic Discovery & Configuration

Once the master server is defined, the wizard scans automatically the network and discover the relevant devices for installation.

> 🚧 **Automatic Scan is currently available for Jetson type Edge appliances only, which were pre-installed with an ansible repository.**



oosto Setup Wizard

Device Type: All

Bulk Installation Available only for the device with the same type

10 DEVICES

DEVICE NAME	DEVICE TYPE	IP ADDRESS	MAC ADDRESS	V.INSTALLED	MODEL NAME
Device # 1	Master server (x86)	10.1.70.44	10.1.70.44	---	---
Device # 2	Master server (x86)	10.1.70.44	10.1.70.44	0.55	---
Device # 3	Edge (Jetson)	10.1.70.44	10.1.70.44	---	---
Device # 4	Edge (Jetson)	10.1.70.44	10.1.70.44	---	---
Device # 5	Edge (Jetson)	10.1.70.44	10.1.70.44	---	---
Device # 6	Edge server (x86 + GPU)		10.1.70.44	---	---
Device # 7	Edge server (x86 + GPU)	10.1.70.44	10.1.70.44	0.55	---
Device # 8	Edge server (x86 + GPU)	10.1.70.44	10.1.70.44	0.55	---

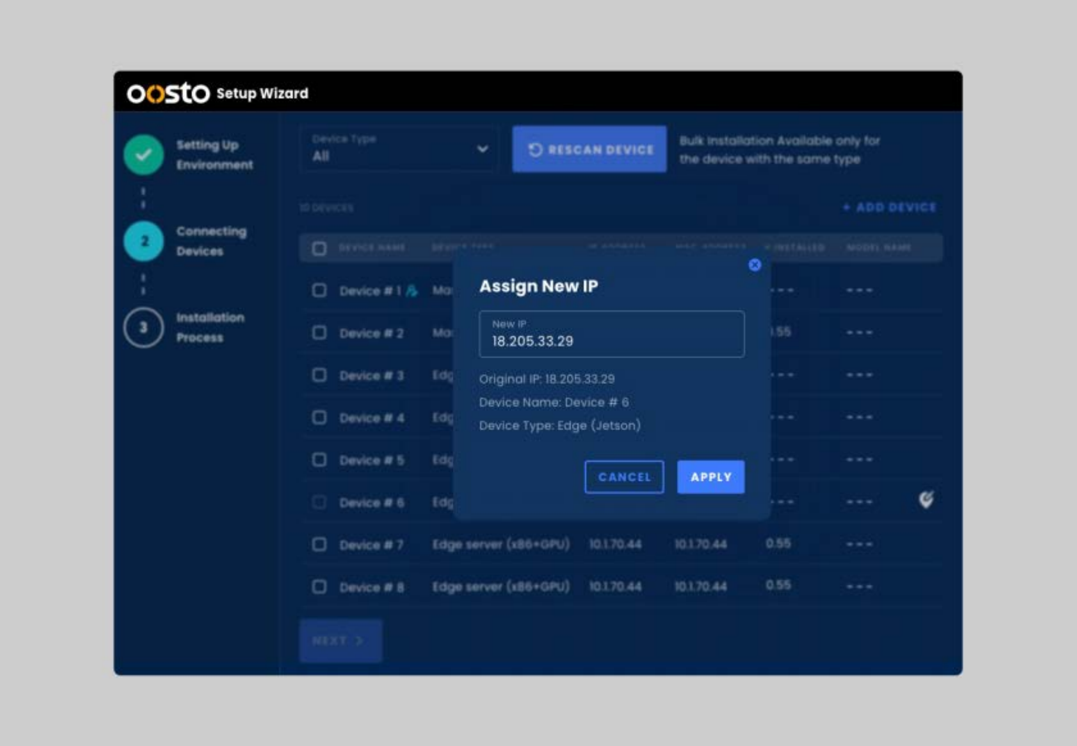
Scanning Device

For a DHCP supported Jetsons, the process will associate the Edge device with a valid IP address. However while non-DHCP Jetsons will still be discovered, the process will provide a generic non-valid IP address which then needs to be manually configured using the following process.

Manual configuration of Non-DHCP Jetson devices

Non-DHCP devices will be recognized using the small tool-tip on the right hand side of each raw (See Device#6 as an example)

By clicking the icon the following screen will appear in which the user will provide a valid IP address -



oosto Setup Wizard

Device Type: All

Bulk Installation Available only for the device with the same type

Assign New IP

New IP: 18.205.33.29

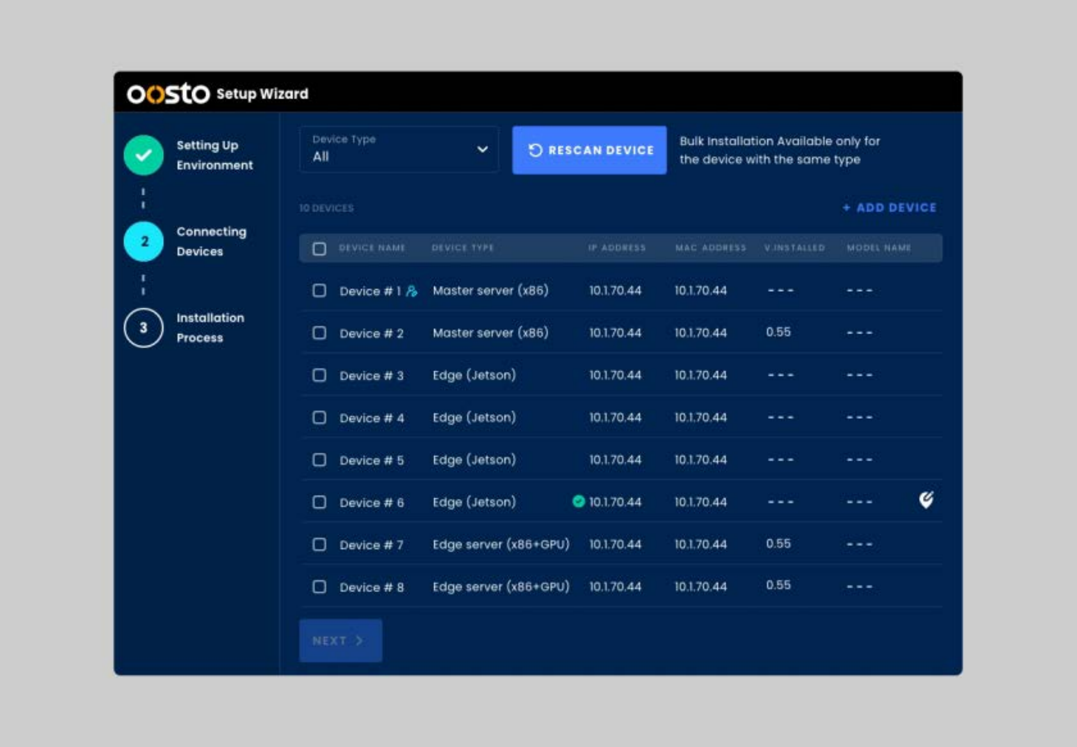
Original IP: 18.205.33.29

Device Name: Device # 6

Device Type: Edge (Jetson)

DEVICE NAME	DEVICE TYPE	IP ADDRESS	MAC ADDRESS	V.INSTALLED	MODEL NAME
Device # 7	Edge server (x86+GPU)	10.1.70.44	10.1.70.44	0.55	---
Device # 8	Edge server (x86+GPU)	10.1.70.44	10.1.70.44	0.55	---

IP assignment



oosto Setup Wizard

- ✓ Setting Up Environment
- 2 Connecting Devices
- 3 Installation Process

Device Type: All

RESCAN DEVICE

Bulk Installation Available only for the device with the same type

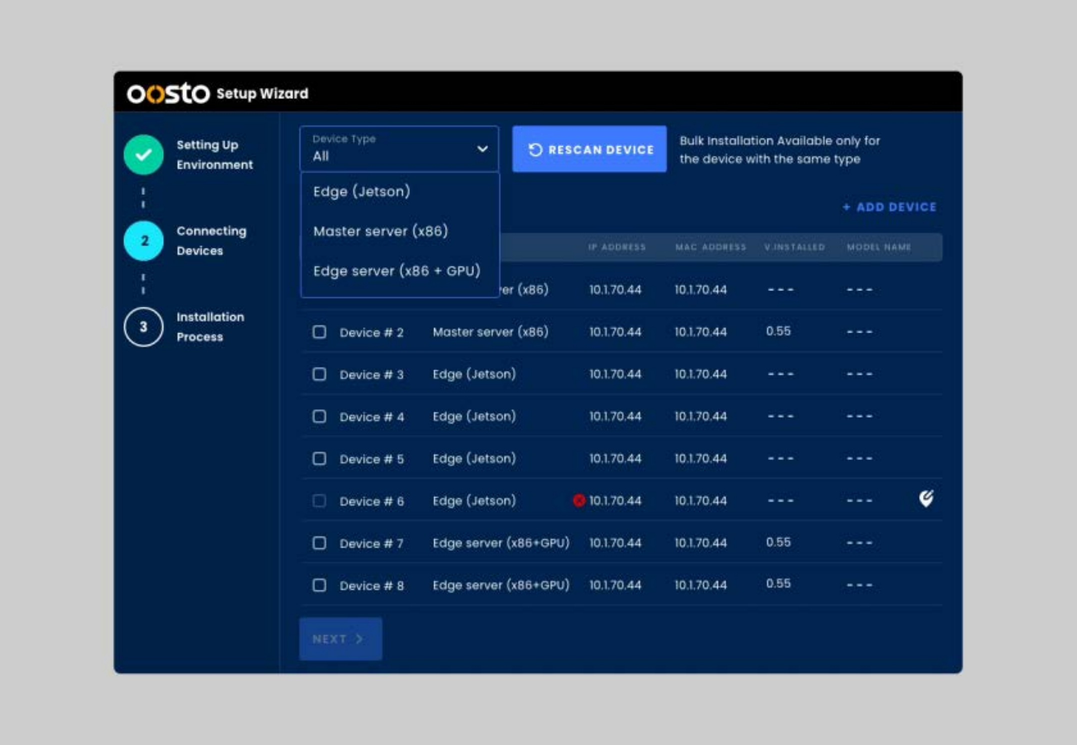
10 DEVICES

+ ADD DEVICE

☐	DEVICE NAME	DEVICE TYPE	IP ADDRESS	MAC ADDRESS	V.INSTALLED	MODEL NAME
☐	Device # 1	Master server (x86)	10.1.70.44	10.1.70.44	---	---
☐	Device # 2	Master server (x86)	10.1.70.44	10.1.70.44	0.55	---
☐	Device # 3	Edge (Jetson)	10.1.70.44	10.1.70.44	---	---
☐	Device # 4	Edge (Jetson)	10.1.70.44	10.1.70.44	---	---
☐	Device # 5	Edge (Jetson)	10.1.70.44	10.1.70.44	---	---
☐	Device # 6	Edge (Jetson)	✓ 10.1.70.44	10.1.70.44	---	---
☐	Device # 7	Edge server (x86+GPU)	10.1.70.44	10.1.70.44	0.55	---
☐	Device # 8	Edge server (x86+GPU)	10.1.70.44	10.1.70.44	0.55	---

NEXT >

Assignment succeeded



oosto Setup Wizard

- ✓ Setting Up Environment
- 2 Connecting Devices
- 3 Installation Process

Device Type: All

- Edge (Jetson)
- Master server (x86)
- Edge server (x86 + GPU)

RESCAN DEVICE

Bulk Installation Available only for the device with the same type

+ ADD DEVICE

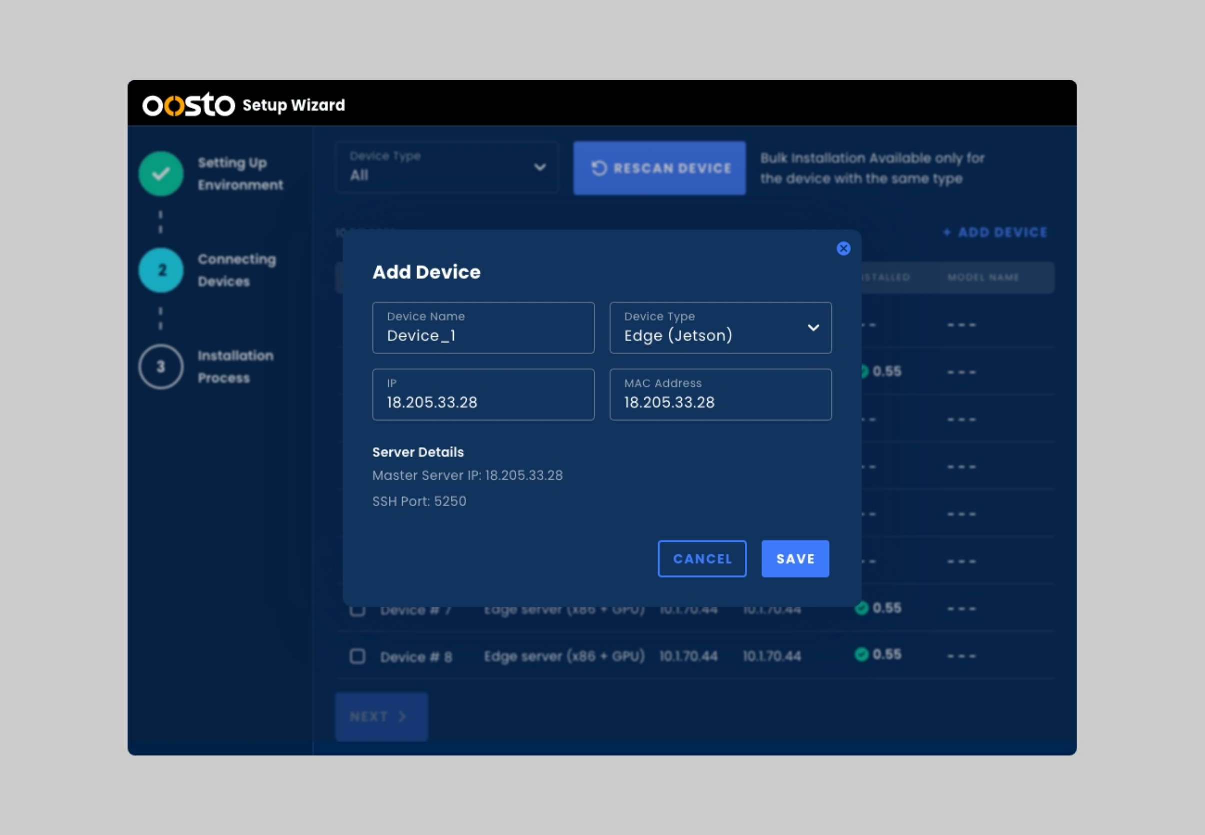
☐	DEVICE NAME	DEVICE TYPE	IP ADDRESS	MAC ADDRESS	V.INSTALLED	MODEL NAME
		er (x86)	10.1.70.44	10.1.70.44	---	---
☐	Device # 2	Master server (x86)	10.1.70.44	10.1.70.44	0.55	---
☐	Device # 3	Edge (Jetson)	10.1.70.44	10.1.70.44	---	---
☐	Device # 4	Edge (Jetson)	10.1.70.44	10.1.70.44	---	---
☐	Device # 5	Edge (Jetson)	10.1.70.44	10.1.70.44	---	---
☐	Device # 6	Edge (Jetson)	✗ 10.1.70.44	10.1.70.44	---	---
☐	Device # 7	Edge server (x86+GPU)	10.1.70.44	10.1.70.44	0.55	---
☐	Device # 8	Edge server (x86+GPU)	10.1.70.44	10.1.70.44	0.55	---

NEXT >

Assignment failed

Manual definition of devices

Non discoverable devices (such as additional Master servers and non-Jetson edge appliances) will be defined using the *ADD DEVICE* button on the top right corner of the screen



Device Type: All

Bulk Installation Available only for the device with the same type

Add Device

Device Name: Device_1

Device Type: Edge (Jetson)

IP: 18.205.33.28

MAC Address: 18.205.33.28

Server Details

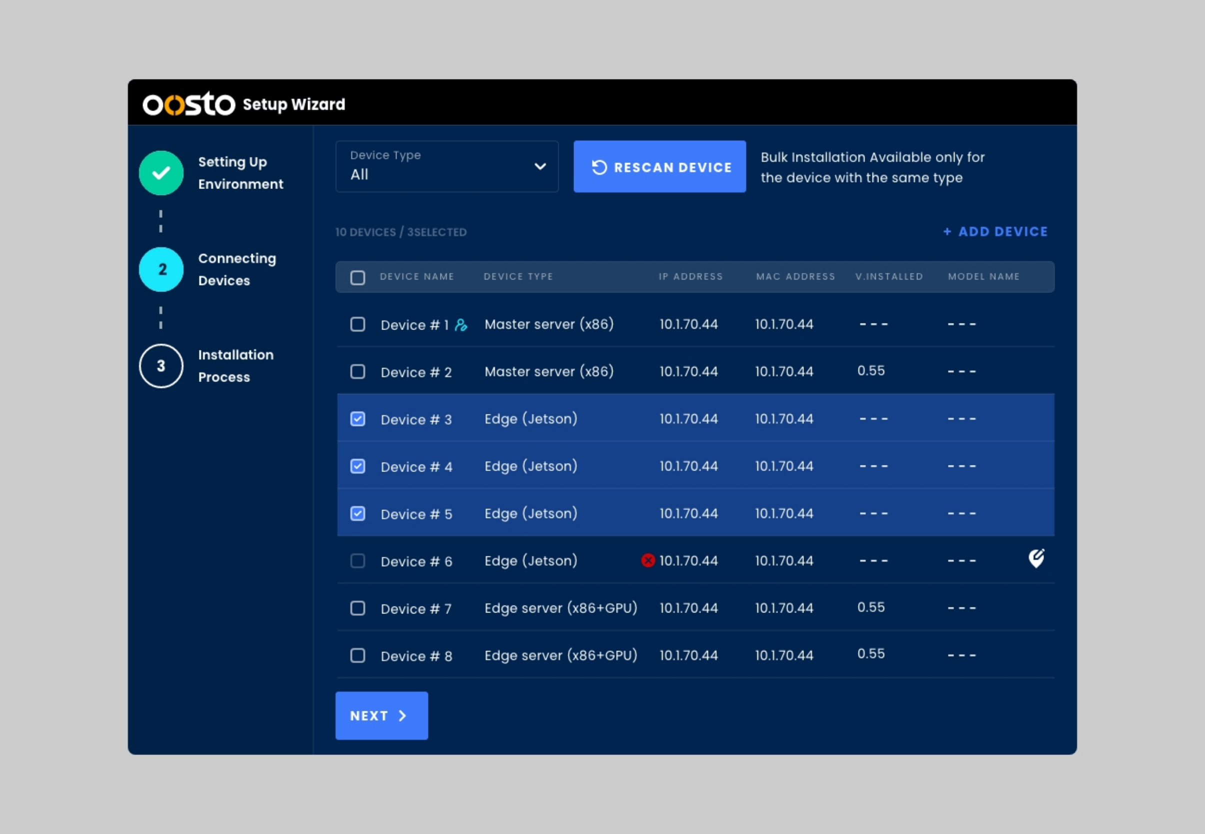
Master Server IP: 18.205.33.28

SSH Port: 5250

CANCEL SAVE

□ Device # 8 Edge server (x86 + GPU) 10.1.70.44 10.1.70.44 0.55 ---

Once a cluster was defined, the user can select one or more devices to install, by selecting the devices's checkboxes and click on *NEXT*



Device Type: All

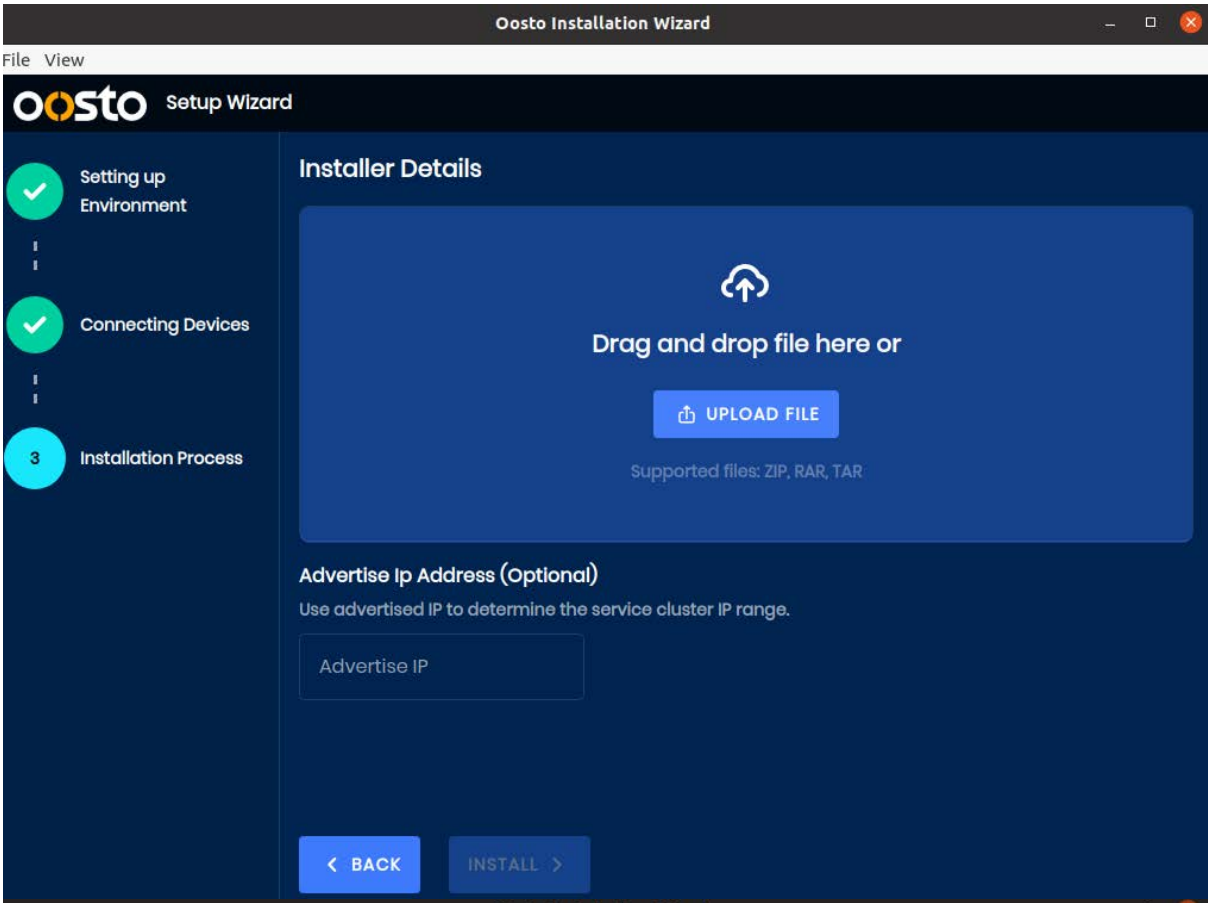
Bulk Installation Available only for the device with the same type

10 DEVICES / 3SELECTED

□	DEVICE NAME	DEVICE TYPE	IP ADDRESS	MAC ADDRESS	V.INSTALLED	MODEL NAME
□	Device # 1	Master server (x86)	10.1.70.44	10.1.70.44	---	---
□	Device # 2	Master server (x86)	10.1.70.44	10.1.70.44	0.55	---
☑	Device # 3	Edge (Jetson)	10.1.70.44	10.1.70.44	---	---
☑	Device # 4	Edge (Jetson)	10.1.70.44	10.1.70.44	---	---
☑	Device # 5	Edge (Jetson)	10.1.70.44	10.1.70.44	---	---
□	Device # 6	Edge (Jetson)	☒ 10.1.70.44	10.1.70.44	---	---
□	Device # 7	Edge server (x86+GPU)	10.1.70.44	10.1.70.44	0.55	---
□	Device # 8	Edge server (x86+GPU)	10.1.70.44	10.1.70.44	0.55	---

Step 3 - Package installation

Once devices were chosen for an installation - the next phase would be to choose the tar.gz package and start installation by clicking the *INSTALL* command button.
And choose advertise ip if desired (Only for All on one systems)



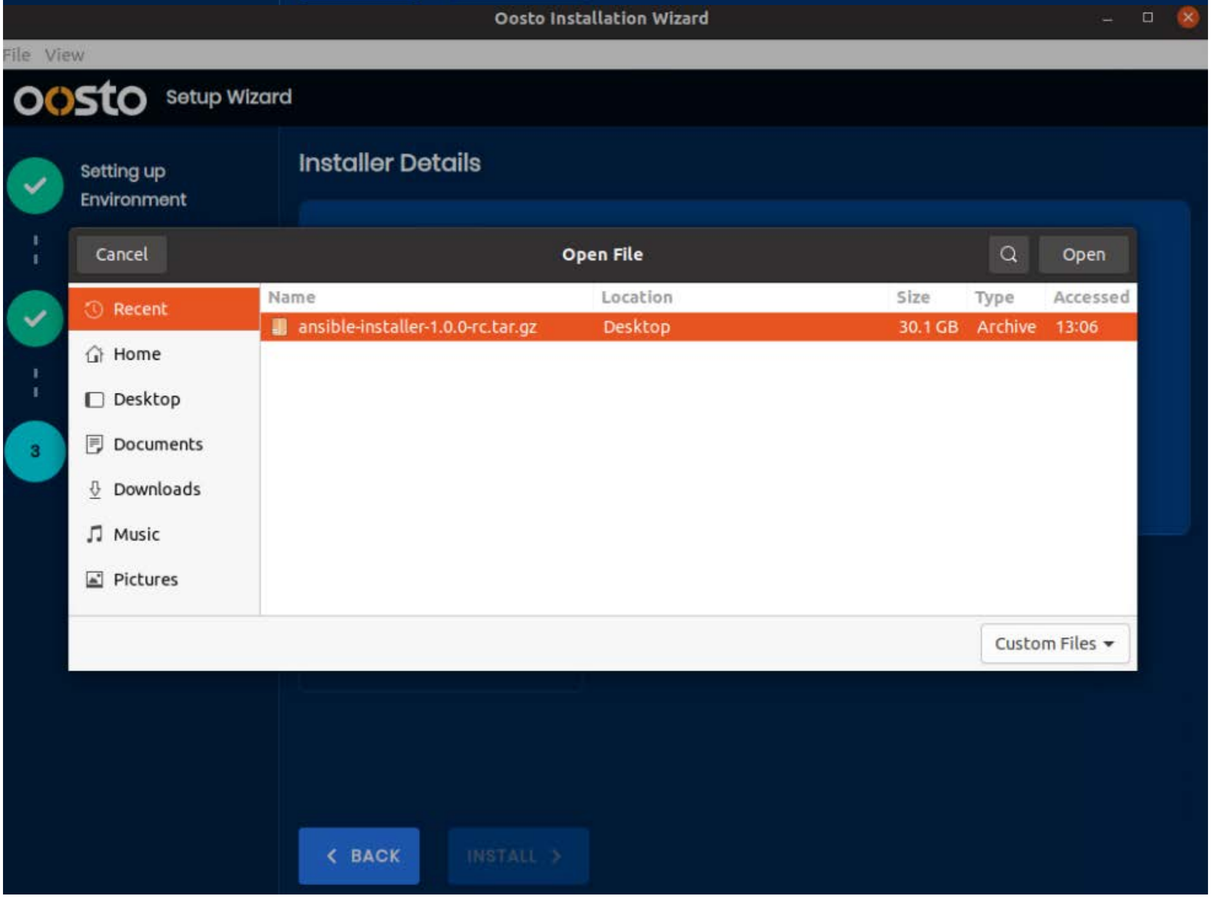
Installer Details

Drag and drop file here or

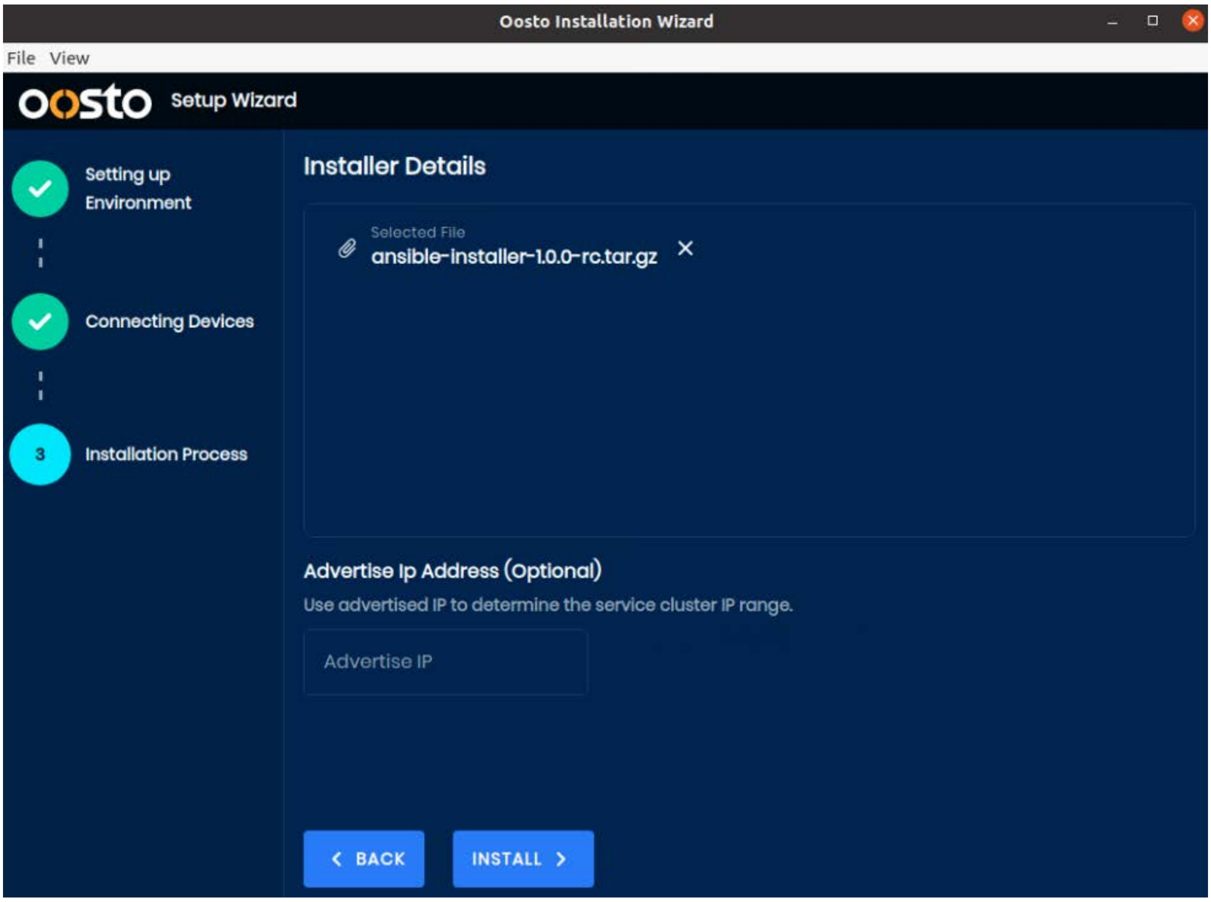
Supported files: ZIP, RAR, TAR

Advertise Ip Address (Optional)

Use advertised IP to determine the service cluster IP range.



Name	Location	Size	Type	Accessed
ansible-installer-1.0.0-rc.tar.gz	Desktop	30.1 GB	Archive	13:06



Installer Details

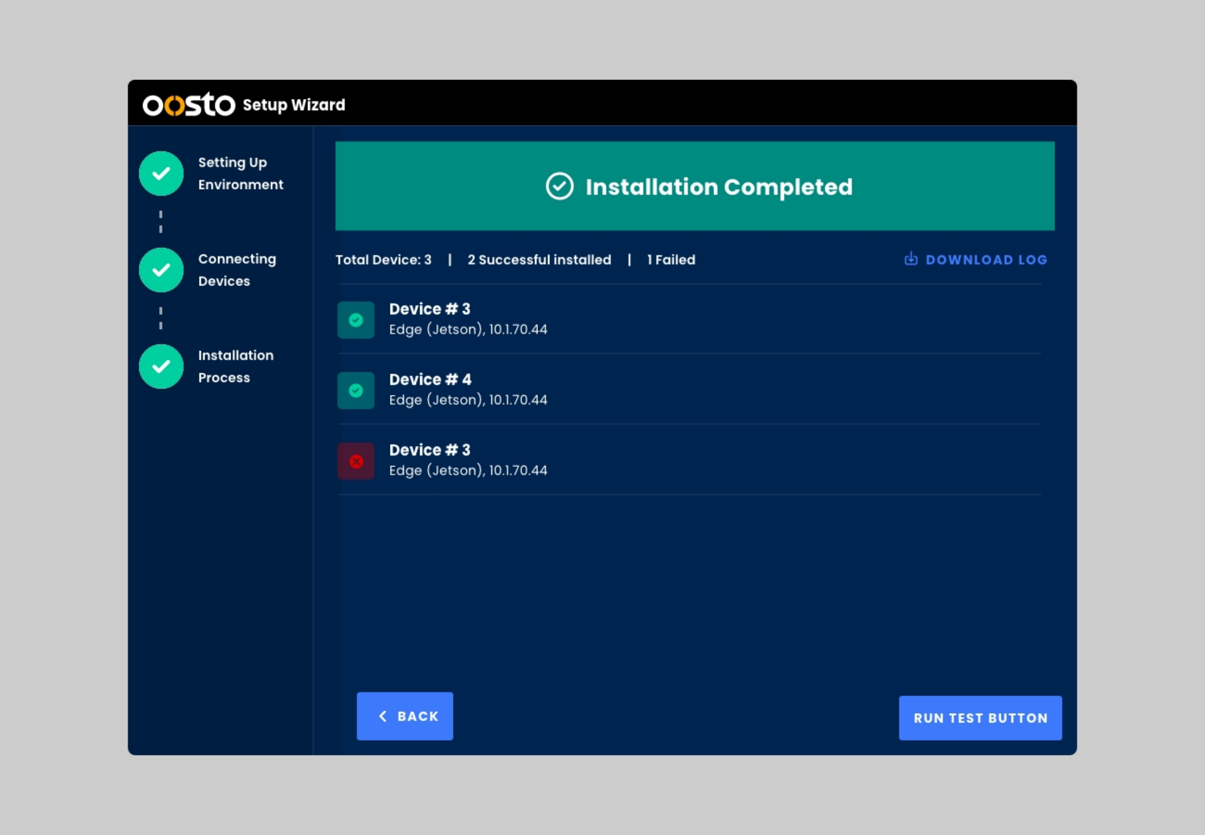
Selected File
ansible-installer-1.0.0-rc.tar.gz ✕

Advertise Ip Address (Optional)

Use advertised IP to determine the service cluster IP range.

Advertise IP

An installation process monitoring will present the status. When installation phase is finished a summary display will be presented.



Installation Completed

Total Device: 3 | 2 Successful installed | 1 Failed

Device # 3
Edge (Jetson), 10.1.70.44

Device # 4
Edge (Jetson), 10.1.70.44

Device # 3
Edge (Jetson), 10.1.70.44

Upgrade Paths

Oosto OnWatch can be upgraded to 2.6.x directly from baseline version 2.5.x.

> 🚧 In case your OnWatch is on a lower version please contact your Ooosto representative to discuss your upgrade path.

Upgrade 2.5.0-x - 2.6.x-y

1. Download Ansible Installer Updated Files

Before updating the ansible installer files, save your existing inventory.ini so the new download won't run it over:

Text

```
mv /opt/ansible-installer-<VERSION>/inventory/inventory.ini /opt/
```

Let's run the ansible-downloader to update the existing files:

> 🚧 **Note**
>
> Please change the line below with the latest (or relevant) installer version: https://oosto-public-scripts.s3.eu-central-1.amazonaws.com/ansible-downloader/INSTALLER_VERSION/ansible-downloader.sh
>
> ** Make sure the key.txt file is located in the same directory you're running the oneliner from

Text

```
wget -qO- https://oosto-public-scripts.s3.eu-central-1.amazonaws.com/ansible-downloader/1.2.4-8/ansible-
```

If your key.txt is located in another path, use --cred-path KEY_PATH, example:

Text

```
wget -qO- https://oosto-public-scripts.s3.eu-central-1.amazonaws.com/ansible-downloader/1.2.4-8/ansible-
```

*Ansible files will be downloaded into /opt/ansible-installer-

Now let's bring back the original inventory.ini:

Text

```
mv /opt/inventory.ini /opt/ansible-installer-<VERSION>/inventory/
```

2. Download Product's New Packages

Edit the inventory/inventory.ini file with the following:

- First, change your working directory to the ansible-installer directory:

Text

```
cd /opt/ansible-installer-<VERSION>
```

- Edit the inventory/inventory.ini file using your preferred editor (Vim, nano, etc.).
- Set product_version to the new version you wish to upgrade to.
- Note that under inventory/product-versions/onwatch-2.6.x-y.yml (the file name of the new version), every layer that is enabled will be “count“ in the upgrade flow. Therefor, if you wish to skip or ignore from one of the layers, please change it to enable: no.
- Comment out the master’s line under [main_master] and all other node groups values (in case it’s an existing cluster).

> 📘 **Clarification**
>
> If the cluster isn’t AIO, make sure to comment out all existing nodes in the inventory

- Comment the line under [download_machine] section:

Text

```
[download_machine]
download1 ansible_host=localhost ansible_connection=local
```

- Run the packages download:

Text

```
./run-playbook.sh -i inventory/inventory.ini install-k3s.yml -t download
```

3. Upgrade From 2.x.x-x To 2.y.y-y

Remove the layers and re-install with the new version:

- Comment back the master’s line under [main_master] with the machine name and it’s internal IP - as it was before

> 🚧 **Note**
>
> The following step will delete the all existing layers and re-install with the version you downloaded and mentioned in the inventory.ini, under product_version

Run the product upgrade:

Text

```
./run-playbook.sh -i inventory/inventory.ini product-upgrade.yml
```

END OF UPGRADE
*N**OT PART OF THE INSTALLATION**
In order to remove/install specific layers, use -t remove-LAYER_NAME and / or -t install-LAYER_NAME with one of the following options:

Tag	Purpose
remove-layers	Remove all the layers
install-layers	Installing all the layers
remove-data, remove-init, remove-app, remove-hq-plugin	Options to remove layer by layer (see example below)
install-data, install-init, install-app, install-hq-plugin	Options to install layer by layer (see example below)

For example to remove with specific tags:

Text

```
./run-playbook.sh -i inventory/inventory.ini product-upgrade.yml -t remove-init,remove-app
```

Or to install:

Text

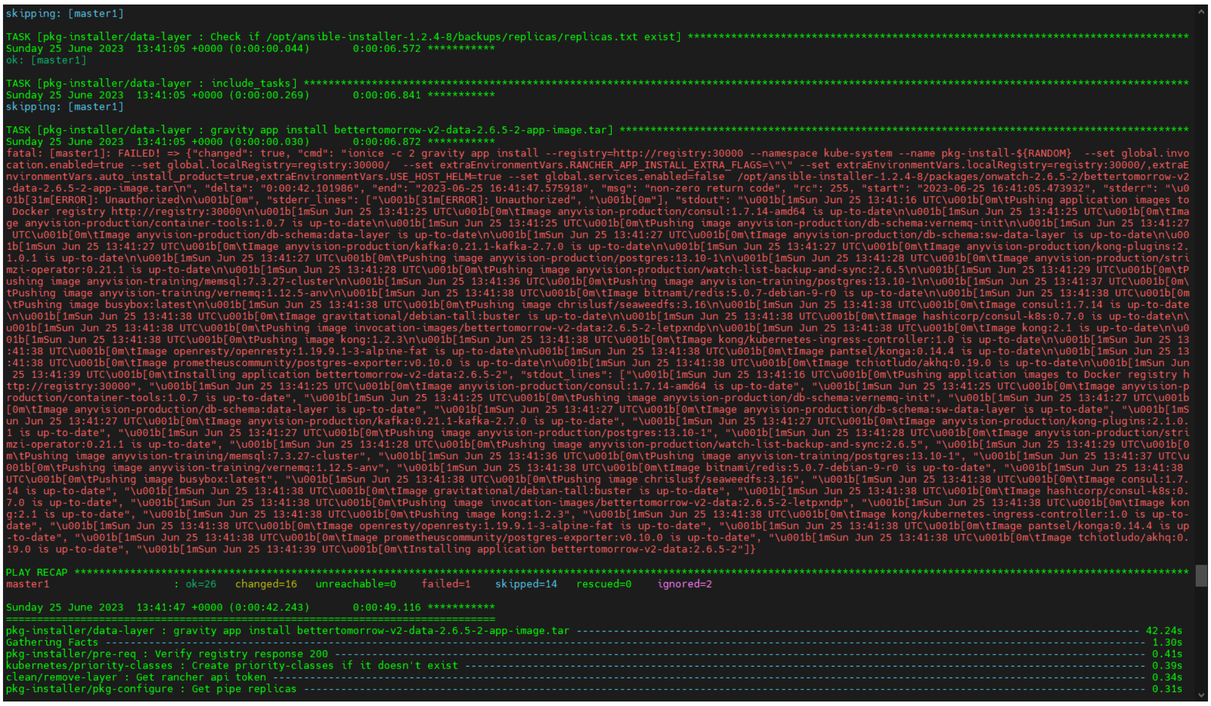
```
./run-playbook.sh -i inventory/inventory.ini product-upgrade.yml -t install-app
```

To delete or install all layers, run:

Text

```
./run-playbook.sh -i inventory/inventory.ini product-upgrade.yml -t remove-layers
```

Known Issue



```
skipping: [master1]

TASK [pkg-installer/data-layer : Check if /opt/ansible-installer-1.2.4-8/backups/replicas/replicas.txt exist] ***************************************************************************
Sunday 25 June 2023  13:41:05 +0000 (0:00:00.044)       0:00:06.572 ***********
ok: [master1]

TASK [pkg-installer/data-layer : include_tasks] *********************************************************************************************************************************************
Sunday 25 June 2023  13:41:05 +0000 (0:00:00.269)       0:00:06.841 ***********
skipping: [master1]

TASK [pkg-installer/data-layer : gravity app install bettertomorrow-v2-data-2.6.5-2-app-image.tar] *************************************************************************************
Sunday 25 June 2023  13:41:05 +0000 (0:00:00.030)       0:00:06.872 ***********
fatal: [master1]: FAILED! => {"changed": true, "cmd": "ionice -c 2 gravity app install --registry=http://registry:30000 --namespace kube-system --name pkg-install-${RANDOM}  --set global.invo
cation.enabled=true --set global.localRegistry=registry:30000/  --set extraEnvironmentVars.RANCHER_APP_INSTALL_EXTRA_FLAGS=\"\" --set extraEnvironmentVars.localRegistry=registry:30000/,extraE
nvironmentVars.auto_install_product=true,extraEnvironmentVars.USE_HOST_HELM=true --set global.services.enabled=false  /opt/ansible-installer-1.2.4-8/packages/onwatch-2.6.5-2/bettertomorrow-v2
-data-2.6.5-2-app-image.tar\n", "delta": "0:00:42.101986", "end": "2023-06-25 16:41:47.575918", "msg": "non-zero return code", "rc": 255, "start": "2023-06-25 16:41:05.473932", "stderr": "\u0
01b[31m[ERROR]: Unauthorized\n\u001b[0m", "stderr_lines": ["\u001b[31m[ERROR]: Unauthorized", "\u001b[0m"], "stdout": "\u001b[1mSun Jun 25 13:41:16 UTC\u001b[0m\tPushing application images to
 Docker registry http://registry:30000\n\u001b[1mSun Jun 25 13:41:25 UTC\u001b[0m\tImage anyvision-production/consul:1.7.14-amd64 is up-to-date\n\u001b[1mSun Jun 25 13:41:25 UTC\u001b[0m\tIma
ge anyvision-production/container-tools:1.0.7 is up-to-date\n\u001b[1mSun Jun 25 13:41:25 UTC\u001b[0m\tPushing image anyvision-production/db-schema:vernemq-init\n\u001b[1mSun Jun 25 13:41:27
 UTC\u001b[0m\tImage anyvision-production/db-schema:data-layer is up-to-date\n\u001b[1mSun Jun 25 13:41:27 UTC\u001b[0m\tImage anyvision-production/db-schema:sw-data-layer is up-to-date\n\u00
1b[1mSun Jun 25 13:41:27 UTC\u001b[0m\tImage anyvision-production/kafka:0.21.1-kafka-2.7.0 is up-to-date\n\u001b[1mSun Jun 25 13:41:27 UTC\u001b[0m\tImage anyvision-production/kong-plugins:2.
1.0.1 is up-to-date\n\u001b[1mSun Jun 25 13:41:27 UTC\u001b[0m\tPushing image anyvision-production/postgres:13.10-1\n\u001b[1mSun Jun 25 13:41:28 UTC\u001b[0m\tImage anyvision-production/stri
mzi-operator:0.21.1 is up-to-date\n\u001b[1mSun Jun 25 13:41:28 UTC\u001b[0m\tPushing image anyvision-production/watch-list-backup-and-sync:2.6.5\n\u001b[1mSun Jun 25 13:41:29 UTC\u001b[0m\tP
ushing image anyvision-training/memsql:7.3.27-cluster\n\u001b[1mSun Jun 25 13:41:36 UTC\u001b[0m\tPushing image anyvision-training/postgres:13.10-1\n\u001b[1mSun Jun 25 13:41:37 UTC\u001b[0m\
tPushing image anyvision-training/vernemq:1.12.5-anv\n\u001b[1mSun Jun 25 13:41:38 UTC\u001b[0m\tImage bitnami/redis:5.0.7-debian-9-r0 is up-to-date\n\u001b[1mSun Jun 25 13:41:38 UTC\u001b[0m
\tPushing image busybox:latest\n\u001b[1mSun Jun 25 13:41:38 UTC\u001b[0m\tPushing image chrislusf/seaweedfs:3.16\n\u001b[1mSun Jun 25 13:41:38 UTC\u001b[0m\tImage consul:1.7.14 is up-to-date
\n\u001b[1mSun Jun 25 13:41:38 UTC\u001b[0m\tImage gravitational/debian-tall:buster is up-to-date\n\u001b[1mSun Jun 25 13:41:38 UTC\u001b[0m\tImage hashicorp/consul-k8s:0.7.0 is up-to-date\n\
u001b[1mSun Jun 25 13:41:38 UTC\u001b[0m\tPushing image invocation-images/bettertomorrow-v2-data:2.6.5-2-letpxndp\n\u001b[1mSun Jun 25 13:41:38 UTC\u001b[0m\tImage kong:2.1 is up-to-date\n\u0
01b[1mSun Jun 25 13:41:38 UTC\u001b[0m\tPushing image kong:1.2.3\n\u001b[1mSun Jun 25 13:41:38 UTC\u001b[0m\tImage kong/kubernetes-ingress-controller:1.0 is up-to-date\n\u001b[1mSun Jun 25 13
:41:38 UTC\u001b[0m\tImage openresty/openresty:1.19.9.1-3-alpine-fat is up-to-date\n\u001b[1mSun Jun 25 13:41:38 UTC\u001b[0m\tImage pantsel/konga:0.14.4 is up-to-date\n\u001b[1mSun Jun 25 13
:41:38 UTC\u001b[0m\tImage prometheuscommunity/postgres-exporter:v0.10.0 is up-to-date\n\u001b[1mSun Jun 25 13:41:38 UTC\u001b[0m\tImage tchiotludo/akhq:0.19.0 is up-to-date\n\u001b[1mSun Jun
 25 13:41:39 UTC\u001b[0m\tInstalling application bettertomorrow-v2-data:2.6.5-2", "stdout_lines": ["\u001b[1mSun Jun 25 13:41:16 UTC\u001b[0m\tPushing application images to Docker registry h
ttp://registry:30000", "\u001b[1mSun Jun 25 13:41:25 UTC\u001b[0m\tImage anyvision-production/consul:1.7.14-amd64 is up-to-date", "\u001b[1mSun Jun 25 13:41:25 UTC\u001b[0m\tImage anyvision-p
roduction/container-tools:1.0.7 is up-to-date", "\u001b[1mSun Jun 25 13:41:25 UTC\u001b[0m\tPushing image anyvision-production/db-schema:vernemq-init", "\u001b[1mSun Jun 25 13:41:27 UTC\u001b
[0m\tImage anyvision-production/db-schema:data-layer is up-to-date", "\u001b[1mSun Jun 25 13:41:27 UTC\u001b[0m\tImage anyvision-production/db-schema:sw-data-layer is up-to-date", "\u001b[1mS
un Jun 25 13:41:27 UTC\u001b[0m\tImage anyvision-production/kafka:0.21.1-kafka-2.7.0 is up-to-date", "\u001b[1mSun Jun 25 13:41:27 UTC\u001b[0m\tImage anyvision-production/kong-plugins:2.1.0.
1 is up-to-date", "\u001b[1mSun Jun 25 13:41:27 UTC\u001b[0m\tPushing image anyvision-production/postgres:13.10-1", "\u001b[1mSun Jun 25 13:41:28 UTC\u001b[0m\tImage anyvision-production/stri
mzi-operator:0.21.1 is up-to-date", "\u001b[1mSun Jun 25 13:41:28 UTC\u001b[0m\tPushing image anyvision-production/watch-list-backup-and-sync:2.6.5", "\u001b[1mSun Jun 25 13:41:29 UTC\u001b[0
m\tPushing image anyvision-training/memsql:7.3.27-cluster", "\u001b[1mSun Jun 25 13:41:36 UTC\u001b[0m\tPushing image anyvision-training/postgres:13.10-1", "\u001b[1mSun Jun 25 13:41:37 UTC\u
001b[0m\tPushing image anyvision-training/vernemq:1.12.5-anv", "\u001b[1mSun Jun 25 13:41:38 UTC\u001b[0m\tImage bitnami/redis:5.0.7-debian-9-r0 is up-to-date", "\u001b[1mSun Jun 25 13:41:38
UTC\u001b[0m\tPushing image busybox:latest", "\u001b[1mSun Jun 25 13:41:38 UTC\u001b[0m\tPushing image chrislusf/seaweedfs:3.16", "\u001b[1mSun Jun 25 13:41:38 UTC\u001b[0m\tImage consul:1.7.
14 is up-to-date", "\u001b[1mSun Jun 25 13:41:38 UTC\u001b[0m\tImage gravitational/debian-tall:buster is up-to-date", "\u001b[1mSun Jun 25 13:41:38 UTC\u001b[0m\tImage hashicorp/consul-k8s:0.
7.0 is up-to-date", "\u001b[1mSun Jun 25 13:41:38 UTC\u001b[0m\tPushing image invocation-images/bettertomorrow-v2-data:2.6.5-2-letpxndp", "\u001b[1mSun Jun 25 13:41:38 UTC\u001b[0m\tImage kon
g:2.1 is up-to-date", "\u001b[1mSun Jun 25 13:41:38 UTC\u001b[0m\tPushing image kong:1.2.3", "\u001b[1mSun Jun 25 13:41:38 UTC\u001b[0m\tImage kong/kubernetes-ingress-controller:1.0 is up-to-
date", "\u001b[1mSun Jun 25 13:41:38 UTC\u001b[0m\tImage openresty/openresty:1.19.9.1-3-alpine-fat is up-to-date", "\u001b[1mSun Jun 25 13:41:38 UTC\u001b[0m\tImage pantsel/konga:0.14.4 is up
-to-date", "\u001b[1mSun Jun 25 13:41:38 UTC\u001b[0m\tImage prometheuscommunity/postgres-exporter:v0.10.0 is up-to-date", "\u001b[1mSun Jun 25 13:41:38 UTC\u001b[0m\tImage tchiotludo/akhq:0.
19.0 is up-to-date", "\u001b[1mSun Jun 25 13:41:39 UTC\u001b[0m\tInstalling application bettertomorrow-v2-data:2.6.5-2"]}

PLAY RECAP ******************************************************************************************************************************************************************************
master1                    : ok=26   changed=16   unreachable=0    failed=1    skipped=14   rescued=0    ignored=2

Sunday 25 June 2023  13:41:47 +0000 (0:00:42.243)       0:00:49.116 ***********
===============================================================================
pkg-installer/data-layer : gravity app install bettertomorrow-v2-data-2.6.5-2-app-image.tar ---------------------------------------------------------------------------------- 42.24s
Gathering Facts ---------------------------------------------------------------------------------------------------------------------------------------------------------------- 1.30s
pkg-installer/pre-req : Verify registry response 200 ------------------------------------------------------------------------------------------------------------------------- 0.41s
kubernetes/priority-classes : Create priority-classes if it doesn't exist ---------------------------------------------------------------------------------------------------- 0.39s
clean/remove-layer : Get rancher api token ----------------------------------------------------------------------------------------------------------------------------------- 0.34s
pkg-installer/pkg-configure : Get pipe replicas ------------------------------------------------------------------------------------------------------------------------------ 0.31s
```

```
gravity app install - Error: Unauthorized
```

This problem seems to happen when 'helm' cannot reach the k3s cluster - mainly because old certificate.
To identify it try to run the following command - should return 'Error: Unauthorized'

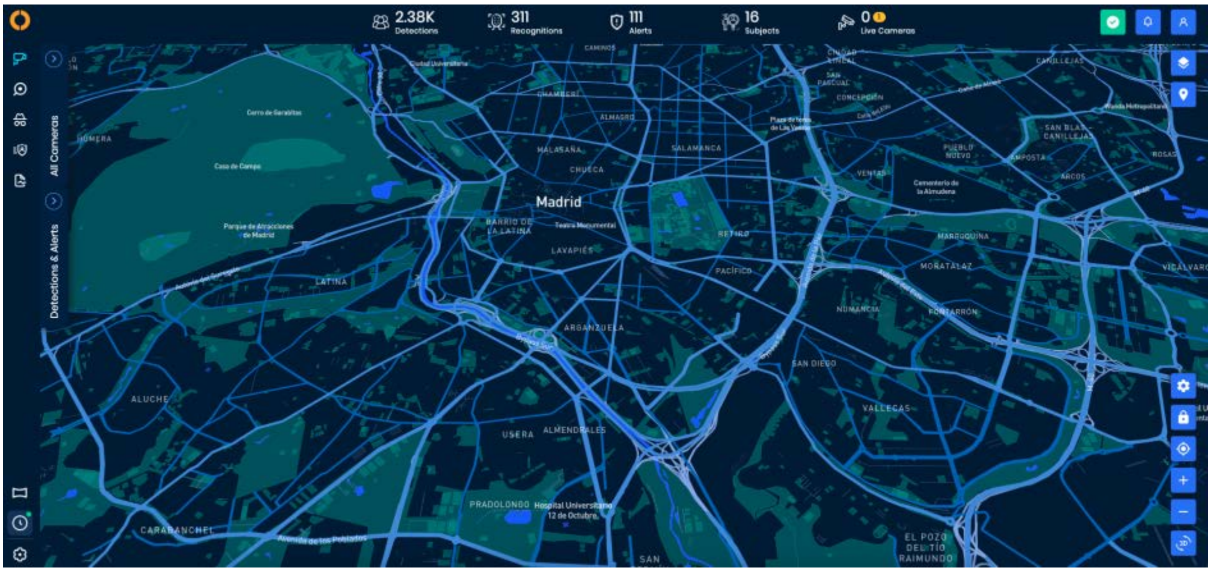
```
helm ls
```

To solve this problem run the following command:

```
cp /etc/rancher/k3s/k3s.yaml /root/.kube/config
```

Site Manual

Dashboard Navigation



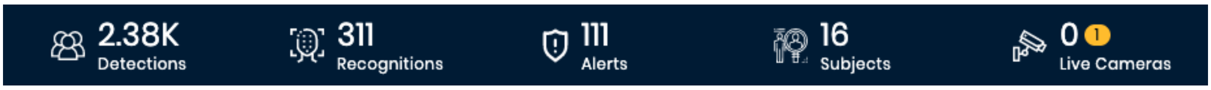
The OnWatch dashboard is comprised of 6 tabs, which are visible on the left side of the screen. The tabs are:

- Live Cameras & Cases (default)
- Search
- Inquiry
- Watch List
- Reports
- Video Wall
- Ongoing Actions
- Settings

> ### 🚧 Available Tabs Depend on Your Role and Licensing
>
> Based on Licensing and Role you were assigned by the system administrator, you may not see all the tabs. If you'd like to access a tab that is not visible for you, please contact your system administrator.
>
> For more information on user roles, click here.

In addition to the navigation tab, the map displayed on the main dashboard provides users with the ability to get an overall view of the location of cameras used by their organization.

Status Bar Overview



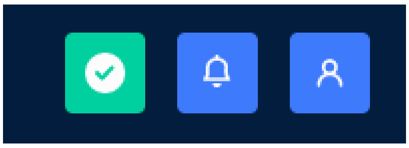
On the top of the dashboard screen, real-time information, statistics, system monitoring status, system notifications and user settings are available.

From this top border, viewers can immediately see statistics according to the role they are assigned:

- The current amount of detections in the system

- The number of sent alerts from the system
- The number of subjects on the watch list
- The number of live cameras with an orange dot that reflect the number of reconnecting cameras.

The top bar also consists of a system status icon that informs the user when there is an internal issue within the system. When the system is not experiencing any internal issues, the system notifications icon will be green. If there is an internal issue, the icon will be shown in red. Clicking on the **system status icon** will show a drop down with all the services also allowing logs to be downloaded.



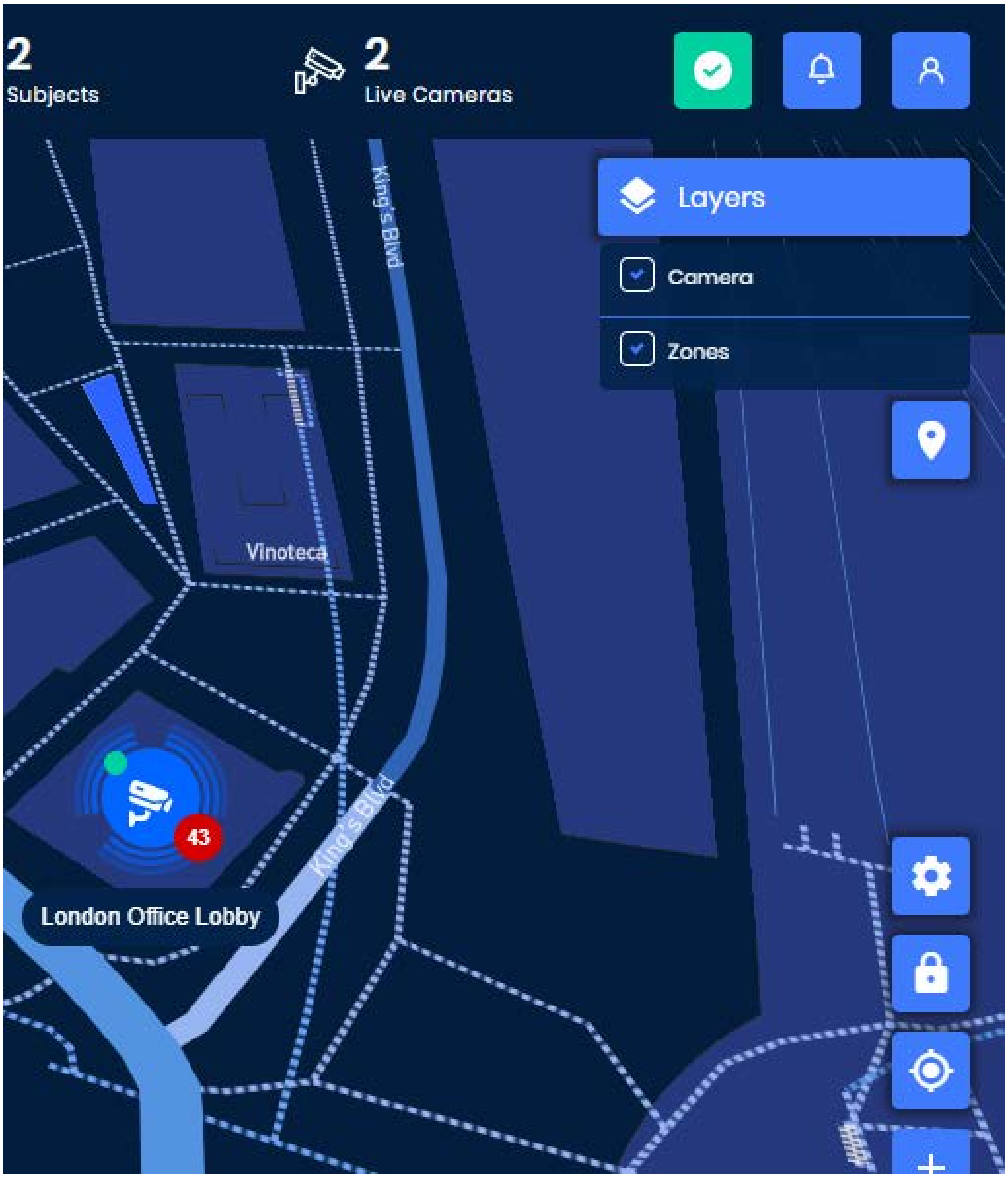
Next to this, a bell icon lists all the notifications that have not been viewed yet by the user. Simply click the **bell icon** to view the list of system notifications.

Lastly, a **user settings** option is available for the user to access their profile, view the end-user licensing agreement and log out of the system.

See Status Bar Controls

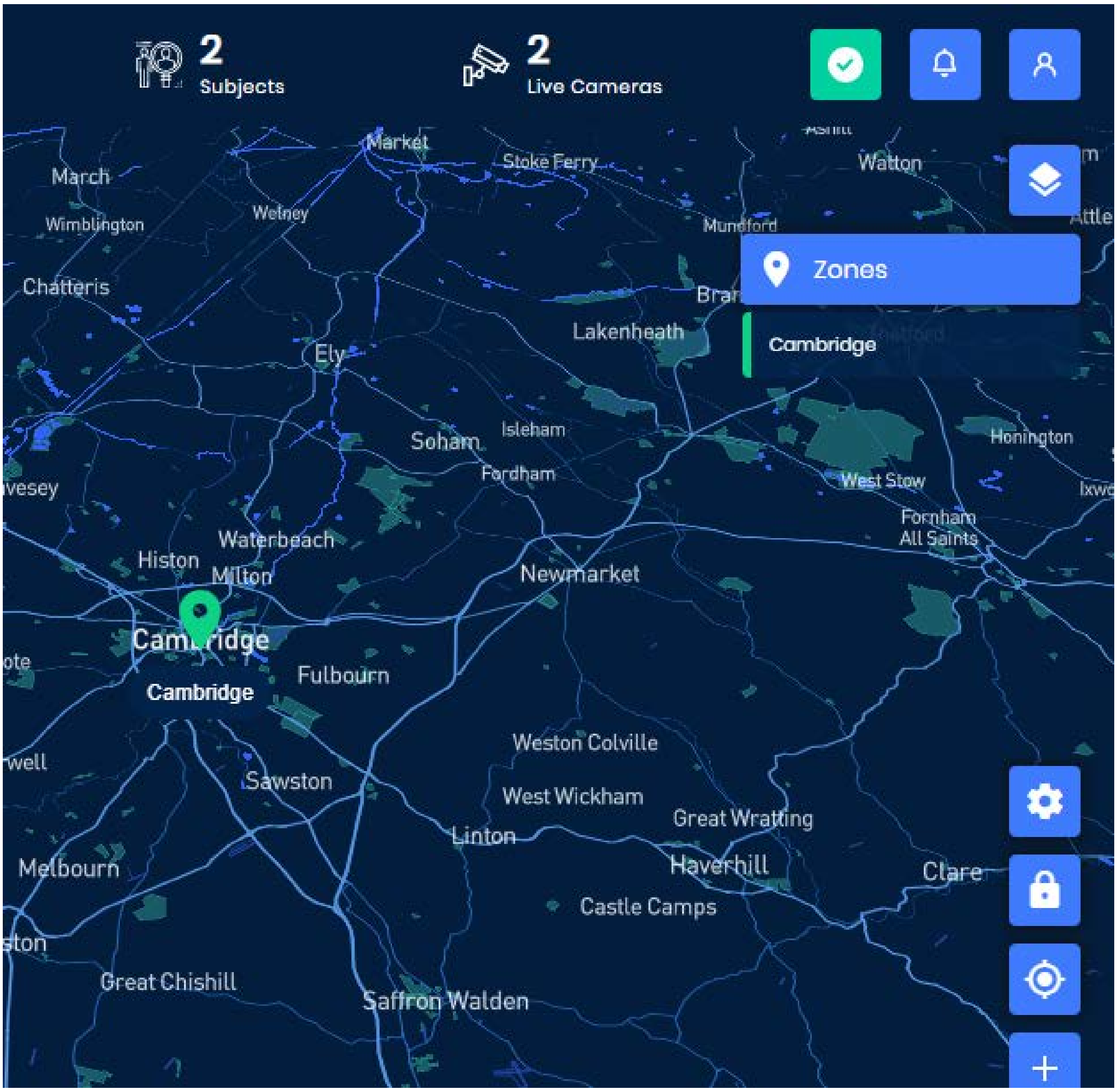
Map Controls

On the far right side of the main dashboard, several icons are displayed.
##Layers
Clicking on the **layers icon** allows you to set the map display according to camera or according to a zone. The world map can be overlaid with specific cameras, or simply with pins indicating zones where cameras are located.



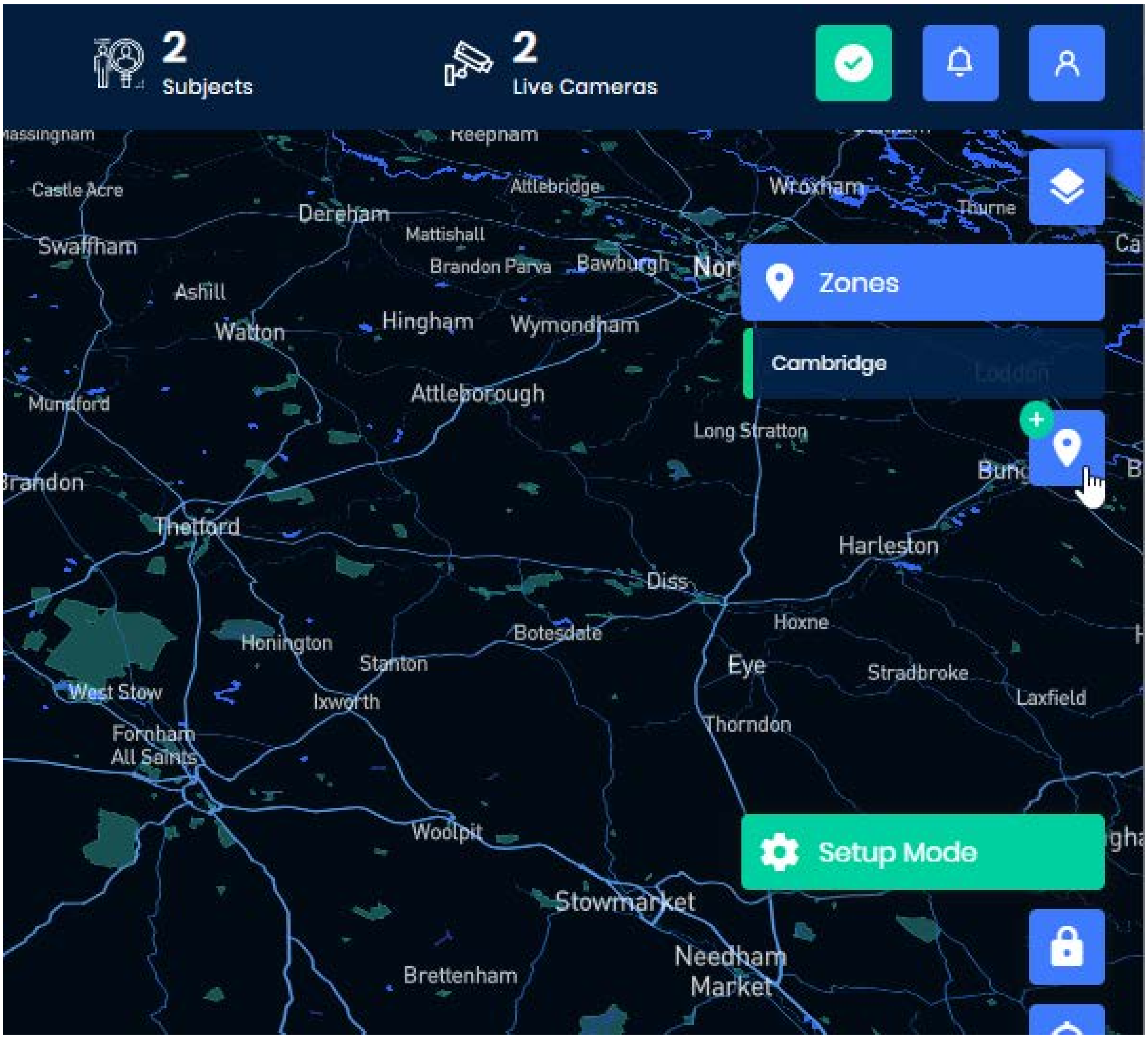
Zones

Clicking on the **zones icon** allows you to quickly navigate a map according to zones. Let's say you are monitoring two separate locations. Instead of zooming in and out and navigating the mouse to move between them, you can automatically go to whichever zone you need by clicking the icon and then selecting your desired location. The map will then refocus there automatically.

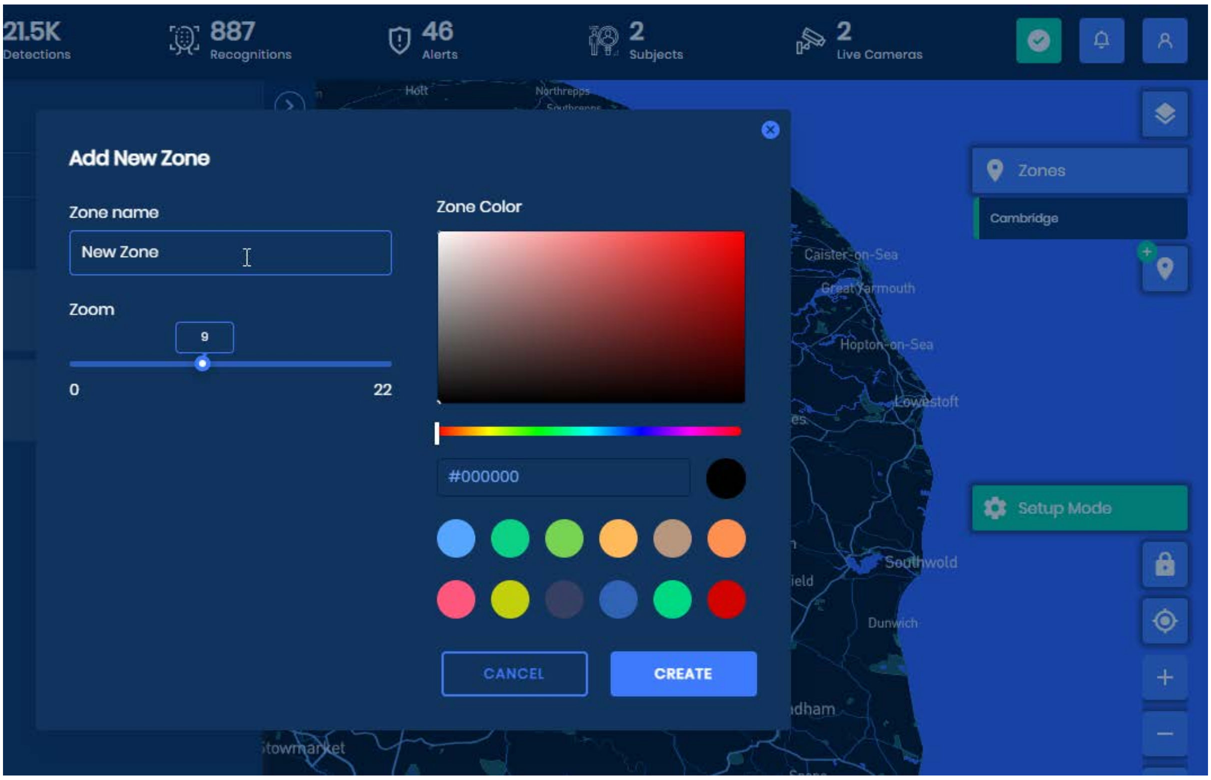


Setup Mode

Clicking on the **setup mode icon** allows you to add another zone to the map or edit an existing zone. When you are in the setup mode, the tab will turn green, and a new icon will appear underneath zones with a plus sign at the top.



Clicking on the **add zone icon** will allow you to drop a pin on the desired map location, and then a pop-up will appear for you to enter the new zone's details.



Add New Zone

Zone name

New Zone

Zoom

9

0 22

Zone Color

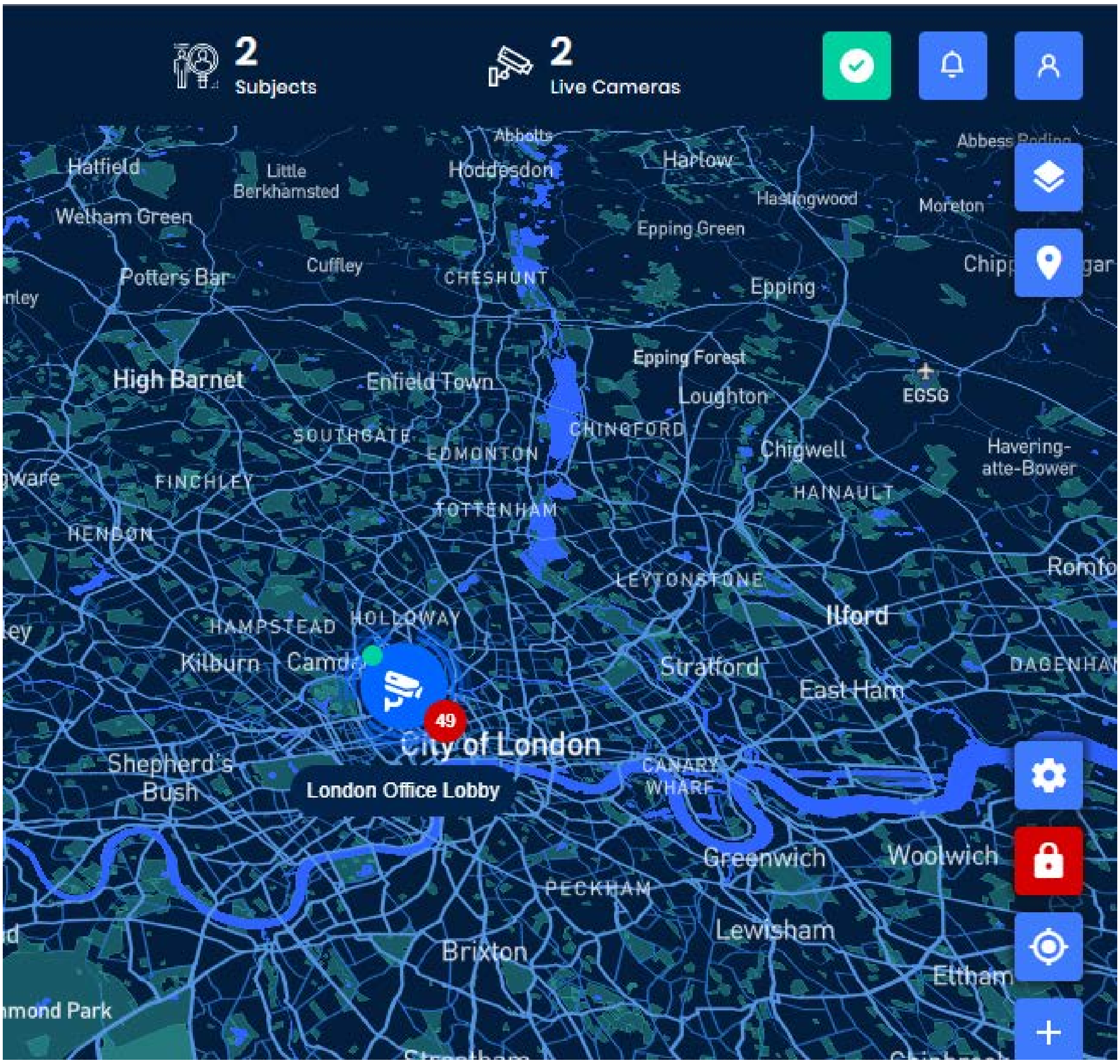
#000000

Input the *Zone name*, use the sliding scale to set the desired default zoom, and select a *Zone Color* to represent that zone. Click **Create**.

To edit an existing zone, navigate to the zone you would like to edit, and click on its name. The pop-up will appear where you can edit the name, zoom, or color.

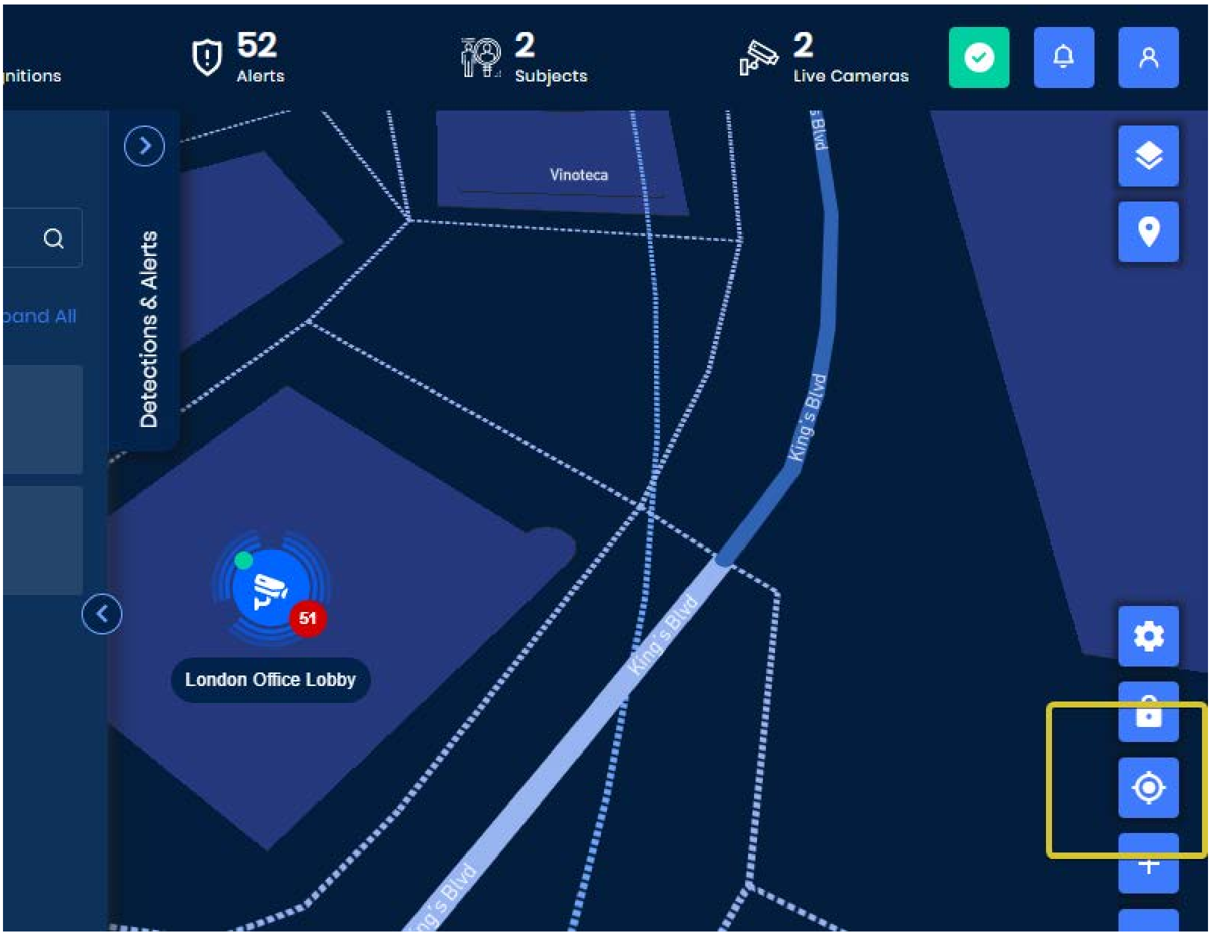
Lock

Clicking on the **lock icon** will turn it red, and means that the map will stay in place. When you are in this mode, you will first have to unlock the map before navigating around it.



Locator

Clicking on the **locator icon** will automatically move the map to the default location. This default map location can be set by the administrator Default Map Settings
System Settings



Zoom In / Zoom Out

Clicking on the **plus and minus zoom icons** will automatically scale the map to zoom in and out for closer and further map views. In addition, the map can be zoomed by using the mouse scroll button.

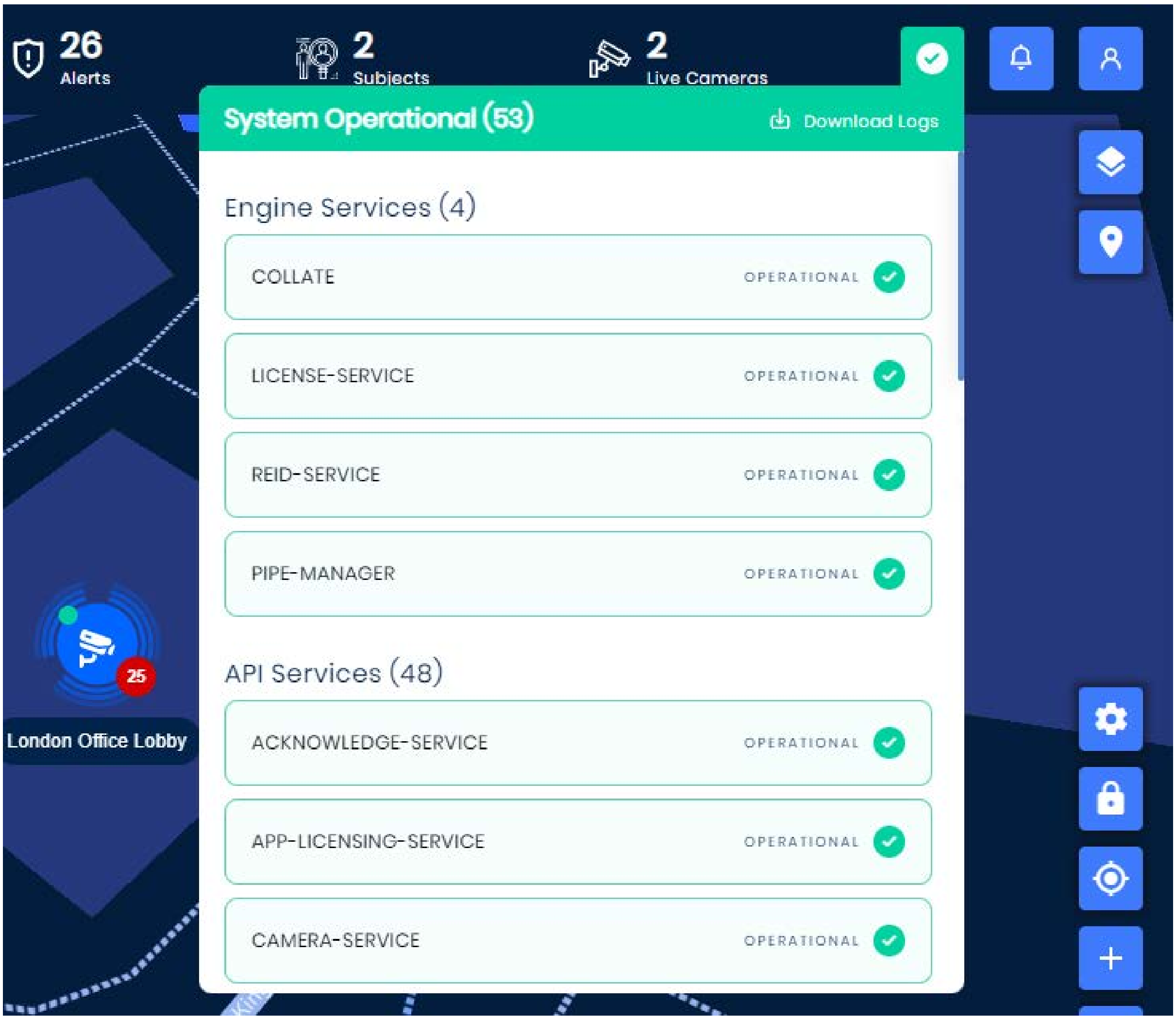
3D Map

Clicking on the **3D icon** enables the user to view the map in 3-dimensions instead of 2-dimensions if the map being viewed allows this.

Status Bar Controls

System Monitoring Status

System Status indicates the current health status of the system and whether OnWatch is functioning properly. The primary purpose of this popup is to help you identify the specific area of system failure should you experience a problem. This will also help Oosto Support to locate and solve the problems quickly.



System Operational (53)

Download Logs

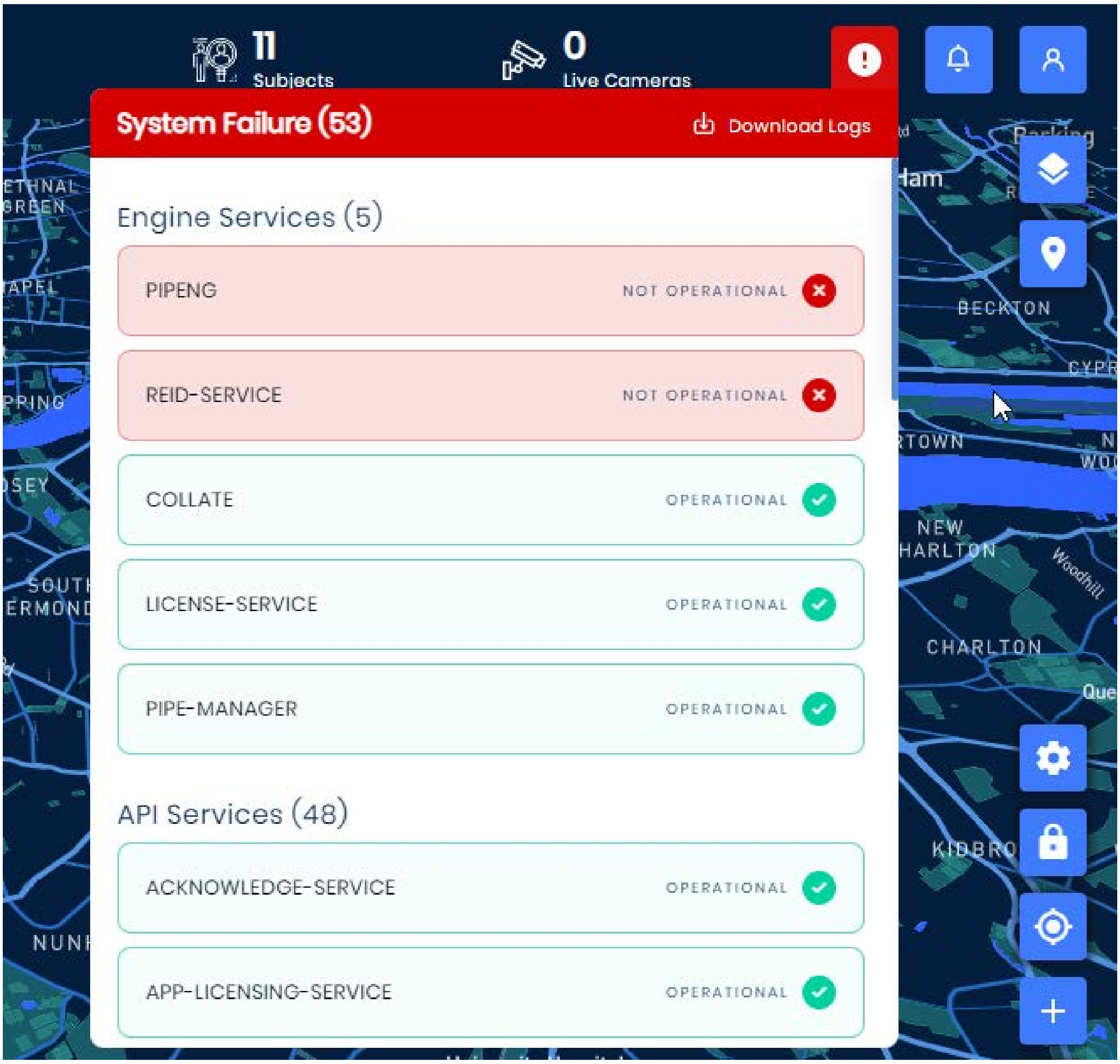
Engine Services (4)

COLLATE	OPERATIONAL ✓
LICENSE-SERVICE	OPERATIONAL ✓
REID-SERVICE	OPERATIONAL ✓
PIPE-MANAGER	OPERATIONAL ✓

API Services (48)

ACKNOWLEDGE-SERVICE	OPERATIONAL ✓
APP-LICENSING-SERVICE	OPERATIONAL ✓
CAMERA-SERVICE	OPERATIONAL ✓

Clicking on the system **status icon** on the top bar shows a breakdown of the system service. If the system is not operating, you will see a *red X* next to the problematic service. If it is functioning properly, you will see a green checkmark.



System Failure (53)

Download Logs

Engine Services (5)

PIPENG NOT OPERATIONAL

REID-SERVICE NOT OPERATIONAL

COLLATE OPERATIONAL

LICENSE-SERVICE OPERATIONAL

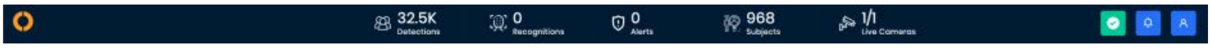
PIPE-MANAGER OPERATIONAL

API Services (48)

ACKNOWLEDGE-SERVICE OPERATIONAL

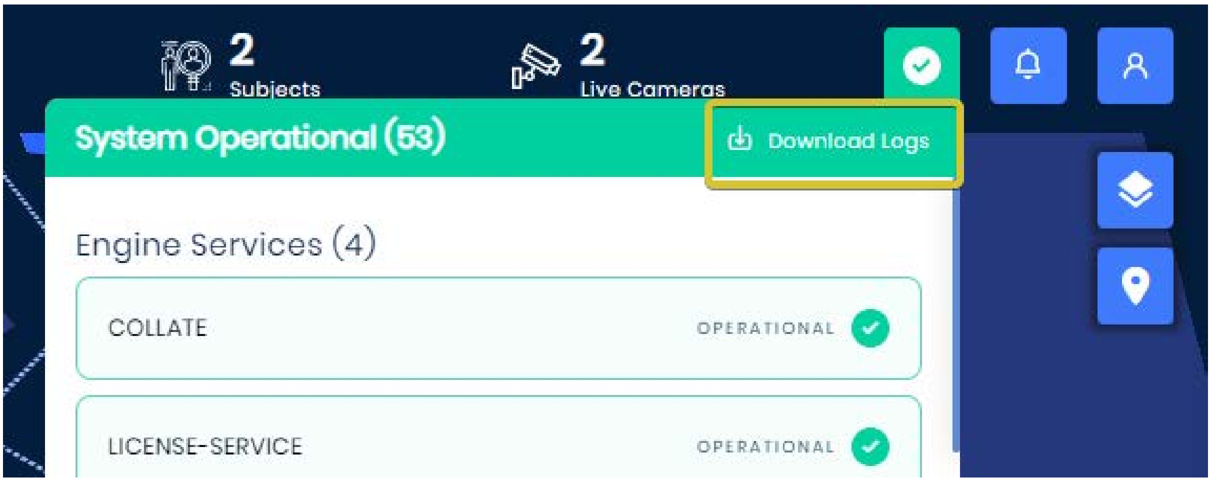
APP-LICENSING-SERVICE OPERATIONAL

The *checkmark* in green remaining at the top tab of the screen means that the system is working. You do not need to check this page for operation unless the green checkmark becomes a *red X*. If this happens, click **System Status** and follow the *red X*'s until you see the issue, then contact Oosto Support.



System Logs

You can also download system logs on this popup. Click **Download Logs** at the top of the page to do so. The system will download all logs.



System Operational (53)

Download Logs

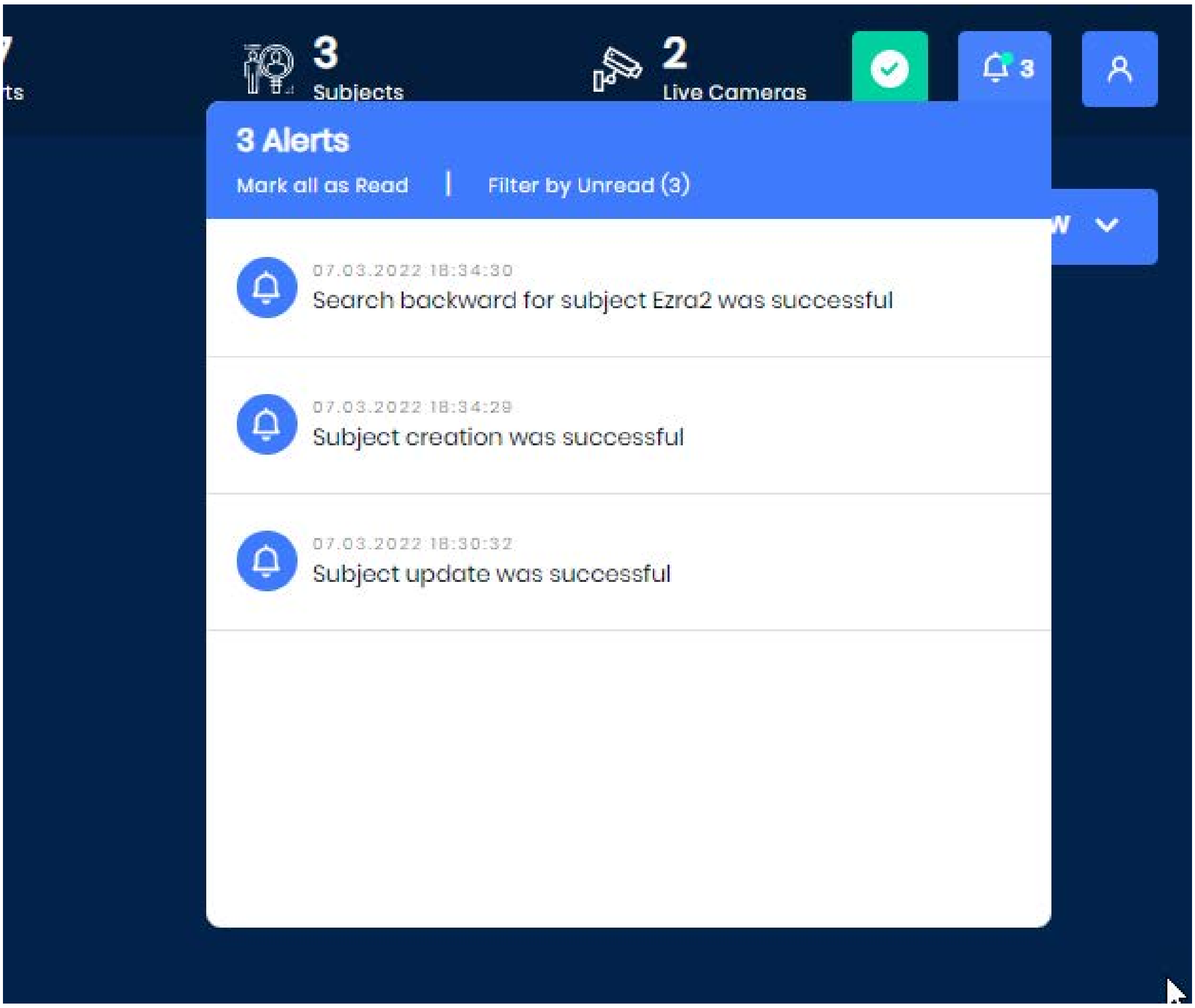
Engine Services (4)

COLLATE OPERATIONAL

LICENSE-SERVICE OPERATIONAL

Notifications

The system notifications tab allows users to see how actions that they have undertaken are completed, these actions:



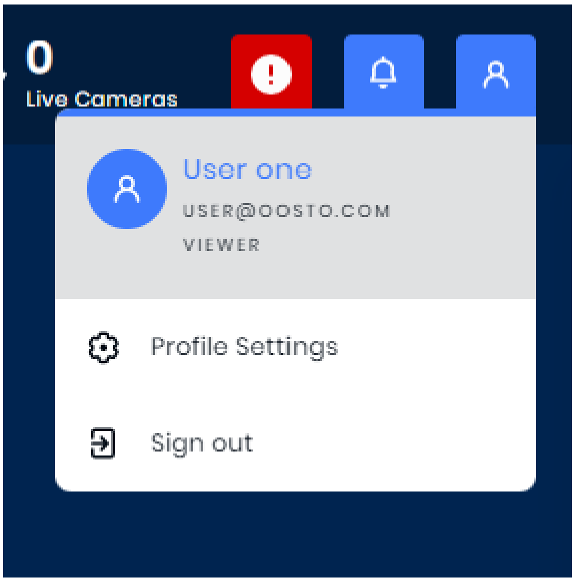
07.03.2022 18:34:30
Search backward for subject Ezra2 was successful

07.03.2022 18:34:29
Subject creation was successful

07.03.2022 18:30:32
Subject update was successful

User Account Settings

A user can easily **Sign out** of the application from here

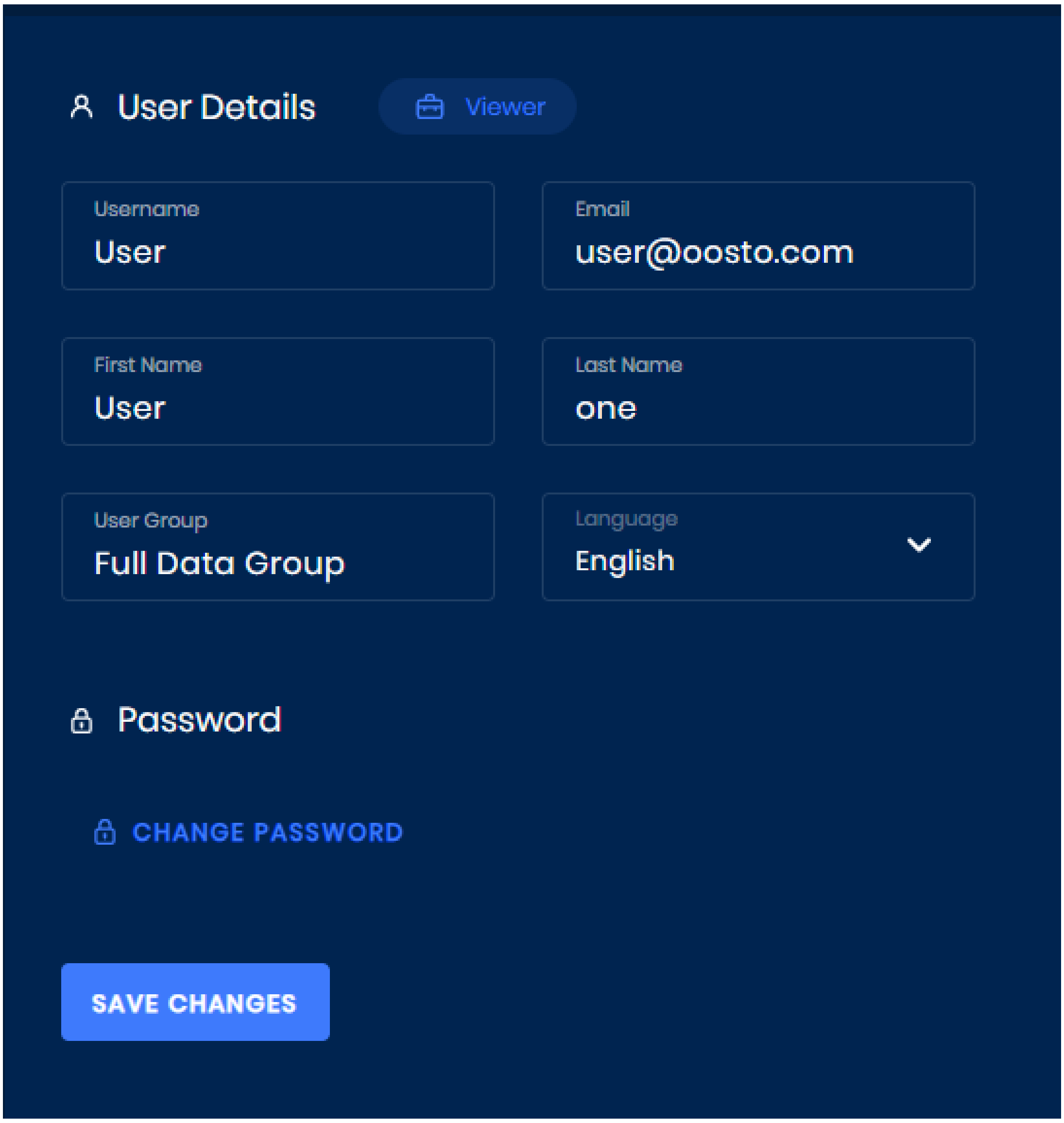


By clicking **Profile Settings** the end user is able to view and edit some of their own account settings including

- First Name
- Last Name

- System Language

In addition a user is able to change their password



User Details

Username: User

Email: user@oosto.com

First Name: User

Last Name: one

User Group: Full Data Group

Language: English

Password

Cameras & Cases "View Sources"

The Cameras & Cases page provides a few capabilities:

- A recent look at the system's detections, recognitions, and alerts
- A status of cameras/cases connected to the system
- An easy way to search and navigate the cameras/cases
- A quick method to preview the processing stream
- An easy deep-link to search a camera group and search or edit a case

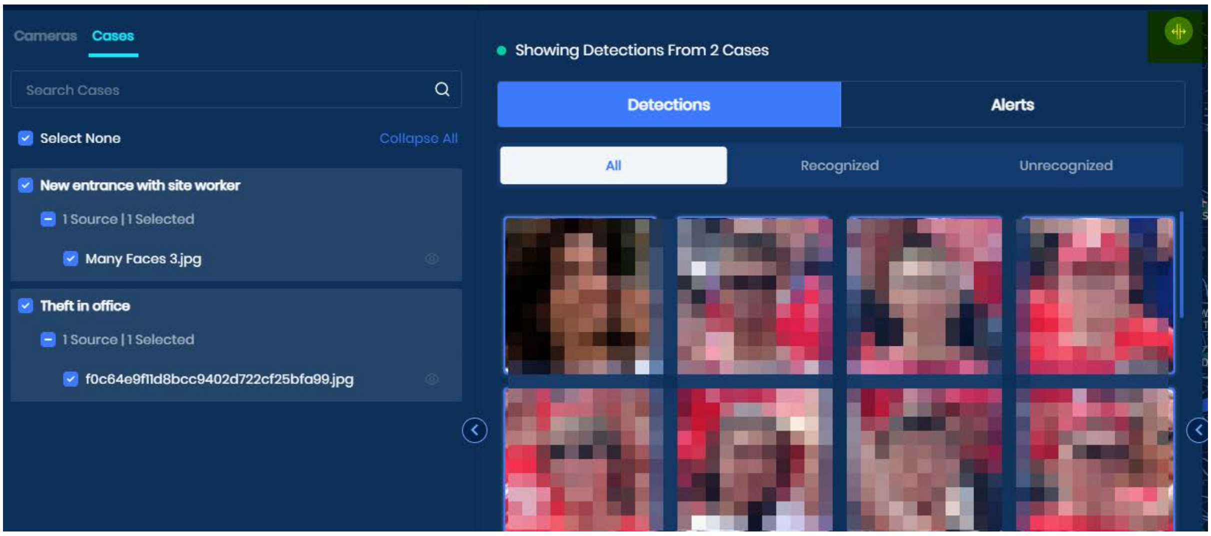
This tab is comprised of two panels, *Cameras / Cases* navigation tree and *Detections / Alerts*.

By default, the system doesn't select any streams as there can be many 100's of active streams which would be overwhelming to the end-user.

The *Cameras* and *Cases* tab shows all the cameras/cases by camera group/case name and allows you to search and select the specific camera streams and files you would like the system to display active detections for.

The *Detection & Alerts* pane shows both a list of detections (with associated actions described below) and a list of alerts, which the user can acknowledge, depending on which tab you toggled to.

To collapse and expand the tabs, use the **left-** and **right-facing arrows** located at the sides of each expandable tab. It is also possible to expand the **Detections window** to show two or four columns by selecting the **expand collapse** button

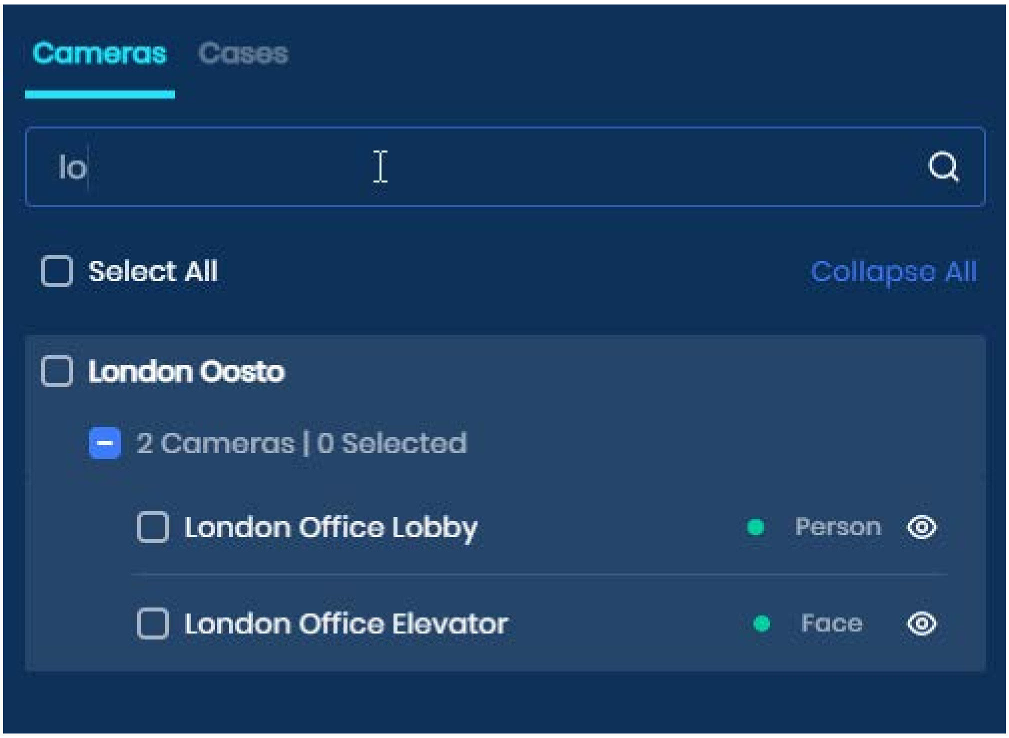


Cameras & Cases

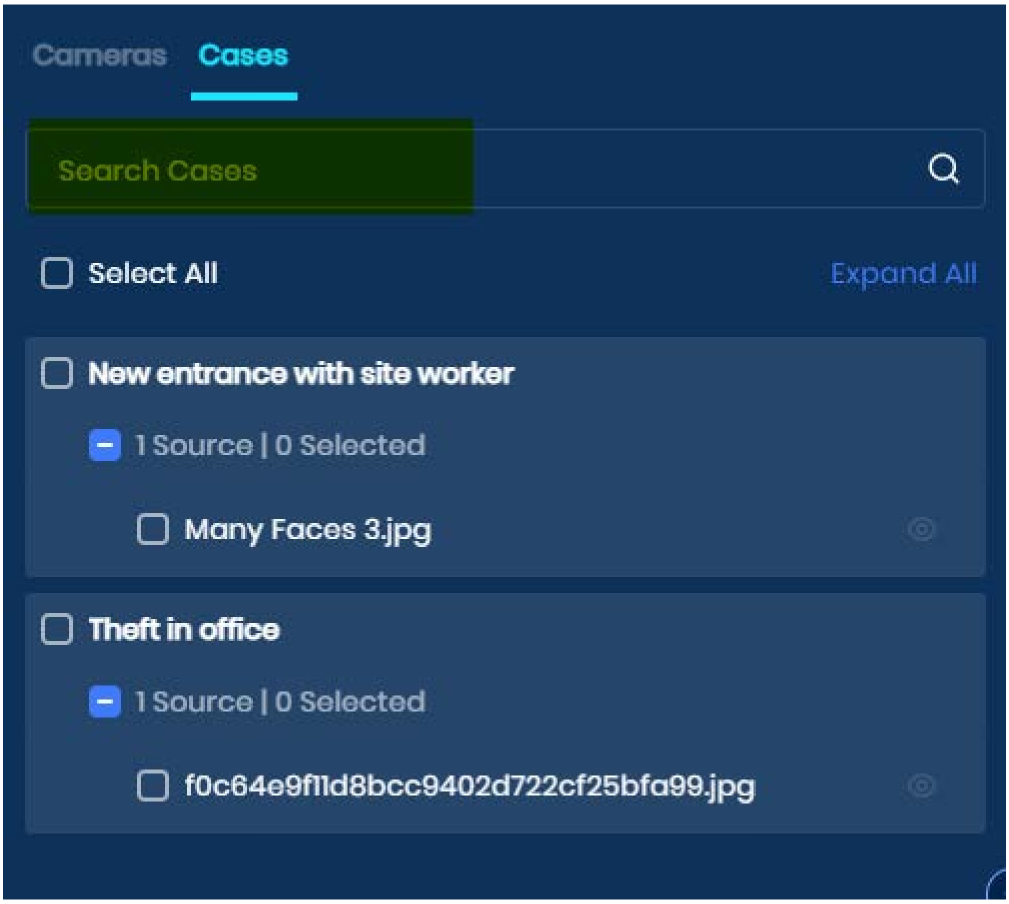
When you click on the **Cameras** or **Cases** tab, it will open and automatically display the camera groups or cases you have rights to view.

At this point, you can find:

The specific camera or camera group you are looking for, by simply "searching" for a camera group or camera name.



The specific image/video files or cases you are looking for by "searching" for a file or case name.



□ Select All

□ New entrance with site worker

1 Source | 0 Selected

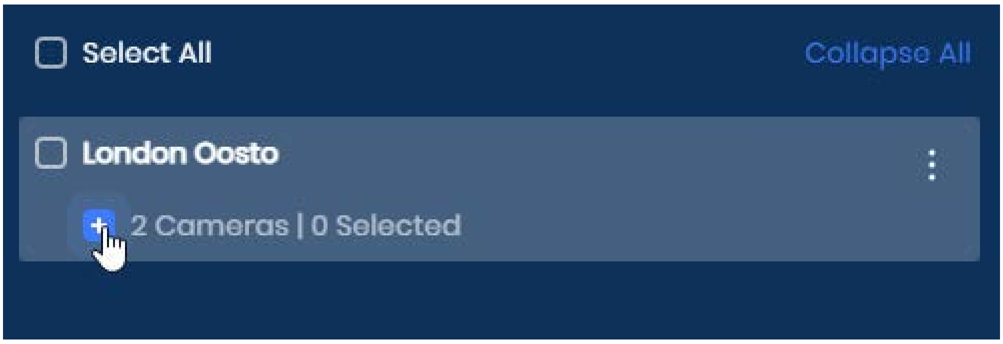
□ Many Faces 3.jpg

□ Theft in office

1 Source | 0 Selected

□ f0c64e9f1d8bcc9402d722cf25bfa99.jpg

You can scroll down the list manually expanding of contracting a single camera groups/cases

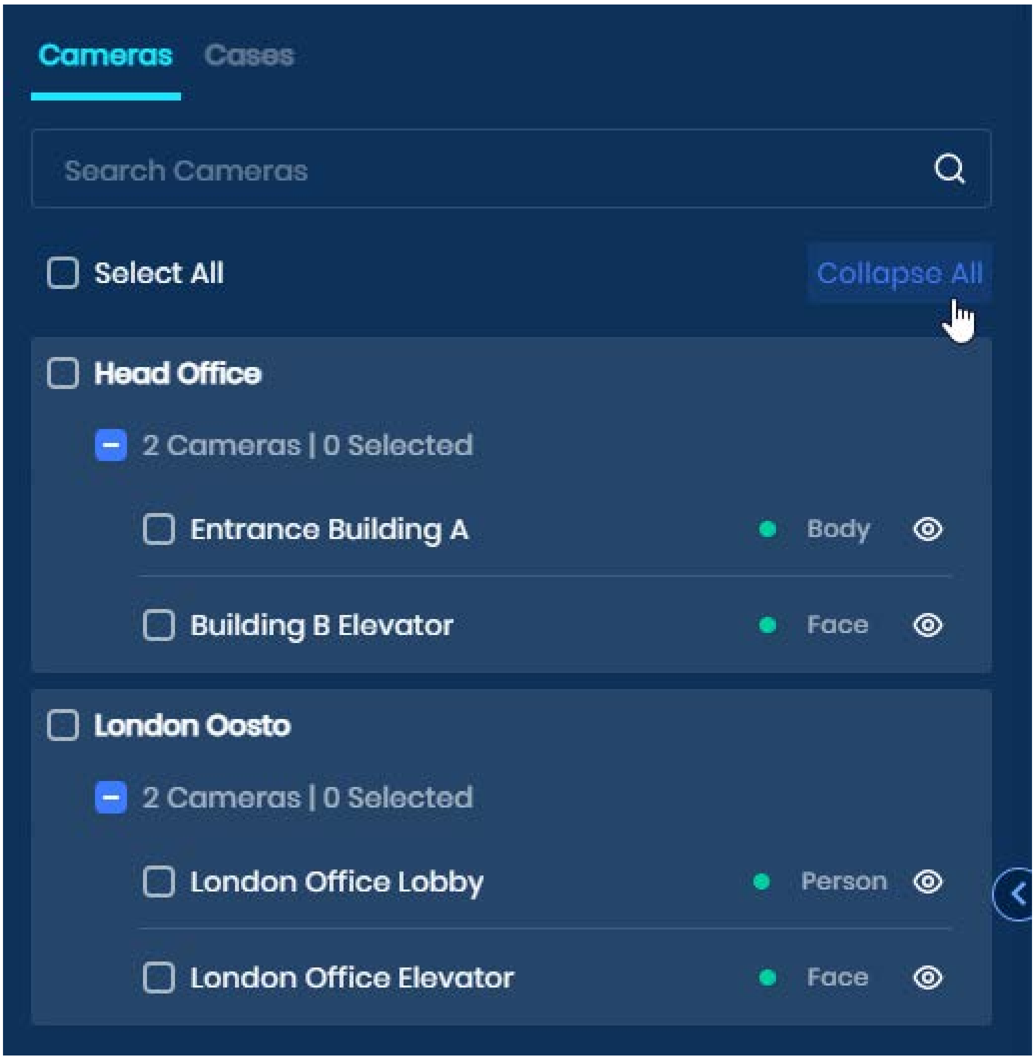


□ Select All

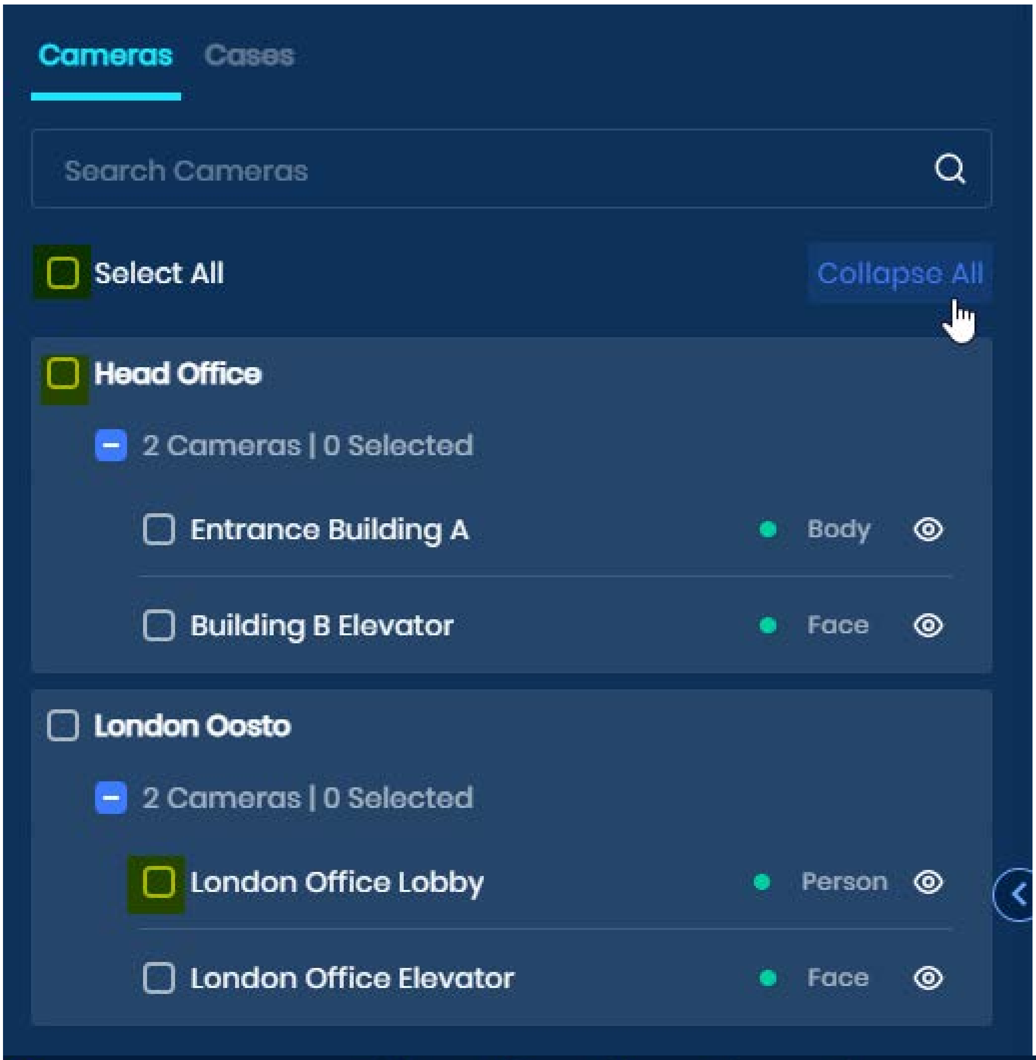
□ London Oosto

2 Cameras | 0 Selected

It is also possible to "expand/collapse" all groups at the same time



When you check the boxes **Select All** or the check box near **Camera group name/Case name** or the check box before the **Cameras name**, the detections and alerts derived from the cameras you selected will appear.



Cameras Cases

Search Cameras

□ Select All Collapse All

□ Head Office

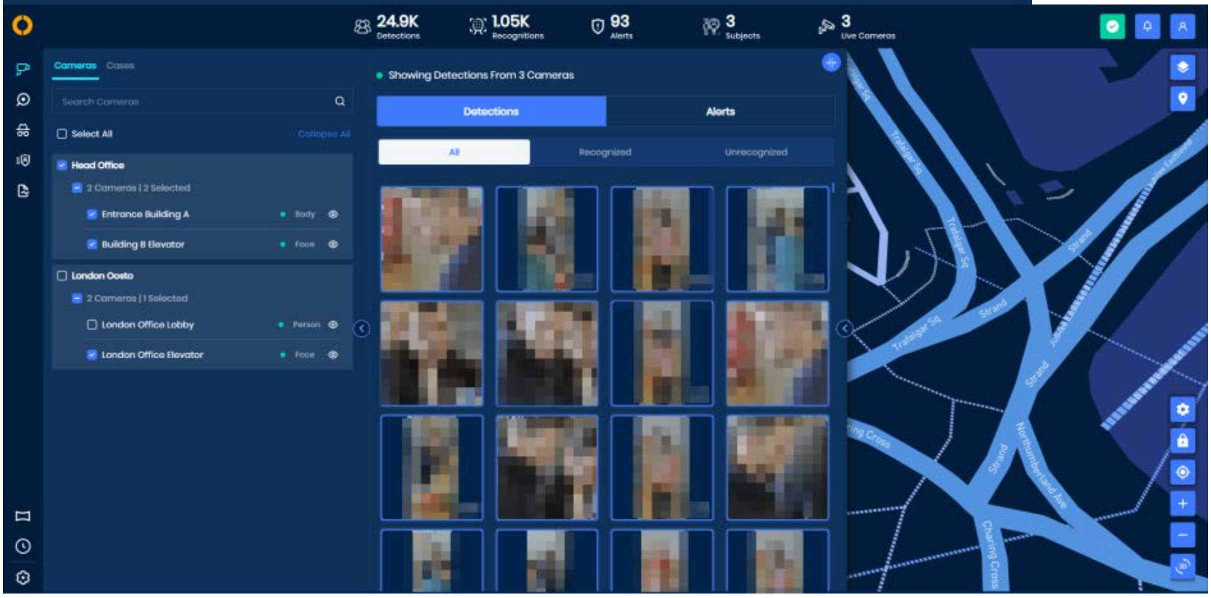
2 Cameras | 0 Selected

- □ Entrance Building A ● Body
- □ Building B Elevator ● Face

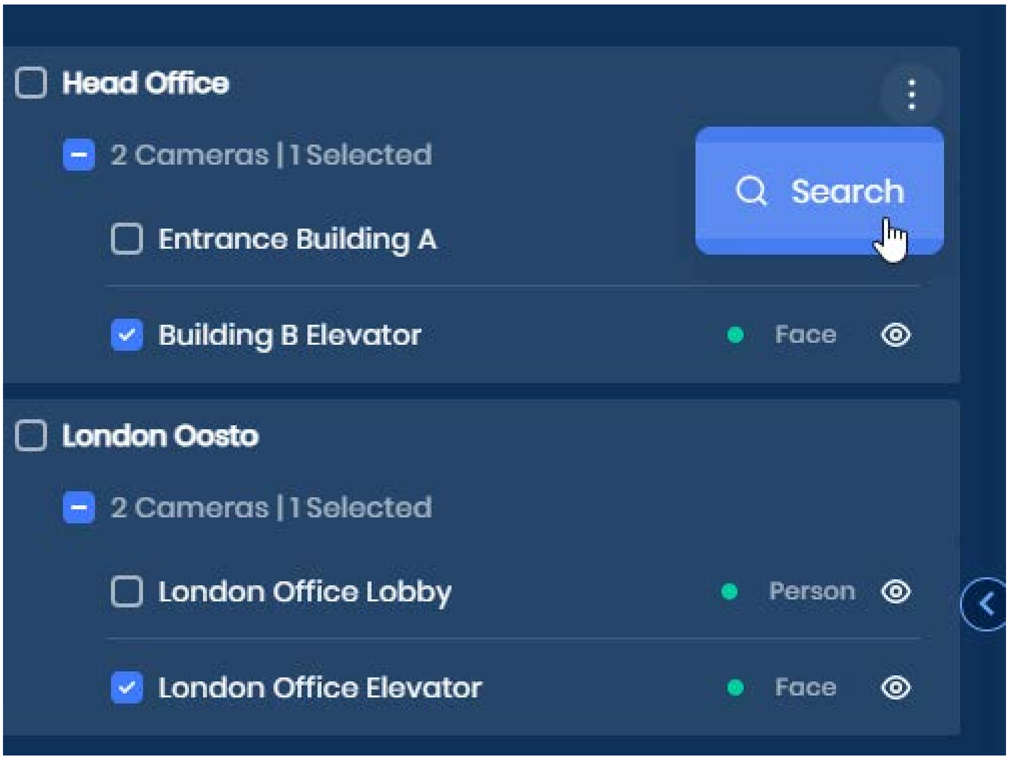
□ London Oosto

2 Cameras | 0 Selected

- □ London Office Lobby ● Person
- □ London Office Elevator ● Face



Each camera group has the ability to deep-link to the search page with all the cameras in that group automatically transferred and selected with the default last 24 hours of detections. The search page can then be used to investigate further. Search



□ Head Office

▬ 2 Cameras | 1 Selected

□ Entrance Building A

☑ Building B Elevator ● Face

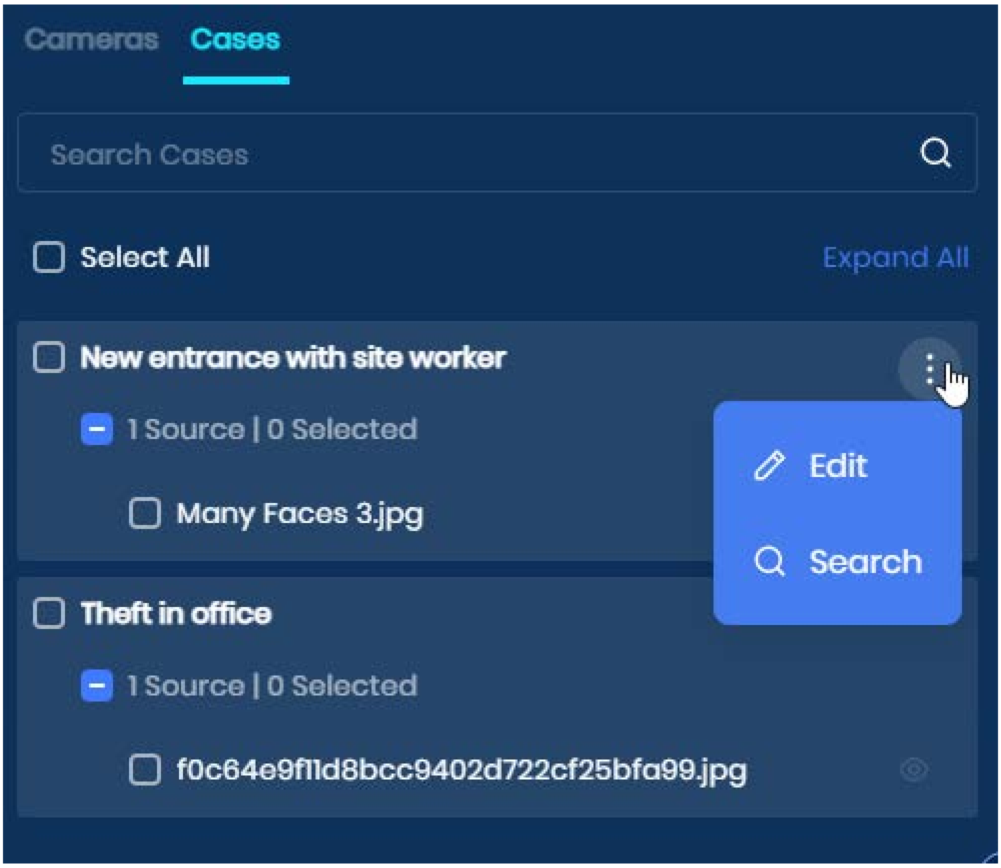
□ London Oosto

▬ 2 Cameras | 1 Selected

□ London Office Lobby ● Person

☑ London Office Elevator ● Face

In addition, each case had the ability to deep-link to edit the specific case content by hovering over the case and clicking the three dots



Cameras Cases

Search Cases

□ Select All Expand All

□ New entrance with site worker

▬ 1 Source | 0 Selected

□ Many Faces 3.jpg

□ Theft in office

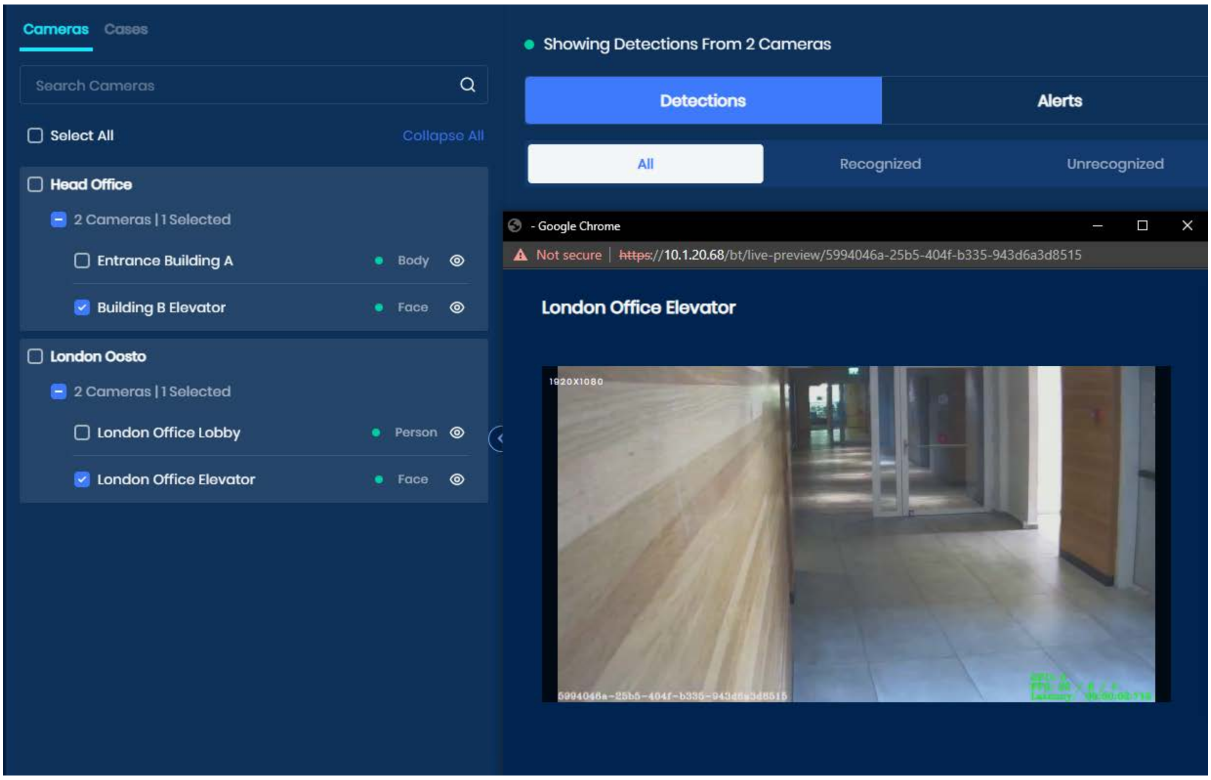
▬ 1 Source | 0 Selected

□ f0c64e9f1ld8bcc9402d722cf25bfa99.jpg

Each camera has the following information related to it:

- Detection type
- Camera Status (Green - Connected, Yellow - Re-connecting, Red - Disconnected)
- Camera analysis stream (When clicking this a preview window will be shown of the current stream with the overlays configured)

Each file is also able to have an analysis preview when it is being processed else the eye will be disabled, as images take millisecond to process no preview window will be available

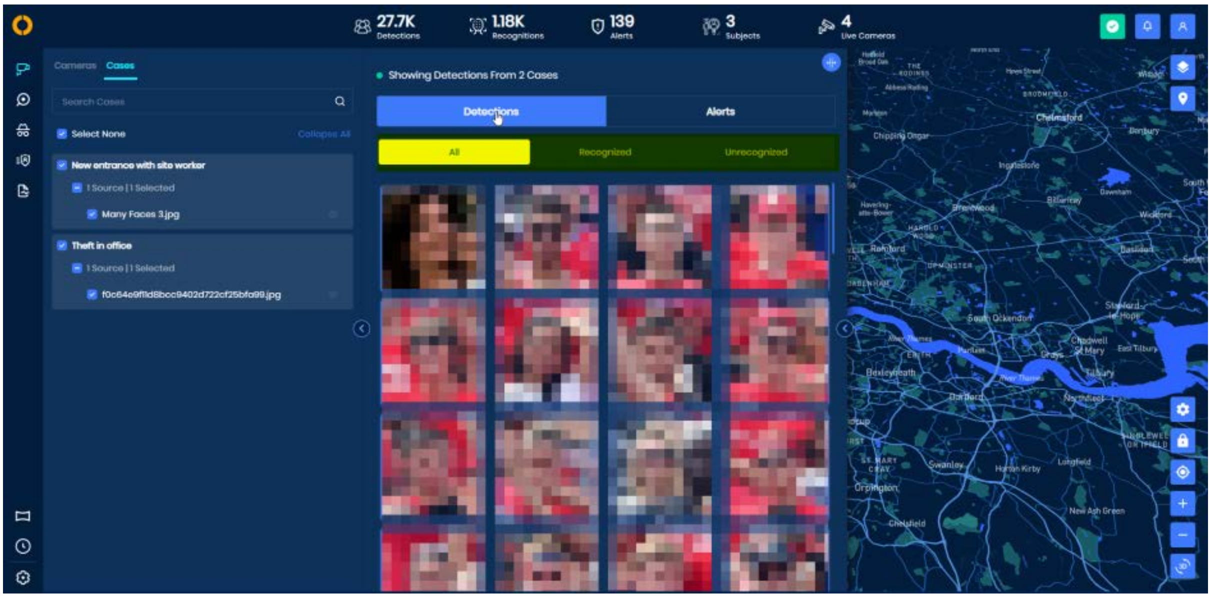


Detections & Alerts

The Detections & Recognitions column shows the detections, recognitions, and alerts within the system for the selected cameras and case files.

Detections

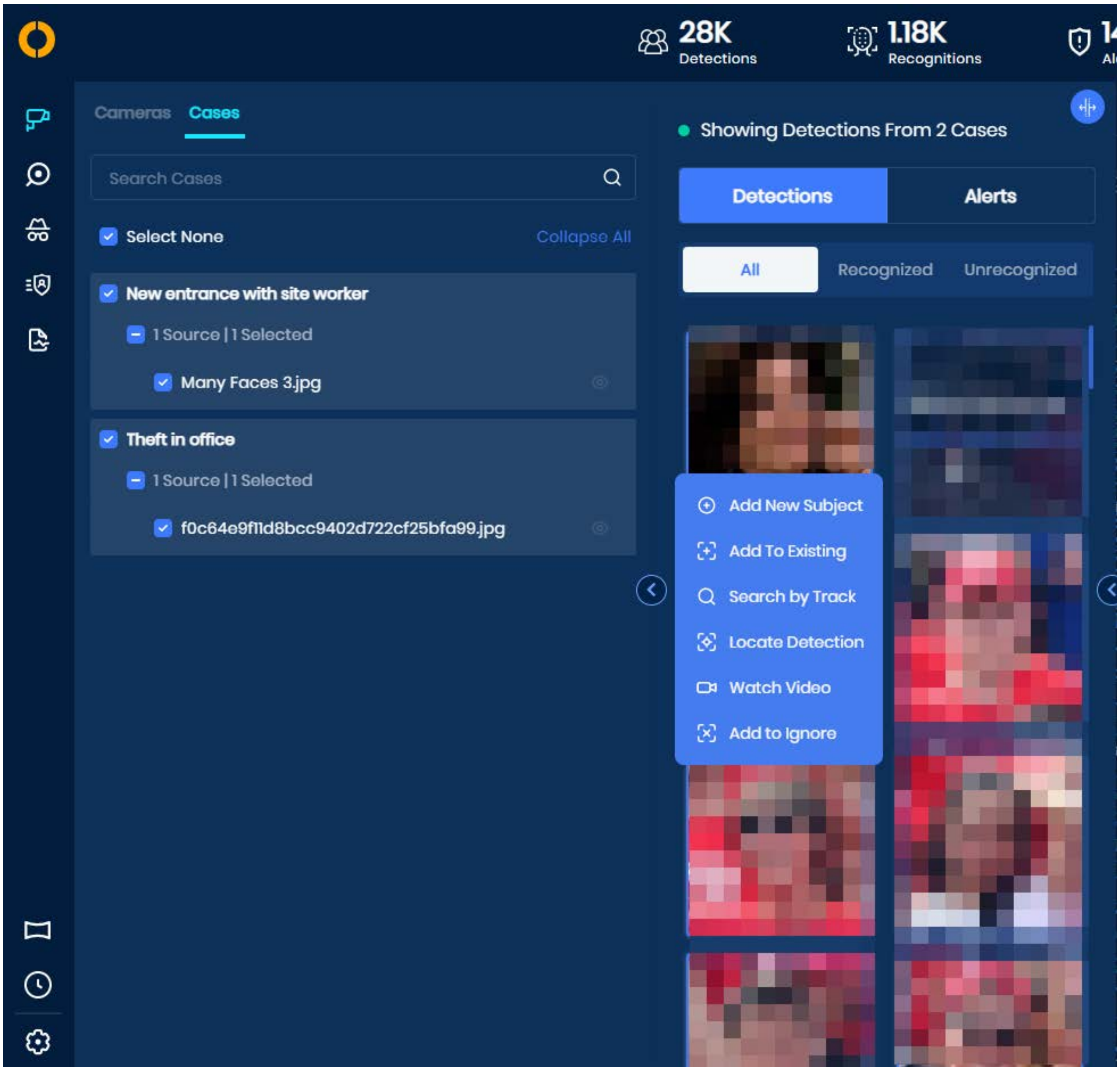
When selecting the *Detections* tab, you can filter by All, Recognized or Unrecognized.



Hovering over one of the images will tell you the name of the detecting camera/case, and the date and time of the detection. Clicking on the **3-dotted icon** will show the following options:

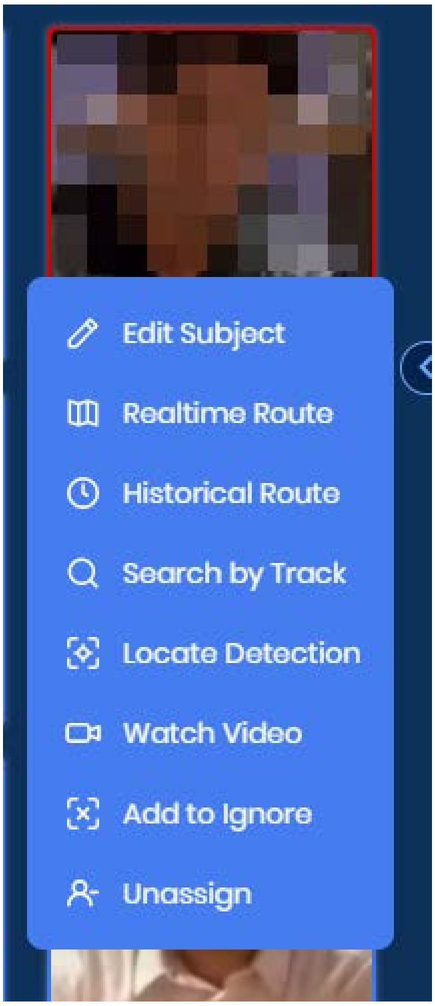
- **Add New Subject**
- **Add to Existing** - allows you to add a detection image to an existing subject's profile to improve the detection accuracy for that subject
- **Search by Track** - allows you to locate all other detections of the given subject

- **Locate Detection** - takes you to all the detections that took place during that period so you may see what other detections took place at the same time frame
- **Watch Video** - displays a 5 to 30-second rendered video snippet of the moment of detection
- **Add to Ignore** - adds the detection to the *Ignore* group in *Settings*

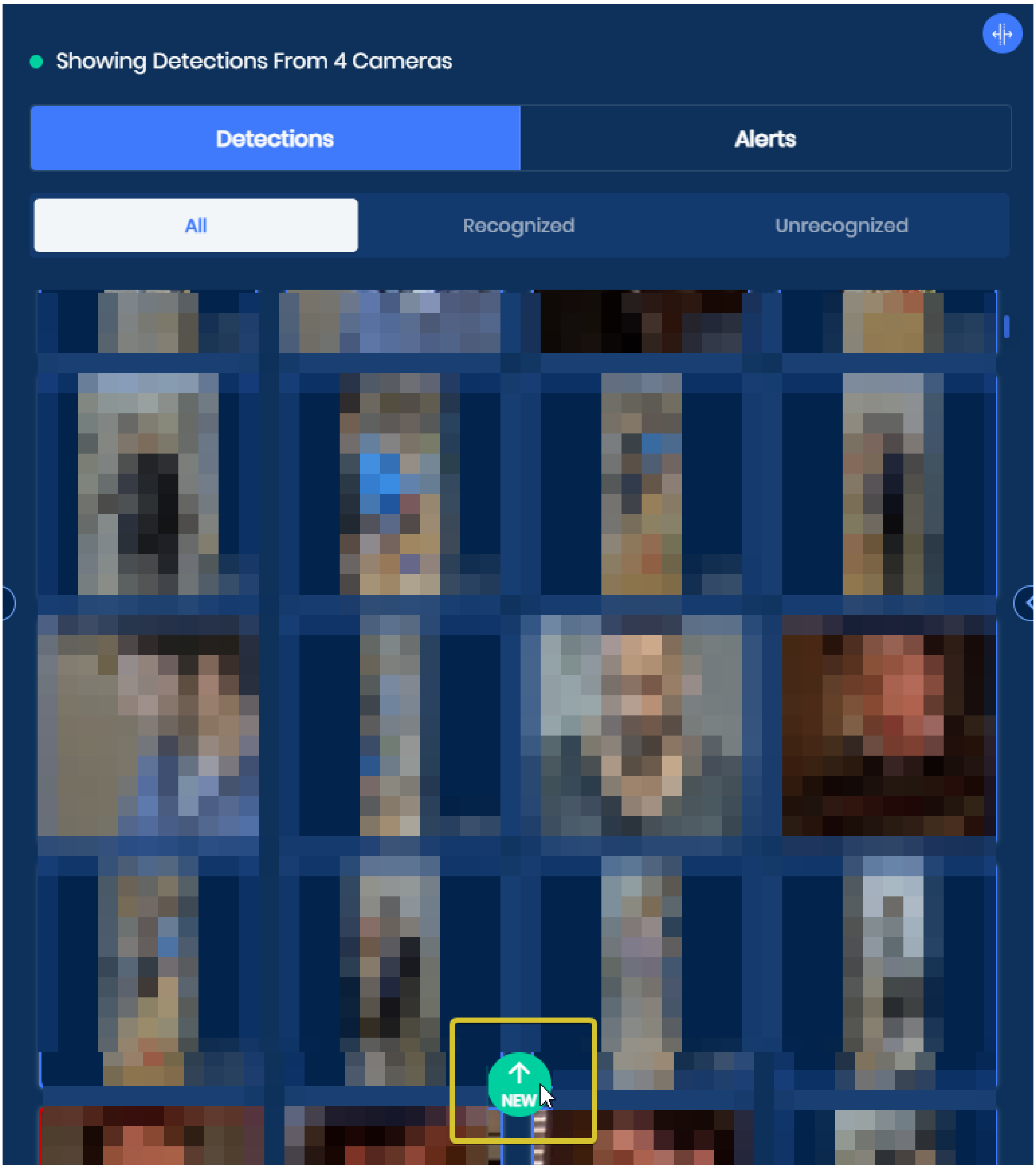


In addition to the above capabilities If the detection of the person is matched (recognized) to the watchlist, the following additional capabilities will be available:

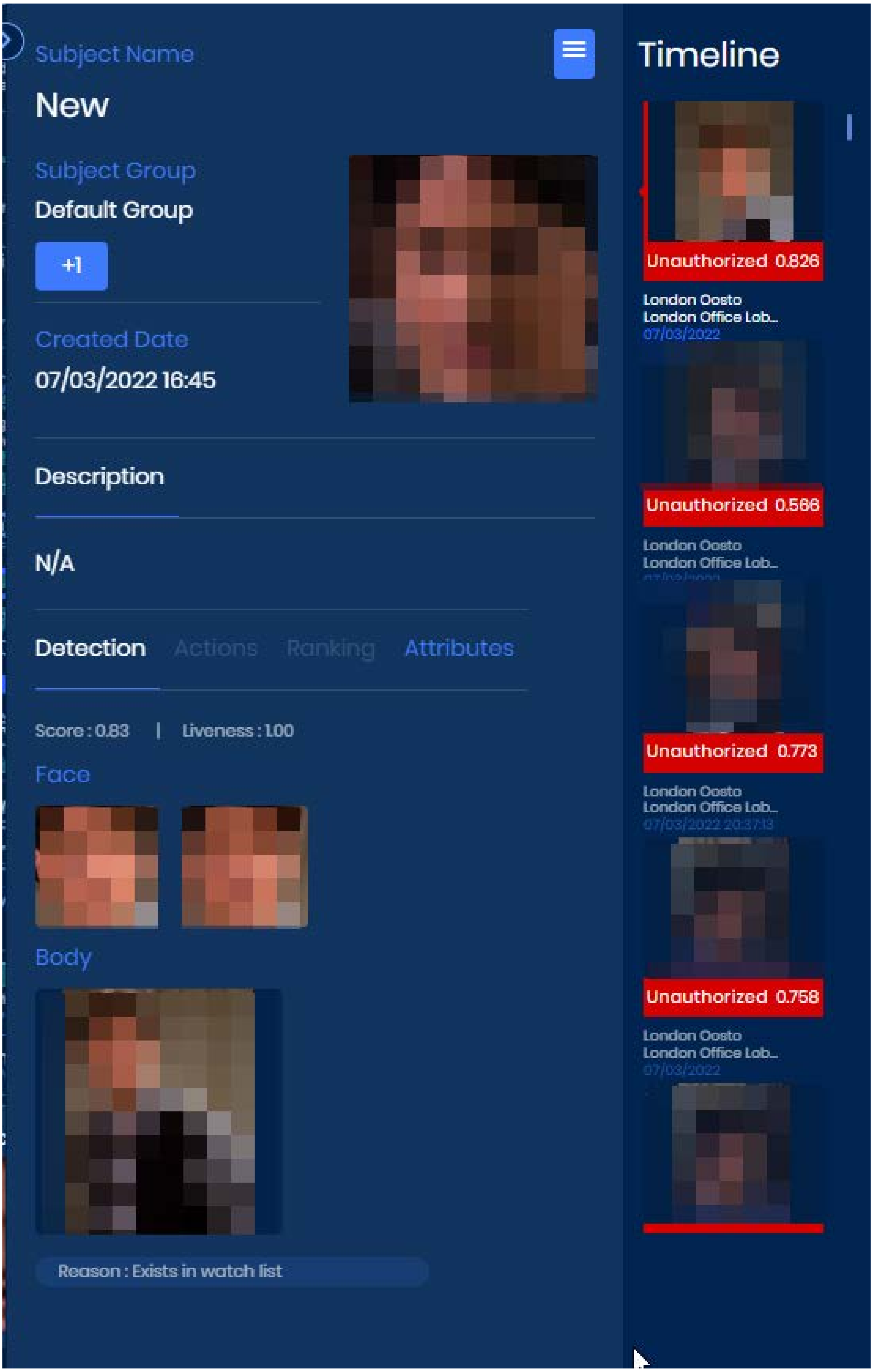
- **Edit Subject**
- **Real-time Route** - view the route of a subject in real-time or near real-time
- **Historical Route** - view the route history of the subject
- **Unassign** - remove the recognition from the subject's timeline



To return to the newest detections after scrolling down, click the **green arrow** at the bottom of the page.



Clicking on a detection image will display information about the detected subject and other detection details including any alerting reason.



Subject Name

New

Subject Group

Default Group

+1

Created Date

07/03/2022 16:45

Description

N/A

Score : 0.83 | Liveness : 1.00

Reason : Exists in watch list

Timeline

Unauthorized 0.826
London Oosto
London Office Lob...
07/03/2022

Unauthorized 0.566
London Oosto
London Office Lob...

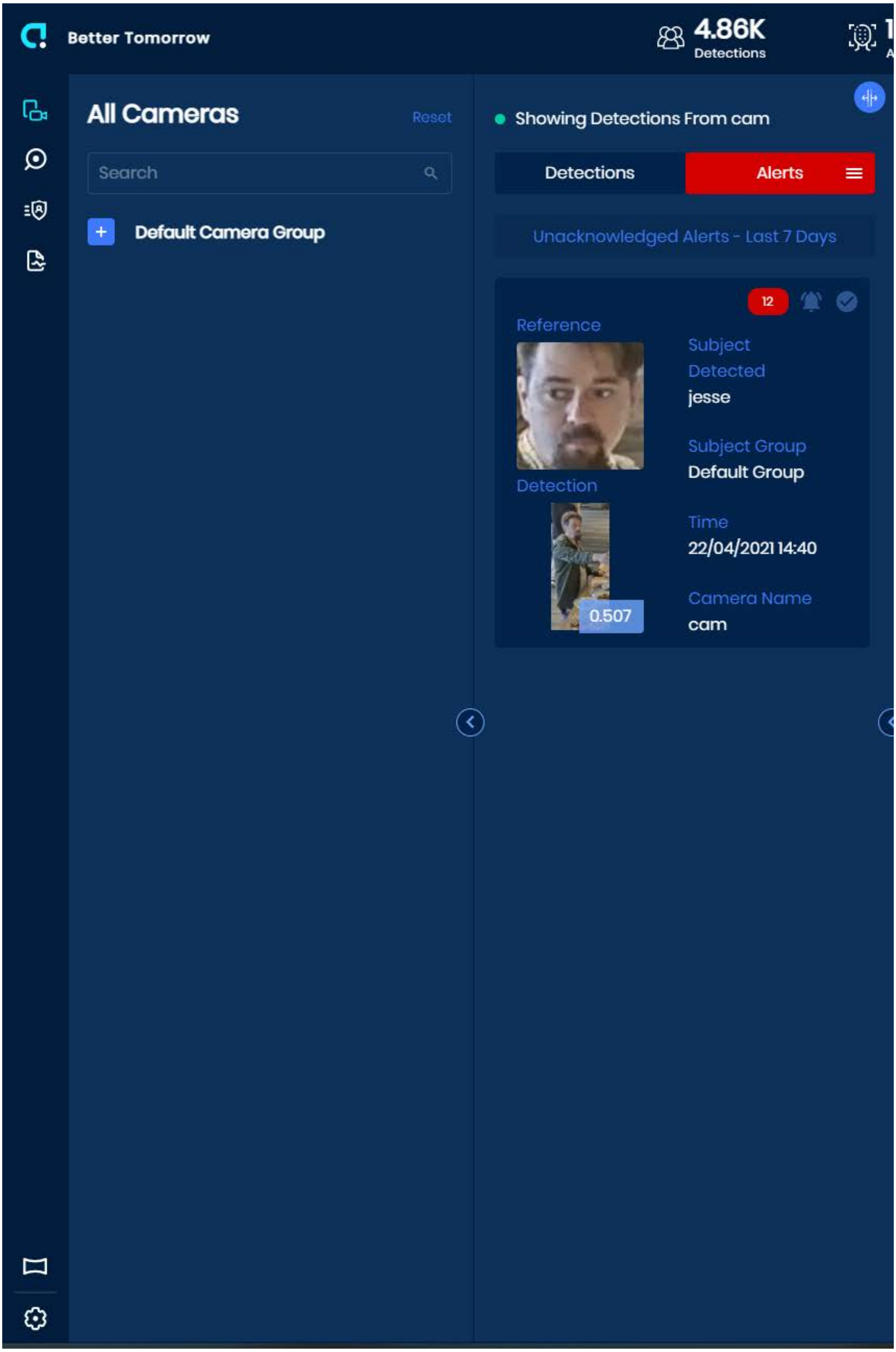
Unauthorized 0.773
London Oosto
London Office Lob...
07/03/2022 20:37:13

Unauthorized 0.758
London Oosto
London Office Lob...
07/03/2022

The first panel will include information about that specific subject and detection, including the *Subject's Name*, *Subject Group*, *Created Date*, *Description*, and associated images.

The second panel will include a *Timeline* of all that subject's detections in the system over time.

Alerts



Showing Detections From cam

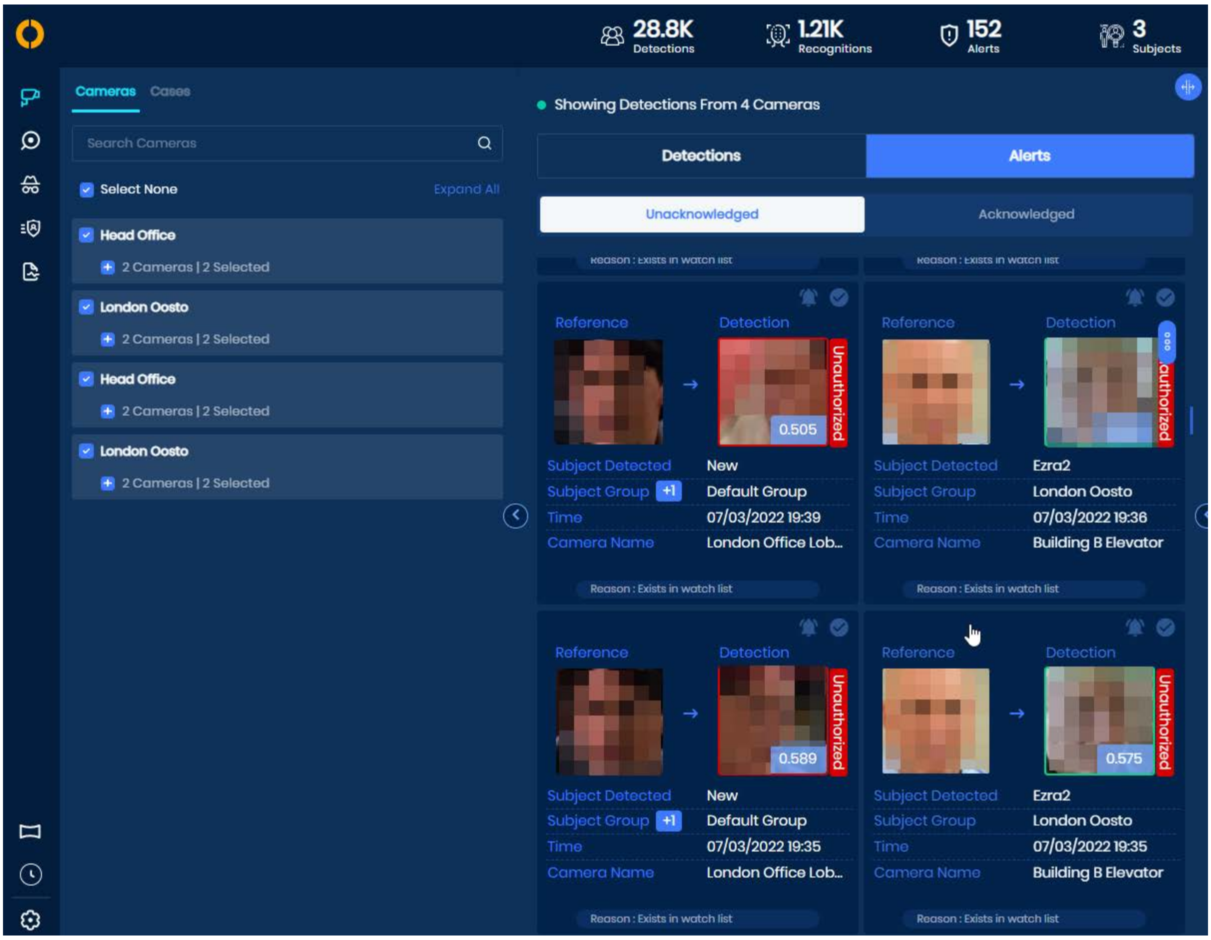
Subject Detected
jesse

Subject Group
Default Group

Time
22/04/2021 14:40

Camera Name
cam

The alerts tab displays all unacknowledged and acknowledged alerts from the top 100results..



Head Office
2 Cameras | 2 Selected

London Oosto
2 Cameras | 2 Selected

Head Office
2 Cameras | 2 Selected

London Oosto
2 Cameras | 2 Selected

Subject Detected	New
Subject Group +1	Default Group
Time	07/03/2022 19:39
Camera Name	London Office Lob...

Reason : Exists in watch list

Subject Detected	Ezra2
Subject Group	London Oosto
Time	07/03/2022 19:36
Camera Name	Building B Elevator

Reason : Exists in watch list

Subject Detected	New
Subject Group +1	Default Group
Time	07/03/2022 19:35
Camera Name	London Office Lob...

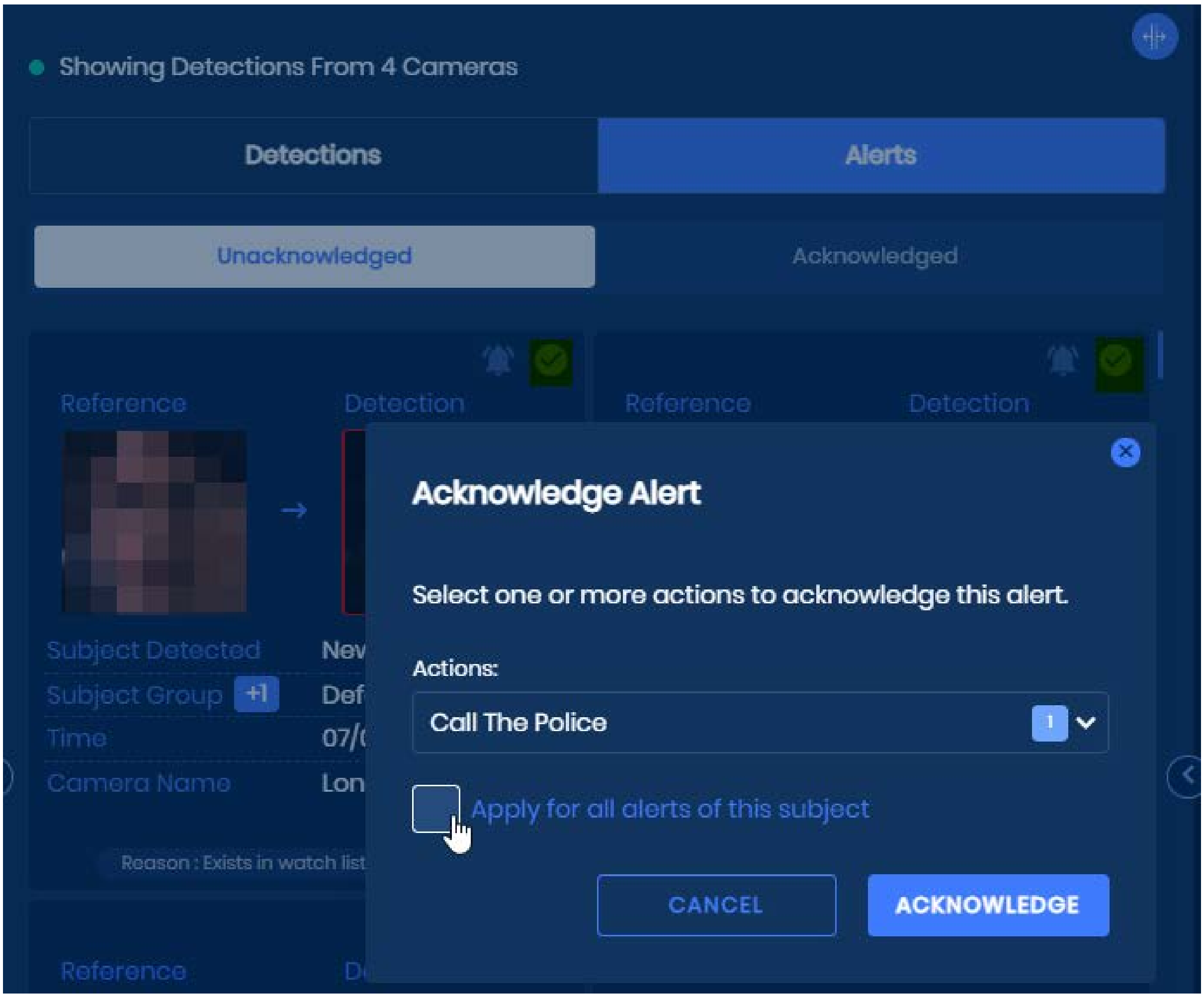
Reason : Exists in watch list

Subject Detected	Ezra2
Subject Group	London Oosto
Time	07/03/2022 19:35
Camera Name	Building B Elevator

Reason : Exists in watch list

Clicking on the **Tick Button** on the far upper right corner of the alert can be

- Acknowledged and dismissed immediately
- Acknowledged with one or more alert actions (Alert actions can be configured by the system administrator) Alert Action Configuration
- Acknowledge all Alerts for the same person (Subject) on the watchlist



Acknowledge Alert

Select one or more actions to acknowledge this alert.

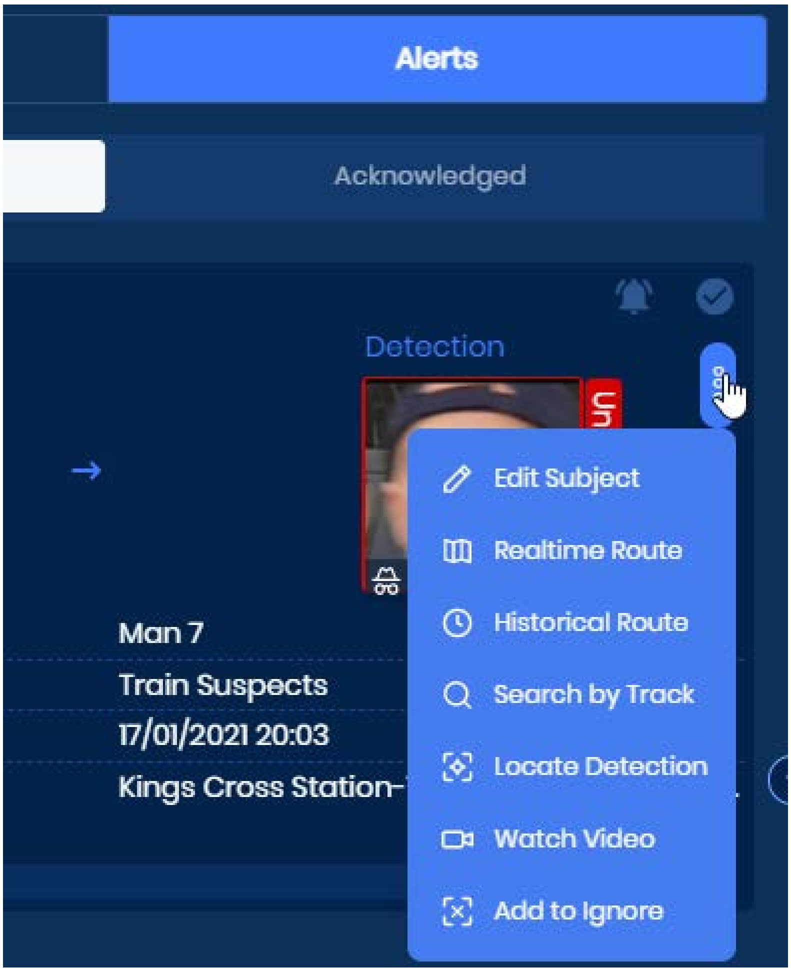
Actions: Call The Police

□ Apply for all alerts of this subject

Each alert will show the reference image and detection image of the detected subject, along with the subject name, group, date and time of detection, and the camera/case that captured the recognition.

Clicking the **3-dotted icon** (which appears when you hover over the alert) generates the following options:

- Edit Subject
- Realtime Route
- Historical Route
- Search by Track
- Locate Detection
- Watch Video
- Add to Ignore



Search

The New Search page has been designed to allow you to view the current search context without having to jump between different views when search adjustments are applied. The search adjustments include:

- Search by person
- Search within sources cameras and cases
- By date/time and newly added case times
- By person attributes
- By association

The search has also been expanded to retrieve a much larger data set up to 50K results when doing the initial filter. This larger dataset is then able to be instantly manipulated within the results pane including:

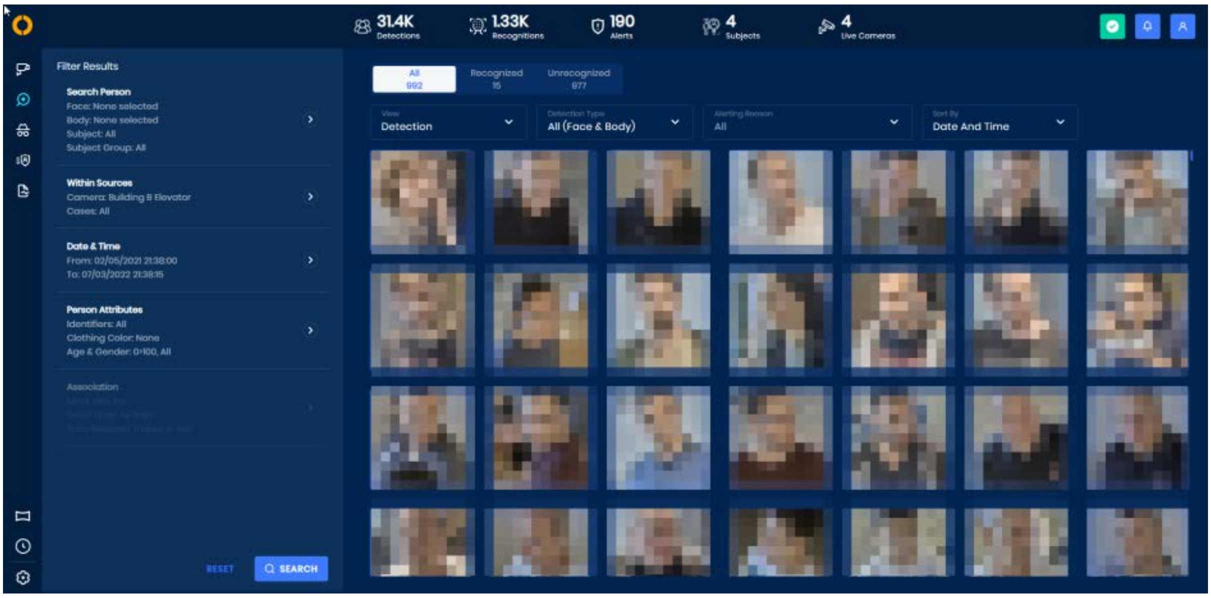
Results Control Bar

- Filtering by recognized/ unrecognized
- Filtering by detection type](#search#section-results-control-bar-second-row)
- Filtering by alerting reason
- view by detections or aggregate (which can reduce the noise of repetitive detections)
- Sort by date/time, score and number of detections

Search Filter Pane

The *Search* tab allows you to serach through the system's detections and recognitions. It also lets you locate specific detections, recognitions, or subjects by defining parameters that pinpoint exactly who or what to search for.

The Search feature is located in the *Search* tab on the far left navigation pane. The pane as operated by selecting a specific category to filter by and selecting those specific filters.



31.4K Detections | 1.33K Recognitions | 190 Alerts | 4 Subjects | 4 Live Cameras

Filter Results

Search Person
Face: None selected
Body: None selected
Subject: All
Subject Group: All

Within Sources
Camera: Building B Elevator
Cases: All

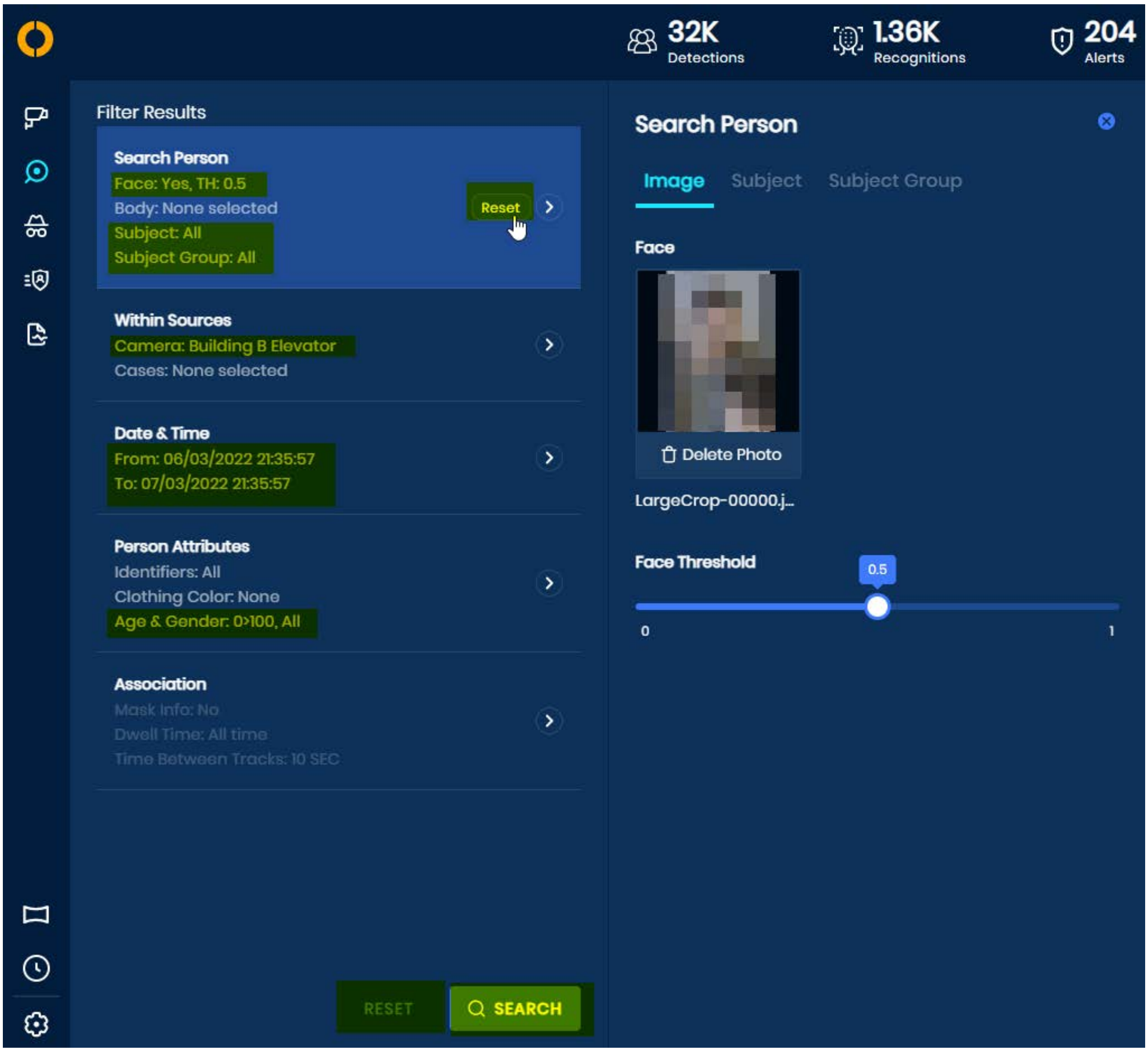
Date & Time
From: 02/05/2021 21:38:00
To: 07/03/2022 21:38:15

Person Attributes
Identifiers: All
Clothing Color: None
Age & Gender: 0>100, All

Association

View: Detection
Detection Type: All (Face & Body)
Alerting Reason: All
Sort By: Date And Time

Once all the filters required are selected you can click the search button to display the top results within the results page. Each section can be reset to its default by hovering over it and selecting the reset button, it is also possible to reset all filters by selecting the reset next to the search button at the bottom of the filter pane.



32K Detections | 1.36K Recognitions | 204 Alerts

Filter Results

Search Person
Face: Yes, TH: 0.5
Body: None selected
Subject: All
Subject Group: All

Within Sources
Camera: Building B Elevator
Cases: None selected

Date & Time
From: 06/03/2022 21:35:57
To: 07/03/2022 21:35:57

Person Attributes
Identifiers: All
Clothing Color: None
Age & Gender: 0>100, All

Association
Mask Info: No
Dwell Time: All time
Time Between Tracks: 10 SEC

Search Person

LargeCrop-00000.j...

Face Threshold: 0.5

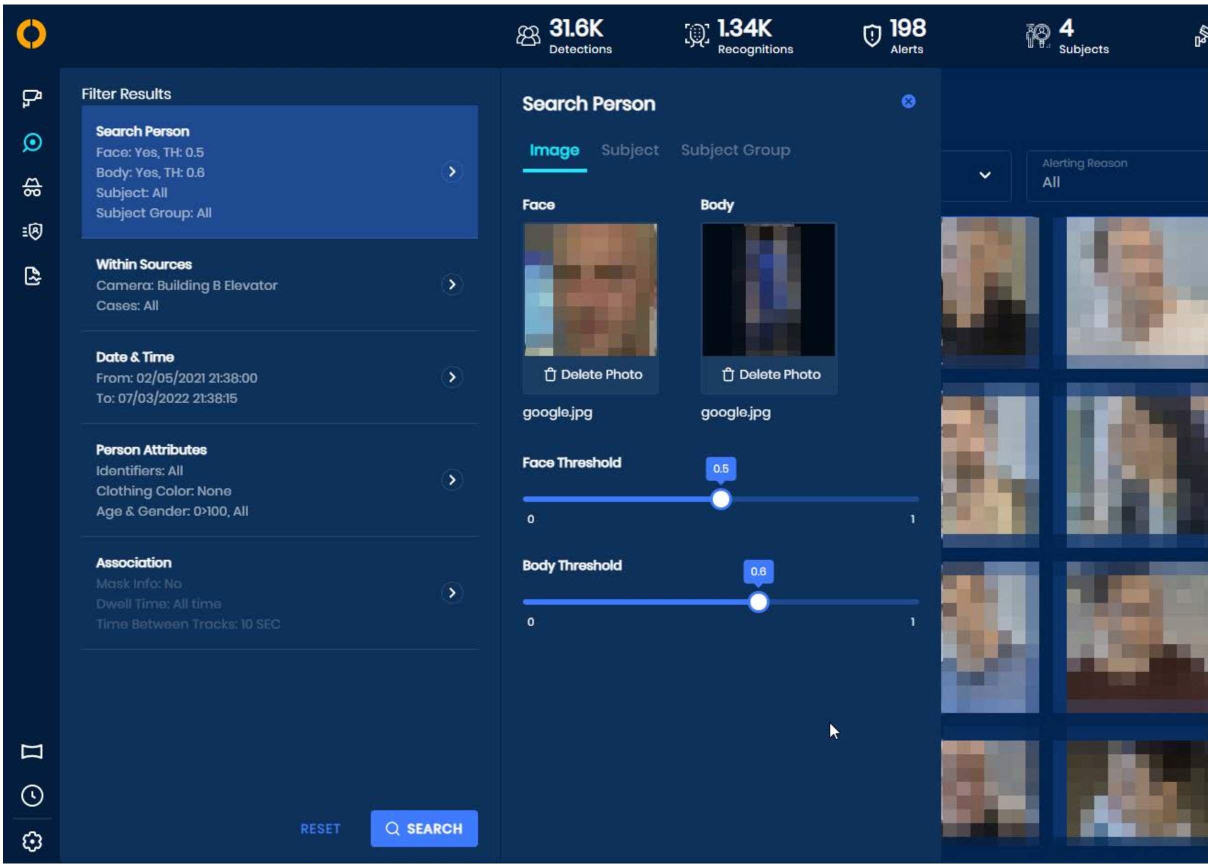
Search by Person

Within *Search Person*, you are able to *Search for* people in a few ways

- By Image (face / body)
- By Existing Track
- By Subjet
- By Watchlist specific Subjet Group

Search By Image

Let's you upload an image (Face / Body / Person) to search for a match in the system, at the same time the thresholds can be set for the face and body images.



Filter Results

Search Person
Face: Yes, TH: 0.5
Body: Yes, TH: 0.6
Subject: All
Subject Group: All

Within Sources
Camera: Building B Elevator
Cases: All

Date & Time
From: 02/05/2021 21:38:00
To: 07/03/2022 21:38:15

Person Attributes
Identifiers: All
Clothing Color: None
Age & Gender: 0>100, All

Association
Mask Info: No
Dwell Time: All time
Time Between Tracks: 10 SEC

Search Person

Image | Subject | Subject Group

Face: google.jpg

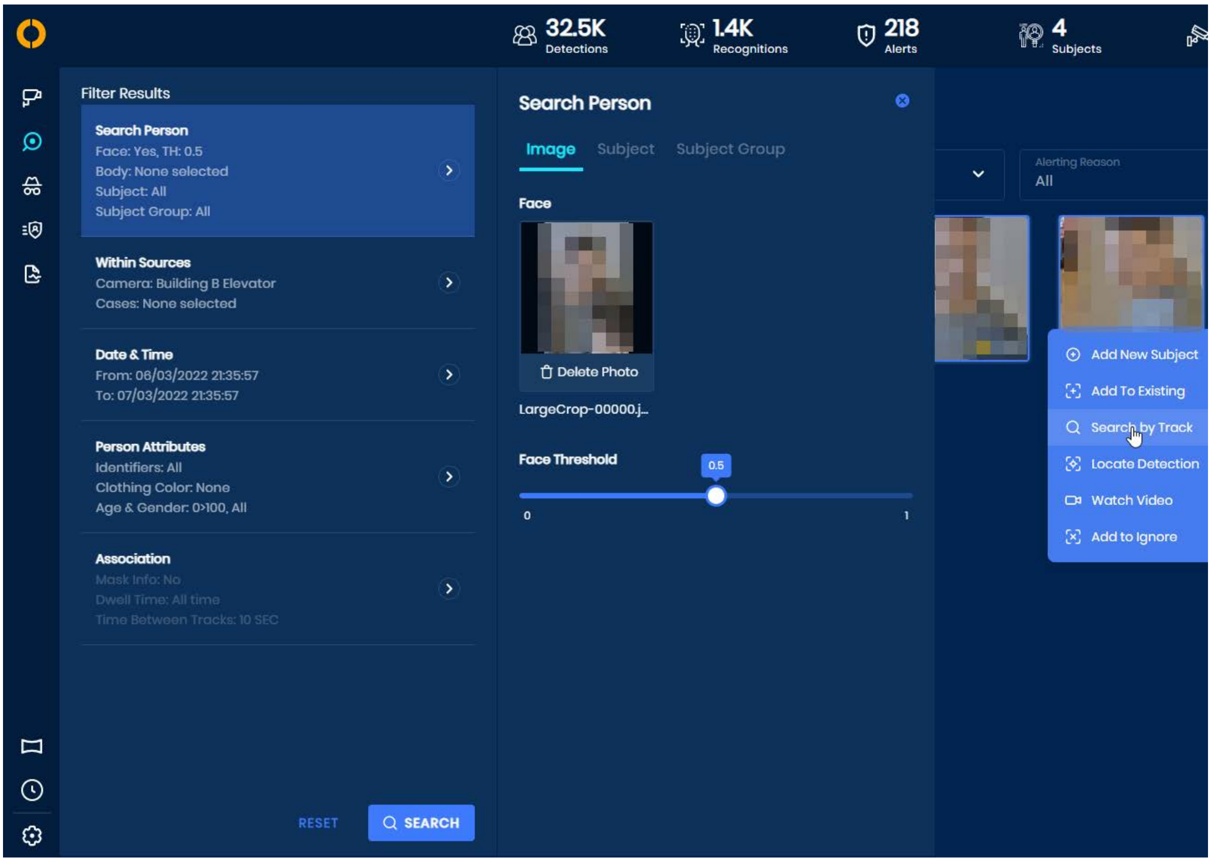
Body: google.jpg

Face Threshold: 0.5 (0 – 1)

Body Threshold: 0.6 (0 – 1)

Search By Existing Track

As above "Search by image" you can select an existing detection in the system and trigger search by track



32.5K Detections | 1.4K Recognitions | 218 Alerts | 4 Subjects

Filter Results

Search Person
Face: Yes, TH: 0.5
Body: None selected
Subject: All
Subject Group: All

Within Sources
Camera: Building B Elevator
Cases: None selected

Date & Time
From: 06/03/2022 21:35:57
To: 07/03/2022 21:35:57

Person Attributes
Identifiers: All
Clothing Color: None
Age & Gender: 0>100, All

Association
Mask Info: No
Dwell Time: All time
Time Between Tracks: 10 SEC

Search Person

Face

LargeCrop-00000.j...

Face Threshold: 0.5

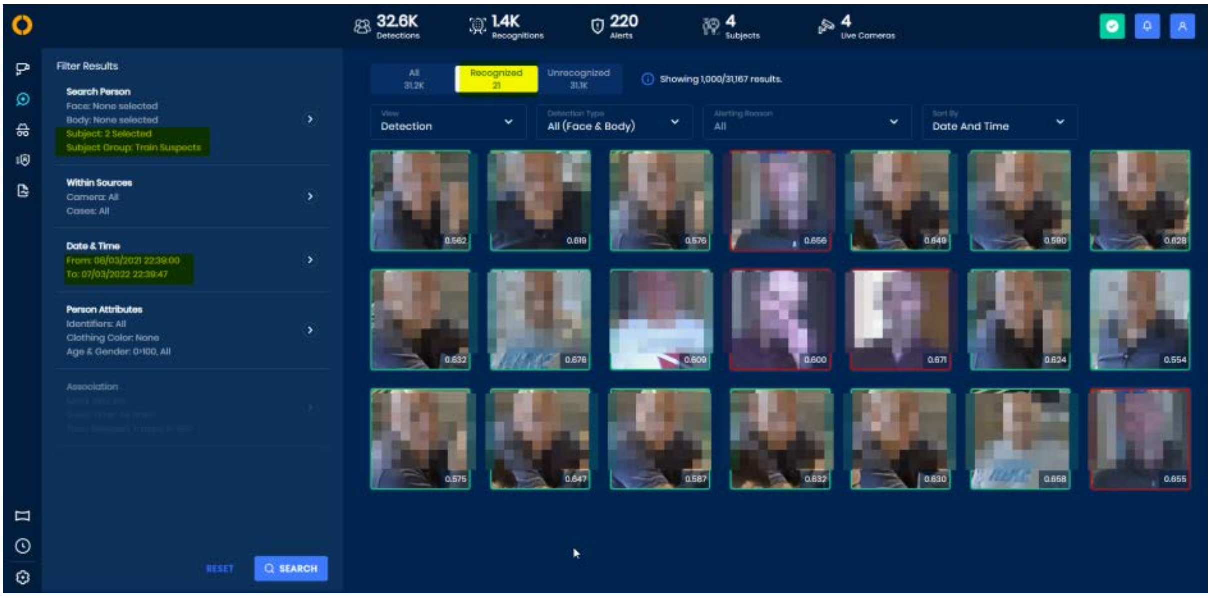
Alerting Reason: All

Filter By Subject / Subject Group

When Selecting by subject or by a subject group you can search for specific subjects by name or multiple subjects (within a group) by subject group name.

It is possible to mix multiple subjects and subject groups. When selecting these subjects or subjects groups the results will filter anyone who is not currently in the person selection (except for unrecognized people).

This allows easy investigations by timeline showing only who you are interested in and anyone you haven't currently identified as known.



32.6K Detections | 1.4K Recognitions | 220 Alerts | 4 Subjects | 4 Live Cameras

Filter Results

Search Person
Face: None selected
Body: None selected
Subject: 2 Selected
Subject Group: Train Suspects

Within Sources
Camera: All
Cases: All

Date & Time
From: 08/03/2021 22:39:00
To: 07/03/2022 22:39:47

Person Attributes
Identifiers: All
Clothing Color: None
Age & Gender: 0>100, All

Association

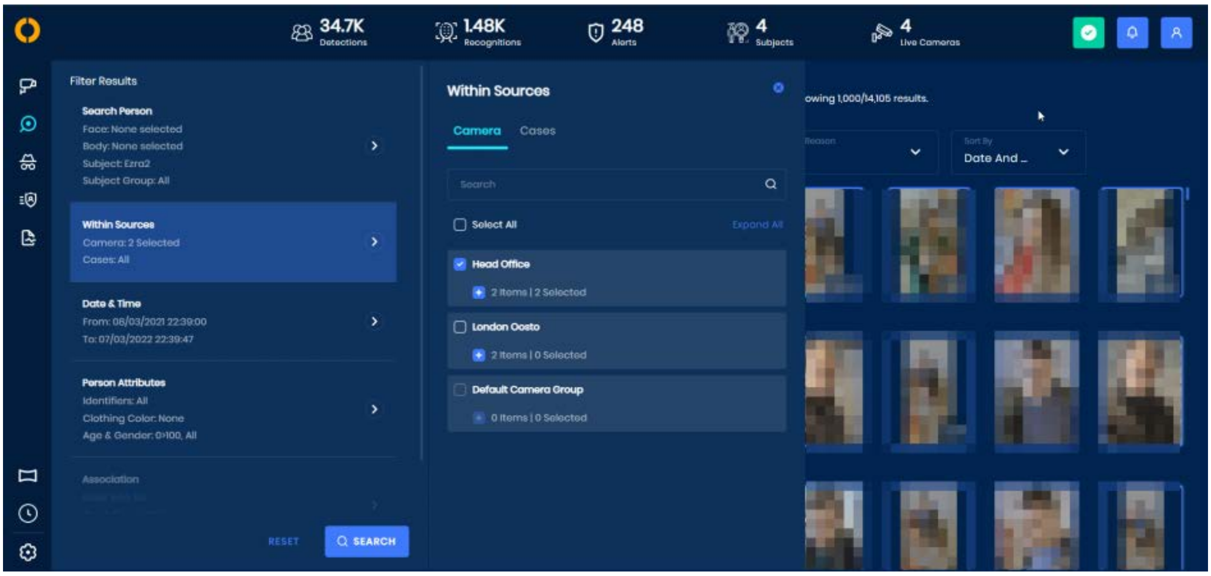
All 31.2K | Recognized 21 | Unrecognized 31.1K

Showing 1,000/31,167 results.

View: Detection
Detection Type: All (Face & Body)
Alerting Reason: All
Sort By: Date And Time

Within Sources

Clicking **Within Sources** allows you to select **cameras/camera groups** and **Cases/files** you would like to search by. As with the live tree view it is easy to search by all entities and select individual cameras/files or case(s)/camera groups(s).



Filter Results

Search Person
Face: None selected
Body: None selected
Subject: Ezra2
Subject Group: All

Within Sources
Camera: 2 Selected
Cases: All

Date & Time
From: 08/03/2021 22:39:00
To: 07/03/2022 22:39:47

Person Attributes
Identifiers: All
Clothing Color: None
Age & Gender: 0>100, All

Association

Within Sources

□ Select All

☑ Head Office
2 Items | 2 Selected

□ London Oosto
2 Items | 0 Selected

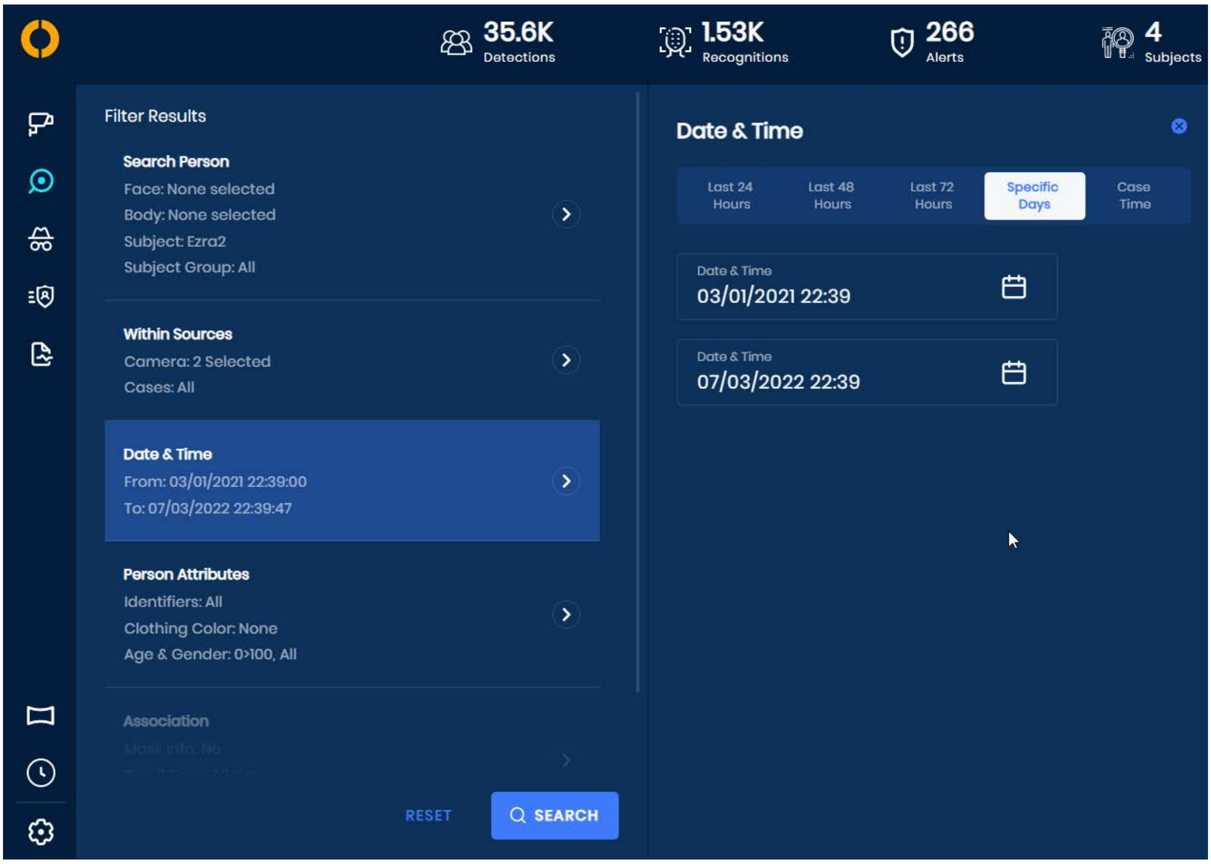
□ Default Camera Group
0 Items | 0 Selected

owing 1,000/14,105 results.

Date and Time

In this section, you can define the date/time frame for when the detections you are searching had taken place. The system allows you to search by specific date/time periods

- Last 24 Hours
- Last 48 Hours
- Last 72 Hours
- Specific Range



Filter Results

Search Person
Face: None selected
Body: None selected
Subject: Ezra2
Subject Group: All

Within Sources
Camera: 2 Selected
Cases: All

Date & Time
From: 03/01/2021 22:39:00
To: 07/03/2022 22:39:47

Person Attributes
Identifiers: All
Clothing Color: None
Age & Gender: 0>100, All

Association
Mask Info: No

Date & Time

Date & Time
03/01/2021 22:39

Date & Time
07/03/2022 22:39

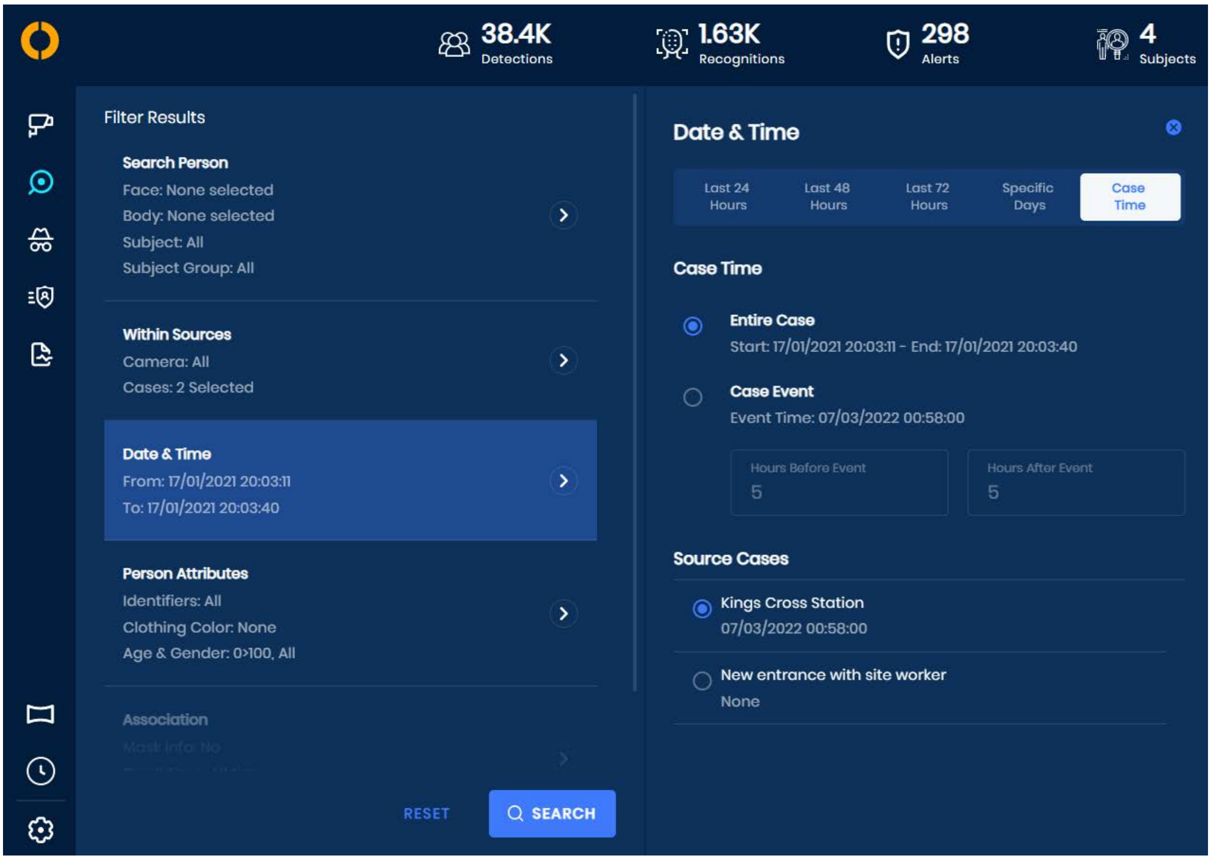
Additionally, the system has two more time frames that are available when cases are selected within sources

- Entire Case Time
- Event Case Time

Entire Case time is automatically calculated based on the entire length of all the file(s)/camera(s) within the selected case. The range is calculated and displayed.

Case Event time is available to be selected if the case selected has a manually entered case event time. This allows you to enter a range of hours around that time if pre-defined. The default is 5 hours before and after the defined time. The currently defined time is shown if set.

If multiple cases are selected within sources you have the option to select which case to define the time range by.



Filter Results

Search Person
Face: None selected
Body: None selected
Subject: All
Subject Group: All

Within Sources
Camera: All
Cases: 2 Selected

Date & Time
From: 17/01/2021 20:03:11
To: 17/01/2021 20:03:40

Person Attributes
Identifiers: All
Clothing Color: None
Age & Gender: 0>100, All

Association
Mask Info: No

Date & Time

Case Time

● Entire Case
Start: 17/01/2021 20:03:11 - End: 17/01/2021 20:03:40

○ Case Event
Event Time: 07/03/2022 00:58:00

Hours Before Event: 5
Hours After Event: 5

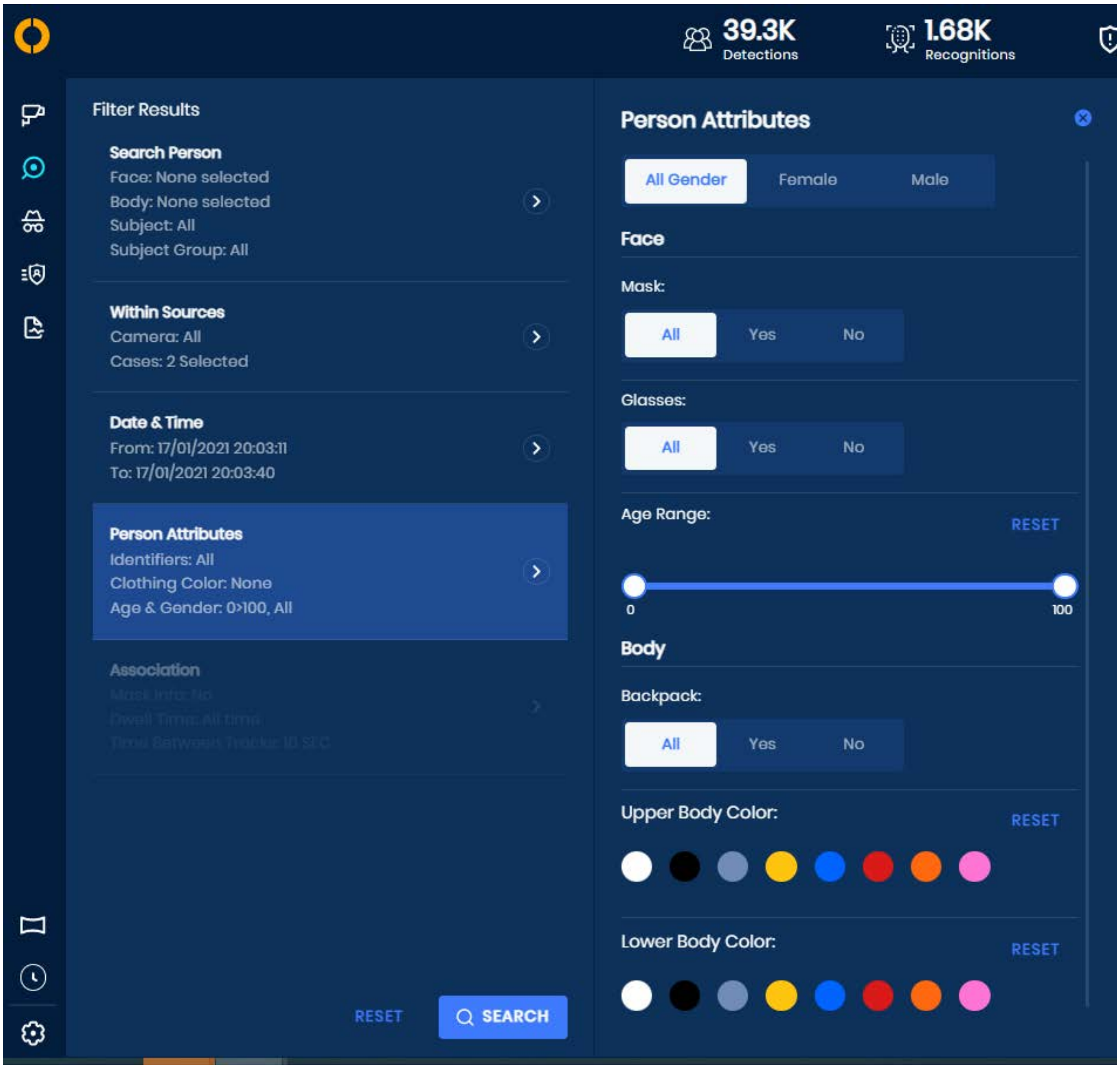
Source Cases

● Kings Cross Station
07/03/2022 00:58:00

○ New entrance with site worker
None

Person Attributes

Attributes search is available to reduce the results based on identifiable traits of the subjects being searched for. Different attributes are available for Face and body detections.



39.3K Detections

1.68K Recognitions

Filter Results

Search Person
Face: None selected
Body: None selected
Subject: All
Subject Group: All

Within Sources
Camera: All
Cases: 2 Selected

Date & Time
From: 17/01/2021 20:03:11
To: 17/01/2021 20:03:40

Person Attributes
Identifiers: All
Clothing Color: None
Age & Gender: 0>100, All

Association
Mask Info: No
Dwell Time: All time
Time Between Tracks: 10 SEC

RESET　SEARCH

Person Attributes

All Gender | Female | Male

Face

Mask: All | Yes | No

Glasses: All | Yes | No

Age Range: 0 – 100　RESET

Body

Backpack: All | Yes | No

Upper Body Color:　RESET

○ ● ● ● ● ● ● ●

Lower Body Color:　RESET

○ ● ● ● ● ● ● ●

Face

- Gender
- Mask
- Glasses
- Age Range

Body

- Backpack
- Top Color
- Bottom Color

Each block of attributes are "AND" queries and between the block, they are "OR" allowing both face and body results to be returned. When searching by image face or body the attributes are filtered accordingly.

Association

Association Section for Contact Tracing

The Association section will bring you to a contact tracing search as opposed to a regular search for a POI. Leave this section empty if you are attempting to conduct a regular search.

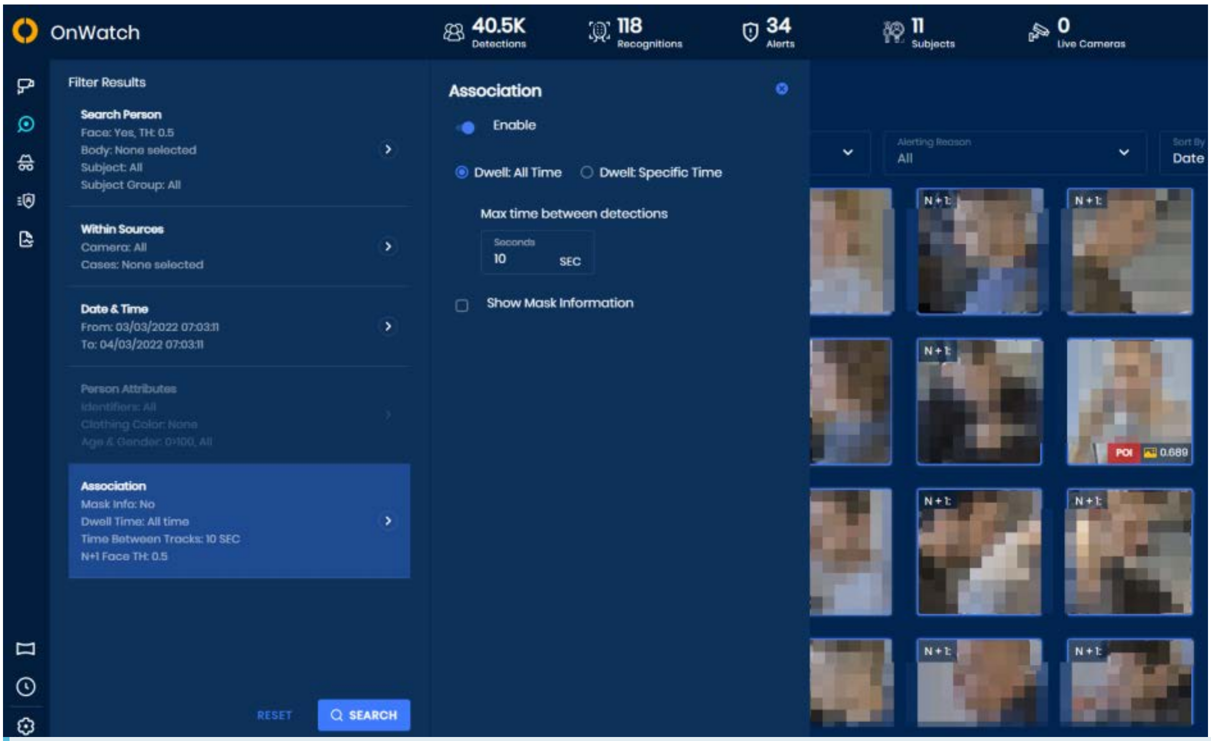
Check out our full contact tracing guide here if you'd like to use association.

Association is the concept of knowing and understanding who a person has been in contact with while located within a camera's FOV. We determine "contact" by calculating dwell time, which essentially translates to how long two people were next to each other.

To use association you should upload an image or search by a track and set a threshold that will enable the association filter. Once the filter becomes available the association search can be selected and enabled. Allowing you to search by:

All associations during the time period

- Without a specific dwell time
- With a specific dwell time
- Show /Hide mask information



Filter Results

Search Person
Face: Yes, TH: 0.5
Body: None selected
Subject: All
Subject Group: All

Within Sources
Camera: All
Cases: None selected

Date & Time
From: 03/03/2022 07:03:11
To: 04/03/2022 07:03:11

Person Attributes
Identifiers: All
Clothing Color: None
Age & Gender: 0-100, All

Association
Mask Info: No
Dwell Time: All time
Time Between Tracks: 10 SEC
N+1 Face TH: 0.5

Association

Enable

● Dwell: All Time ○ Dwell: Specific Time

Max time between detections

Seconds
10 SEC

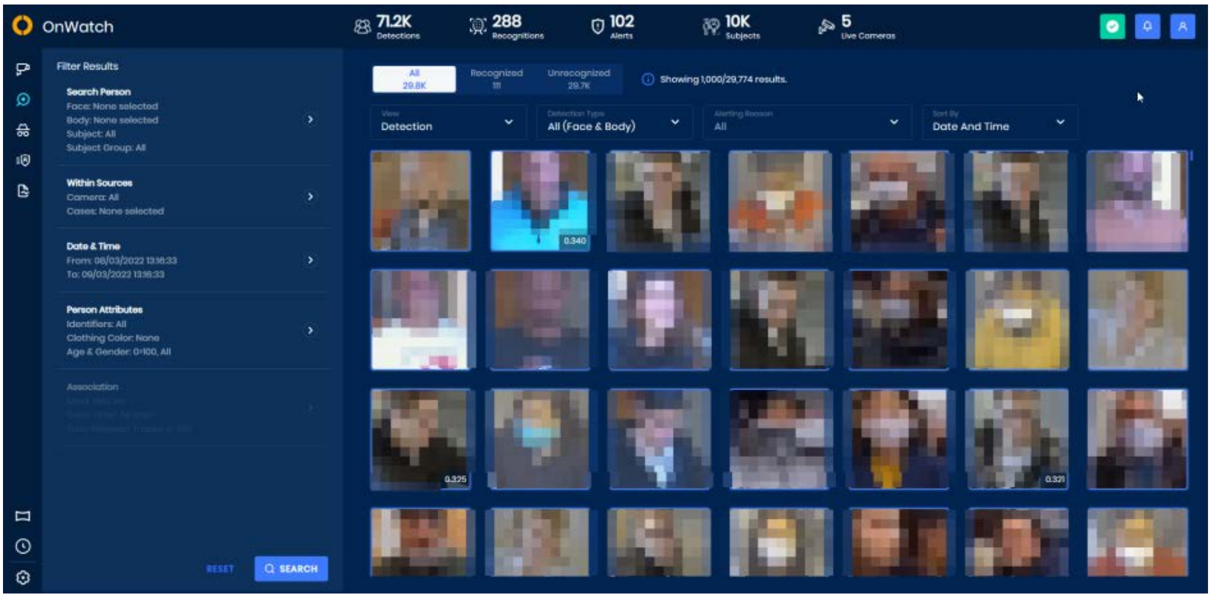
□ Show Mask Information

Want to know more?

Check out our full contact tracing guide here.

Results Pane

After clicking **Search**, the system will display the detections that match the filters and parameters placed in the search filter tab. The results pane will display the top 1000 recognition in the user interface but works with up to 50,000 results on the server.



Search Person
Face: None selected
Body: None selected
Subject: All
Subject Group: All

Within Sources
Camera: All
Cases: None selected

Date & Time
From: 08/03/2022 13:36:33
To: 09/03/2022 13:36:33

Person Attributes
Identifiers: All
Clothing Color: None
Age & Gender: 0-100, All

All 29.8K | Recognized 111 | Unrecognized 29.7K

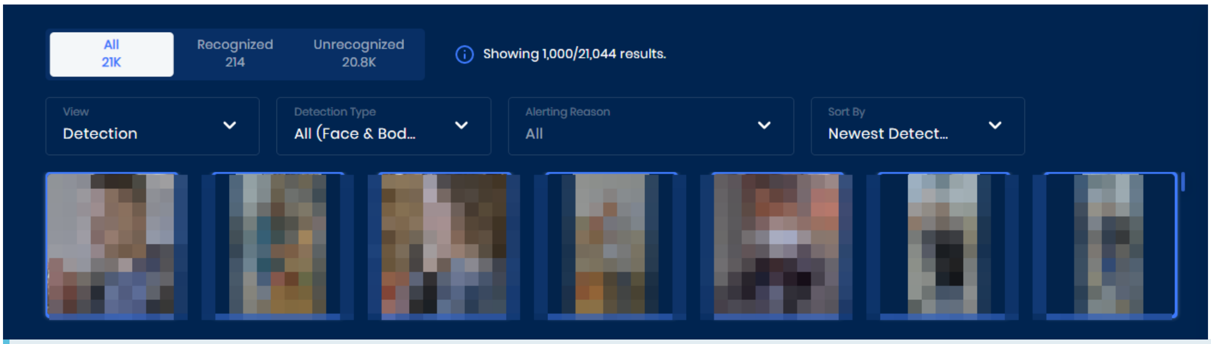
Showing 1,000/29,774 results.

View: Detection
Detection Type: All (Face & Body)
Alerting Reason: All
Sort By: Date And Time

The search results pane is organized to quickly filter the subset of results obtained in the original large database search query. Once the subset of results are available they can be quickly manipulated.

Results Control Bar (first row)

Within the results, the first row shows:
All, **Recognized** and **Unrecognized** which also have a count of results under them. When selecting it will show the relevant detections.



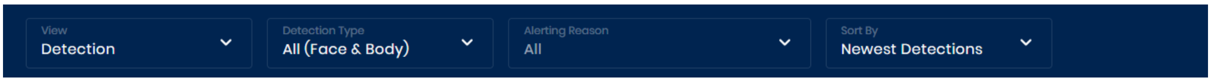
All 21K | Recognized 214 | Unrecognized 20.8K

Showing 1,000/21,044 results.

View: Detection
Detection Type: All (Face & Bod...
Alerting Reason: All
Sort By: Newest Detect...

> **Note**
>
> If the initial search is over 1000 results a total count will be displayed

Results control bar (second row)



View: Detection
Detection Type: All (Face & Body)
Alerting Reason: All
Sort By: Newest Detections

The following options can be selected:

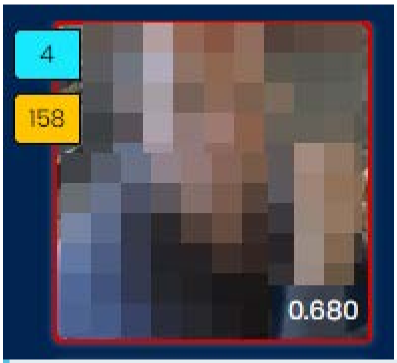
View

- *Detection* - Provides a view of each individual detection within the search results
- *Aggregate* - Provides a view that aggregates recognitions and detections showing a count of the number of detections as well as the number of sources those detections were found within. This can be useful to reduce noise within the view.

📘 **Note**

The image shown on is the image with the highest recognition score

The example below is: Martin who was a Recognized Subject (Red Border) was seen in 4 sources (Blue tab) detected 158 times (Yellow tab)



📘 **Note**

When aggregating recognized subjects the database is able to match all detections of the individual across all cameras.

When aggregating unrecognized people the system will do this on the same camera group as long as we have less than 90 seconds gap between detections

Detection Type Allows the recognition types of face/body to be filtered. Each type has a number count.

- *All*
- *Face*
- *Body*

📘 **Note**

Disabled in "aggregate view"

Alerting Reason - Any detection that was triggered via an alerting rule can be filtered within the 50K results

- *All*
- *Unauthorized Subject Matched*
- *Unauthorized Time Restricted Subject Matched*
- *Unauthorized Unknown Person*
- *Authorized Subject Matched*
- *Subject has No Mask (Not Allowed)*
- *Subject has No Mask (Allowed)*
- *Spoof attempt (Not Allowed)*
- *Spoof attempt (Blocked)*
- *None*

> 📘 Note
>
> Disabled in "aggregate view"

Sort by

- Newest Detections - Sort by latest detections time/date order
- Number of Detections - Sort by most recognitions in the aggregate view
- Score - Sort by Score of recognition

View the detection
At any time a detection/recognition can be hovered above, clicked to view the timeline and controlled with actions

- When hovering you will see the camera/case name
- When clicking you will view the full timeline "unfiltered to the search" For more information please view View a Subject's Detection Timeline
- When selecting the three circles you will receive an actions menu

Inquiry Management

Overview

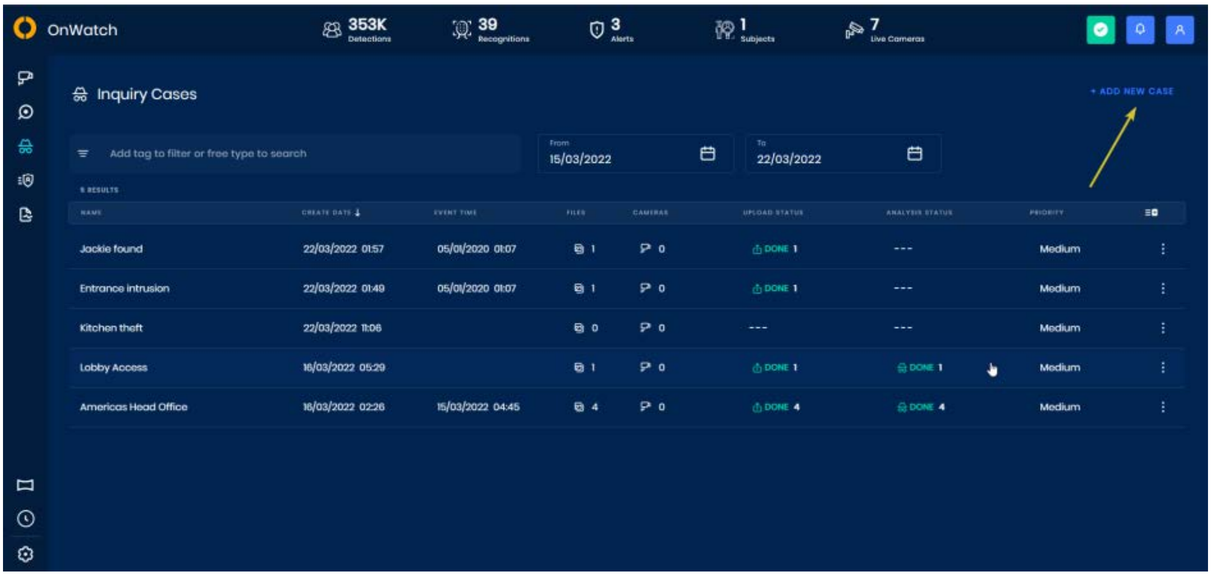
Easily manage and investigate all your open security cases by searching through hours of offline video footage for persons of interest in a matter of seconds.

By breaking down your security events into cases and monitoring each case independently with cutting-edge facial recognition, OnWatch helps you investigate any appearances of bad actors to gain situational awareness and understand previous attacks.

> 📘 For step-by-step instructions on how to open an inquiry case, click here.

Case Management

Navigate to the **Inquiry** section of the OnWatch system to view all your existing cases and add new ones. Each case can contain multiple video or image files as well as associated live cameras that you can analyze and search for subjects or persons of interest.



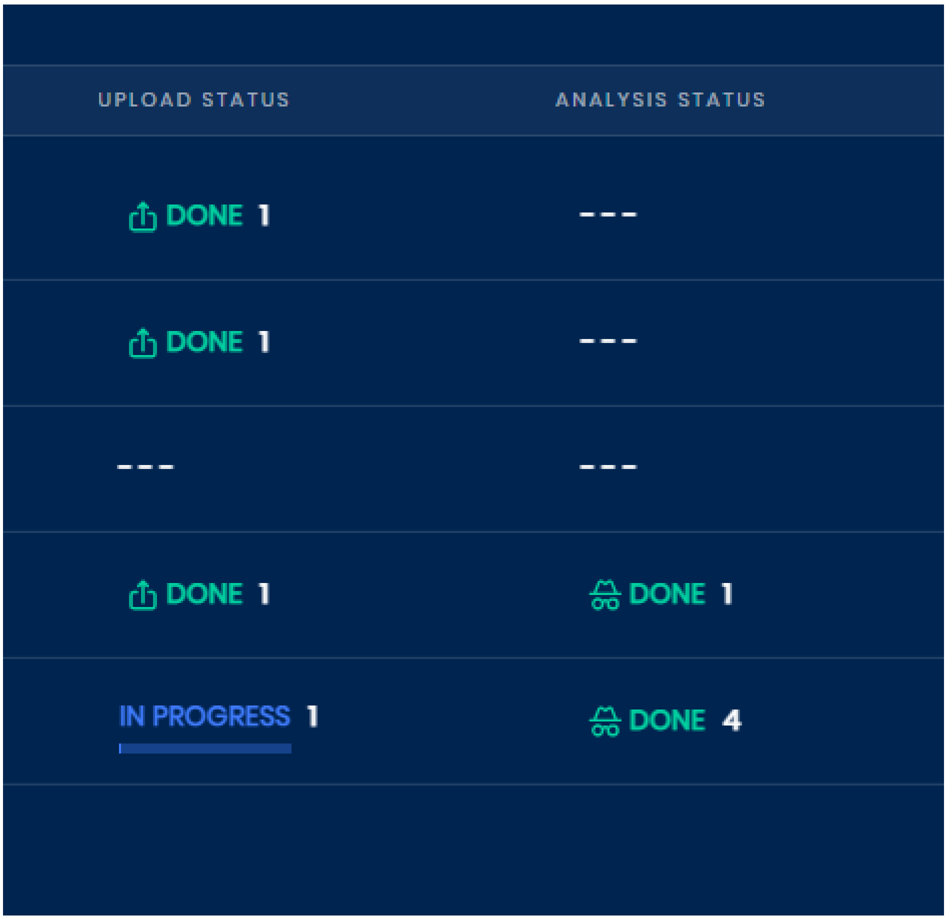
NAME	CREATE DATE	EVENT TIME	FILES	CAMERAS	UPLOAD STATUS	ANALYSIS STATUS	PRIORITY
Jackie found	22/03/2022 01:57	05/01/2020 01:07	1	0	DONE 1	---	Medium
Entrance intrusion	22/03/2022 01:49	05/01/2020 01:07	1	0	DONE 1	---	Medium
Kitchen theft	22/03/2022 11:06		0	0	---	---	Medium
Lobby Access	16/03/2022 05:29		1	0	DONE 1	DONE 1	Medium
Americas Head Office	16/03/2022 02:26	15/03/2022 04:45	4	0	DONE 4	DONE 4	Medium

You can add a new case by clicking **Add New Case** at the top of the screen. Once added, they will appear on the main Inquiry screen and the case will be opened waiting for files to be uploaded or cameras to be associated .

> ## 👍 Supported File Types and Size
>
> We currently support AVI, MP4, MKV, PNG, JPG, TIFF, BMP
> Supported file size: 15GB per file
> Standard codec support: Mpeg-4 H264/5, MPEG transport stream H264/5, Webm - VP8/9, Motion jpeg

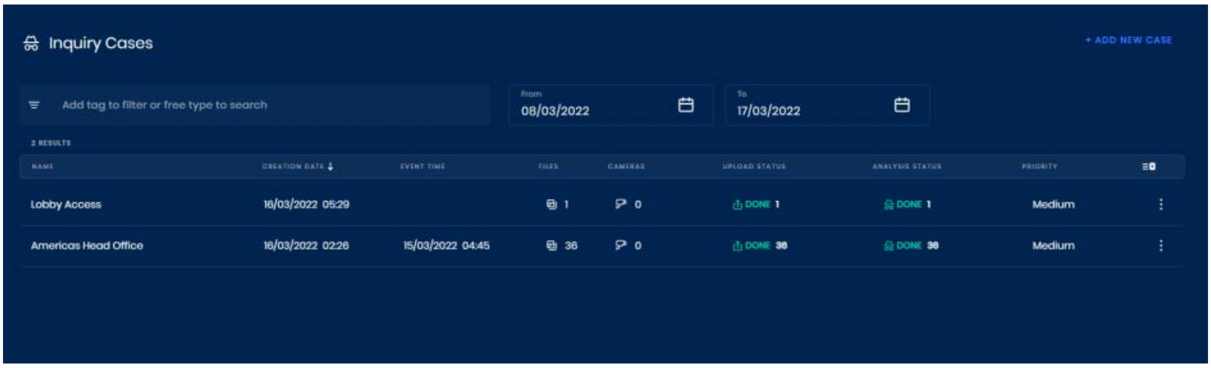
You are able to view the overall current status of the uploaded and analyzing files.

- - - - indicating no files in this stage
- **Progress** (Count of files left) - How many files are still actively being actioned at this stage
- **Completed** (count of completed/total files) - Indicated how many files are completed successfully showing if any are no longer being actioned. When editing the case details for each file can be seen
- **Done** (All files have successfully completed this stage)



UPLOAD STATUS	ANALYSIS STATUS
DONE 1	---
DONE 1	---
---	---
DONE 1	DONE 1
IN PROGRESS 1	DONE 4

You can search through the case video for subject names as well as filter by the creation date range.



From 08/03/2022

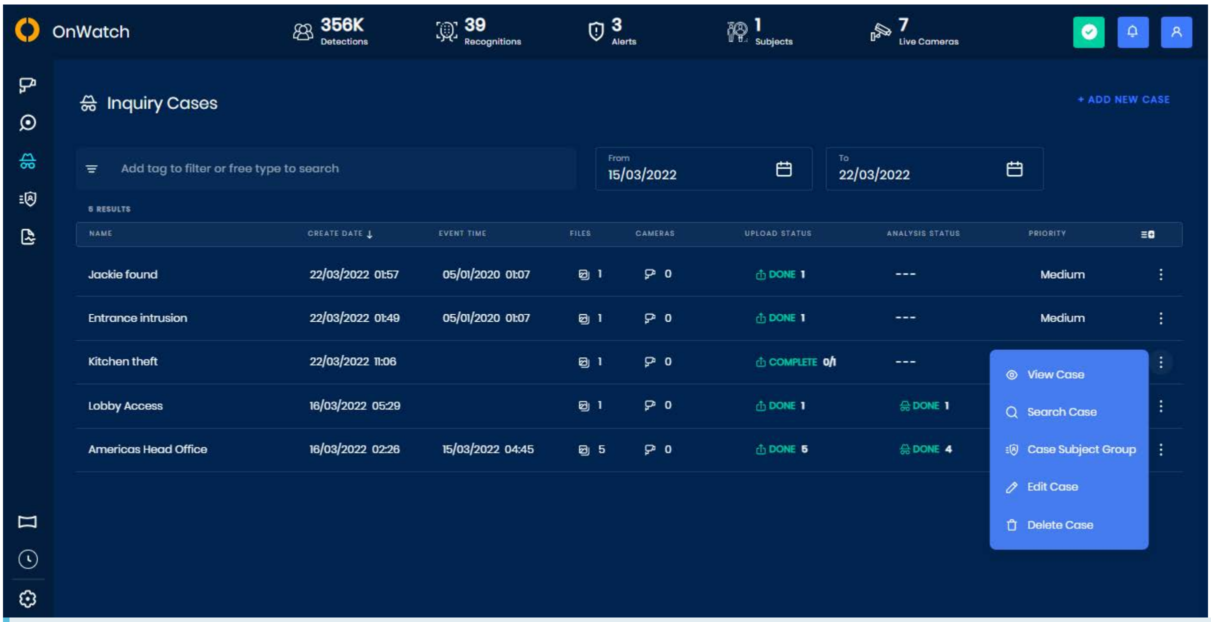
To 17/03/2022

2 RESULTS

NAME	CREATION DATE ↓	EVENT TIME	FILES	CAMERAS	UPLOAD STATUS	ANALYSIS STATUS	PRIORITY
Lobby Access	16/03/2022 05:29		1	0	DONE 1	DONE 1	Medium
Americas Head Office	16/03/2022 02:26	15/03/2022 04:45	36	0	DONE 36	DONE 36	Medium

At this stage, you can Open any existing case by selecting it or from the action dialogue clicking edit
You can also action each case by:

- Deleting the case - Cases will be auto-deleted with the case retention time
- View Case - You will be directed to the **View Sources** screen. to see the latest cases detections and alerts
- Search the case - You will be directed to the **Search** with all the cases detections utilizing the search capabilities to investigate the case content
- View the cases associated subject groups - You will be directed to the **Watchlist** with the current cases selected subject groups



Inquiry Cases

+ ADD NEW CASE

Add tag to filter or free type to search

From 15/03/2022

To 22/03/2022

5 RESULTS

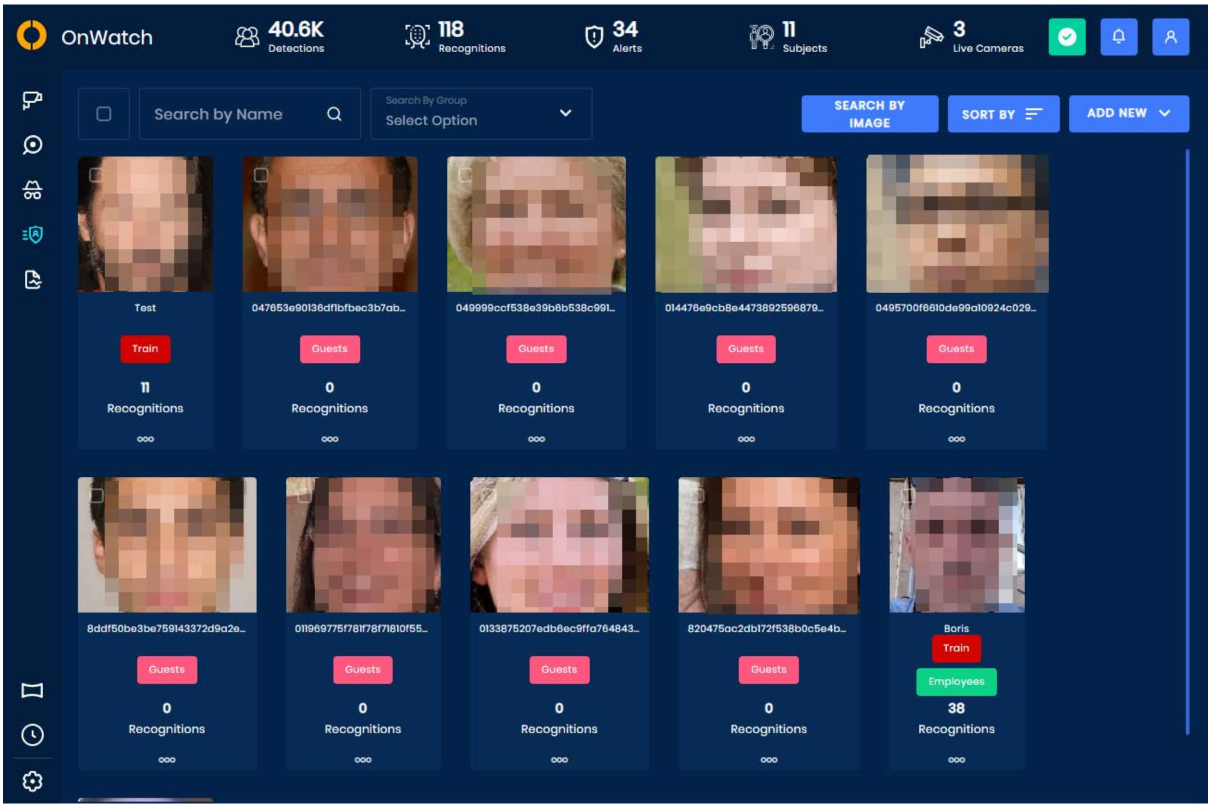
NAME	CREATE DATE ↓	EVENT TIME	FILES	CAMERAS	UPLOAD STATUS	ANALYSIS STATUS	PRIORITY
Jackie found	22/03/2022 01:57	05/01/2020 01:07	1	0	DONE 1	---	Medium
Entrance intrusion	22/03/2022 01:49	05/01/2020 01:07	1	0	DONE 1	---	Medium
Kitchen theft	22/03/2022 11:06		1	0	COMPLETE 0/1	---	
Lobby Access	16/03/2022 05:29		1	0	DONE 1	DONE 1	
Americas Head Office	16/03/2022 02:26	15/03/2022 04:45	5	0	DONE 5	DONE 4	

Concurrent Usage

- If the system is utilized with live streams concurrently the least used GPU will be used to initiate the inquiry processing
- Live streams are given resource preference over any inquiry streams on a shared GPU
- If the system is dedicated to Inquiry only please ask your Oosto representative to adjust the configuration for "target_framerate" to unlimited which will override live stream preferences

Watch List

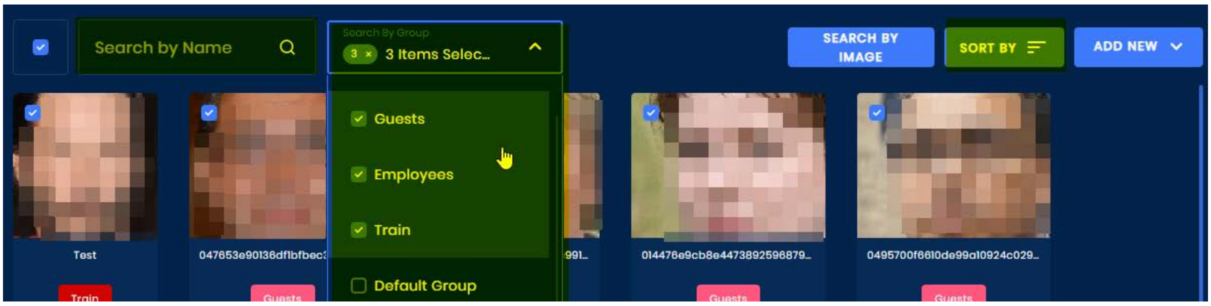
The Watch List is a library of all subjects defined in the system. It can be accessed by clicking on the **Watch List** tab on the left navigation pane.



Organize and Find Watchlist Subjects

The Watchlist allows subjects to be easily managed:

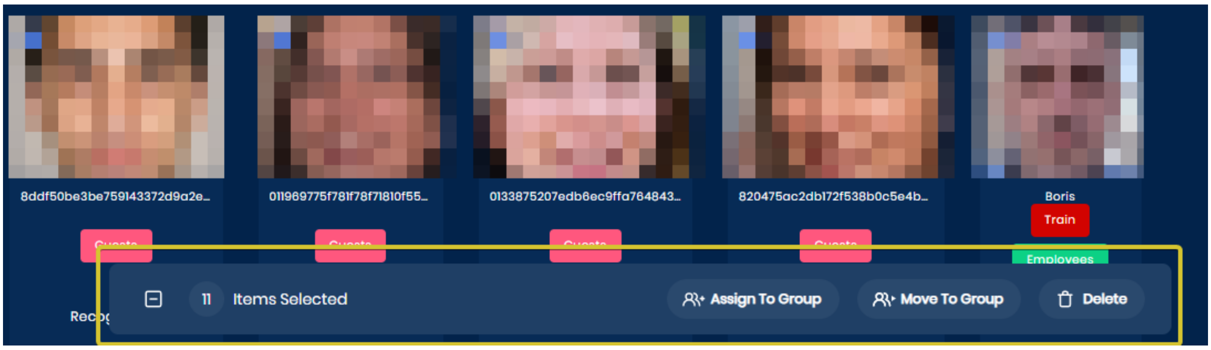
- Search by Subject Name
- Filter by Subject Group Name(s) (This dialogue allows searching, multi-selection and clearing of selected names)
- Sort by (Name, Most recognitions, Newest recognitions and creation date)



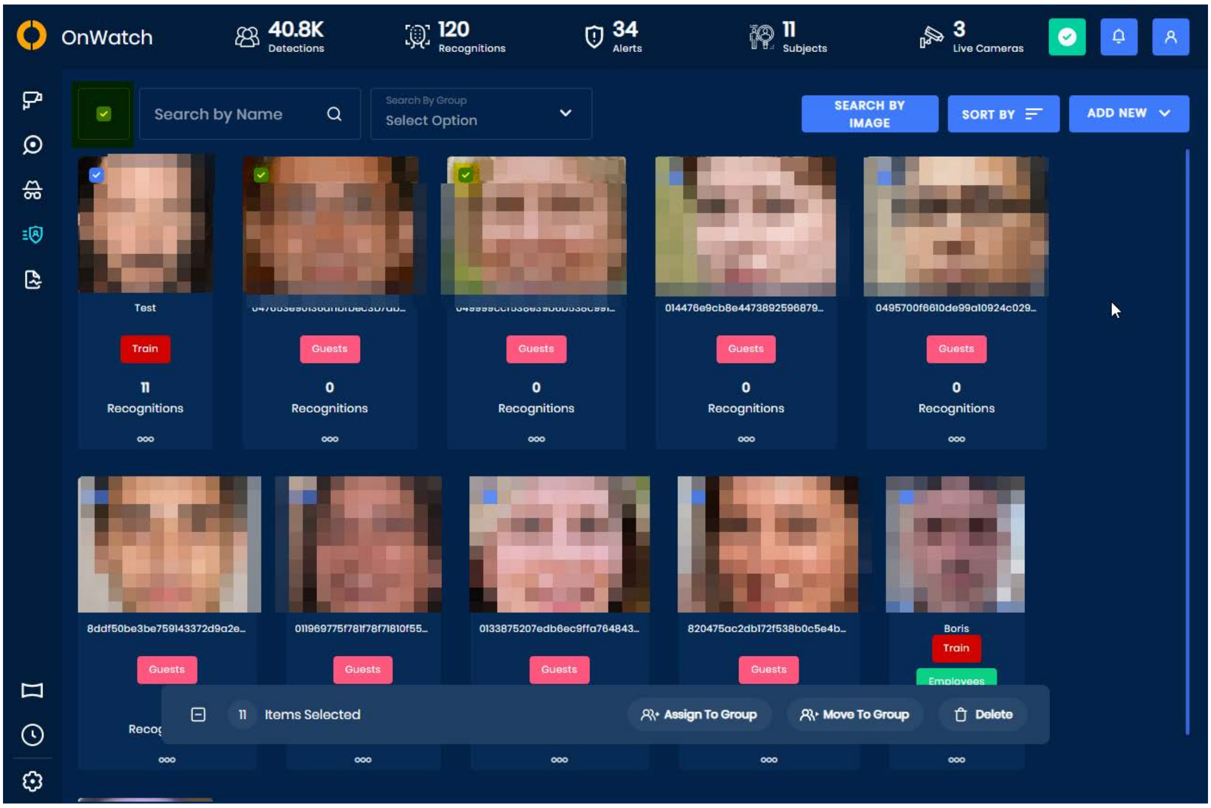
Bulk Watchlist Actions

In addition, multiple subjects can be selected at the same time and bulk actions can be carried out:

- Assign to an additional group
- Move subject to a group (removing them from all existing groups)
- Delete all selected subjects

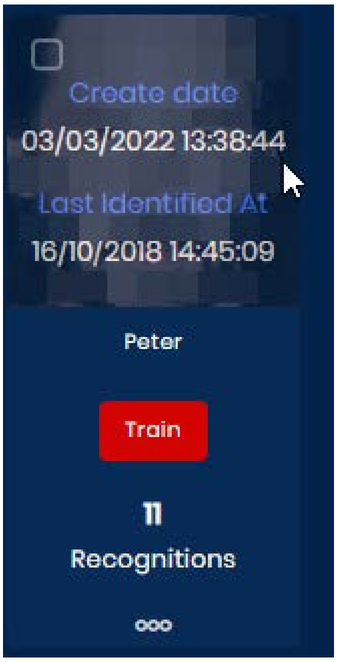

8ddf50be3be759143372d9a2e…
011969775f781f78f71810f55…
0133875207edb6ec9ffa764843…
820475ac2db172f538b0c5e4b…
Boris
Train
Employees
Guests
Recog
11 Items Selected
Assign To Group
Move To Group
Delete

It is possible to select/unselect multiple subjects individually or via a bulk selection check box, when bulk selecting via the check box the system will select all subjects within the current search and not only the ones currently displayed in the user interface.



View, Edit, Delete and Individual Subject

You can see the subject's reference image, name, subject group name(s), and the number of recognitions within the watch list itself.



□

Create date

03/03/2022 13:38:44

Last Identified At

16/10/2018 14:45:09

Peter

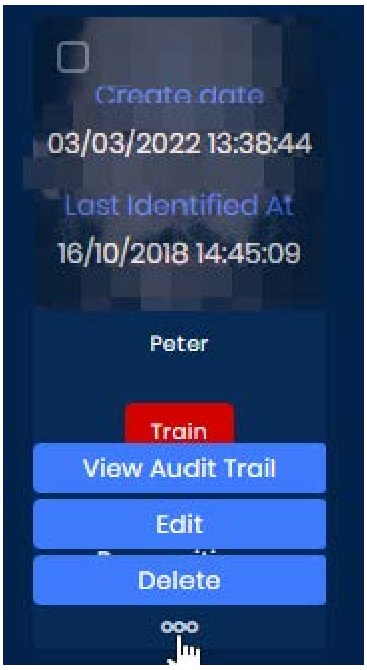
Train

11

Recognitions

Hovering over a specific subject will show the date/time that the subject was created, and the date/time of the most recent recognition.

Clicking the **3-dotted icon** at the bottom of the subject image allows you to *Edit* or *Delete* the subject. As well as showing an audit of changes that have occurred

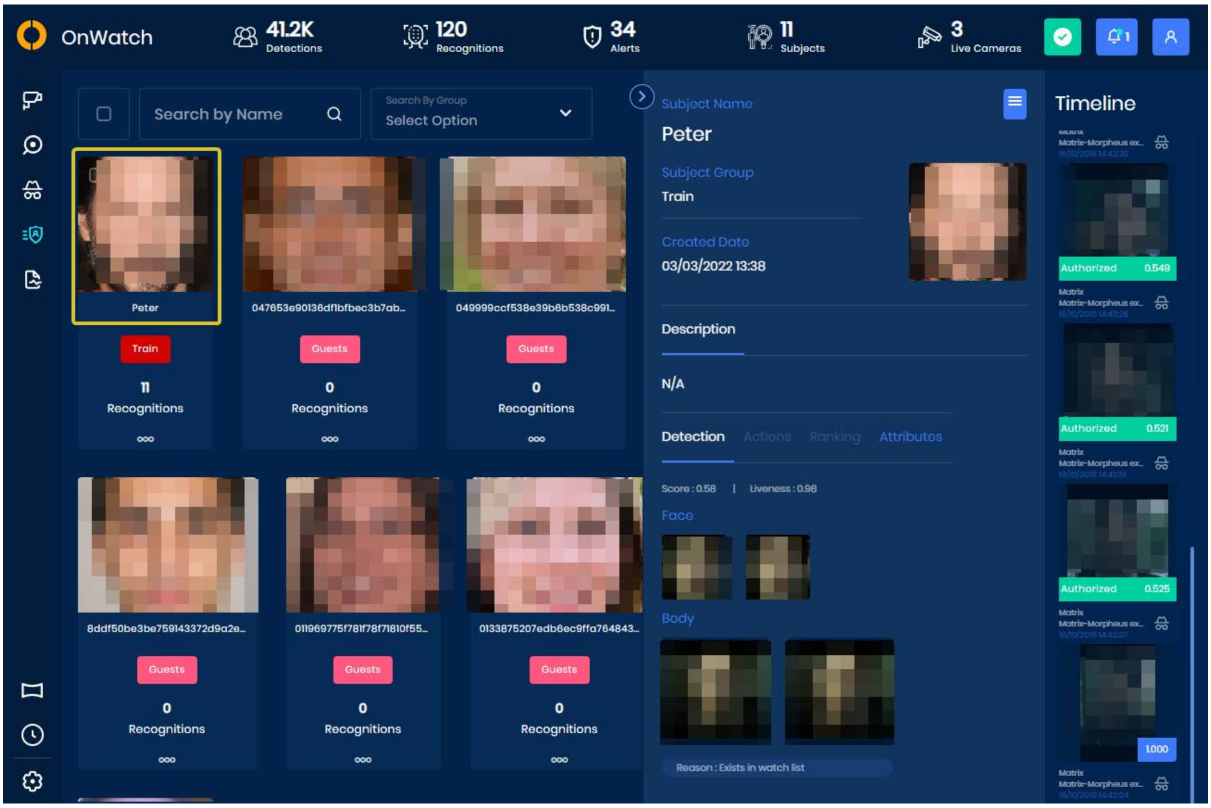


Create date
03/03/2022 13:38:44

Last Identified At
16/10/2018 14:45:09

Peter

Clicking on the subject image itself displays information about the recognized subject's timeline and other detection details.



Subject Name
Peter

Subject Group
Train

Created Date
03/03/2022 13:38

Description

N/A

Score : 0.58 | Liveness : 0.98

Reason : Exists in watch list

Search by Image

Please see the following Search and Sort Subjects in the Watch List

Add a Subject

Please see the following Add, Edit & Delete Subjects

Mass Upload a Large Subject List

Please see the following [Add Subjects via Mass Import]

Reports

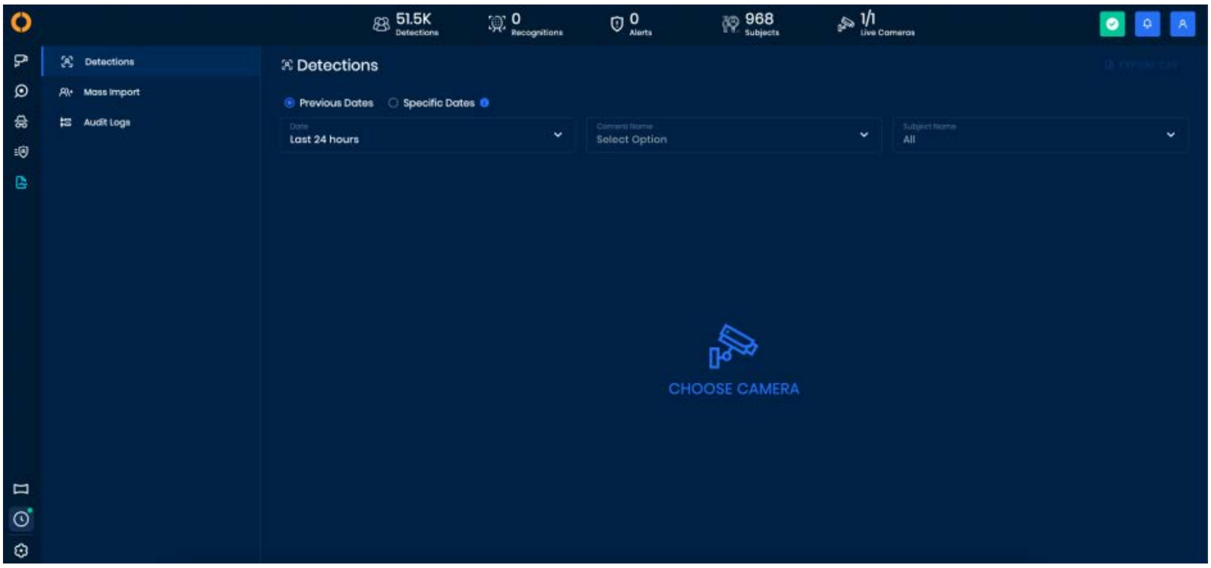
The *Reports* tab provides users with helpful information regarding camera configuration and detection. There are three sections within the Reports tab.

1. Detections - helps users calibrate their camera thresholds and export detection reports
2. Mass Import - showcases the status of a mass subject import
3. Audit Logs - displays actions taken by users of the system

Detections

The **Detections Reports** page has two goals. The first is to help integrators determine and calibrate each camera threshold by investigating how low the threshold can go per camera before incorrect detections are made. The second goal is to enable OnWatch users to export detection reports according to configurable timelines. This helpful information provides users with the total number of detections generated from selected cameras throughout a specified time.

Creating a Detection Report



● Previous Dates ○ Specific Dates

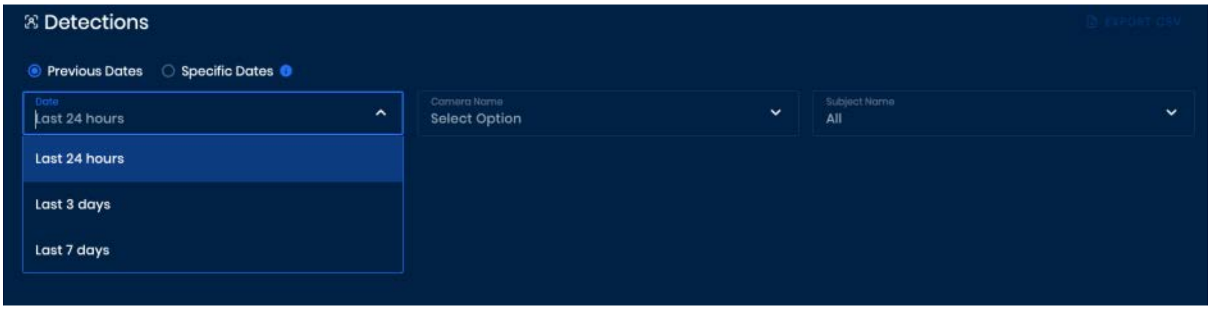
Date: Last 24 hours

Camera Name: Select Option

Subject Name: All

1. Within the *Detections Report* page, fill in the fields at the top of the screen to determine the parameters for the report.

2. On the far left, select the amount of time over which you would like the system to pull the report.



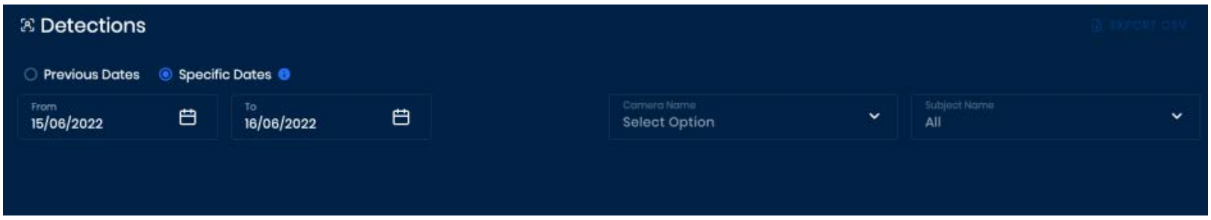
● Previous Dates ○ Specific Dates

Date: Last 24 hours

Camera Name: Select Option

Subject Name: All

Or choose a specific dates -



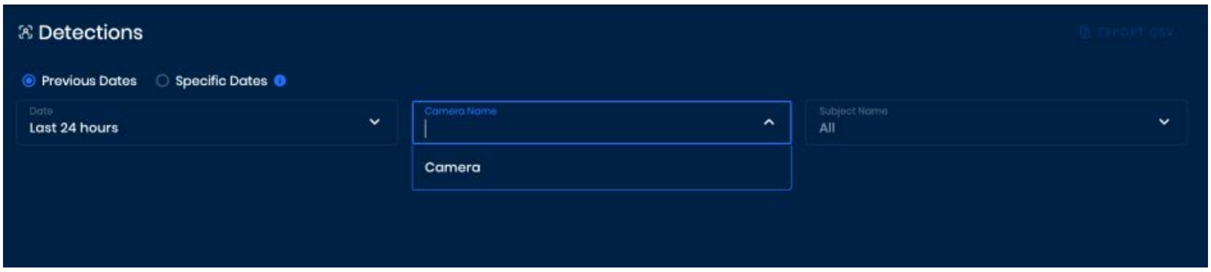
From: 15/06/2022

To: 16/06/2022

Camera Name: Select Option

Subject Name: All

3. In the next box, specify the camera from which you would like the system to pull the report.

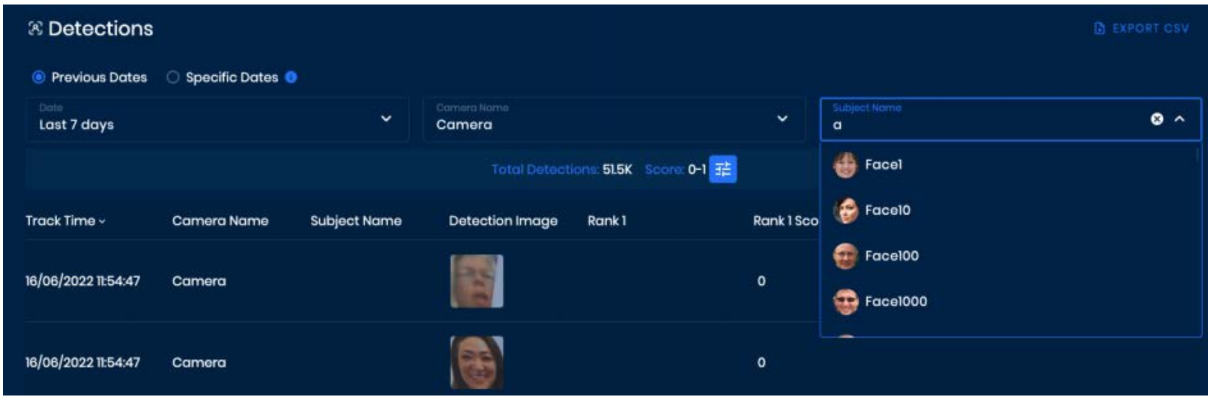


Date: Last 24 hours

Camera Name:

Subject Name: All

4. Fill out the third box if you would like to pull a report on a specific subject if required.



Date: Last 7 days

Camera Name: Camera

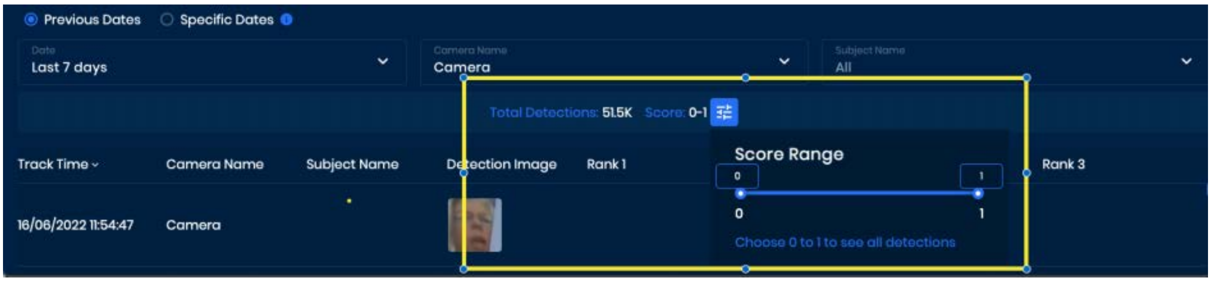
Subject Name: a

Total Detections: 51.5K Score: 0-1

Track Time ⌄	Camera Name	Subject Name	Detection Image	Rank 1	Rank 1 Sco
16/06/2022 11:54:47	Camera				0
16/06/2022 11:54:47	Camera				0

5. Once you have input the parameters, the results will be displayed.

6. At the top of the report, a blue bar will appear detailing the *Total Detections* amount and the *Score* range. Here, you can configure the threshold score range for the report by clicking on the **threshold icon**. Use the sliding scale, which has a total range between 0 and 1 to filter the results.



Date: Last 7 days

Camera Name: Camera

Subject Name: All

Total Detections: 51.5K Score: 0-1

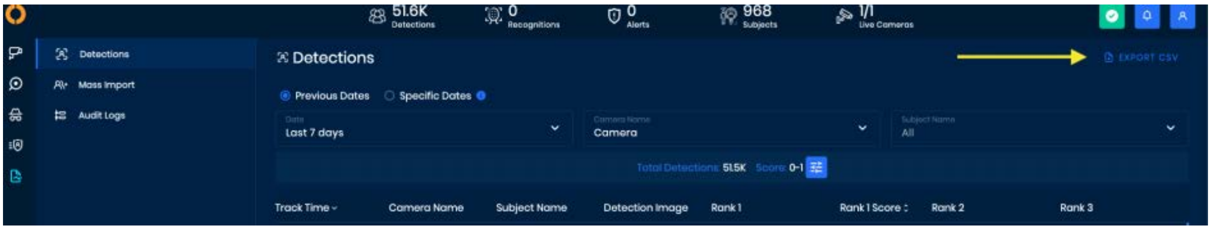
Track Time ⌄	Camera Name	Subject Name	Detection Image	Rank 1	Rank 3
16/06/2022 11:54:47	Camera				

The report is broken into the following categorical columns (listed in order of appearance from left to right):

- *Track Time*: the time at which this track was captured on the camera stream.
- *Camera Name*: the name of the camera that captured the track.
- *Subject Name*: the name of the subject in the track, if he/she is a subject within the system.
- *Detection Image*: the image used to make the detection. If you click the thumbnail, you will see the full-size image.
- *Rank 1*: the subject in the system who is the closest match to the *Detection Image*. Clicking the thumbnail will show the full-size image. A subject will only be shown as a Rank if it exceeds at least a 0.3 score match.
- *Score*: the score conveying the strength of the match between *Rank 1* and the *Detection Image*.
- *Rank 2*: if there is another subject in the system who is the second closest match to the *Detection Image*, it will be shown here. This metric is shown alongside a corresponding match score. Clicking the thumbnail will show the full-size image.

- *Rank 3*: if there is another possible subject in the system who is the third closest match to the *Detection Image*, it will be shown here. This metric is shown alongside a corresponding match score. Clicking the thumbnail will show the full-size image.

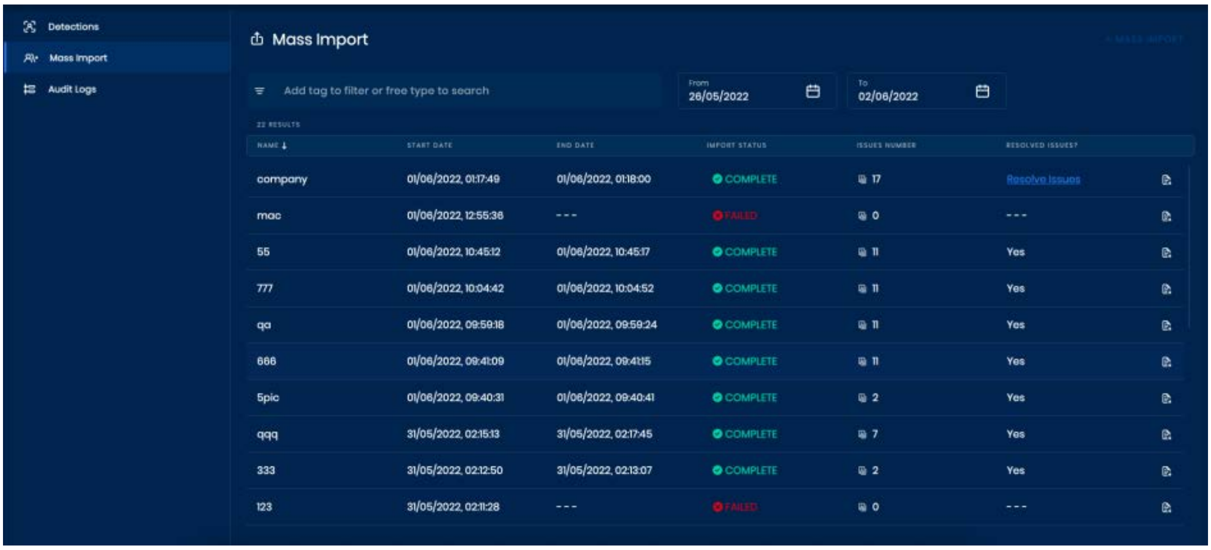
To export the report as a CSV file, click the **Export** tab on the upper right-hand corner of the page. Then, click **Export CSV**.



The file will be downloaded into your browser download folder.

Mass Import

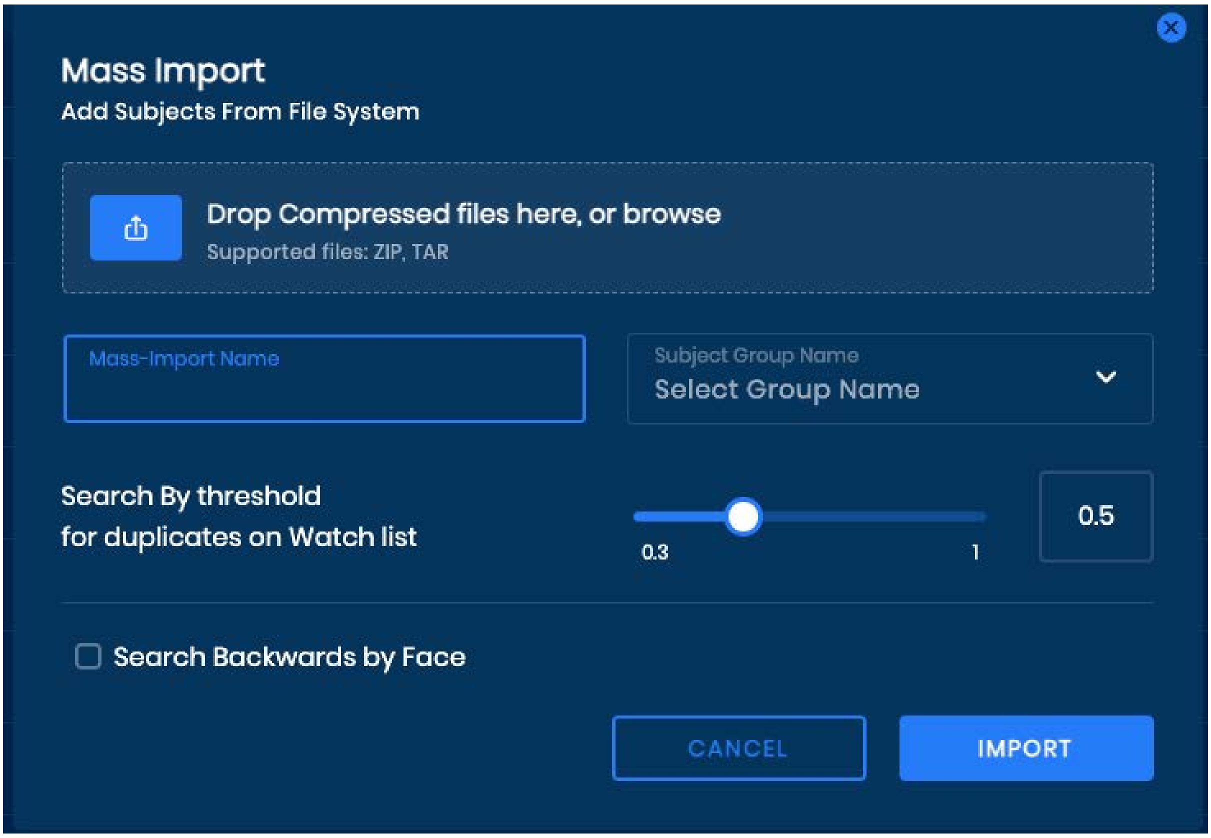
The Mass Import Reports page provides a status summary of mass imports that are made within the system. It allows you to understand which subjects were successfully added to the watch list and which ones failed.
In part of the Mass Import process, the system is checking the uploaded files against all system watchlists (according to user permission) for duplicated names and pictures based on facial features and after the Mass Import uploading is completed there is an option to see all the issues found by the system.



NAME ↓	START DATE	END DATE	IMPORT STATUS	ISSUES NUMBER	RESOLVED ISSUES?
company	01/06/2022, 01:17:49	01/06/2022, 01:18:00	COMPLETE	17	Resolve Issues
mac	01/06/2022, 12:55:36	---	FAILED	0	---
55	01/06/2022, 10:45:12	01/06/2022, 10:45:17	COMPLETE	11	Yes
777	01/06/2022, 10:04:42	01/06/2022, 10:04:52	COMPLETE	11	Yes
qa	01/06/2022, 09:59:18	01/06/2022, 09:59:24	COMPLETE	11	Yes
666	01/06/2022, 09:41:09	01/06/2022, 09:41:15	COMPLETE	11	Yes
5pic	01/06/2022, 09:40:31	01/06/2022, 09:40:41	COMPLETE	2	Yes
qqq	31/05/2022, 02:15:13	31/05/2022, 02:17:45	COMPLETE	7	Yes
333	31/05/2022, 02:12:50	31/05/2022, 02:13:07	COMPLETE	2	Yes
123	31/05/2022, 02:11:28	---	FAILED	0	---

Upload flow

When the user clicks on Mass Import from the reports screen or from the watchlist screen he will get a popup window with the option to create a new Mass Import.



Mass Import

Add Subjects From File System

Drop Compressed files here, or browse

Supported files: ZIP, TAR

Mass-Import Name

Subject Group Name: Select Group Name

Search By threshold for duplicates on Watch list: 0.5

□ Search Backwards by Face

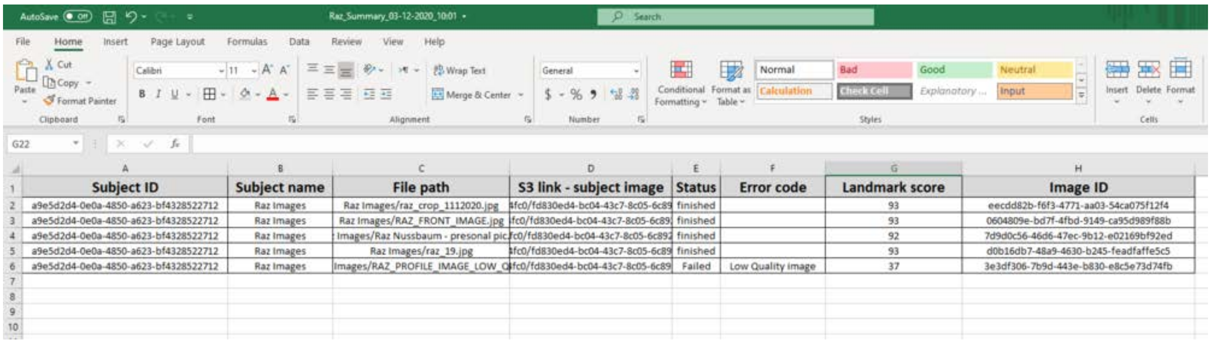
- User set threshold for Mass Import (range between 0.4 to 0.9)
- Mass Import name must be unique
- Must choose a subject groups destination
- Supported files type - zip & tar

> **Note**
>
> Results with the same image as on the Watch list picture & same name as on the Watch List subject will be dismissed.
> Results with bad image quality will be dismissed.

After the uploading is started there is a grid with Mass Imports details,
The information is arranged categorically in the following columns:

- *Name*: the name of the mass import
- *Start Date*: the date and time at which the import began
- *End Date*: the date and time at which the import ended
- *Import Status*: the completion status of the import(Done, completed, failed, uploading, extracting, processing)
- *Issues Number*: the number of issues found during the upload process
- *Resolved issues?*: if there are unresolved issues its a link to the resolve issues screen

Click the corresponding **report icon** under the *Download Report* column to download the report to your device.



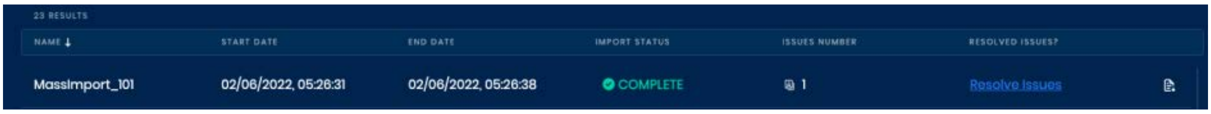
Subject ID	Subject name	File path	S3 link - subject image	Status	Error code	Landmark score	Image ID
a9e5d2d4-0e0a-4850-a623-bf4328522712	Raz Images	Raz Images/raz_crop_1112020.jpg	4fc0/fd830ed4-bc04-43c7-8c05-6c89	finished		93	eecdd82b-f6f3-4771-aa03-54ca075f12f4
a9e5d2d4-0e0a-4850-a623-bf4328522712	Raz Images	Raz Images/RAZ_FRONT_IMAGE.jpg	fc0/fd830ed4-bc04-43c7-8c05-6c89	finished		93	0604809e-bd7f-4fbd-9149-ca95d989f88b
a9e5d2d4-0e0a-4850-a623-bf4328522712	Raz Images	Images/Raz Nussbaum - presonal pic.	fc0/fd830ed4-bc04-43c7-8c05-6c892	finished		92	7d9d0c56-46d6-47ec-9b12-e02169bf92ed
a9e5d2d4-0e0a-4850-a623-bf4328522712	Raz Images	Raz Images/raz_19.jpg	4fc0/fd830ed4-bc04-43c7-8c05-6c89	finished		93	d0b16db7-48a9-4630-b245-feadfaffe5c5
a9e5d2d4-0e0a-4850-a623-bf4328522712	Raz Images	Images/RAZ_PROFILE_IMAGE_LOW_Q	fc0/fd830ed4-bc04-43c7-8c05-6c89	Failed	Low Quality image	37	3e3df306-7b9d-443e-b830-e8c5e73d74fb

Resolve issues Flow

On the Mass Imports grid, users get information about the Mass Import status and if there are Issues they can resolve them by clicking on Resolve Issues.

Possible Issues:

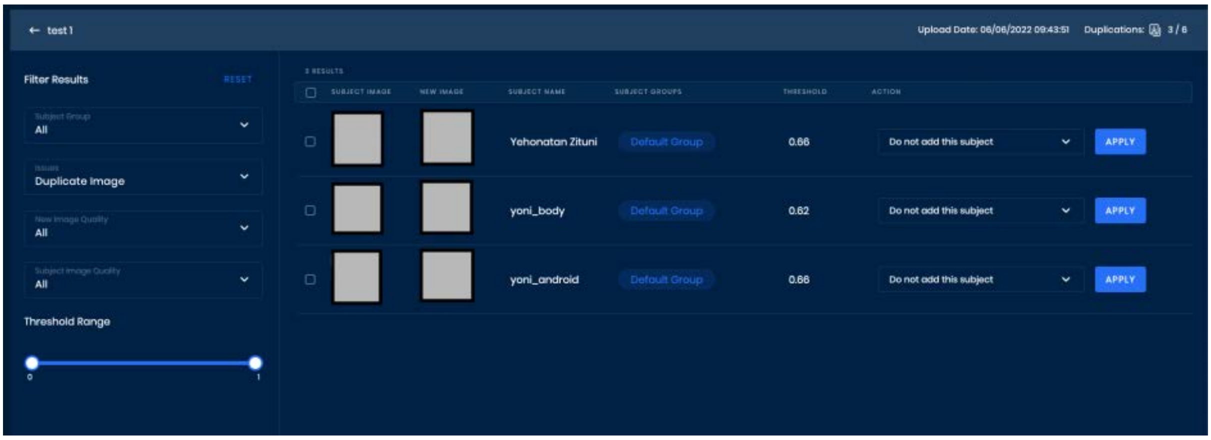
- Image duplication
- Name duplication
- No face detected


23 RESULTS

NAME ↓	START DATE	END DATE	IMPORT STATUS	ISSUES NUMBER	RESOLVED ISSUES?
MassImport_101	02/06/2022, 05:26:31	02/06/2022, 05:26:38	COMPLETE	1	Resolve Issues

by clicking on Resolve Issues the user navigates to the Resolve issues screen.

> **Note**
>
> Watchlist permissions will affect the number of issues.
> Issues will be opened only to the permitted user watchlists.


← test 1

Upload Date: 06/06/2022 09:43:51 Duplications: 3 / 6

Filter Results RESET

Subject Group: All

Issues: Duplicate image

New Image Quality: All

Subject Image Quality: All

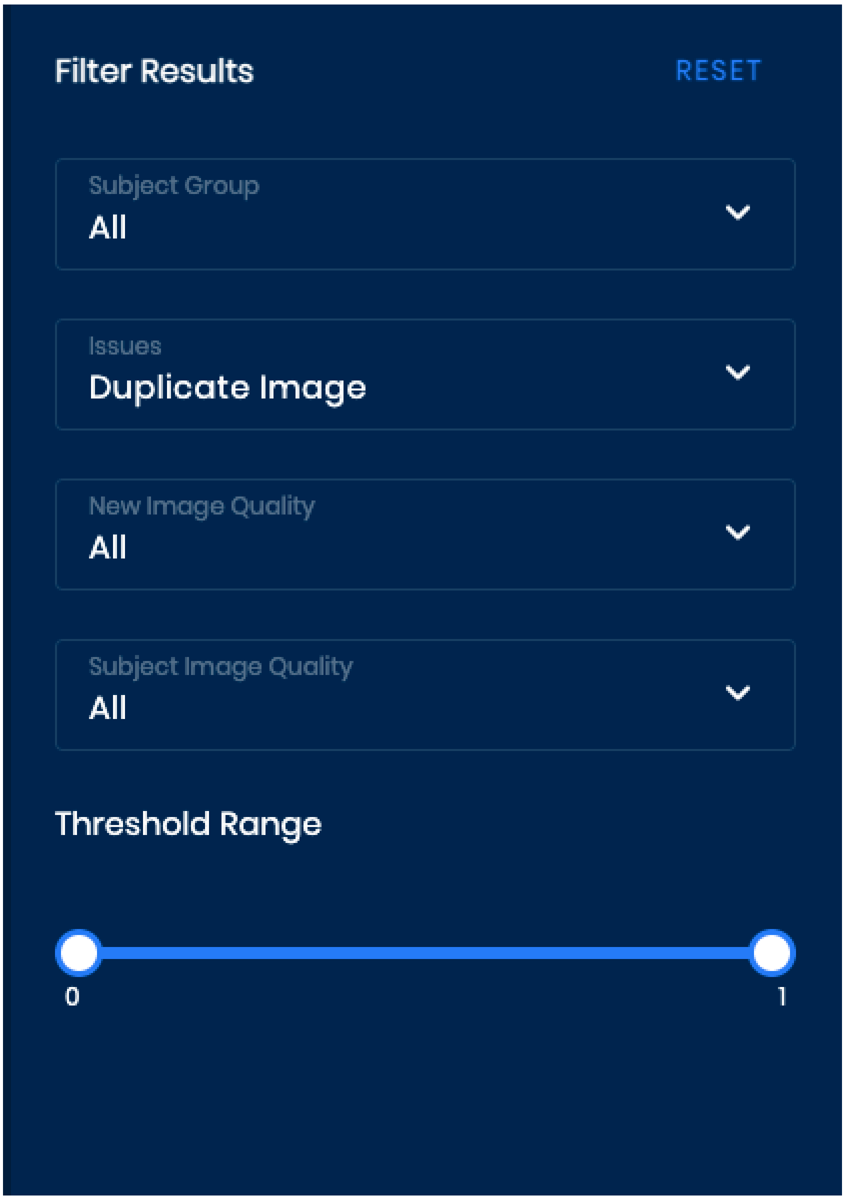
Threshold Range

3 RESULTS

□	SUBJECT IMAGE	NEW IMAGE	SUBJECT NAME	SUBJECT GROUPS	THRESHOLD	ACTION	
□			Yehonatan Zituni	Default Group	0.66	Do not add this subject	APPLY
□			yoni_body	Default Group	0.62	Do not add this subject	APPLY
□			yoni_android	Default Group	0.66	Do not add this subject	APPLY

The user will have the option to filter the issues by -

- Issues subject groups
- Issues type
- Subject image quality
- New Image quality
- TH range - available only for duplicate image issue



Filter Results

Subject Group: All

Issues: Duplicate Image

New Image Quality: All

Subject Image Quality: All

Threshold Range

The actions to resolve issues are:

- “Add Reference Image to an Existing Subject” - Will add the new image as an ADDITIONAL reference image to the existing subject.
- “Add as New Subject” - will create a new subject in the system with this reference image.
- “Replace Old Reference Image With Newly Imported Image” - Replace the reference image & keep deleting the old one.
- “Do Not Add This Subject” - In case the user doesn’t want to add this image to an existing subject or create a subject with this picture.

There is an option for bulk actions.

> **Note**
>
> User will need to handle all issues until they are all “resolved” to perform another Mass Import upload

Understanding Mass Import Report Errors

If a subject was not successfully added to OnWatch when conducting a mass import of subjects, an error code will appear on that subject's row within the downloaded report (CSV file). This will tell you exactly what went wrong so that you can try again.

Below is a table that indicates all the possible reasons why a subject would not be successfully added to the system via mass import. This chart can also be referred to when creating a mass import file to ensure all subject data is provided correctly.

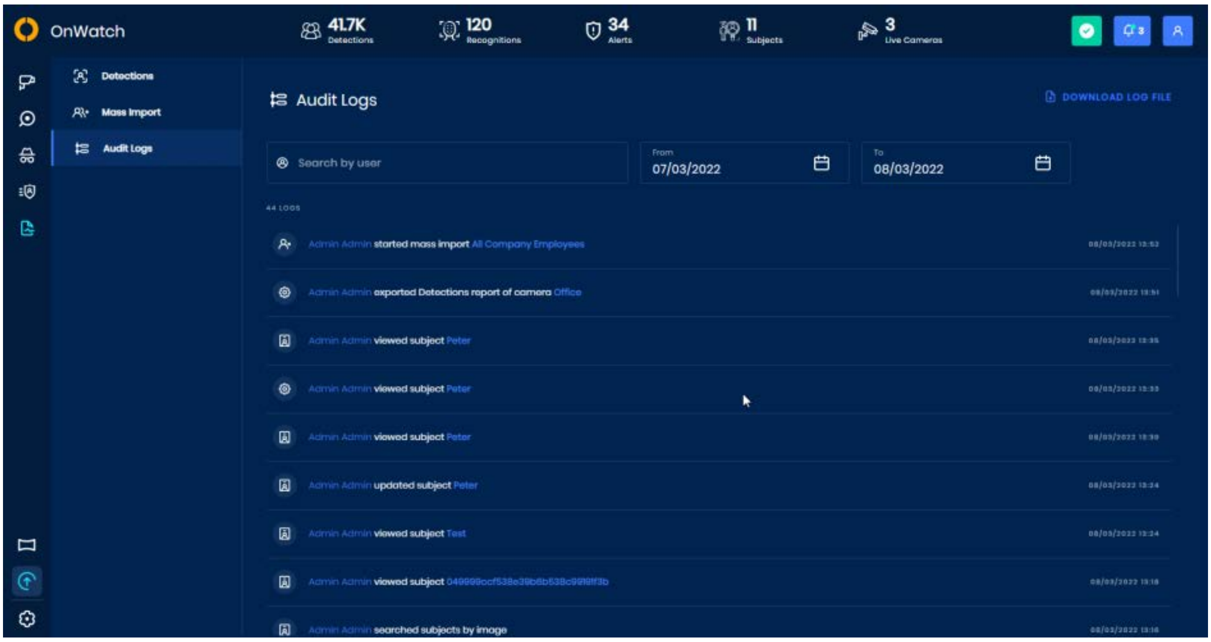
Errors that Caused the Entire Mass Import to Fail

Error Message	Description
`Failed in uploading files to object-store`	The compressed file wasn't successfully uploaded to OnWatch's storage.
`Failed in extracting files from compressed files` -	The compressed file was damaged while attempting to upload to OnWatch. Could be due to connectivity issues or service failures. We suggest trying one more time.
`An unknown error occurred handling job`	The reason for failure is unknown. Please try again.

Errors that Caused Specific Subjects to Fail

Error Messages	Description
`Upload Error - Invalid file name length`	The length of a subject file name within the compressed file can be maximum 120 characters.
`Upload Error - Invalid file hierarchy`	The hierarchy of files in the uploaded compressed file is invalid. OnWatch supports a compressed file containing a directory which stores subject files and/or other directories with subject files in them.
`Upload Error - Invalid file extension`	The image file type was not valid. OnWatch currently supports the following image file types: bmp, pbm, pgm, ppm, sr, ras, jpeg, jpg, jpe, jp2, jtif, tiff, tif, png, jfif.
`No faces detected in image`	The reference image uploaded for the specific subject did not contain a person or a person was not found in the image. Please use a different photo.
`Multiple faces detected in the image`	The reference image uploaded for a specific subject contained more than one person. Please upload a different image that only has the subject's face.
`maximum number of files in directory exceeded, the maximum is 15`	The maximum number of images allowed per subject is 15 images. If the subject's file contains more than 15 images, you will get an error. Please delete images as necessary.
`An unknown error occurred while handling the file`	The reason for failure is unknown. Please try again.
`Low quality image`	The subject's reference image is poor and must be replaced with a better quality image as low quality images result in false alarms. **If the subject receives a low landmark score and you cannot upload them via mass import, add the subject through the OnWatch dashboard.
'Image already exist in watch list'	The same image for the same subject is existing on the watch list

Audit Logs



Audit Logs

From 07/03/2022

To 08/03/2022

44 LOGS

Admin Admin started mass import All Company Employees 08/03/2022 13:53

Admin Admin exported Detections report of camera Office 08/03/2022 13:51

Admin Admin viewed subject Peter 08/03/2022 13:35

Admin Admin viewed subject Peter 08/03/2022 13:33

Admin Admin viewed subject Peter 08/03/2022 13:30

Admin Admin updated subject Peter 08/03/2022 13:24

Admin Admin viewed subject Test 08/03/2022 13:24

Admin Admin viewed subject 049999acf538e39b6b538c9919f3b 08/03/2022 13:18

Admin Admin searched subjects by image 08/03/2022 13:16

By navigating to the Audit Logs section of the Reports tab, you'll be able to view a complete list of all the actions taken by all your OnWatch users. You can filter through the actions by date or by the user to get a better understanding of the changes made in the system. You can also view what searches were made and if new subjects were added to the system.

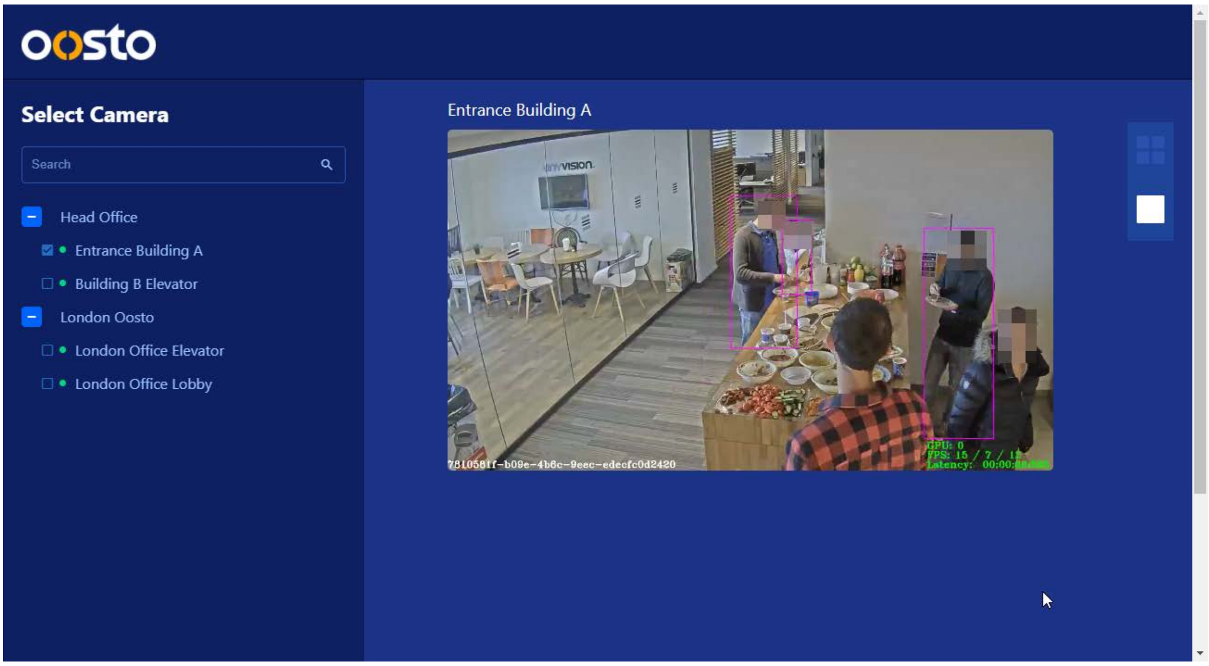
Video Wall

> ### Video Wall (depreciation)
>
> The Video wall is expected to be depreciated in the next release, the functionality has been superseded within the "View Sources". The "View Sources" is able to show a preview of any active camera or case file, with the added benefit of a more advanced tree and search mechanism.

The Video Wall tab allows users to see the live stream of cameras connected to the OnWatch system.

The left-side pane within the Video Wall screen displays all cameras that are connected. The cameras are separated into sections according to the camera group. Simply click on any camera you'd like to see and a **checkmark** will appear next to the camera name.

You can view several cameras at a time and determine how you'd like to display those camera streams using the **square options** visible on the right side.



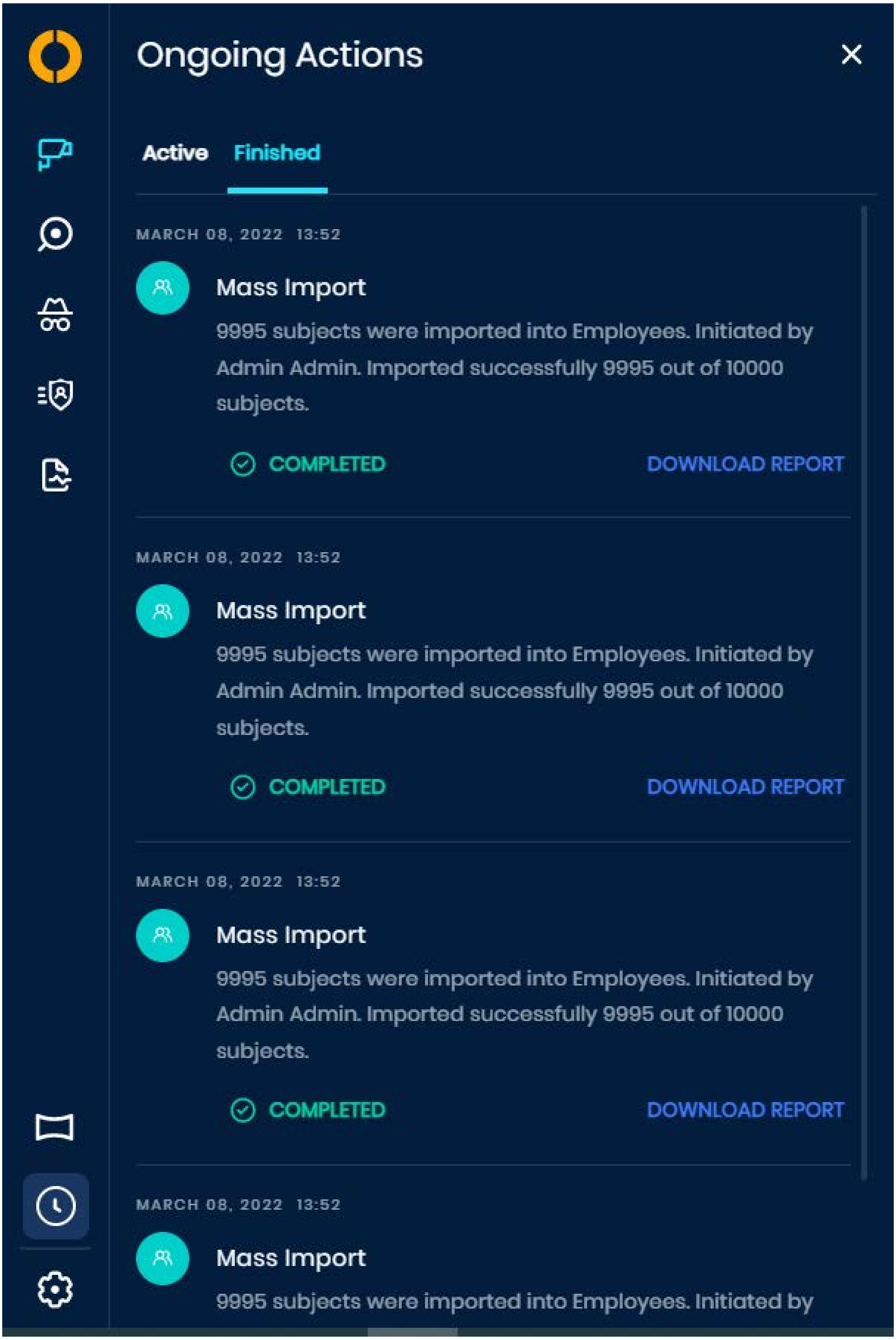
Ongoing Actions

Ongoing Actions offers the real-time status of mass import and Access Control integration processes, as well as a downloadable report per process for additional information and data.

From this page, you can view the status and report for the following activities:

- Mass import of new Personnel into the system via a compressed file

Ongoing Actions tab by clicking the Ongoing Actions icon from the left-side navigation.



Ongoing Actions

MARCH 08, 2022 13:52

Mass Import

9995 subjects were imported into Employees. Initiated by Admin Admin. Imported successfully 9995 out of 10000 subjects.

✓ COMPLETED

MARCH 08, 2022 13:52

Mass Import

9995 subjects were imported into Employees. Initiated by Admin Admin. Imported successfully 9995 out of 10000 subjects.

✓ COMPLETED

MARCH 08, 2022 13:52

Mass Import

9995 subjects were imported into Employees. Initiated by Admin Admin. Imported successfully 9995 out of 10000 subjects.

✓ COMPLETED

MARCH 08, 2022 13:52

Mass Import

9995 subjects were imported into Employees. Initiated by

Whenever an action is completed, the icon will contain a green dot.

You can view current actions that are taking place, under the *Active* tab, or download the report of a finished process, from the *Finished* tab.

In addition, from the *Finished* tab, you can clearly see if any process was cancelled without being completed.

Understanding Integration Reports (Sync)

Download the report (CSV file) of any integration process from the *Ongoing Actions* tab and select the **Finished** panel. Integration reports are only available for processes that are considered complete or cancelled.

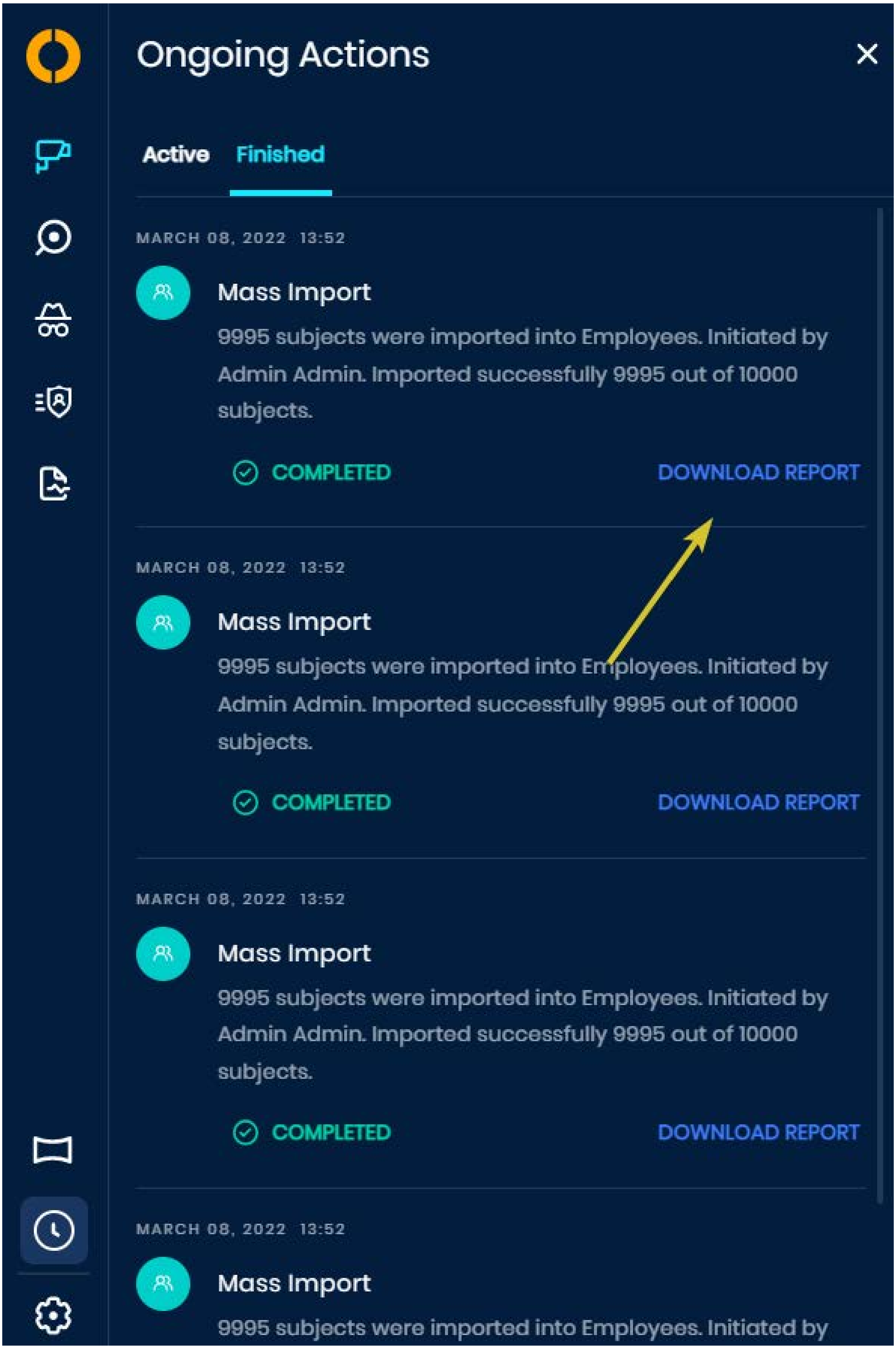
For each Personnel within the integration, a row will appear within the report. You can see whether each Personnel was successfully synced and imported into the system or whether an error occurred.

Below is a table that indicates all the possible reasons why a Personnel would not be uploaded to OnWatch.

Error Message	Description
`Could not detect face`	The reference image uploaded for the specific Personnel did not contain a person or a person was not found in the image. Please use a different photo.
`Failed to create member`	The system was unable to successfully add the subject

Understanding Mass Import Reports

Download the report (CSV file) of any mass import process from the *Ongoing Actions* tab and selecting the **Finished** panel. Mass import reports are only available for processes that are considered complete or cancelled.



MARCH 08, 2022 13:52

Mass Import

9995 subjects were imported into Employees. Initiated by Admin Admin. Imported successfully 9995 out of 10000 subjects.

MARCH 08, 2022 13:52

Mass Import

9995 subjects were imported into Employees. Initiated by Admin Admin. Imported successfully 9995 out of 10000 subjects.

MARCH 08, 2022 13:52

Mass Import

9995 subjects were imported into Employees. Initiated by Admin Admin. Imported successfully 9995 out of 10000 subjects.

MARCH 08, 2022 13:52

Mass Import

9995 subjects were imported into Employees. Initiated by

If a person is not successfully added when conducting a mass import of Personnel, an error code will appear on that person's row within the downloaded report (CSV file). This will tell you exactly what went wrong so that you can try again.

For example, in the image above, the mass import is declared complete but 0 Personnel were imported. By downloading the report, I can see exactly why each Personnel was not imported successfully.

Below is a table that indicates all the possible reasons why a Personnel would not be successfully added to Abraxas via mass import.

Errors that Caused the Entire Mass Import to Fail

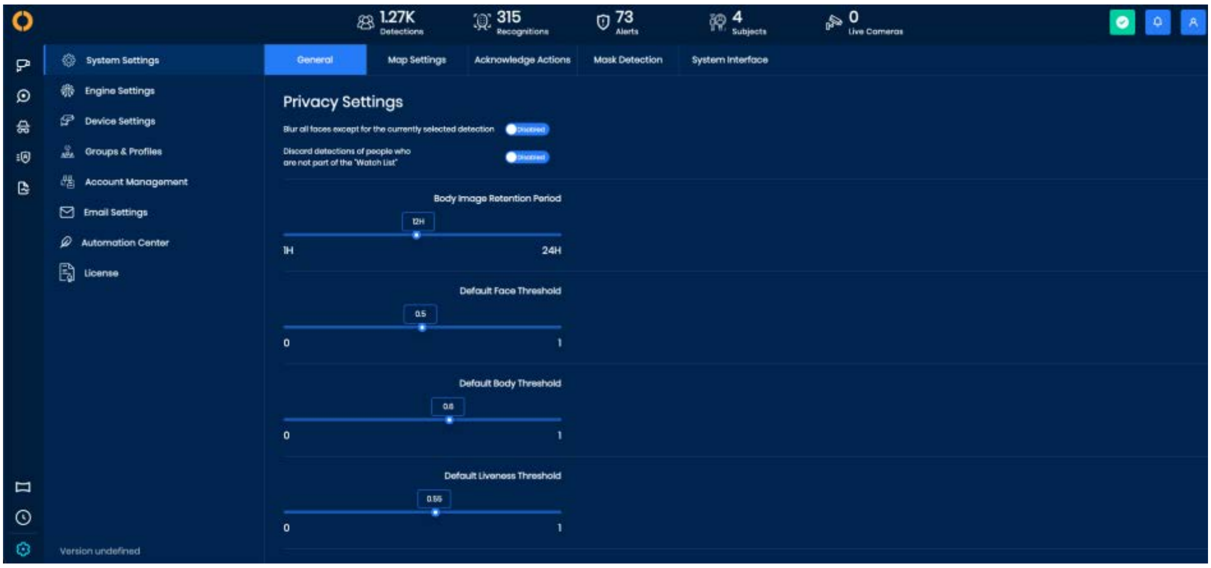
Error Message	Description
`Failed in uploading files to object-store`	The compressed file wasn't successfully uploaded to the storage.
`Failed in extracting files from compressed files` -	The compressed file was damaged while attempting to upload to OnWatch. Could be due to connectivity issues or service failures. We suggest trying one more time.
`An unknown error occurred handling job`	The reason for failure is unknown. Please try again.

Errors that Caused Specific Subjects to Fail

Error Messages	Description
`Upload Error - Invalid file name length`	The length of a subject file name within the compressed file can be maximum 30 characters.
`Upload Error - Invalid file hierarchy`	The hierarchy of files in the uploaded compressed file is invalid. OnWatch supports a compressed file containing a directory which stores Personnel files and/or other directories with Personnel files in them.
`Upload Error - Invalid file extension`	The image file type was not valid. OnWatch currently supports the following image file types: bmp, pbm, pgm, ppm, sr, ras, jpeg, jpg, jpe, jp2, jtif, tiff, tif, png, jfif.
`No faces detected in image`	The reference image uploaded for the specific Personnel did not contain a person or a person was not found in the image. Please use a different photo.
`Multiple faces detected in the image`	The reference image uploaded for a specific Personnel contained more than one person. Please upload a different image that only has the Personnel's face.
`maximum number of files in directory exceeded, the maximum is 15`	The maximum number of images allowed per Personnel is 15 images. If the subject's file contains more than 15 images, you will get an error. Please delete images as necessary.
`An unknown error occurred while handling the file`	The reason for failure is unknown. Please try again.

Settings

The Settings tab enables Admins and Super Admins to configure the OnWatch platform in a way that is most useful for their organization.



Privacy Settings

Blur all faces except for the currently selected detection: Disabled

Discard detections of people who are not part of the "Watch List": Disabled

Body Image Retention Period: 12H (1H – 24H)

Default Face Threshold: 0.5 (0 – 1)

Default Body Threshold: 0.6 (0 – 1)

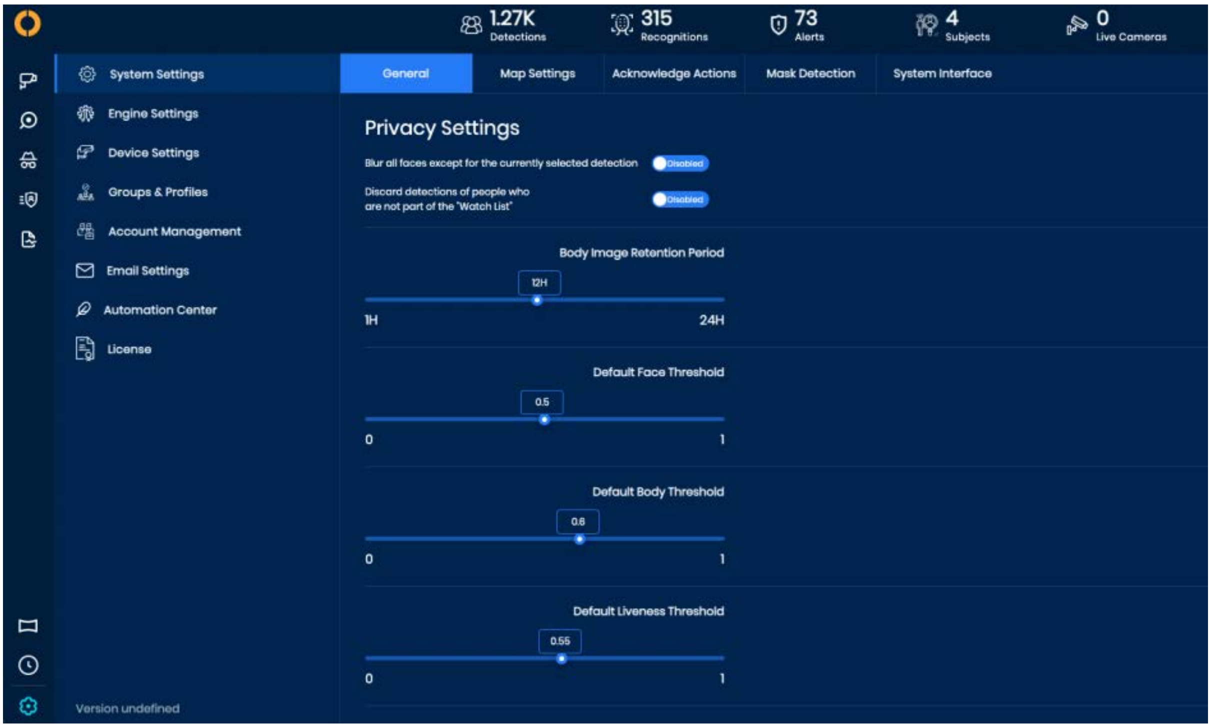
Default Liveness Threshold: 0.55 (0 – 1)

The Settings tab of OnWatch is comprised of the following sections:

- System Settings:
  Select privacy modes, determine map configurations, set specific acknowledged actions, mask detections settings and modify the system interface.
- Engine Settings:
  Define video, detection, recognition storage policies, retention times, alerts storage, and inquiry storage.
- Device Settings:
  Add and connect cameras or accessories to the system, as well as configure those cameras/accessories for specific use cases and purposes. The Device Settings section also enables OnPatrol Remote.
- Groups & Profiles:
  Combine subjects, cameras, profiles, and detections into groups to add a layer of security and receive specific alerts from the system.
- Account Management:
  Establish roles and permissions for users by categorizing each one as either a viewer, operator, super operator, admin, or super admin. The account management section also contains the Active Directory and SAML SSO panels.
- Email Settings:
  Integrate with your email server in order to receive email notifications from the system.
- Automation Center - Draft:
  The Automation Center was designed so users can define the email notifications they would like to receive on specific subject groups in the system.
- License:
  Get license information, activate or update your license.

System Settings

General



Privacy Settings

Blur all faces except for the currently selected detection: Disabled

Discard detections of people who are not part of the "Watch List": Disabled

Body Image Retention Period: 12H (1H – 24H)

Default Face Threshold: 0.5 (0 – 1)

Default Body Threshold: 0.6 (0 – 1)

Default Liveness Threshold: 0.55 (0 – 1)

The OnWatch system can limit the detection information generated for compliance with local privacy laws and regulations. Two modes of privacy can be activated in OnWatch.

Clicking **Blur all faces* will enable the OnWatch system to automatically blur the faces of subjects visible in rendered video snippets, aside from the detected subject.

Clicking **Discard detections** will enable the system to portray and save only subject recognitions and to not generate detections of non-subjects.

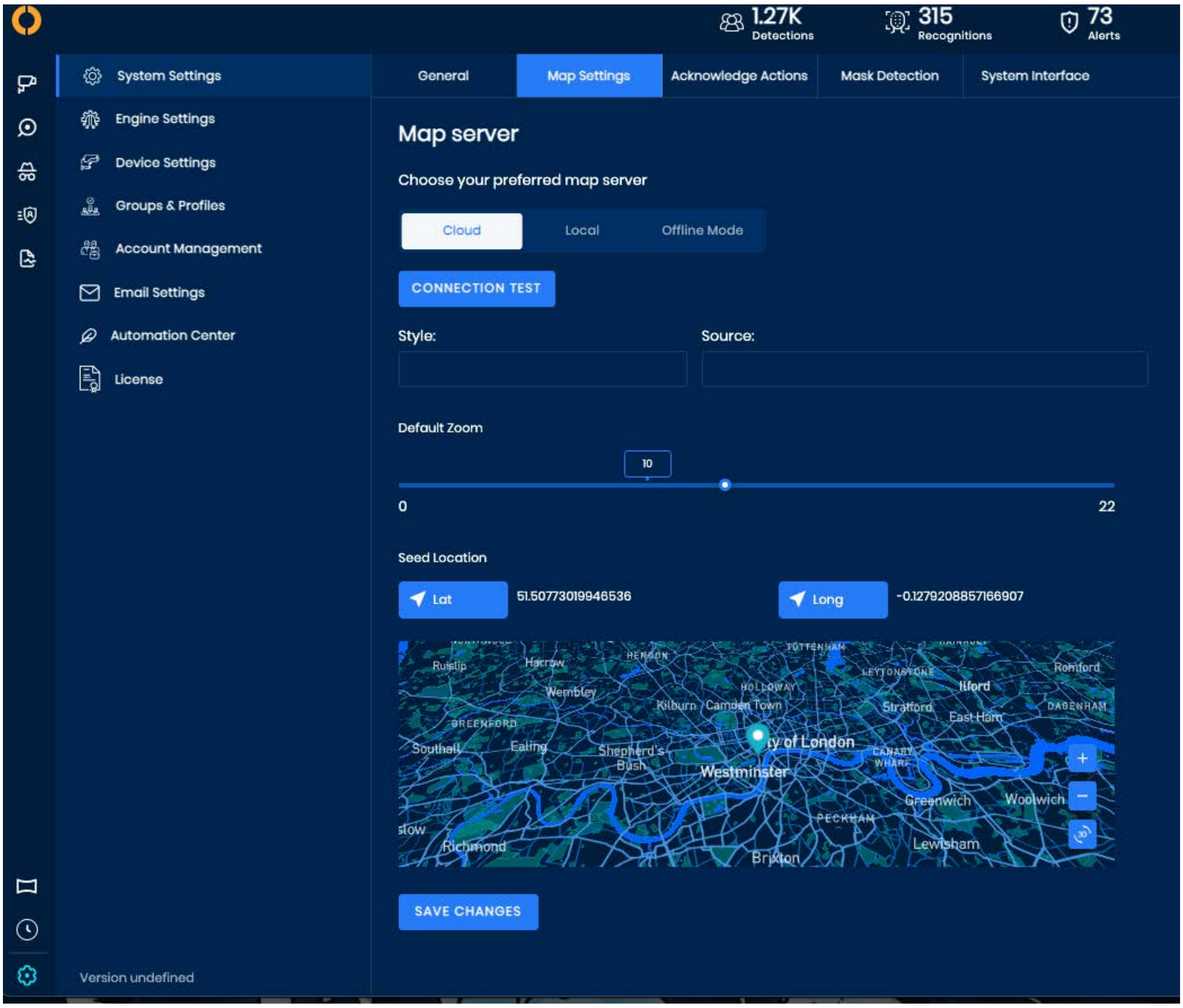
Use the toggle to activate Blur Mode and/or Discard detections within the system. A mode is on when the toggle is set to *Enabled* and is shown in the color green. A mode is off when the toggle is set to *Disabled* and is shown in the color blue.

The **Body Image Retention Period** determines the amount of time the system should save and use a body reference image that is associated with a subject. For example, if the Body Image Retention Period is set to 12H, the system will use anybody's reference image for 10 hours and then discard it.

Use the sliding scales to set the **Default Body Threshold** and **Default Face Threshold**. These values set the minimum level of similarity between the reference image and detection image needed for recognition. The value is defined between 0 and 1.

Once these inputs are set, click **Save Changes**.

Map Settings



Map server

Choose your preferred map server

Style:

Source:

Default Zoom

10

0 22

Seed Location

Lat 51.50773019946536

Long -0.1279208857166907

OnWatch includes mapping to correlate with the analyzed data and cameras.

In the *Map Server* section, determine if you want the map server to connect through the cloud or locally. Click on your preferred option, **Cloud** , **Local**, or **Offline Mode**. Choose the local option if you are uploading a map image or are connected to a map server.

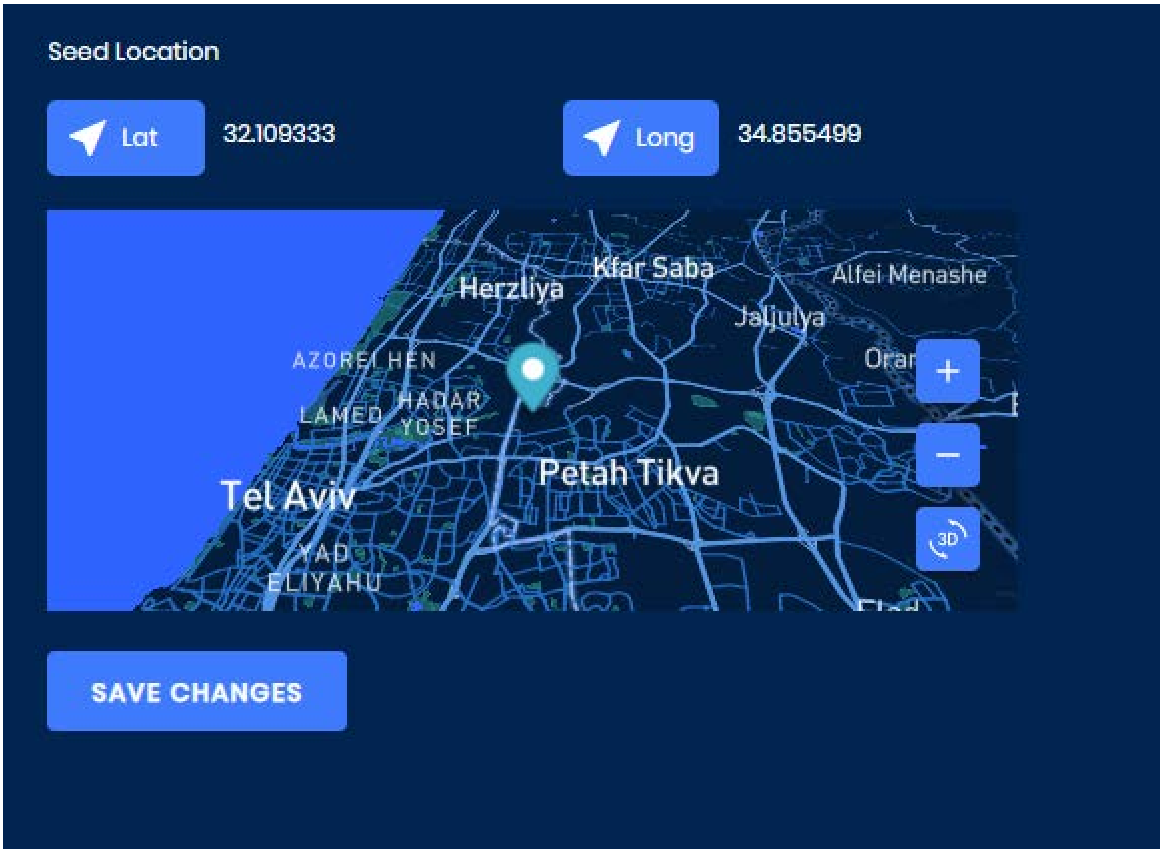
If you selected the Local connection, you will be asked to input your *Local Map Server Address* and *Token*.

> ### 🚧 Mapbox Offline Server
>
> To enable a local offline map server you must purchase and install a map server from Mapbox

Click **Connection Test** to make sure that it has been correctly connected. If the connection has failed, the button will turn red and show *Fail*. If the connection was successful, it will turn green and show *Success*.

Use the sliding bar to set the **Default Zoom**, which determines the automatic size of the map when you open a page. The map at the bottom of the page will zoom in and out to size as you slide so that you can see what the values look like.

The **Seed Location** is a point on the map where your premises are located. Set the exact location by zooming in on the map to the exact location, and clicking on it. This will drop a pin, and the latitude and longitude of that pin will automatically update accordingly. These values are displayed at the top as *Lat* and *Long*.



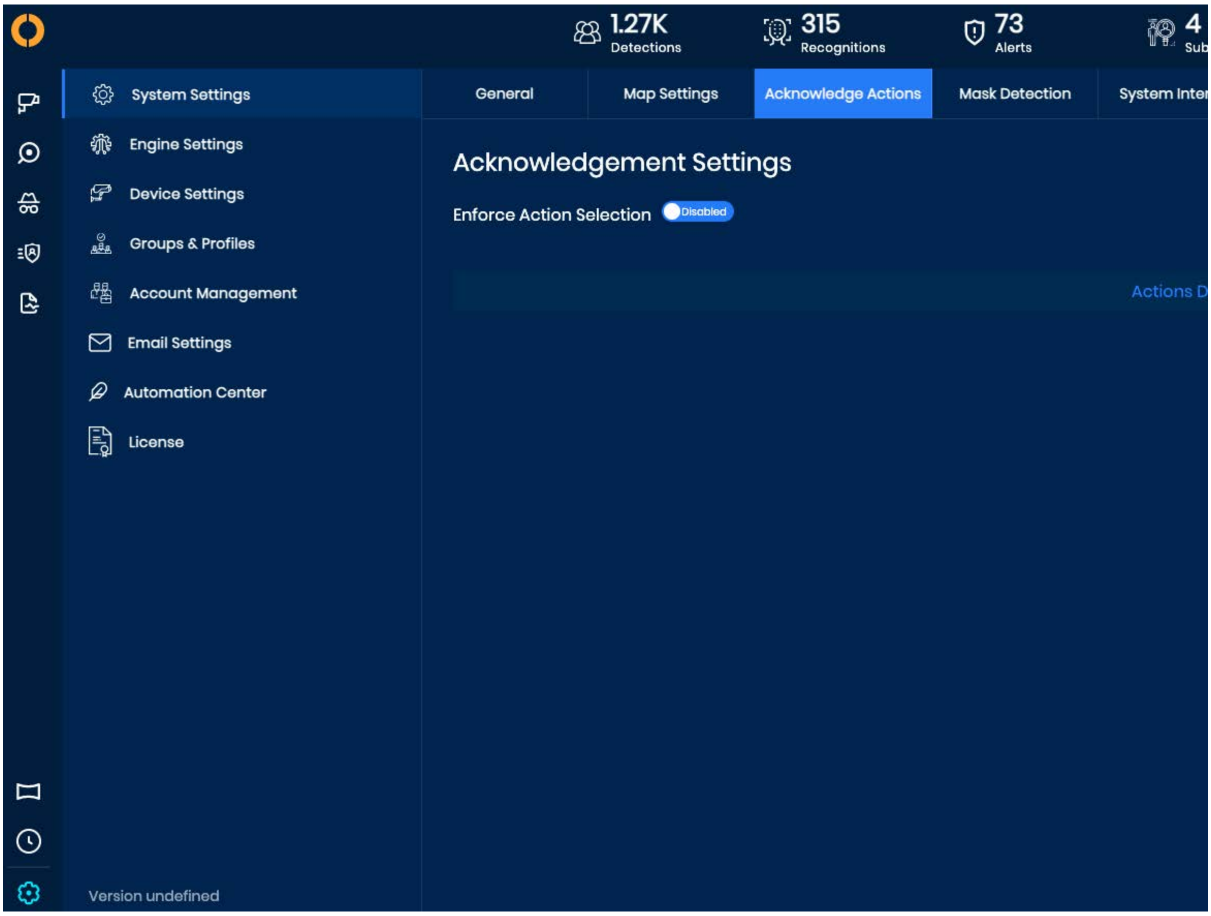
Seed Location

Lat 32.109333

Long 34.855499

Click **Save Changes**.

Acknowledged Actions



Acknowledgement Settings

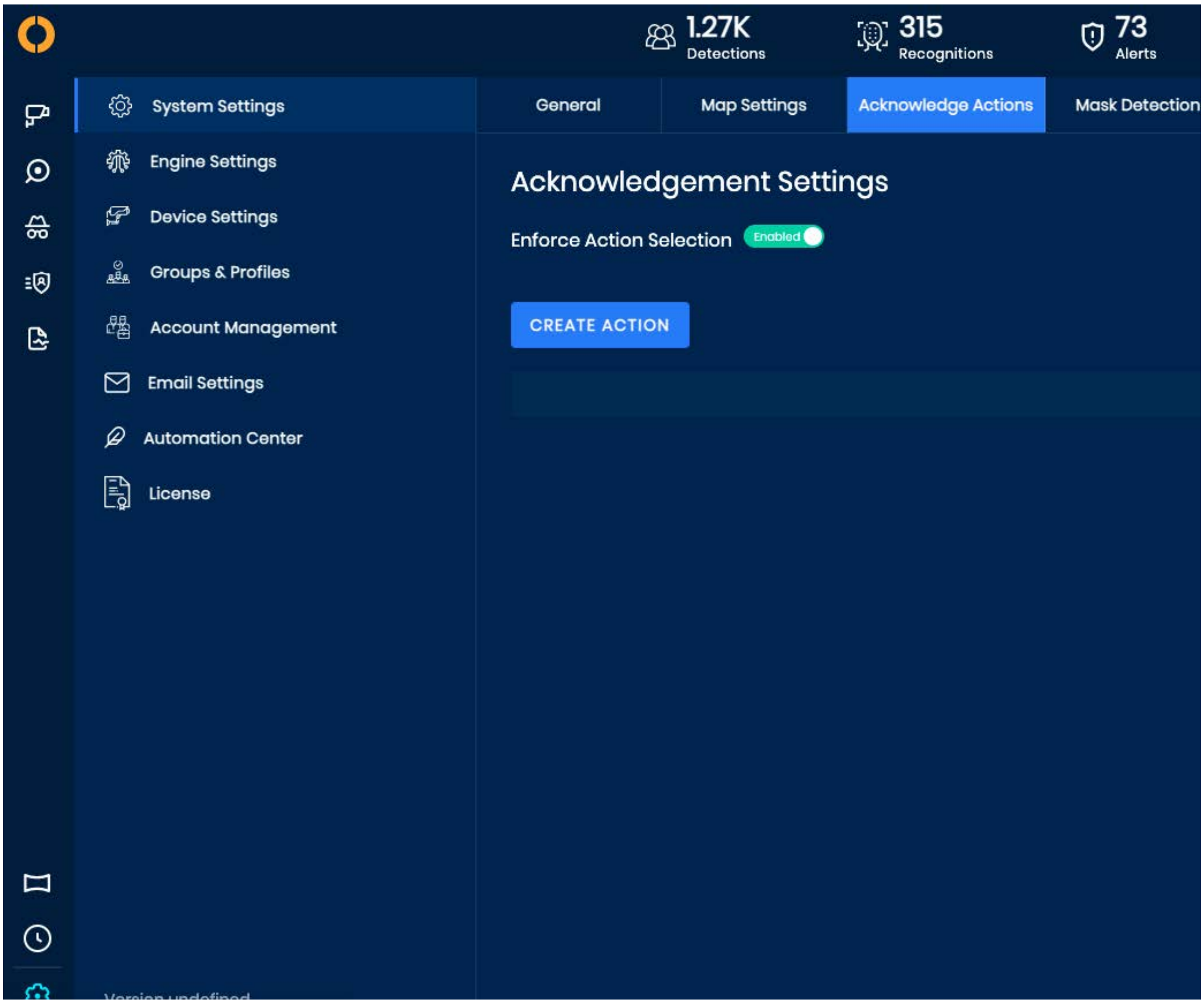
Enforce Action Selection: Disabled

Users can create actions in the system that reflect what actions were taken in real-time once a recognition took place and a notification was sent out. The Acknowledgement Settings section of the Settings tab permits users to create and describe these actions to match the tasks their security personnel will take.

This feature is only available when turned on. To activate and enforce acknowledgement actions:

1. Go to the **Settings** tab in the system.
2. Under the *System Settings* section, select the **Acknowledge Action** tab.
3. Next to *Enforce Action Selection*, use the toggle to enable the feature. The feature is enabled once the toggle is green and reads “Enabled”.

All actions created will appear on the Acknowledgement Settings page. To edit or delete any action, simply click the **three-dotted icon** under *Action Menu* and select **Edit Action** or **Delete**.



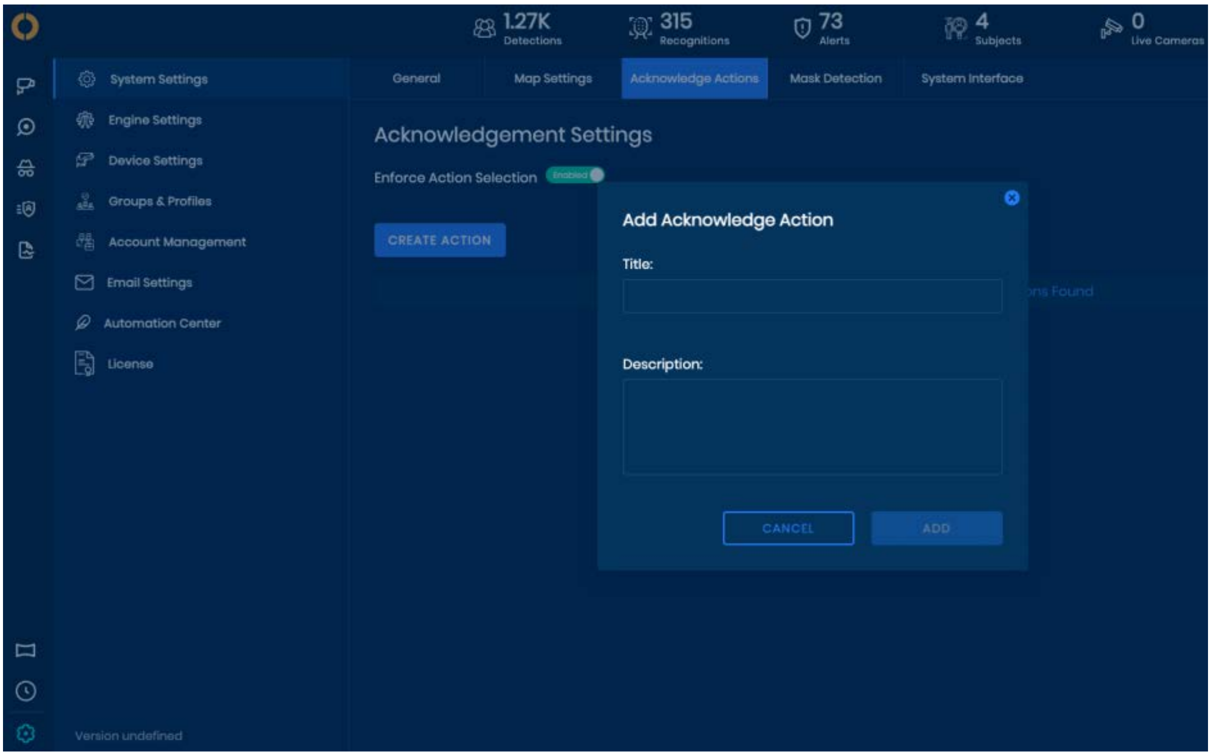
Acknowledgement Settings

Enforce Action Selection: Enabled

Create an Acknowledgement Action to Acknowledge Alerts

Create Acknowledgement Actions to let your team know what actions took place after a recognition occurred and an alert was displayed. You can acknowledge alerts by selecting what acknowledgement action took place.

1. Go to the **Settings** tab in the system.
2. Under the *System Settings* section, select the **Acknowledge Action** tab.
3. Click the **Create Action** button.
4. A popup will appear requesting the title and description of the action.
5. After all information is inputted, select **Add**.



Acknowledgement Settings

Enforce Action Selection: Enabled

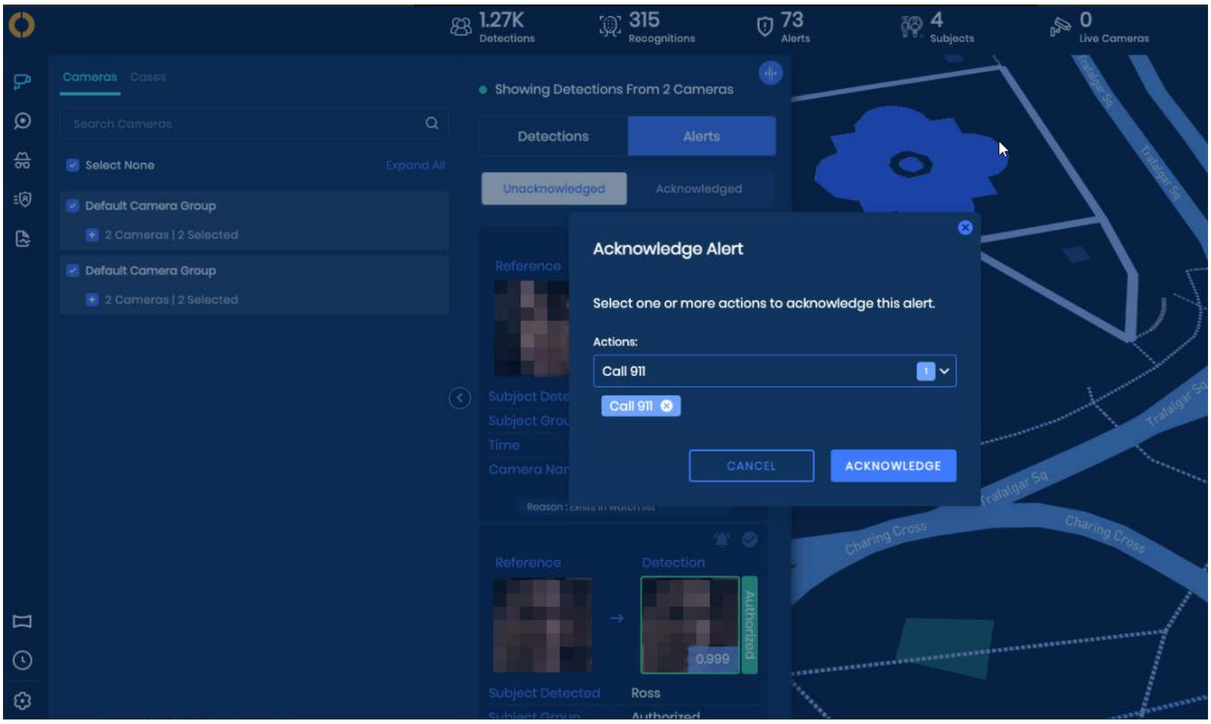
Add Acknowledge Action

Title:

Description:

Once you've added alert acknowledgments, whenever a team member needs to acknowledge an alert from the Live Cameras screen, he or she will see the list of acknowledge options you've created and can easily indicate what actions he or she took once the alert was acknowledged.

In the example below, a "call 911" action was created in the system. Now, team members can indicate when they contact 911 and for who by using this action.



Acknowledge Alert

Select one or more actions to acknowledge this alert.

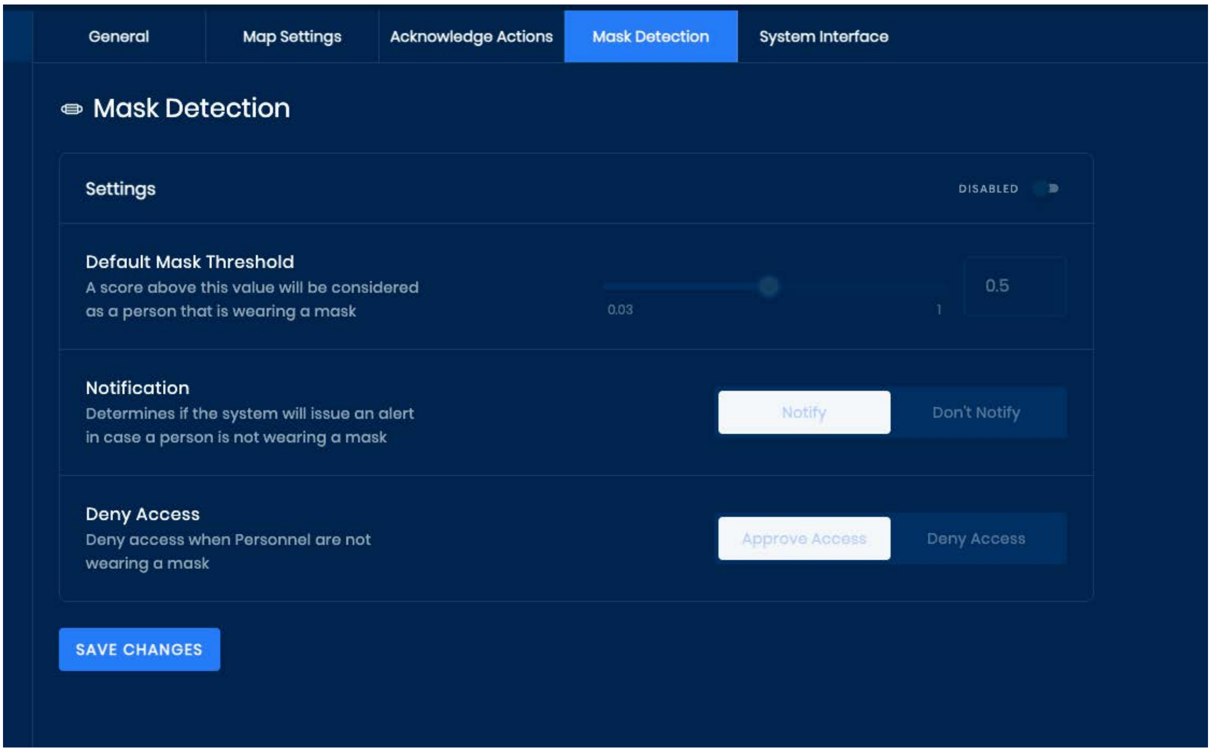
Actions: Call 911

Call 911

Mask Detection

Users can control mask detection, by turning this option On the user will get access to 3 options-

1. Set a threshold value for a person that may be wearing a mask.
2. Choose to notify about a person not wearing a mask.
3. Option to deny access for a person that not wearing a mask



Mask Detection

Settings

DISABLED

Default Mask Threshold

A score above this value will be considered as a person that is wearing a mask

0.03 – 1: 0.5

Notification

Determines if the system will issue an alert in case a person is not wearing a mask

Deny Access

Deny access when Personnel are not wearing a mask

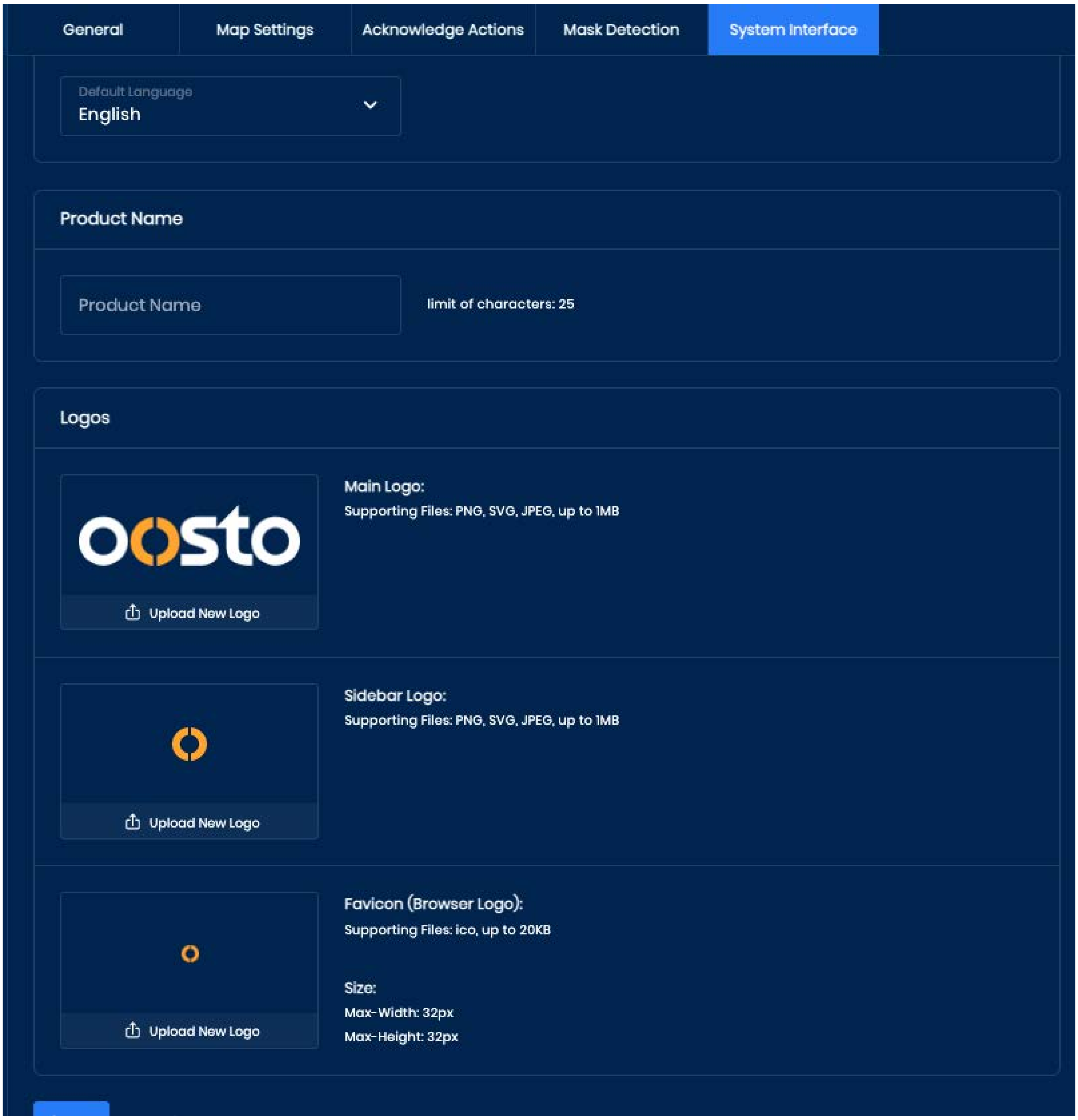
Customizing the System Interface

Admin and super admin can change the system interface, they can change language, product name, and logos.

System Language

The user can change the system language by choosing language from predefined list of languages.

> **Note**
>
> There are some default GA languages, and there may be others, depending on system implementation.
> Numbers and user inputs are not affected by the translation, only the system texts.
> Contact Oosto for more information.



Default Language
English

Product Name

Product Name

limit of characters: 25

Logos

Main Logo:
Supporting Files: PNG, SVG, JPEG, up to 1MB

Sidebar Logo:
Supporting Files: PNG, SVG, JPEG, up to 1MB

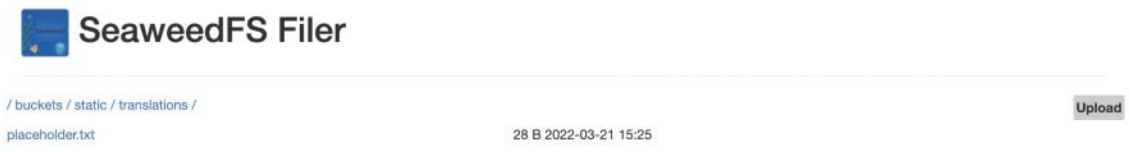
Favicon (Browser Logo):
Supporting Files: ico, up to 20KB

Size:
Max-Width: 32px
Max-Height: 32px

Default Language File	Download from Knowledge Portal
	Please download the Zip file. Unzip and use the JSON contained within
2.6	https://knowledge.oosto.com/wp-content/uploads/2022/10/English-2.6.2.zip

Add new Language

*connect to SeaweedFS Filer by adding /sw-filer/buckets/static/translations/ to your IP address,
User name - Contact Oosto.
Password - Contact Oosto.



SeaweedFS Filer

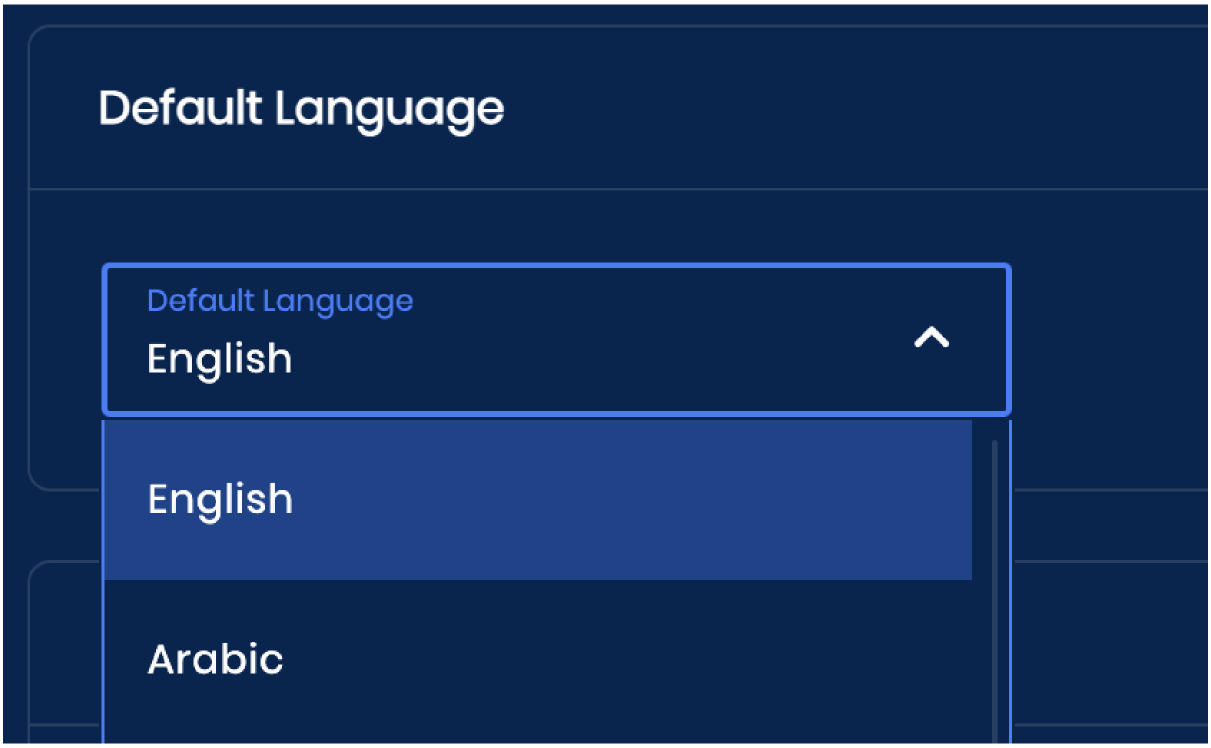
/ buckets / static / translations /

placeholder.txt 28 B 2022-03-21 15:25

Upload your Json file - Must be FileName.Json

Go to system settings>System interface or Refresh your page

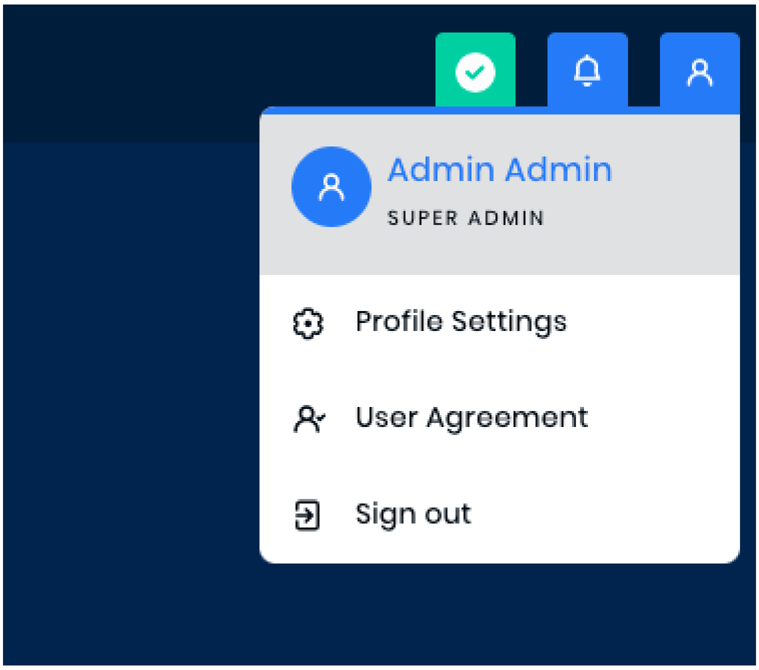
*Choose your language



Default Language

Default Language: English

*Click 'Save' and Refresh your system.



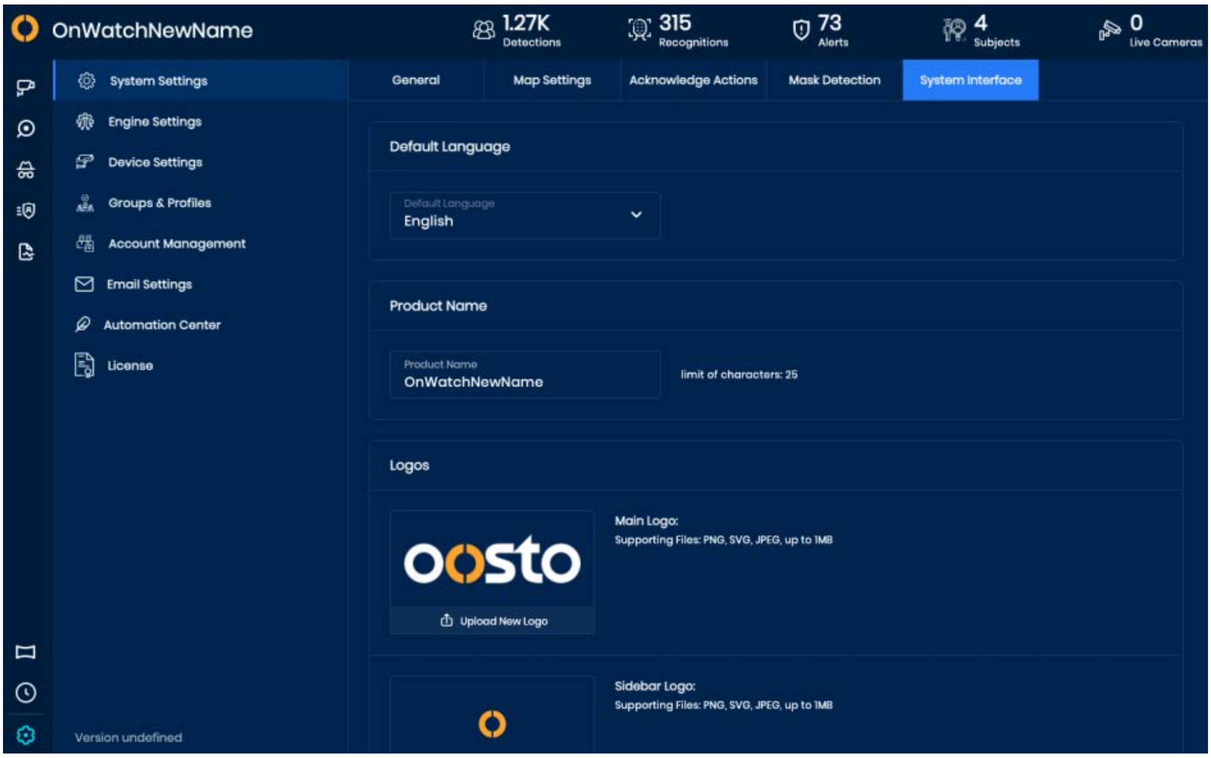
Admin Admin

SUPER ADMIN

*Go to 'Profile Settings' and change user language then click Save changes.

Product Name

The Super Admin can give a name to the product, the name will be appear at the left corner.



Default Language

Default Language: English

Product Name

Product Name: OnWatchNewName

limit of characters: 25

Logos

Main Logo:
Supporting Files: PNG, SVG, JPEG, up to 1MB

Sidebar Logo:
Supporting Files: PNG, SVG, JPEG, up to 1MB

Logos

The user can change the system logos so that he can customize the system to his needs.
The logos change will affect the logging screen, main screen, and Email alerts.

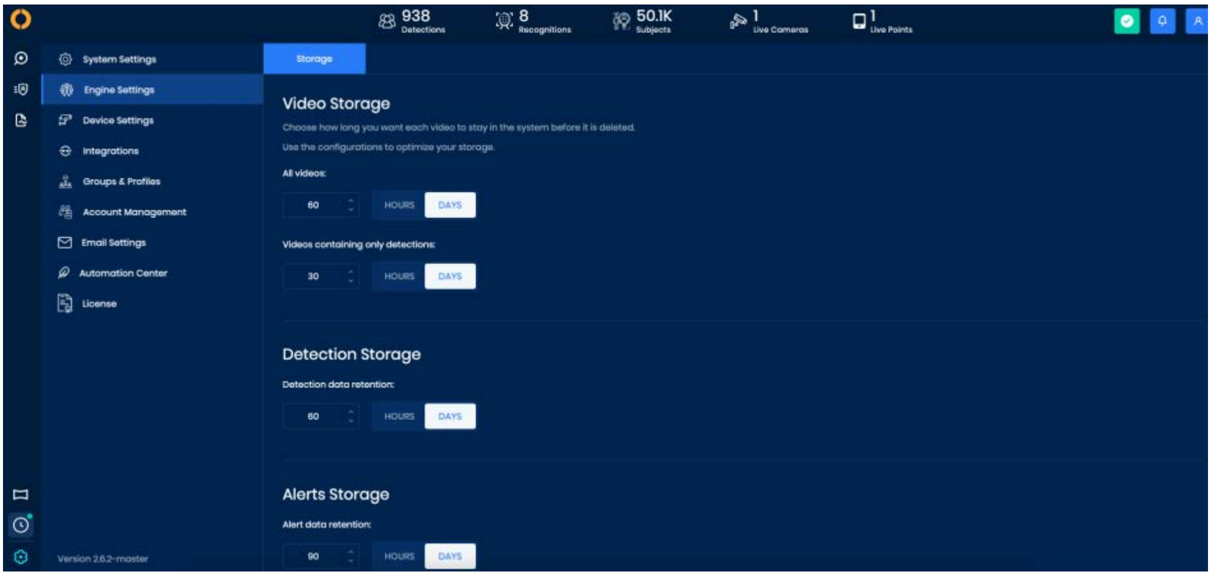
> **Note**
>
> Logos must follow mentioned restrictions.

Reset

There is an option for the super admin to reset the changes and go back to the original default settings.

Engine Settings

Set retention times for videos, detections, and recognitions within the **Engine Settings** section of the *Settings* tab.



Video Storage

Choose how long you want each video to stay in the system before it is deleted.

Use the configurations to optimize your storage.

All videos: 60 DAYS

Videos containing only detections: 30 DAYS

Detection Storage

Detection data retention: 60 DAYS

Alerts Storage

Alert data retention: 90 DAYS

Video Storage

The storage of OnWatch is set up using a "first-in, first-out" approach. This simply means that older videos and content will be deleted first.

You can determine exactly how long you would like videos to be saved within the system based on the content in each video. There are 2 video types.

1. All Videos - includes videos with detections and recognitions
2. Videos that contain only detections - include videos of non-subjects or unknowns.

> 👍 **Storage Retention Policy**
>
> We suggest keeping videos of subjects for as long as possible, Therefore, the storage time frame for All Videos **must** be larger than the storage time frame for detection-only videos.

Detection Storage

The Detection Storage section refers to detection images generated by the system. These are the images that appear on the Live Camera screen, for example. Set the detection storage time frame based on your use case.

Alerts Storage

The Alerts Storage section refers to alerts that appear on the system. These are the details that appear within the Alerts massages of a detected subject from the watch list, for example. Set the Alerts storage time frame based on your use case.

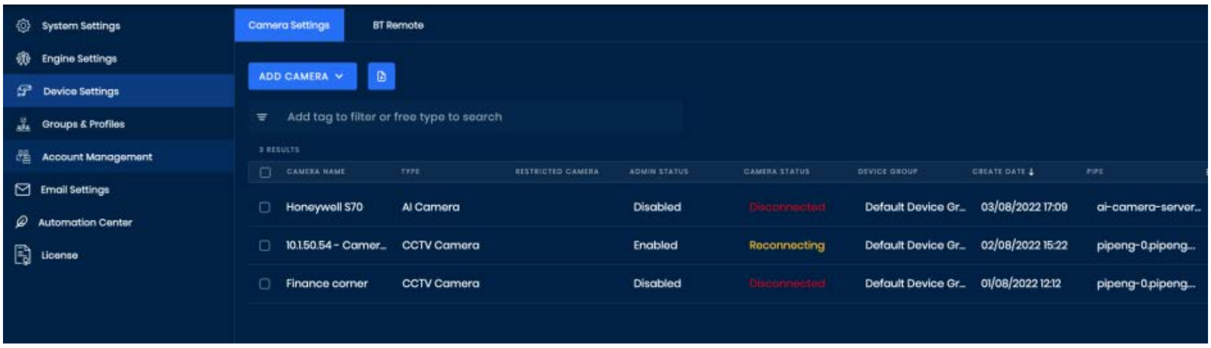
Inquiry Storage

The Inquiry Storage section refers to Inquiry data uploaded to the system. By setting this retention it sets the deletion date time of cases created. Individual cases can be kept for longer periods by overriding the auto-delete function.

Device Settings

The **Device Settings** section of the *Settings _tab allows users to configure cameras, accessories, and OnWatch remote. In _Camera Settings*, you will see all cameras connected to the system, along with selected information about each one. You can also add new CCTV or AI cameras here, search for a specific camera by the filters, and export the camera grid to CSV. In *Accessories* are third-party hardware devices that act as a middleman between a door controller and the OnWatch system. They are used to lock and unlock a door or gate based on whether the system recognizes an individual attempting to enter as an authorized Personnel. In *OnPatrol Remote*, you'll be able to enable OnPatrol Remote functionality so you can access OnWatch on the go through your phone.

Camera Settings



Add tag to filter or free type to search

3 RESULTS

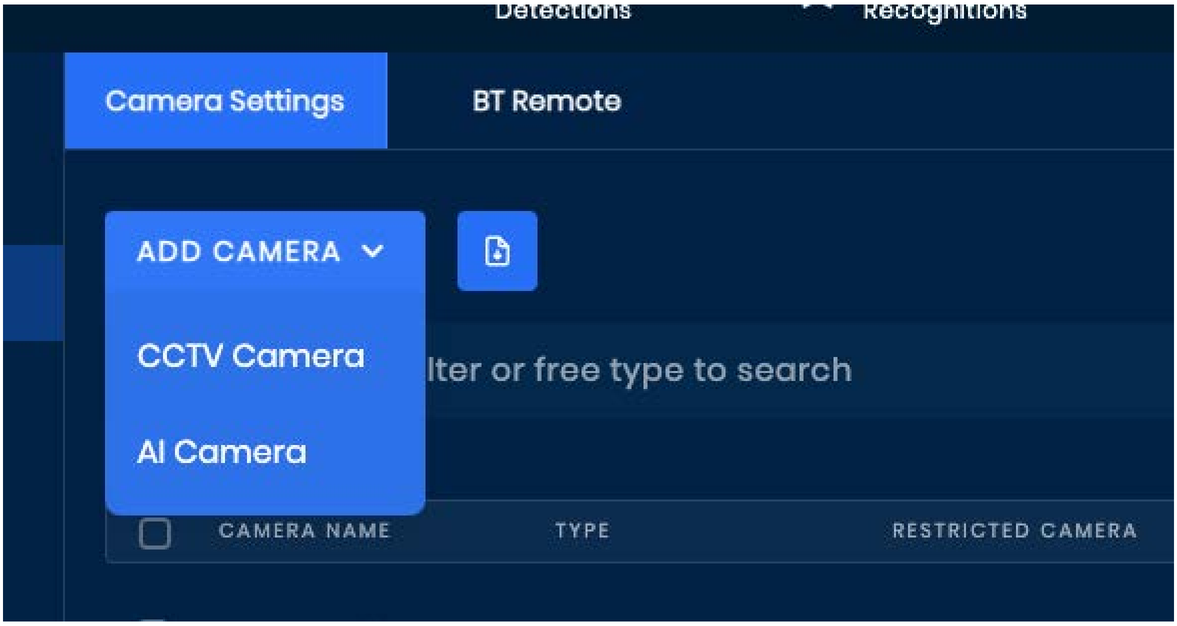
☐	CAMERA NAME	TYPE	RESTRICTED CAMERA	ADMIN STATUS	CAMERA STATUS	DEVICE GROUP	CREATE DATE ↓	PIPE
☐	Honeywell S70	AI Camera		Disabled	Disconnected	Default Device Gr...	03/08/2022 17:09	ai-camera-server...
☐	10.1.50.54 - Camer...	CCTV Camera		Enabled	Reconnecting	Default Device Gr...	02/08/2022 15:22	pipeng-0.pipeng...
☐	Finance corner	CCTV Camera		Disabled	Disconnected	Default Device Gr...	01/08/2022 12:12	pipeng-0.pipeng...

Add a Camera

When clicking on **Add Camera** there are 2 options -

- AI camera
- CCTV camera

> ### Camera types
>
> CCTV camera - Regular RTSP connection camera.
> AI camera - Honeywell S70 cameras that run Oosto's image processing pipeline, therefore AI camera can be Face only and have limited configuration options - no option to control camera type, camera calibration and security access.



After choosing the camera type, a window will open where you will be asked to input information about the new camera.

> 🚧 **Non Latin Group and Camera Names**
>
> When using non-latin letters need to open the CSV file with Excel on unicode UTF 8

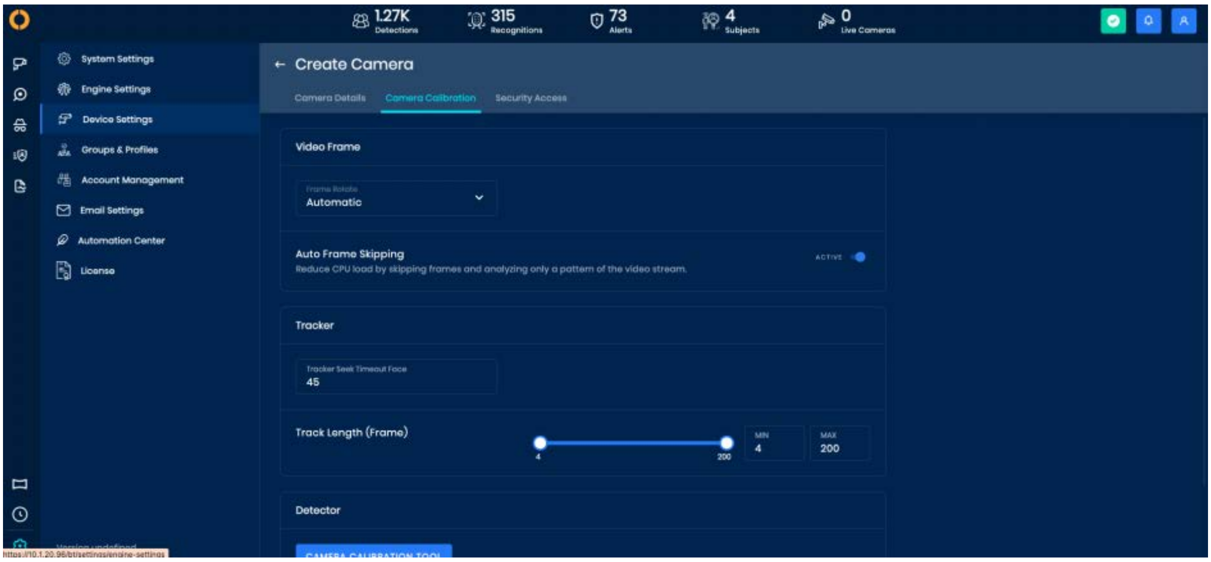
Fill out the camera's *Name*, select a *Camera Group*, and for CCTV camera you can choose *Camera Mode*. The mode determines whether the camera will analyze faces, bodies, or Person (both faces and bodies). When the blue toggle shows next to *Auto Start*, it means that the system will automatically activate the camera as soon as it is added.

> 📘 **Note**
>
> Camera name should be unique as the system does not allow 2 cameras with the same name.

Camera calibration

The *Pipe _will be filled out automatically, and you can add a _Description if one is relevant. Use the longitude and latitude fields or the pin to set the camera _Location*, input the *Video URL*, and set the _Threshold *for recognition.

Once all details are filled, you will be able to click **Camera Calibration** for the next stage of details.



← Create Camera

Video Frame

Frame Rotate: Automatic

Auto Frame Skipping — ACTIVE
Reduce CPU load by skipping frames and analyzing only a pattern of the video stream.

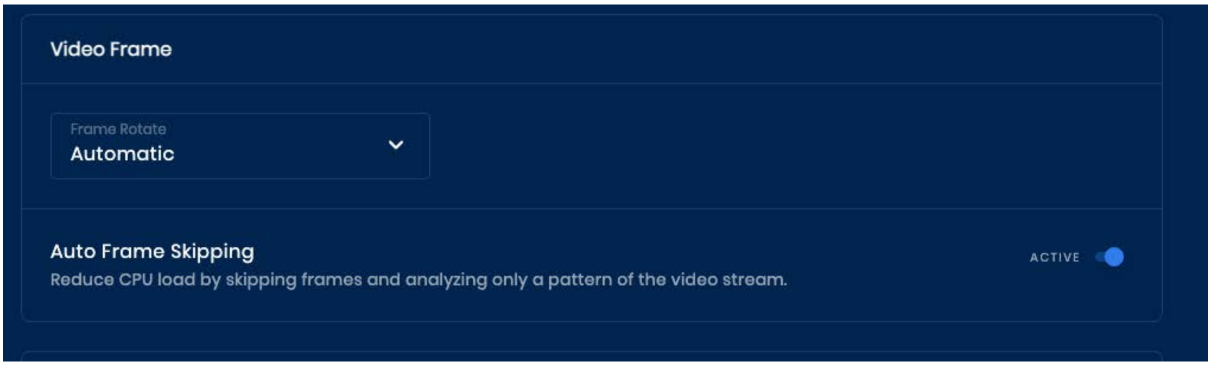
Tracker

Tracker Seek Timeout Face: 45

Track Length (Frame): MIN 4, MAX 200

Detector

Within this window, the first section on the left side of the screen is the *Video Processor* section.



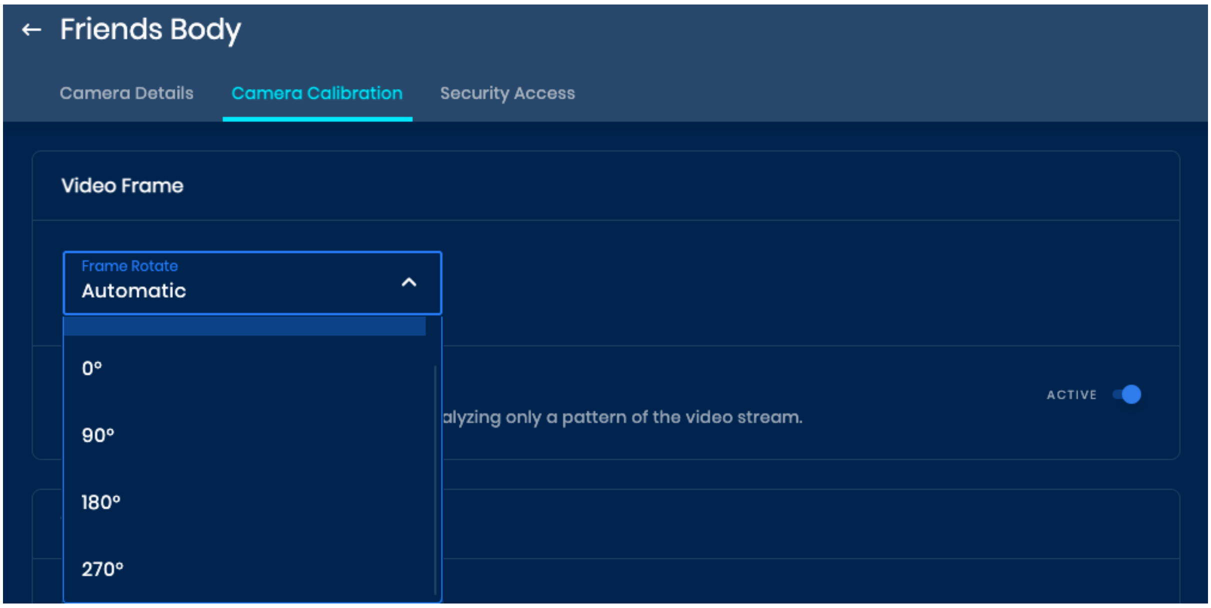
Video Frame

Frame Rotate: Automatic

Auto Frame Skipping — ACTIVE
Reduce CPU load by skipping frames and analyzing only a pattern of the video stream.

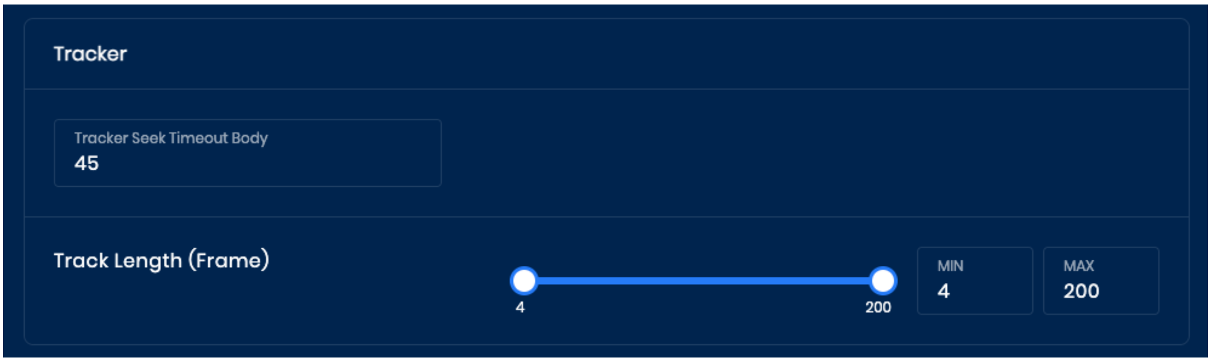
Fill out the *Frame Rotate* from the drop-down menu. Use this option to correct the incoming camera stream for cameras that are installed upside down or sideways. For example, if I have a camera installed upside down at an entrance, I will rotate the frame by 180 degrees so OnWatch can analyze the stream right-side-up.

You can choose to rote the camera 0, 90, 180, or 270 degrees.



Frame Rotate
Automatic

By enabling *Auto Frame Skipping*, the system will not analyze every single frame, instead it will automatically analyze only a portion of the frames to reduce CPU load and minimize delay. Green indicates it is enabled, and blue means it is disabled and the system will analyze each individual frame.



Tracker Seek Timeout Body
45

Track Length (Frame)

MIN
4

MAX
200

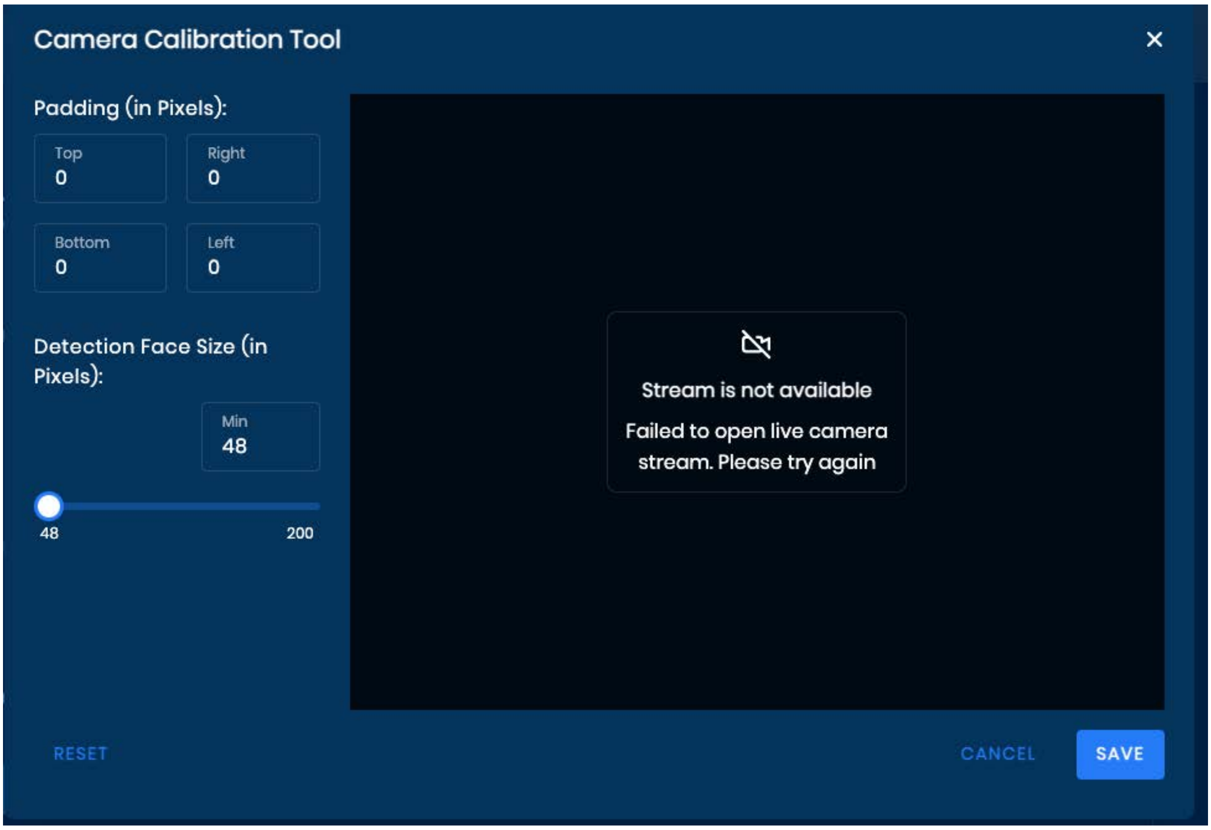
Under the Tracker section, input the *Tracker Minimum Length* and *Maximum Length* in frames. These values describe the range of how many frames the system includes in every track that is sent to the server. Usually, only the Tracker Maximum Length will need to change, depending on your use case.

The *Tracker Minimum Length* setting is automatically set at 4 frames, which means that the system will only send a track to the server if it detects a face in a minimum of 4 continuous frames. If the same person appears in just 3 continuous frames (for example if he/she moved in a different direction in the 4th frame, and his/her face is no longer detectable), the track will not be sent to the server.

The *Tracker Maximum Length* setting determines the maximum number of frames that each track will contain. For example, if this value is set at 200 frames, after a person's face is detected in 200 continuous frames, the system will send the track to the server and begin a new one. If you are using a camera of 25 FPS, it will take 8 seconds of the static person to reach the track maximum length (200 frames / 25 frames per second).

Input a value for *Tracker Seek Timeout*. This determines the number of frames that can pass by before the system sends a new detection track. For example, after OnWatch starts detecting and tracking a person, that person might not appear in a certain number of frames. Let's say that person passes behind a pole while walking. The value in this field specifies the number of frames that the person is not detected by OnWatch, but is still tracked. This would enable the system to still include that person in the track after they come out from behind the pole, rather than sending a new track.

Next, fill out the details for the **Detector** section.



Camera Calibration Tool

Padding (in Pixels):

Top 0

Right 0

Bottom 0

Left 0

Detection Face Size (in Pixels):

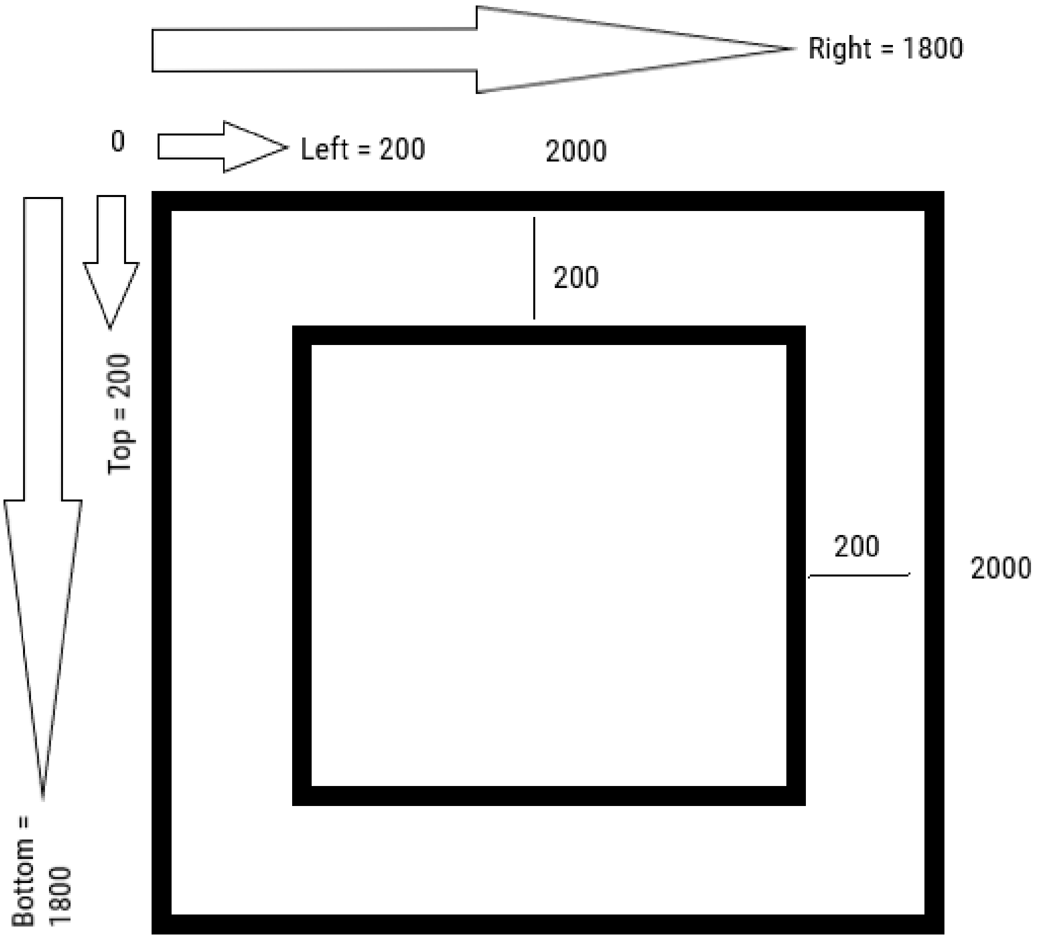
Min 48

Stream is not available

Failed to open live camera stream. Please try again

Camera Padding allows you to determine exactly which areas of the camera's field of view you would like OnWatch to analyze. Input the pixels you would like the system to ignore from each side of the camera FOV, separating the values with a comma. The remaining space will be analyzed by the system.

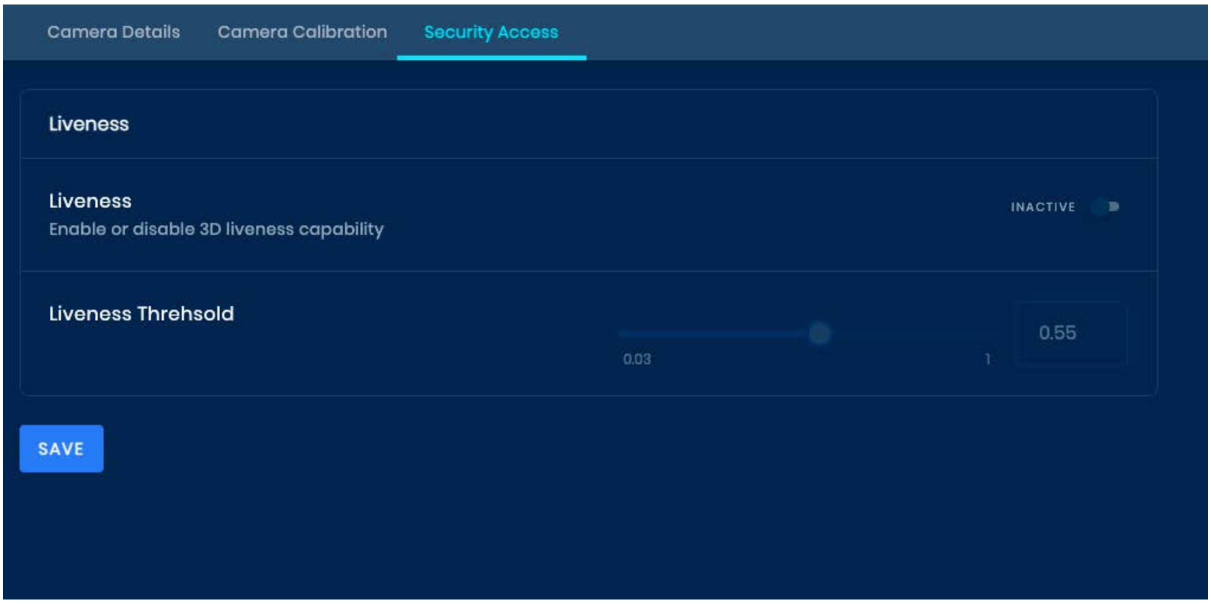
> ### 📘 Camera Padding Values
>
> Note that camera padding pixel values are determined in proportion to the number of pixels in the area of the screen.
> A pixel value for camera padding represents a perimeter line to be cropped from the field of view.
> The lines are either vertical or horizontal (top/bottom or left/right).
> The length of the line is derived along the axis from the top-left corner of the screen, which is the zero point.
> The reference image directly below shows an example, which we will walk through here:
>
> - The outer square in the image represents the camera field of view, which measures 2000 pixels by 2000 pixels. The inner square, which reduces each side by 200 pixels, is the area you want OnWatch to analyze.
> - In this instance, the _Top _value to input for camera padding is 200 (this means you are telling the system to disregard the top 200 pixels).
> - The *Right* value for camera padding is 1800 (you are telling the system to disregard the remaining 200 pixels left between 1800 and 2000 on the right side of the area).
> - The *Bottom* value is 1800 (you are telling the system to disregard the remaining 200 pixels left between 1800 and 2000 at the bottom of the area).
> - The *Left* value is 200 (you are telling the system to disregard the first 200 pixels on the left).



Clicking the Reset button on the corner of this section will reset the values for detector settings.

Security Access

Allow you the option to activate (if supported) 3D liveness capability and set a threshold for liveness.



Liveness

Liveness
Enable or disable 3D liveness capability
INACTIVE

Liveness Threhsold
0.03
1
0.55

Click **Save.**

Groups & Profiles

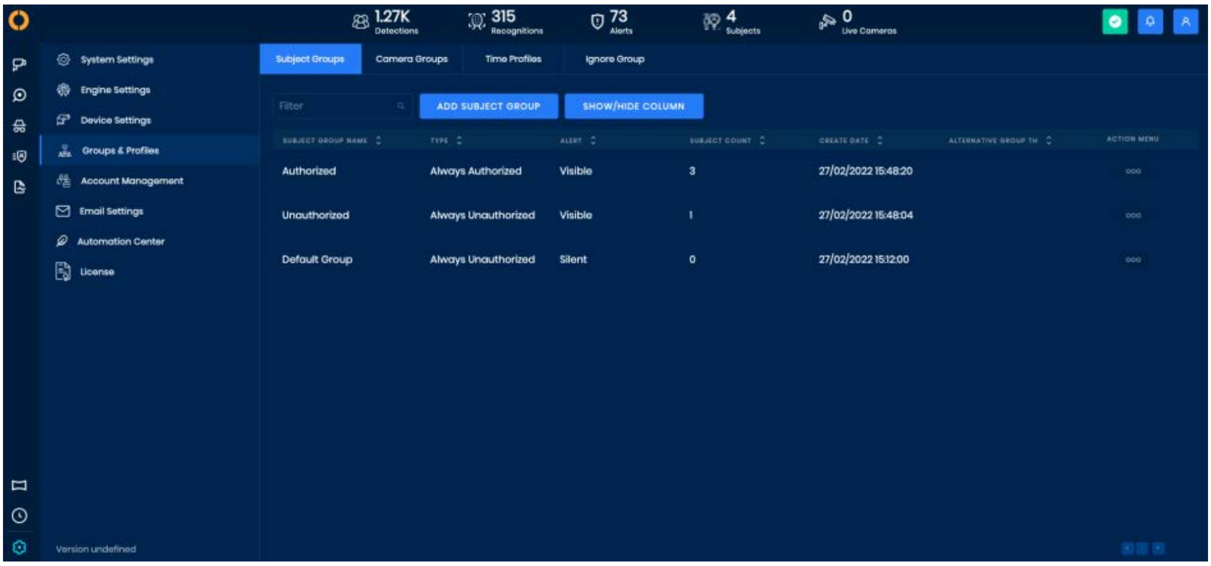
Within OnWatch, you can create groups to differentiate between a variety of subjects and cameras. Head to *Groups & Profiles* in *Settings* to create subject groups and camera groups, as well as establish time profiles for your conditionally authorized subject groups.

Within *Groups & Profiles*, you can also see your ignore group. The ignore group is comprised of all the detections you would like the system to purposely ignore.

Subject Groups

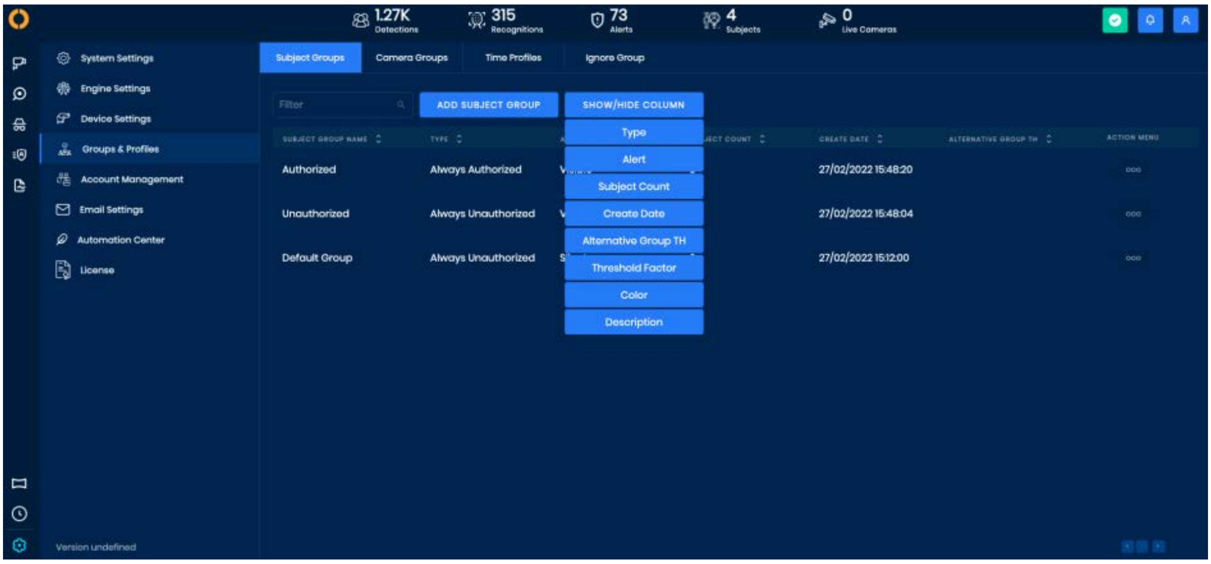
The Subject Groups tab allows you to add subject groups the the system and edit or delete existing groups.

You can see any existing subject group listed here, along with information like *Subject Group Name*, *Type*, *Alert*, *Subject Count* and *Create Date*.

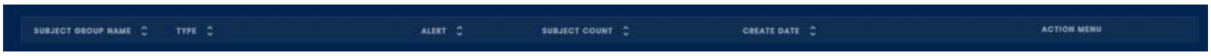


SUBJECT GROUP NAME	TYPE	ALERT	SUBJECT COUNT	CREATE DATE	ALTERNATIVE GROUP TH	ACTION MENU
Authorized	Always Authorized	Visible	3	27/02/2022 15:48:20		ooo
Unauthorized	Always Unauthorized	Visible	1	27/02/2022 15:48:04		ooo
Default Group	Always Unauthorized	Silent	0	27/02/2022 15:12:00		ooo

Clicking **Show/Hide Column** allows you to configure the information shown and add more or fewer categories. You can also filter your results by group name in the search bar.



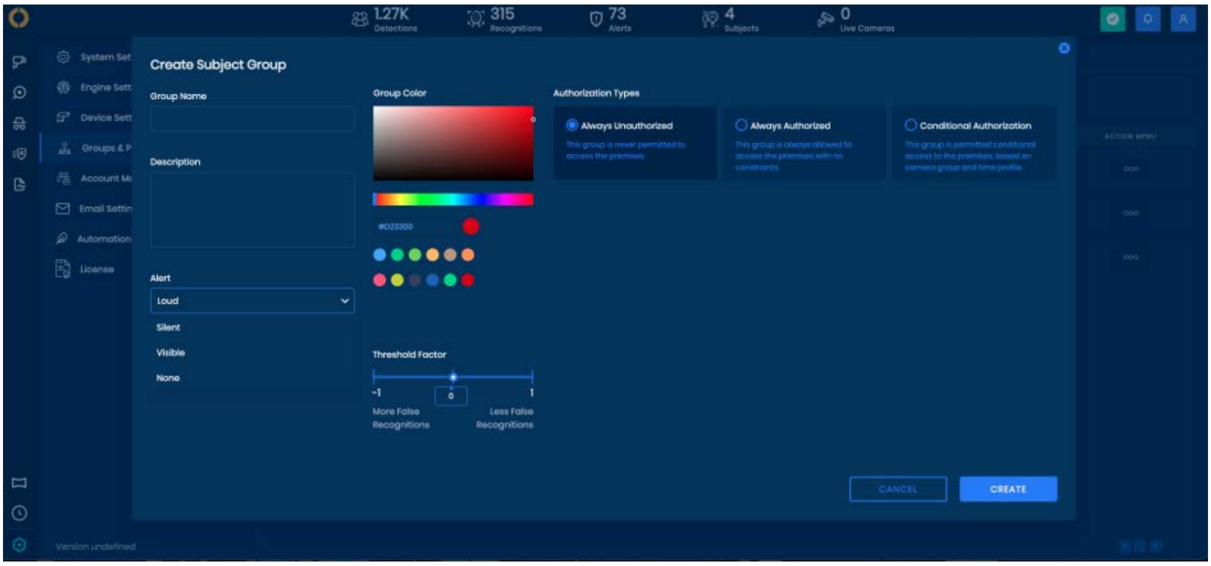
Click on the **arrows** next to each column header to sort by column.



SUBJECT GROUP NAME	TYPE	ALERT	SUBJECT COUNT	CREATE DATE	ACTION MENU

Create a New Subject Group

1. Click **Add Subject Group**. A pop-up will open where you can input information, such as name, description, alert status, color, camera groups, and authorization type, in order to add a new subject group to the system.


Create Subject Group

Authorization Types

● Always Unauthorized: This group is never permitted to access the premises.

○ Always Authorized: This group is always allowed to access the premises with no constraints.

○ Conditional Authorization: This group is permitted conditional access to the premises, based on camera group and time profile.

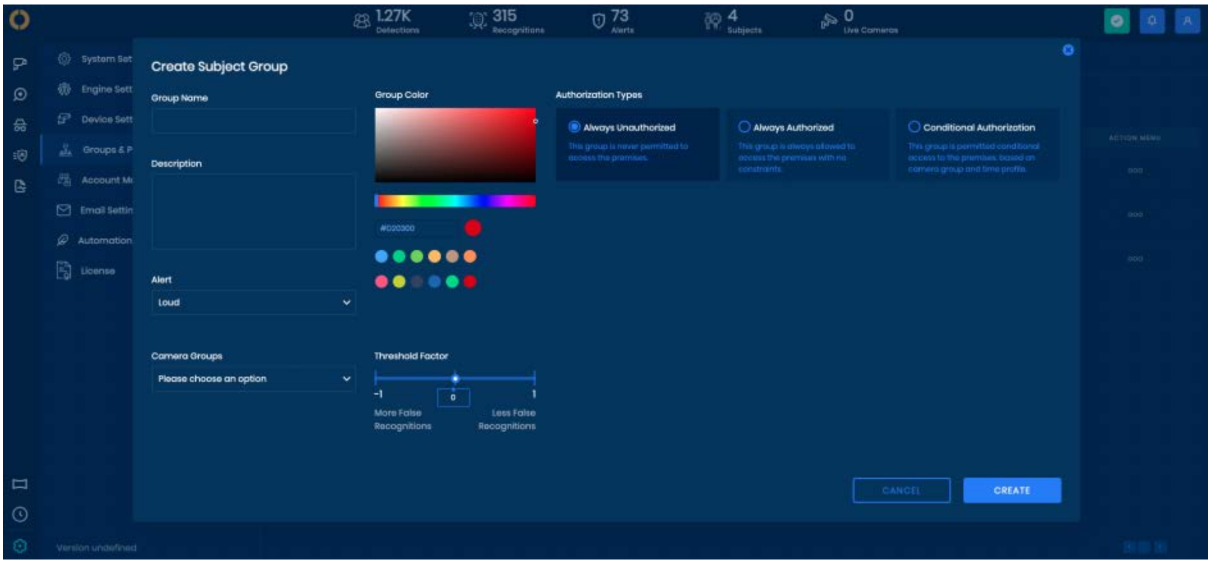
Alert: Loud

Group Color: #D20300

Threshold Factor: 0

2. Add a *Group Name* and type a *Description* if relevant.
3. Click the **Alert** tab to set what type of alert you would like the system to apply to this group. The options are:

- **Loud**: This is the default option. The system will generate an audible noise and popup message when subjects are identified, and will show a detection snapshot in the *Alerts* tab in **Live Cameras**.
- **Visible**: The system will not generate any noise, but will apply a popup messages and show a detection snapshot in *Alerts*.
- **Silent**: The system will not generate any noise or popup message, but a detection snapshot will appear in the *Alerts* tab.
- **None**: The system will not generate any noise, popup message, or detection snapshot in *Alerts*.


Create Subject Group

Authorization Types

● Always Unauthorized: This group is never permitted to access the premises.

○ Always Authorized: This group is always allowed to access the premises with no constraints.

○ Conditional Authorization: This group is permitted conditional access to the premises, based on camera group and time profile.

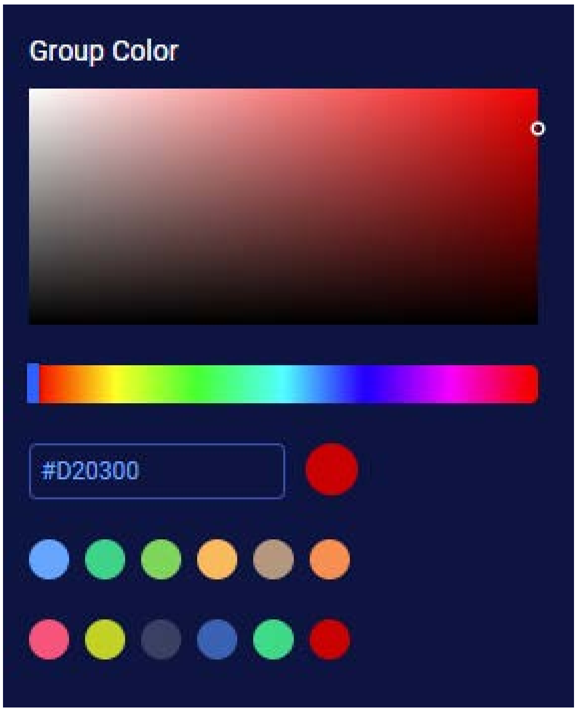
Alert: Loud

Camera Groups: Please choose an option

Group Color: #D20300

Threshold Factor: 0

4. Determine the threshold factor for the group. Based on the threshold factor you choose for this subject group, the camera threshold will change.
5. Select a **color** that will represent your group. **Group Color** options help the user identify between multiple subject groups in the *Alerts* tab within the **Live Cameras** window.



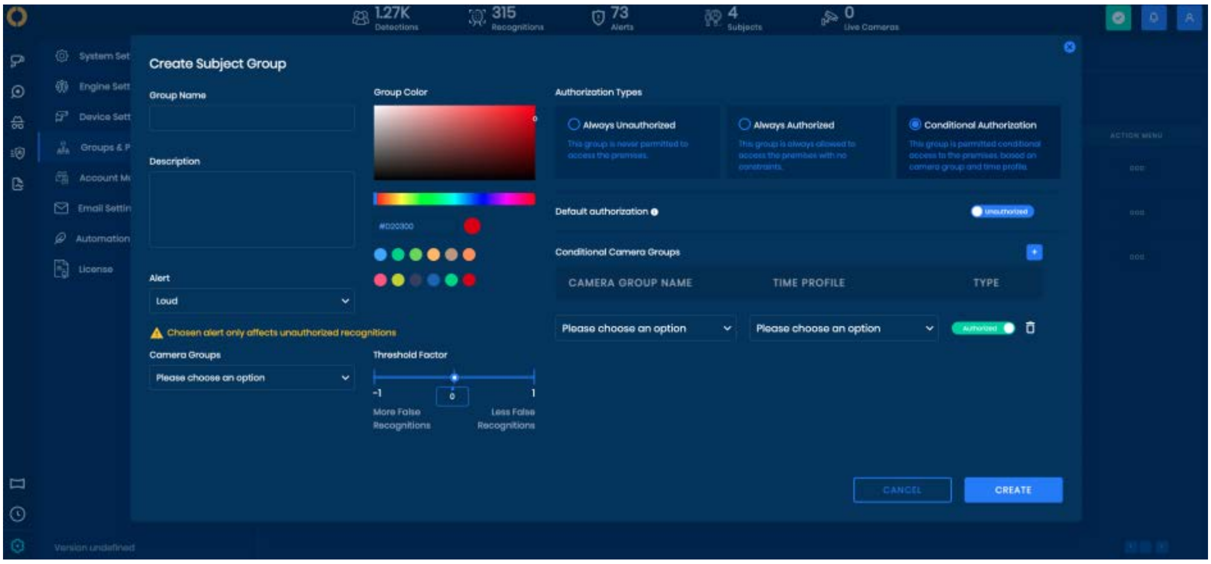
Group Color

#D20300

6. Select an option from the *Authorization Types* for your group.

- **Always Unauthorized** means that the group is never permitted to access the premises.
- **Always Authorized** means that the group is allowed to access the premises with no constraints.
- **Conditionally Un/Authorized** means that the group is permitted conditional access to the premises, based on camera group and time profile. If you select this option, more fields will appear.
  You can set these fields in the *Camera Groups* and *Time Profiles* sections, respectively.

7. Select options from the *Group Name* drop-down list and *Time Profile* drop-down. Click the **plus icon** to add more conditions, and click on the **trash icon** to remove.



Create Subject Group

Group Name

Description

Alert: Loud

⚠ Chosen alert only affects unauthorized recognitions

Camera Groups: Please choose an option

Group Color: #D20300

Threshold Factor: 0

Authorization Types

○ Always Unauthorized — This group is never permitted to access the premises.

○ Always Authorized — This group is always allowed to access the premises with no constraints.

● Conditional Authorization — This group is permitted conditional access to the premises, based on camera group and time profile.

Default authorization: Unauthorized

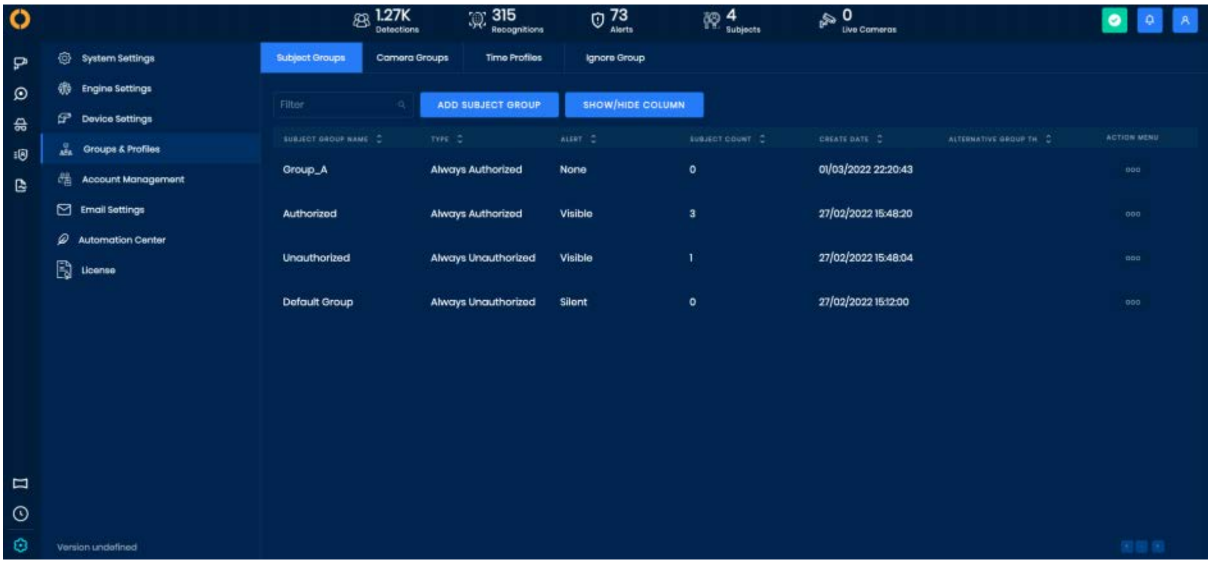
Conditional Camera Groups

CAMERA GROUP NAME	TIME PROFILE	TYPE
Please choose an option	Please choose an option	Authorized

8. When you've finished, click **Create** to generate the new subject group.

Edit, Clone, or Delete a Subject Group

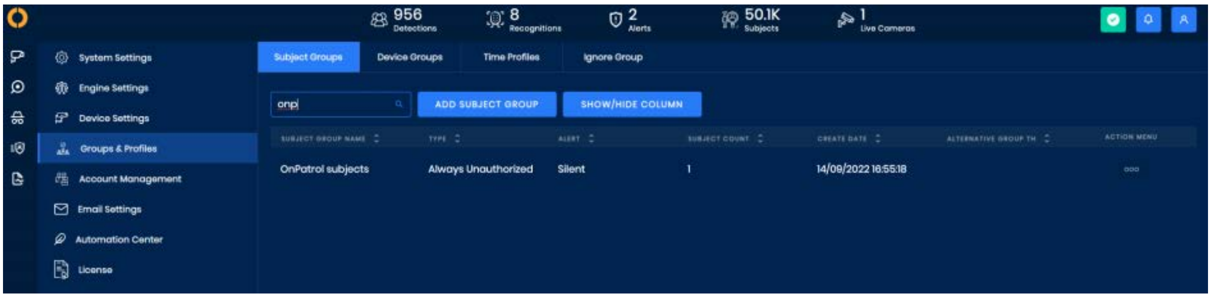
You can *Edit*, *Clone*, or *Delete* a group by clicking on the **3-dotted icon** under the *Action Menu*.



SUBJECT GROUP NAME	TYPE	ALERT	SUBJECT COUNT	CREATE DATE	ALTERNATIVE GROUP TH	ACTION MENU
Group_A	Always Authorized	None	0	01/03/2022 22:20:43		
Authorized	Always Authorized	Visible	3	27/02/2022 15:48:20		
Unauthorized	Always Unauthorized	Visible	1	27/02/2022 15:48:04		
Default Group	Always Unauthorized	Silent	0	27/02/2022 15:12:00		

Synced Subject Group

There is an option to sync the "OnPatrol subjects" subject group to OnPatrol devices.
The sync is triggered from the side of the devices by adding OnWatch server creds.



SUBJECT GROUP NAME	TYPE	ALERT	SUBJECT COUNT	CREATE DATE	ALTERNATIVE GROUP TH	ACTION MENU
OnPatrol subjects	Always Unauthorized	Silent	1	14/09/2022 16:55:18		

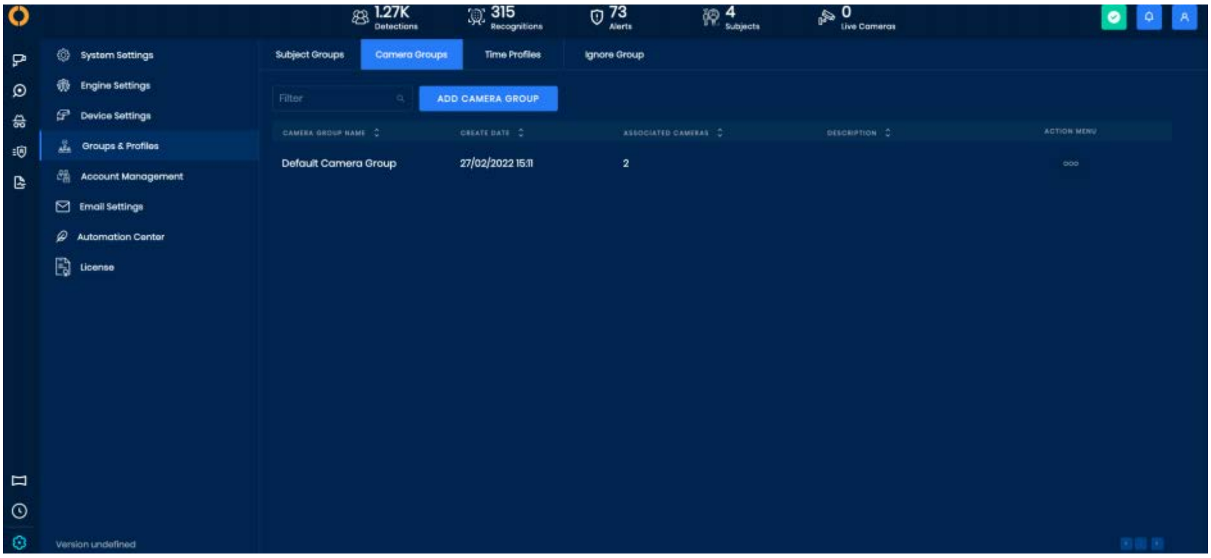
For more information go to OnPatrol Sync subject

Camera Groups

The Camera Groups tab allows you to add camera groups to the system and edit or delete existing groups.

Cameras should be grouped together based on their purpose and location.

You can see any existing camera group listed here, along with the group's associated *Create Date*, *Associated Cameras*, and *Description*. You can also filter your results by group name in the search bar.



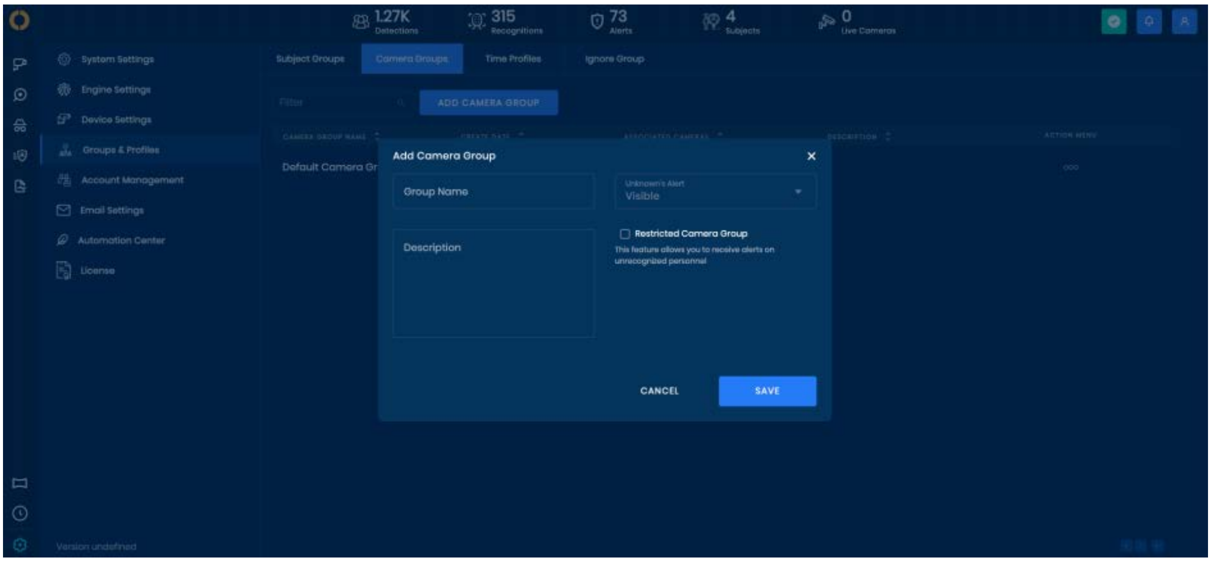
CAMERA GROUP NAME	CREATE DATE	ASSOCIATED CAMERAS	DESCRIPTION	ACTION MENU
Default Camera Group	27/02/2022 15:11	2		

Click on the **arrows** next to each column header to sort by column.

CAMERA GROUP NAME	CREATE DATE	ASSOCIATED CAMERAS	DESCRIPTION	ACTION MENU

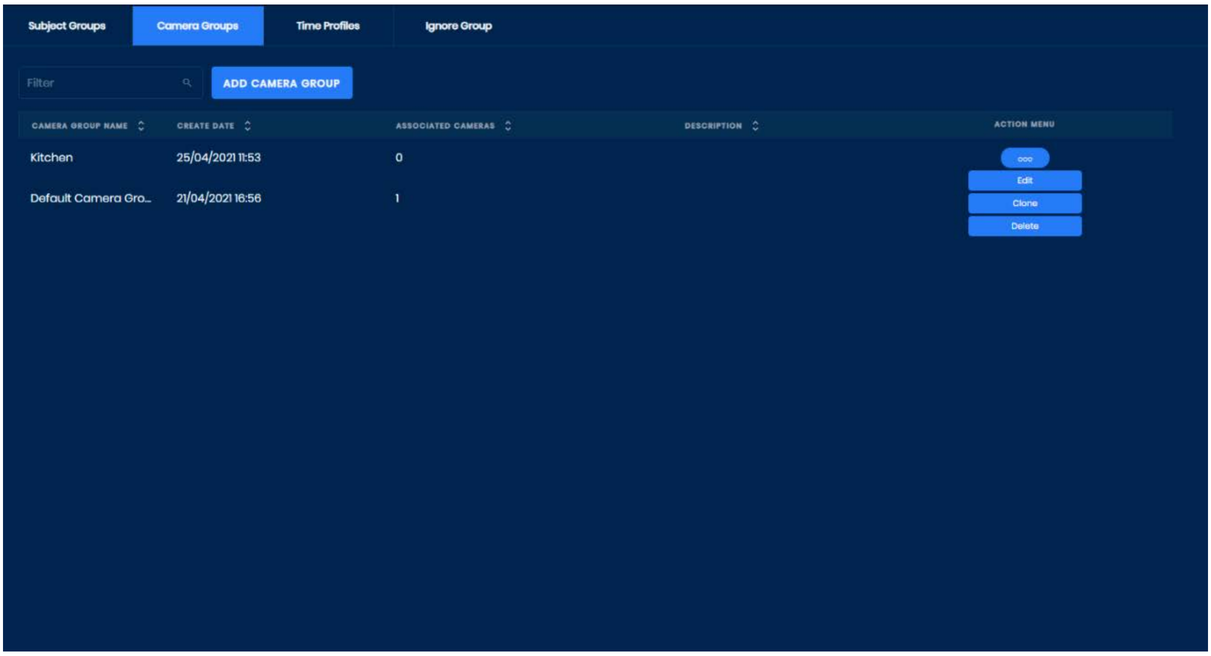
Create a New Camera Group

1. Click **Add Camera Group**. A pop-up will open where you can input the *Group Name* and *Description*. Click **Save**.



Edit, Clone, or Delete Camera Groups

You can *Edit*, *Clone*, or *Delete* a group by clicking on the **3-dotted icon** under the *Action Menu*.

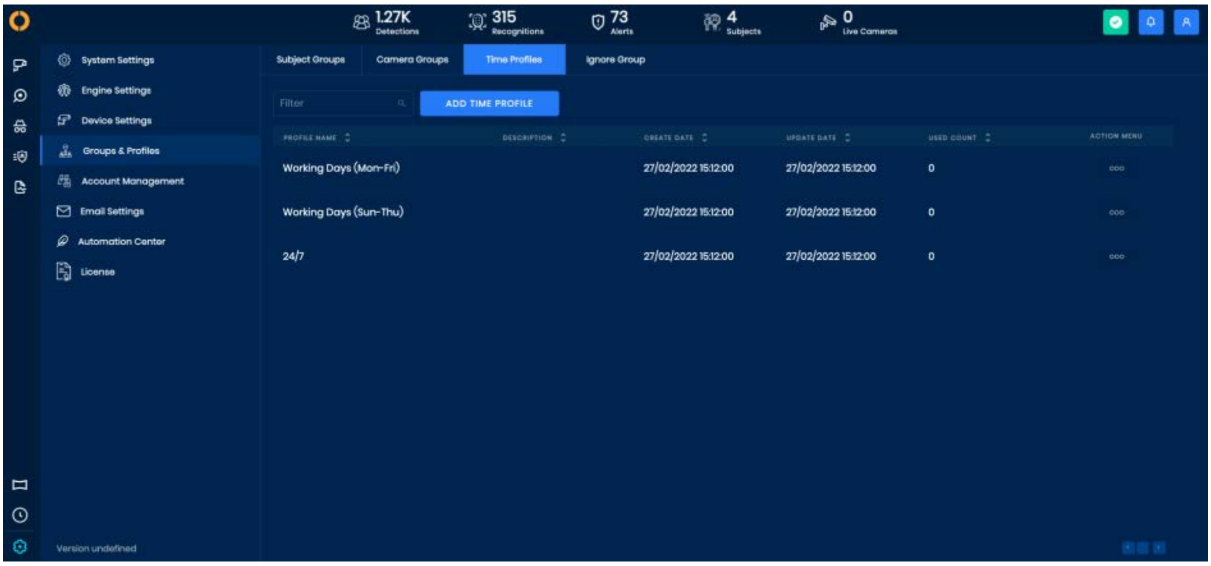


CAMERA GROUP NAME	CREATE DATE	ASSOCIATED CAMERAS	DESCRIPTION	ACTION MENU
Kitchen	25/04/2021 11:53	0		ooo
Default Camera Gro...	21/04/2021 16:56	1		

Time Profiles

The Time Profiles tab allows you to add time profiles, which you can then apply to conditionally authorized subjects in the *Subject Groups* tab.

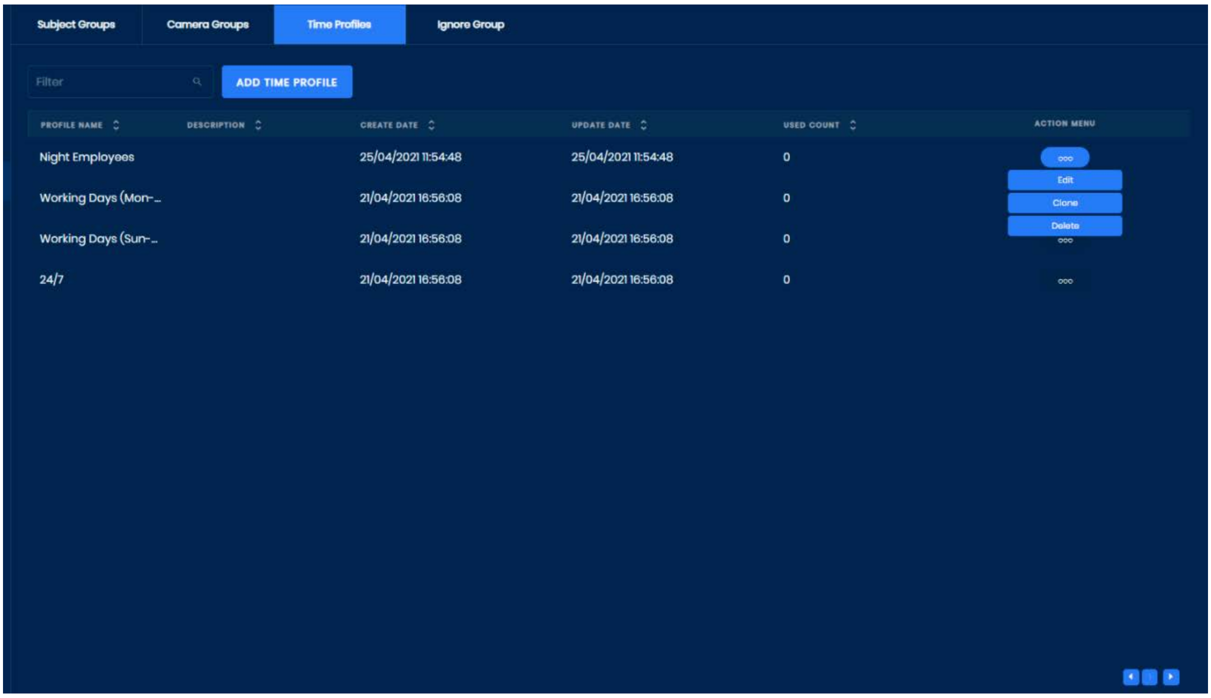
You can see any defined time profile listed here, along with the profile's associated *Status*, *Description*, and *Create Date*, *Update Date*, and *Used Count*. You can also filter your results by group name in the search bar.



PROFILE NAME	DESCRIPTION	CREATE DATE	UPDATE DATE	USED COUNT	ACTION MENU
Working Days (Mon-Fri)		27/02/2022 15:12:00	27/02/2022 15:12:00	0	ooo
Working Days (Sun-Thu)		27/02/2022 15:12:00	27/02/2022 15:12:00	0	ooo
24/7		27/02/2022 15:12:00	27/02/2022 15:12:00	0	ooo

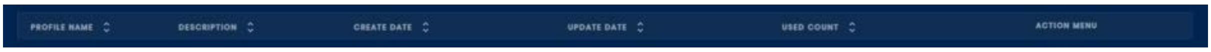
Edit, Clone, or Delete Time Profiles

You can *Edit*, *Clone*, or *Delete* a group by clicking on the **3-dotted icon** under the *Action Menu*.



PROFILE NAME	DESCRIPTION	CREATE DATE	UPDATE DATE	USED COUNT	ACTION MENU
Night Employees		25/04/2021 11:54:48	25/04/2021 11:54:48	0	ooo
Working Days (Mon-...		21/04/2021 16:56:08	21/04/2021 16:56:08	0	
Working Days (Sun-...		21/04/2021 16:56:08	21/04/2021 16:56:08	0	ooo
24/7		21/04/2021 16:56:08	21/04/2021 16:56:08	0	ooo

Click on the **arrows** next to each column header to sort by column.

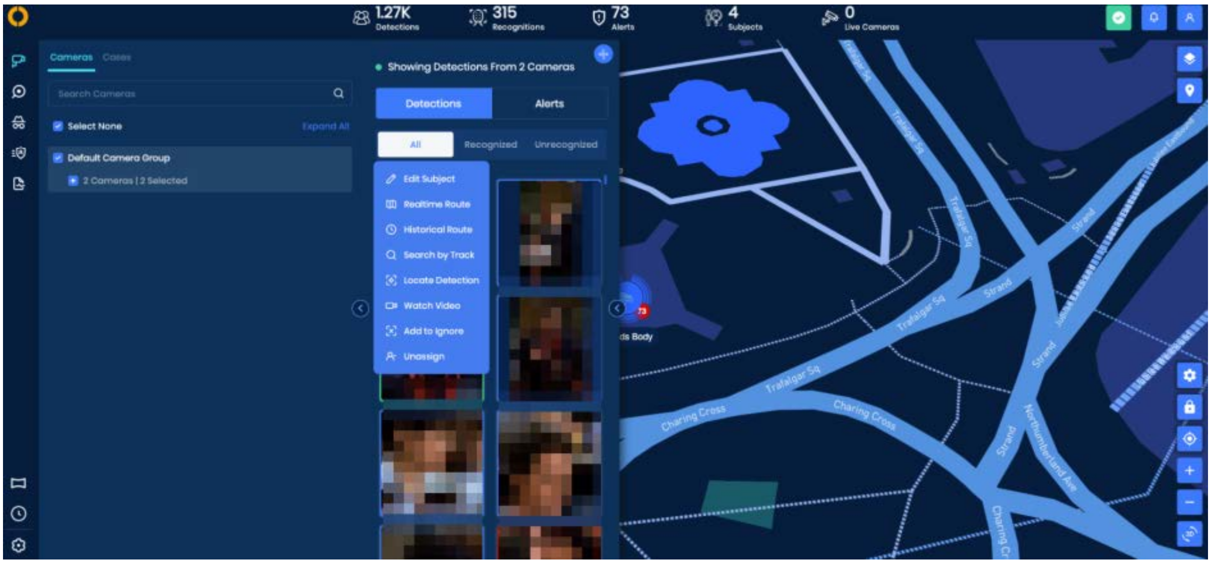


Ignore Group

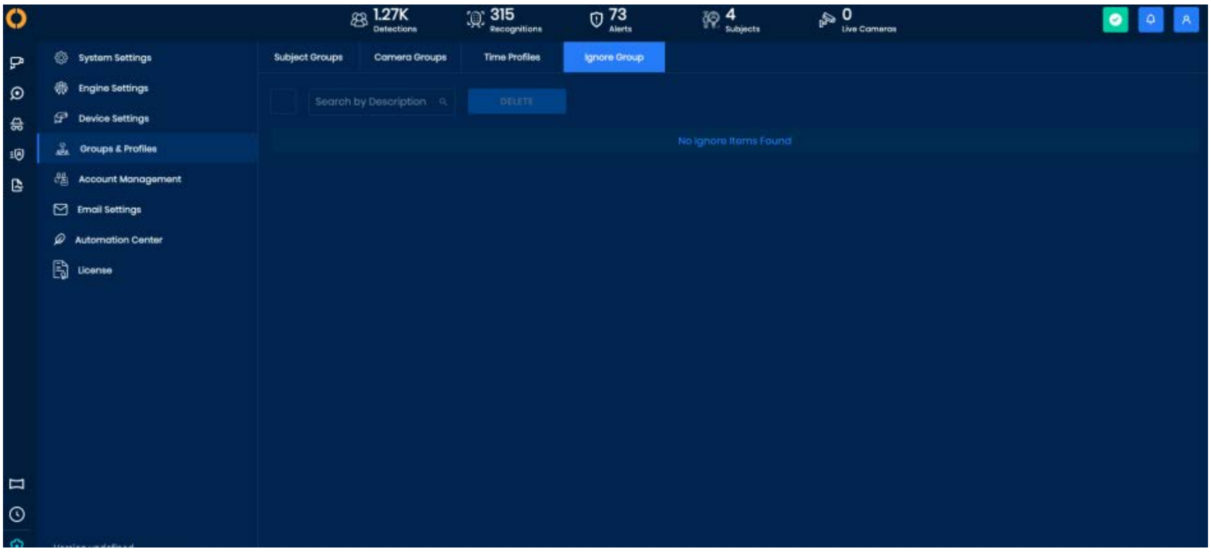
You can ignore any detection captured by your cameras. You'll want to ignore faulty detections, such as detections of objects, in order to teach the system that those detections are not valid.

Ignore a Detection from Live Cameras

1. Navigate to the Live Cameras tab and locate the detection you would like to ignore.
2. Click on the **three-dotted icon** on the detection image.
3. Select **Add to Ignore** from the drop-down.



All detections that you ignore can be found in the *Ignore Group* section of *Groups & Profiles*.



Account Management

Within Account Management, there are 4 tabs:

1. User Accounts
2. User Groups
3. Active Directory
4. SAML SSO

Set up the roles and permissions for all your system users depending on your company's use case.

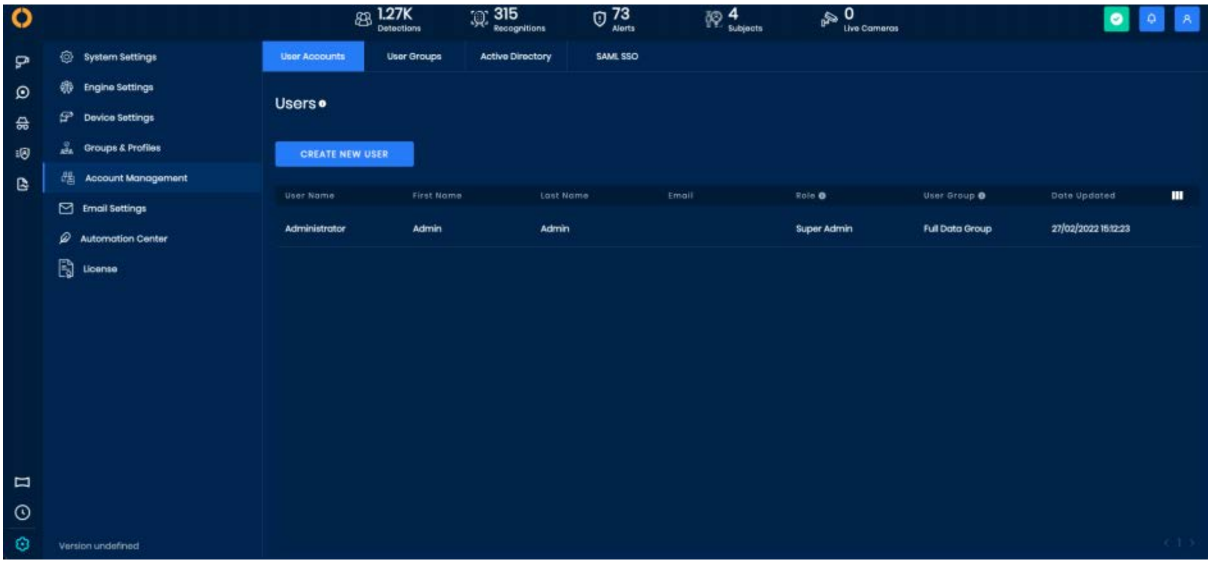
Below is a comparison of the differences between the account methods

	OnWatch Local Account	LDAP	SAML
What are the differences in administration between the types?	Username/password Administered within on watch, Manual management. If a user leaves the org he needs to be removed manually from OnWatch.	User/pass and all of their management (complexity, JIT, other controls) is administered externally from the customers Active Directory environment.	User/pass is fully managed in the IDP of the customer, similar to LDAP but not with Active Directory and other IDP vendors.
What are the differences to the end-user?	User adds user password to the login page of OnWatch, they needs= to comply with pass requirements setup within OnWatch.	User uses his Active Directory Credential to manually add to the login page of the OnWatch, no new credential are generated. The users are administer in Active directory groups that can be mapped to our user groups.	When the user goes to our login page they will be presented with an option to login via SSO which will redirect them via the SSO system and that systems login process which will then redirect back to our application this can be seamless depending on how the IDP is setup.

> 👍 **Set Up Your User Groups First**
>
> You will need to have your User Groups already configured if you plan to manually add users to the system or will be using LDAP / SAML SSO to add users.

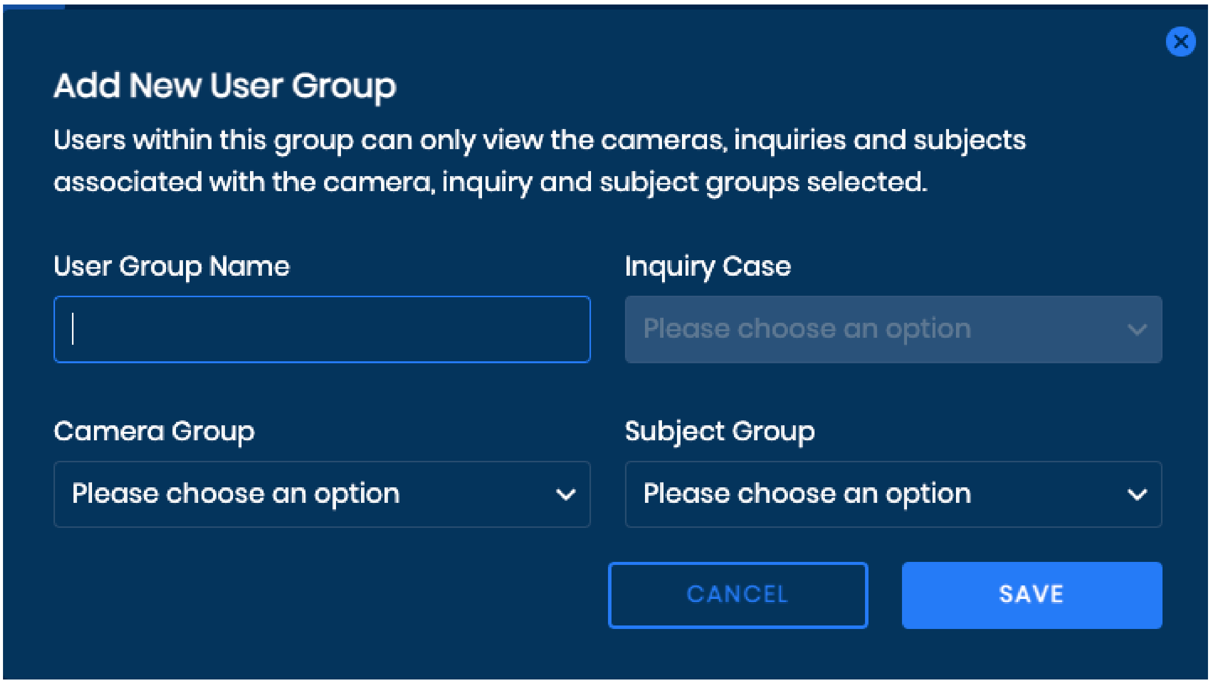
User Groups

1. Navigate to the **Account Management** section of *Settings*.



User Name	First Name	Last Name	Email	Role	User Group	Date Updated
Administrator	Admin	Admin		Super Admin	Full Data Group	27/02/2022 15:12:23

2. Select the **User Groups** tab.
3. Click **Add New User Group**.



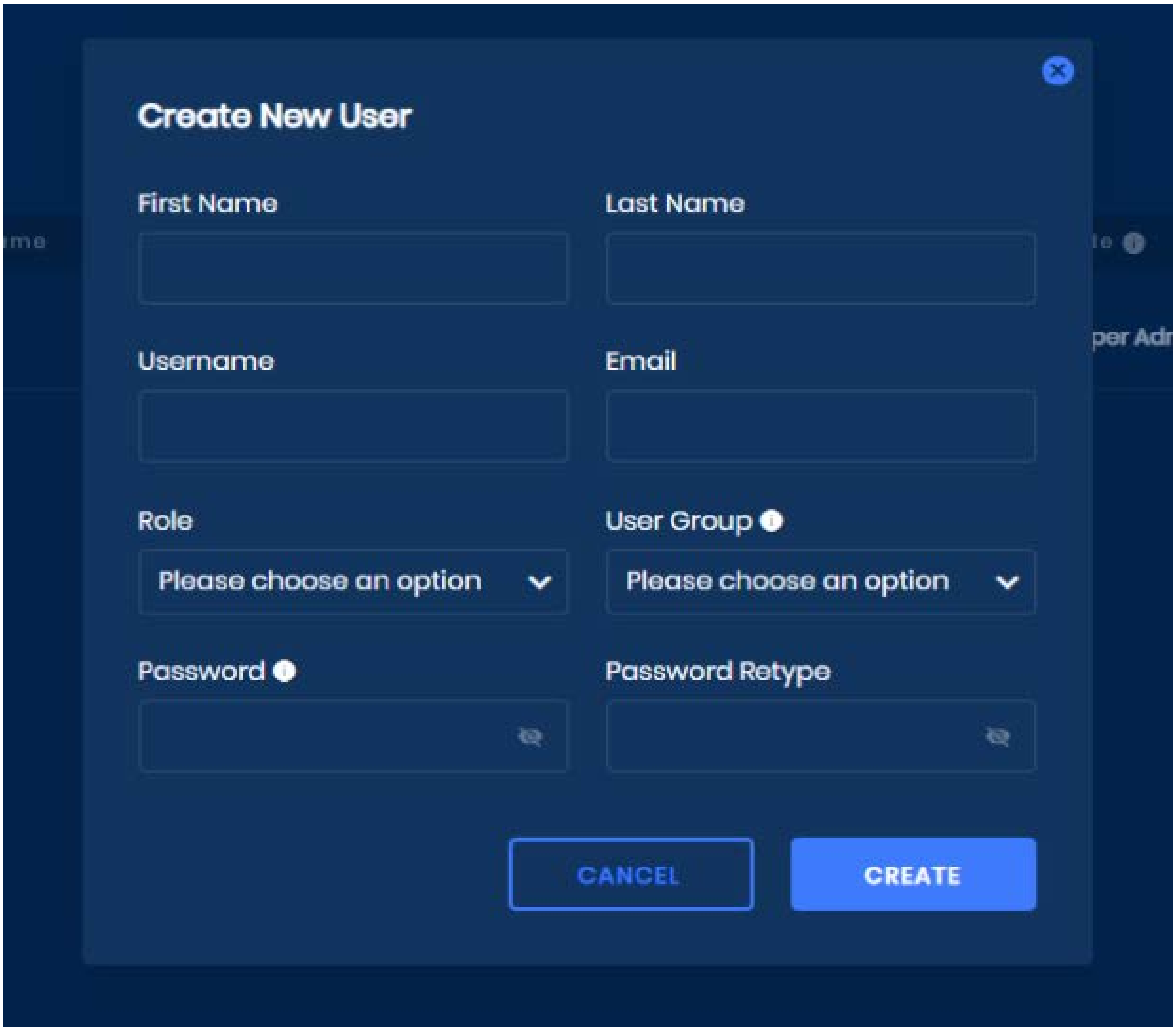
Add New User Group

Users within this group can only view the cameras, inquiries and subjects associated with the camera, inquiry and subject groups selected.

4. Input a **User Group Name**.
5. Select **Inquiry Case**.
6. Select the relevant *Camera Group*(s) and *Subject Group*(s).
7. Click **Save** when finished.

User Accounts

1. To add new users to the system, navigate to the *User Accounts* tab in *Account Management*.
2. Click **Create New User**.



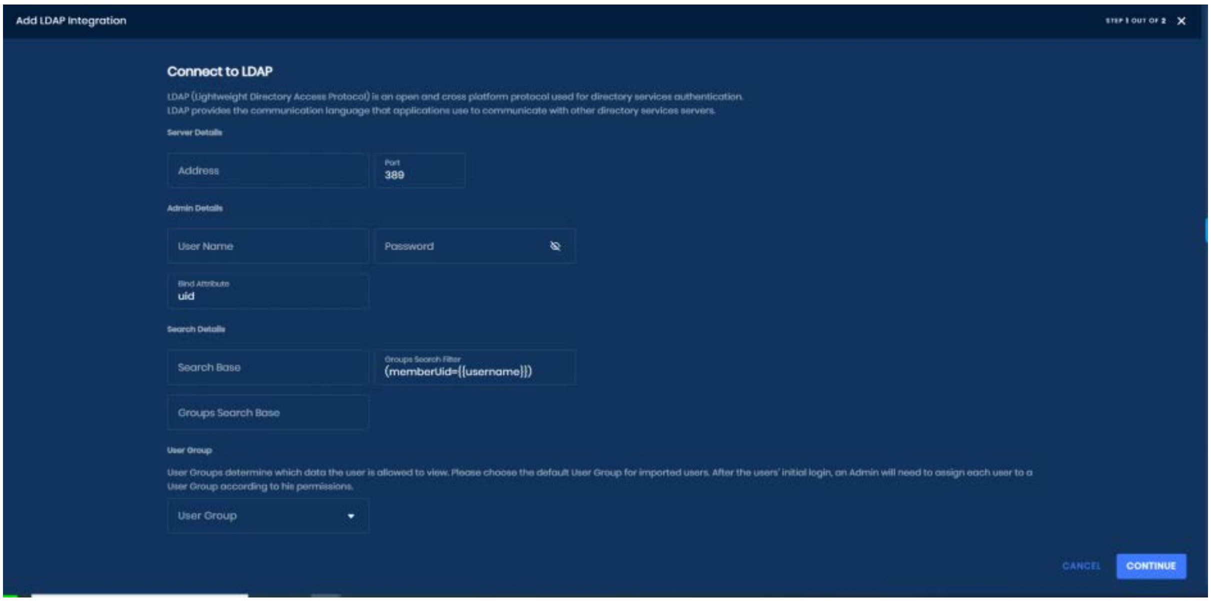
3. Input the user's *First Name*, *Last Name*, *Username*, and *Email* in the pop-up window.
4. Select a *Role* for the user from the options. This will determine the actions that the user can perform in the system.
5. Choose a *User Group* for the user from the options. This will determine the subject groups and cameras that the user will be able to see in the system.
6. Set and reconfirm a *Password*.
7. Click **Create**.

> 📘 **Don't know what role to assign a user?**
>
> Learn more about each **Role** in OnWatch, what permission levels they have, and how **User Groups** provide an extra layer of security through data permissions.

Active Directory

By establishing a connection with your Active Directory, your users can access the OnWatch system with their existing credentials.

You can complete the integration process directly within the OnWatch dashboard simply by navigating to the **Active Directory** section within the *Account Management* tab.



Connect to LDAP

LDAP (Lightweight Directory Access Protocol) is an open and cross platform protocol used for directory services authentication.
LDAP provides the communication language that applications use to communicate with other directory services servers.

Server Details

Address
Port
389

Admin Details

User Name
Password

Bind Attribute
uid

Search Details

Search Base
Groups Search Filter
(memberUid={{username}})
Groups Search Base

User Group

User Groups determine which data the user is allowed to view. Please choose the default User Group for imported users. After the users' initial login, an Admin will need to assign each user to a User Group according to his permissions.

User Group ▾

Start by inputting the **Server IP Address** and the **Port** for the Identity Provider. The address will usually start with ldap://. You will also need to include the Admin's credentials (username and password) for the Identity Provider.

Next, determine the **Bind Attribute**. This part is an option and is only required if you do not want the `Uid` (unique identifier) to be the technical searching field within the Active Directory.

Before continuing to the next page, input the **Search Base** - which defines the starting point for the search in the directory tree - and, if relevant, the **Group Search Base** as well.

Click **Continue** once you've finished inputting the parameters.

With the **Search & Select AD Groups** screen, a list of all your user groups associated with the Active Directory will appear. If you would like to move over the entire user group to the OnWatch system, use the + Select role key and select a role for this user group.

All user groups that do not have a Role assigned will not be migrated over to the OnWatch system.

> 📘 **Need Help Choosing a Role?**
>
> In essence, Roles determine what a user can do or see within the OnWatch system. Check out this chart to understand the different aspects of each Role.
>
> FYI: If a user is associated with more than one user group that is being synced with OnWatch, that user will be assigned the highest role.

Now that you've selected a Role for the groups you would like to move over, click **Add Group** at the bottom of the page.

You can then view the groups on the main Active Directory screen and can always add more groups by clicking + **Add Another Group**.

To enable the users to log in, you must Activate the Active Directory by **switching the toggle to Active**.

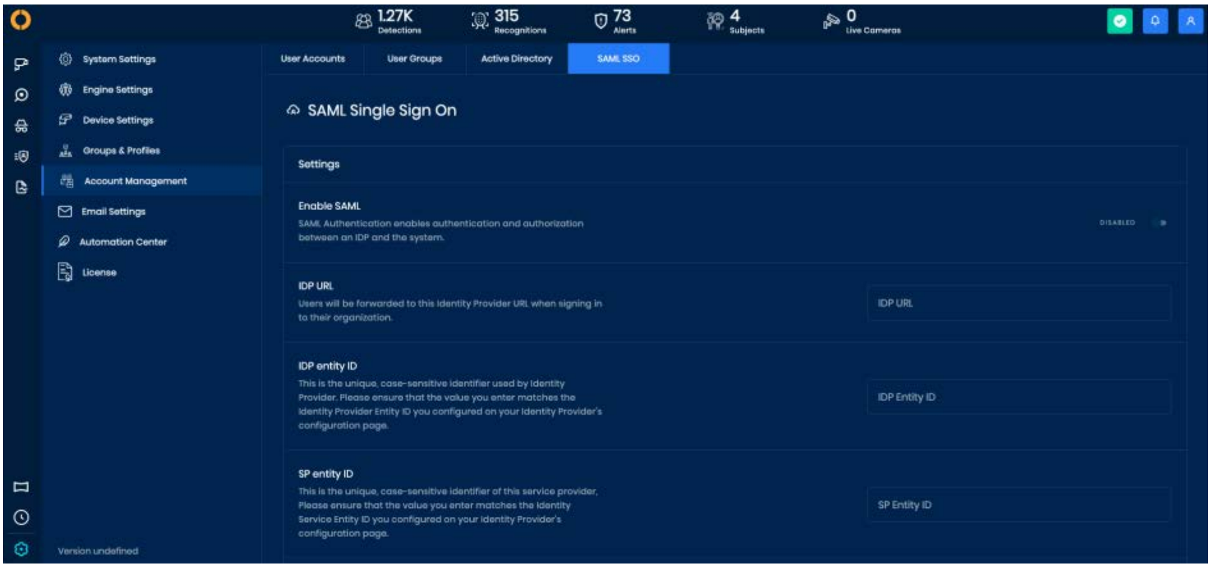
SAML

Overview

The Security Assertion Markup Language, or SAML for short, is a standard for logging users into multiple connected platforms at once using a single set of credentials per user and enables registered users to utilize SSO (single-sign on).

SAML SSO works by connecting an Identity Provider (IDP), such as Novell or JumpCloud, with an external platform, such as OnWatch, thereby sharing the credentials of each and every user already established in the Identity Provider database and making those credentials valid for all connected platforms.

OnWatch Configuration



SAML Single Sign On

Settings

Enable SAML
SAML Authentication enables authentication and authorization between an IDP and the system.
DISABLED

IDP URL
Users will be forwarded to this Identity Provider URL when signing in to their organization.
IDP URL

IDP entity ID
This is the unique, case-sensitive identifier used by Identity Provider. Please ensure that the value you enter matches the Identity Provider Entity ID you configured on your Identity Provider's configuration page.
IDP Entity ID

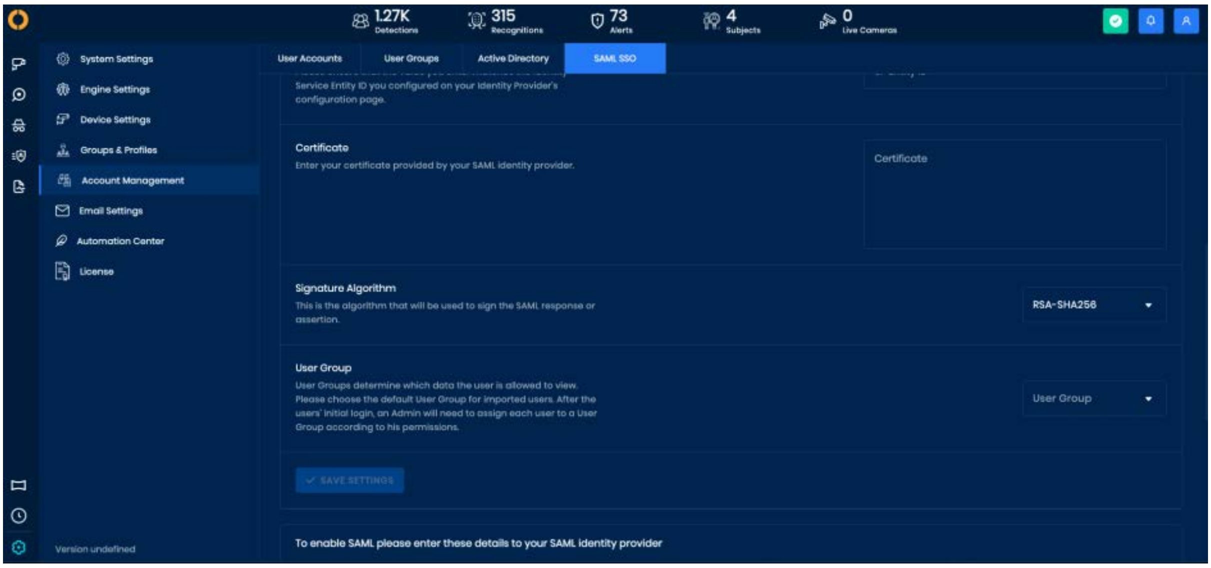
SP entity ID
This is the unique, case-sensitive identifier of this service provider, Please ensure that the value you enter matches the Identity Service Entity ID you configured on your Identity Provider's configuration page.
SP Entity ID

On the *SAML* page, the following configurations must be set:

- **IDP URL** - The user will be forward to this Identity Provider URL when signing in to your organization. This param should be provided by the IDP (Identity Provider).
- **IdP Entity ID** - This is the unique, case-sensitive identifier used by the Identity Provider. Please ensure that the value you enter matches the Identity Provider Entity ID you configured on your Identity Provider's configuration page.
- **SP Entity ID** - This is the unique, case-sensitive identifier of the service provider (you). Please ensure that the value you enter matches the Identity Service Entity ID you configured on your Identity Provider's configuration page. This can be configured by the customer, as long as it matches the SP Entity ID in the IDP, and it can be any value. The standard format, though, is the application's domain.
- **Certificate** - The Public Certificate provided by the IDP.
- **Signature Algorithm** - This is the algorithm that will be used to sign the SAML response or assertion. We recommend using RSA-SHA256.

Our public certificate and metadata can be exported and inputted into the IDP side of the configuration.

Once you finish activating the SAML configuration on the IDP side, within the *OnWatch SAML Settings*, you'll need to activate the SAML SSO login.



Service Entity ID you configured on your Identity Provider's configuration page.

Certificate
Enter your certificate provided by your SAML identity provider.
Certificate

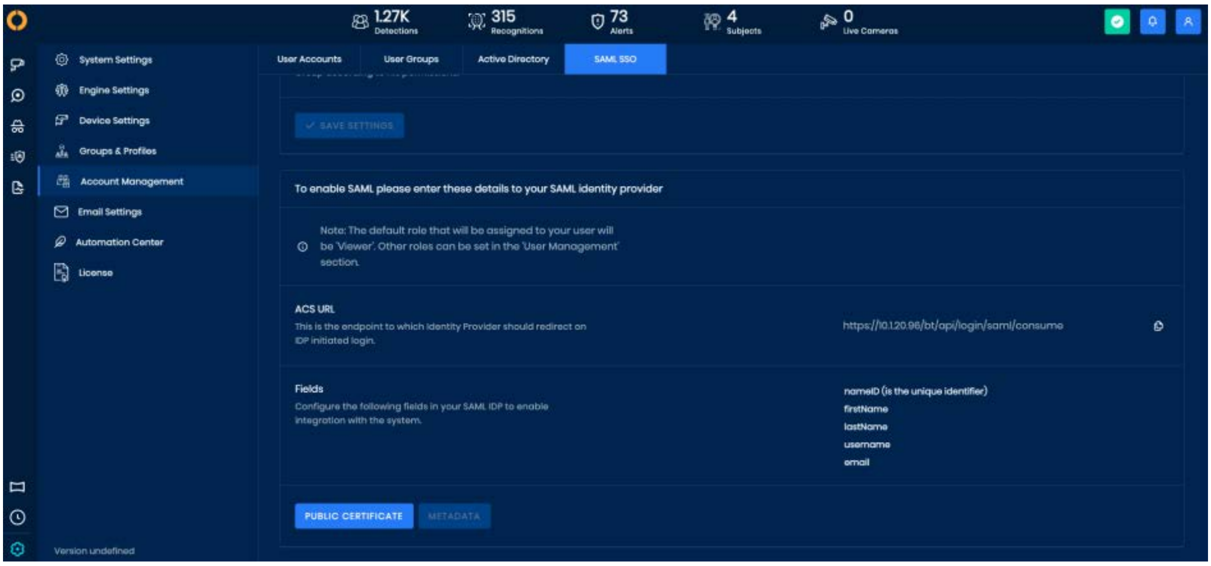
Signature Algorithm
This is the algorithm that will be used to sign the SAML response or assertion.
RSA-SHA256

User Group
User Groups determine which data the user is allowed to view. Please choose the default User Group for imported users. After the users' initial login, an Admin will need to assign each user to a User Group according to his permissions.
User Group

To enable SAML please enter these details to your SAML identity provider

IDP Configuration

On the Identity Provider side, create a new custom application and configure it according to the following



To enable SAML please enter these details to your SAML identity provider

Note: The default role that will be assigned to your user will be 'Viewer'. Other roles can be set in the 'User Management' section.

ACS URL
This is the endpoint to which Identity Provider should redirect on IDP initiated login.
https://10.1.20.96/bt/api/login/saml/consume

Fields
Configure the following fields in your SAML IDP to enable integration with the system.
nameID (is the unique identifier)
firstName
lastName
username
email

1. Upload the metadata we exported in order to auto-complete most of the fields.
   a. Make sure the IDP Entity ID matches the IDP Entity ID we configured on the Abraxas side.
   b. Make sure the SP Entity ID matches the SP Entity ID we configured on Abraxas side.
2. If the ACS URL is not automatically filled by the metadata, input the URL displayed in the image above.
3. Set `nameID` as the SAMLSubjects NameID. (For OnWatch, it should be uid or the user's username.)

In order to support the SAML configuration, it is recommended to map the following fields, as mentioned in the image above:

- nameID
- firstName
- lastName
- username
- email

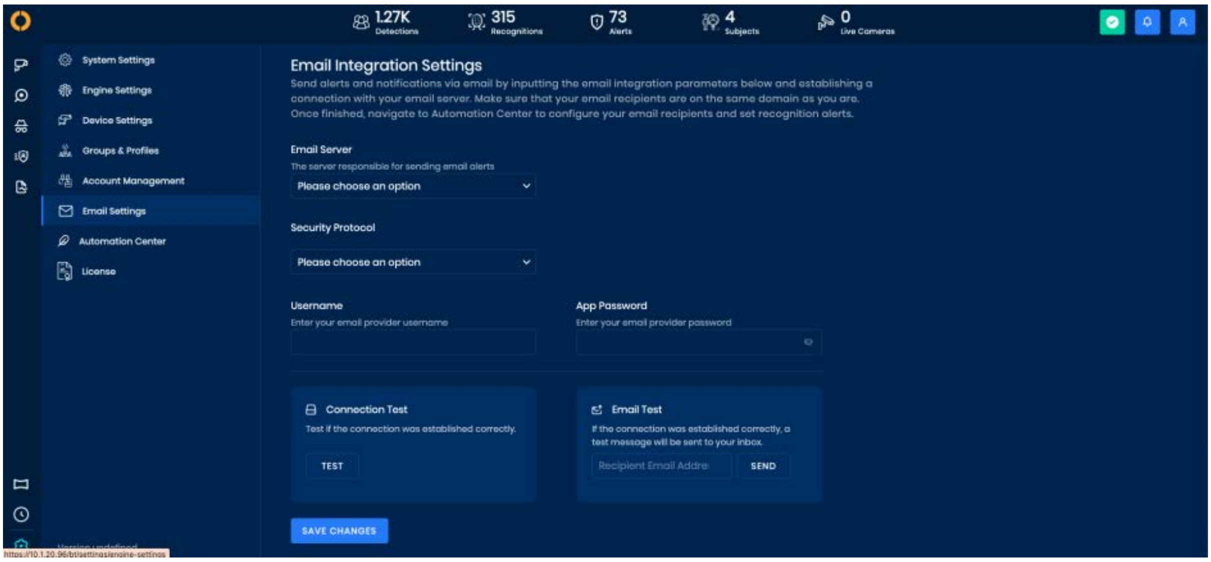
For some Identity providers, user groups need to be activated to use SAML. Users will be matched by their respective usernames in case they already exist and they can log in with SAML. The default role for SAML users will be access viewer.

OnPatrol: User Notifications by Subject Group

User groups and notifications by the subject group are reflected in the OnPatrol system as well as in the OnWatch system. This is a method allowing admins to control user alerts so that users only receive alerts for OnPatrol subject groups that are relevant to them.

Email Settings

Integrate with your email server in order to receive email notifications from the system.



Email Integration Settings

Send alerts and notifications via email by inputting the email integration parameters below and establishing a connection with your email server. Make sure that your email recipients are on the same domain as you are. Once finished, navigate to Automation Center to configure your email recipients and set recognition alerts.

Email Server

The server responsible for sending email alerts

Please choose an option

Security Protocol

Please choose an option

Username

Enter your email provider username

App Password

Enter your email provider password

Connection Test

Test if the connection was established correctly.

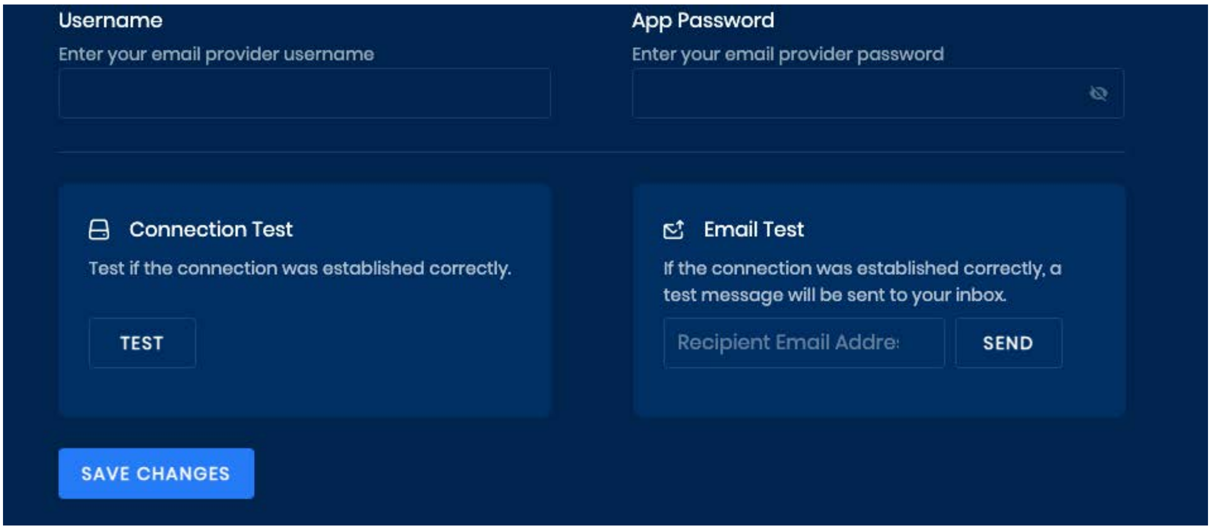
Email Test

If the connection was established correctly, a test message will be sent to your inbox.

Recipient Email Addre

How to Conduct an Email Integration

1. Start the integration processes by indicating what email server your organization uses (OnWatch can currently integrate with **Gmail** or **Exchange** only).
2. Input the type of security protocol your server infrastructure is based on (either **TLS**, **SSL**, or **none**).
3. Provide an email address from which all OnWatch emails will be sent. For example, if you would like the system to send emails from the address "info@yourbusinessname.com", create an email account for this address and input the email credentials (username and password) here.



Username

Enter your email provider username

App Password

Enter your email provider password

Connection Test

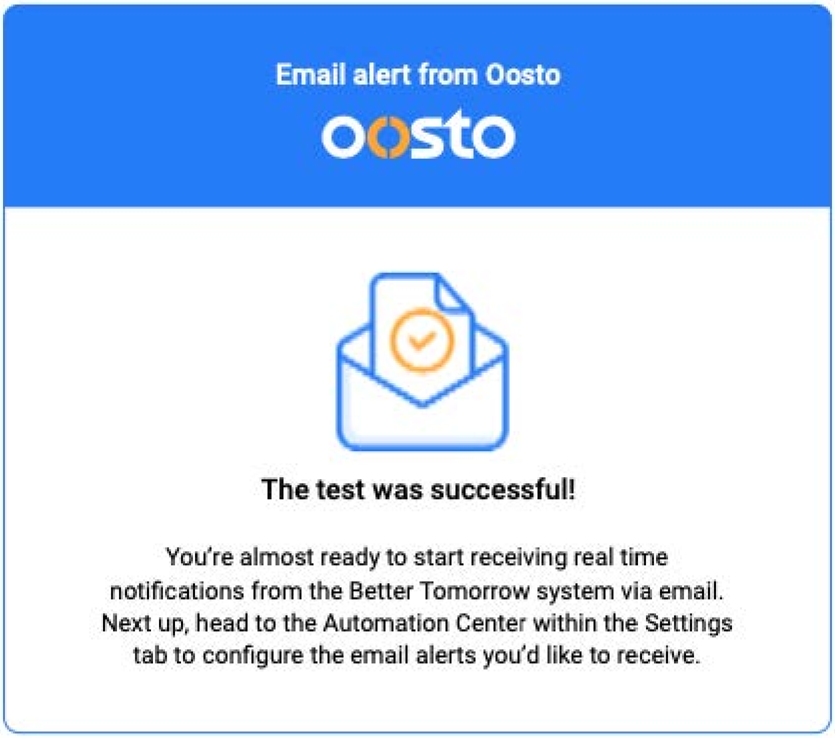
Test if the connection was established correctly.

Email Test

If the connection was established correctly, a test message will be sent to your inbox.

Recipient Email Addre

4. Test the connection between the server and OnWatch by clicking **Test** under *Connection Test*.
5. If the connection is successful, proceed by conducting an email test. Input your email address, press **Send**, then check your inbox to make sure you received the test.



Email alert from Oosto

The test was successful!

You're almost ready to start receiving real time notifications from the Better Tomorrow system via email. Next up, head to the Automation Center within the Settings tab to configure the email alerts you'd like to receive.

Once you've integrated, configure the types of emails you would like to receive within the Automation Center in *Settings*.

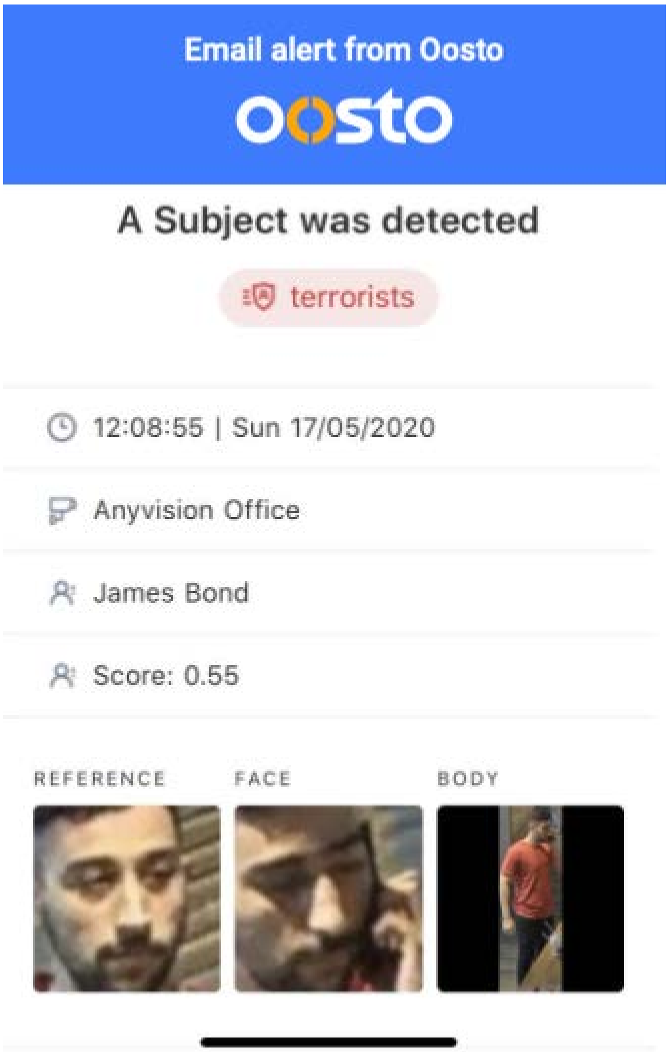
Automation Center

The Automation Center was designed so users can define the email notifications they would like to receive on specific subject groups in the system.

Automation Center Overview

The **Automation Center** within the OnWatch *Settings* allows users to establish automation that the system should follow. Currently, our Automation Center can automatically send out notification emails whenever a subject from a specific subject group or camera group is recognized. You can send these notification emails to any relevant email address (that's in your network) simply by creating an Automation, or a *Rule*, in the system.

This is how the notification email looks like, for reference.



Email alert from Oosto

oosto

A Subject was detected

terrorists

12:08:55 | Sun 17/05/2020

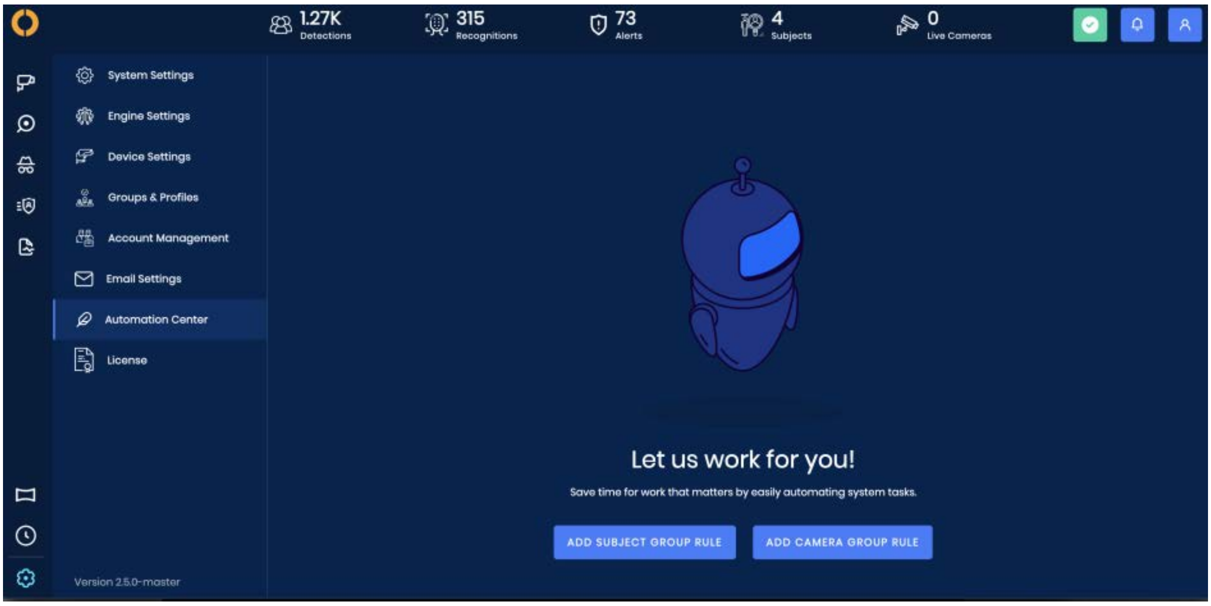
Anyvision Office

James Bond

Score: 0.55

Creating Rules

Click **Start Now** when you're ready to create your first *Rule* in the system in order to automate an email task.



Let us work for you!

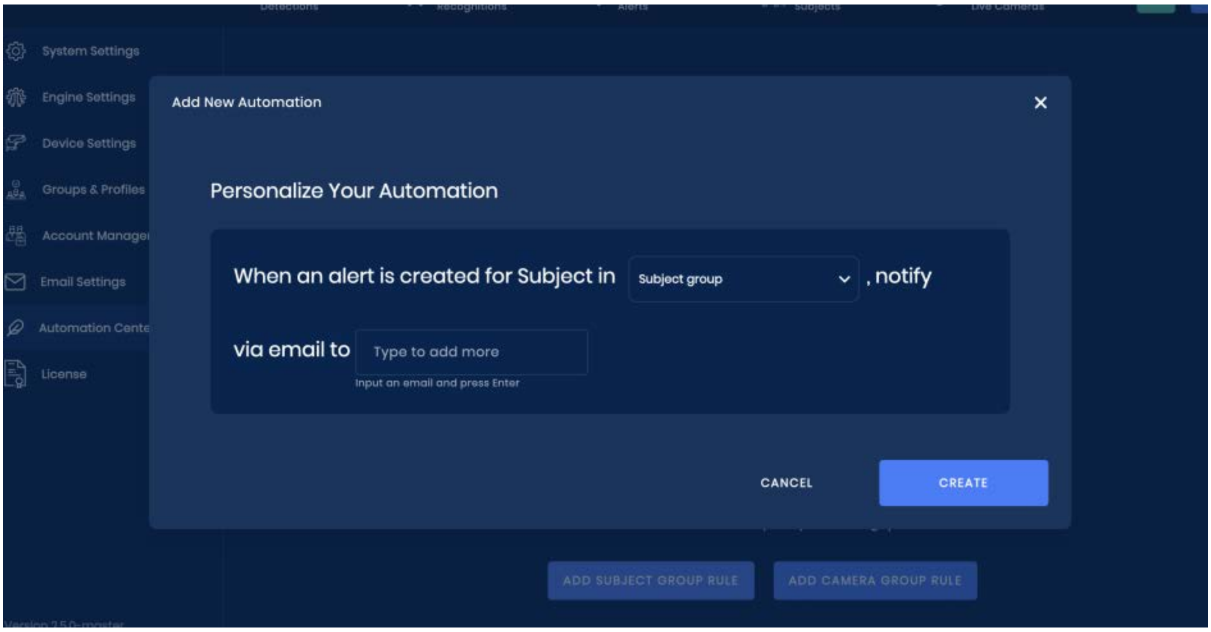
Save time for work that matters by easily automating system tasks.

Fill in the sentence according to your organization's use case. Here's an example of how one might fill it out: "*When a subject from < VIP Members > is being recognized, notify via email to example@oosto.com.*"

What this means is that *example@oosto.com* will receive a notification email whenever any subject enlisted in the VIP Members subject group is recognized by the system.

Subject and Camera Groups

Remember, you can create your own subject/camera groups. Click here to learn more about those groups and how to add cameras and subject to a group.

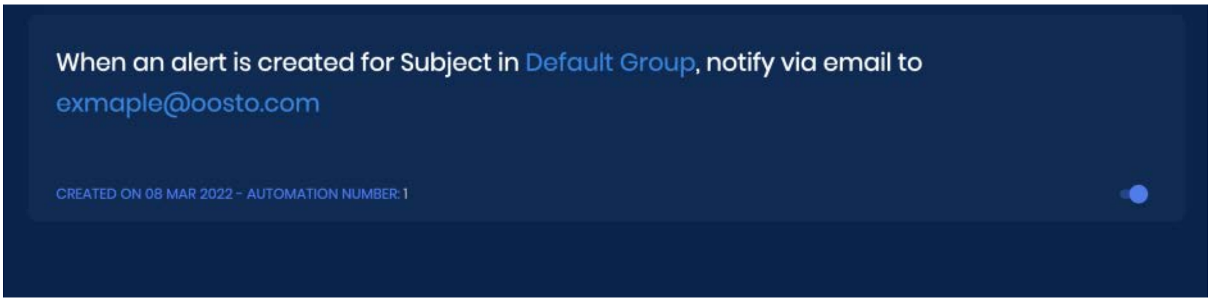

Add New Automation

Personalize Your Automation

When an alert is created for Subject in Subject group , notify via email to Type to add more

Input an email and press Enter

All your rules will appear under *My Automations*. Feel free to add more by clicking **ADD NEW** at the top of the page.


When an alert is created for Subject in Default Group, notify via email to exmaple@oosto.com

CREATED ON 08 MAR 2022 - AUTOMATION NUMBER: 1

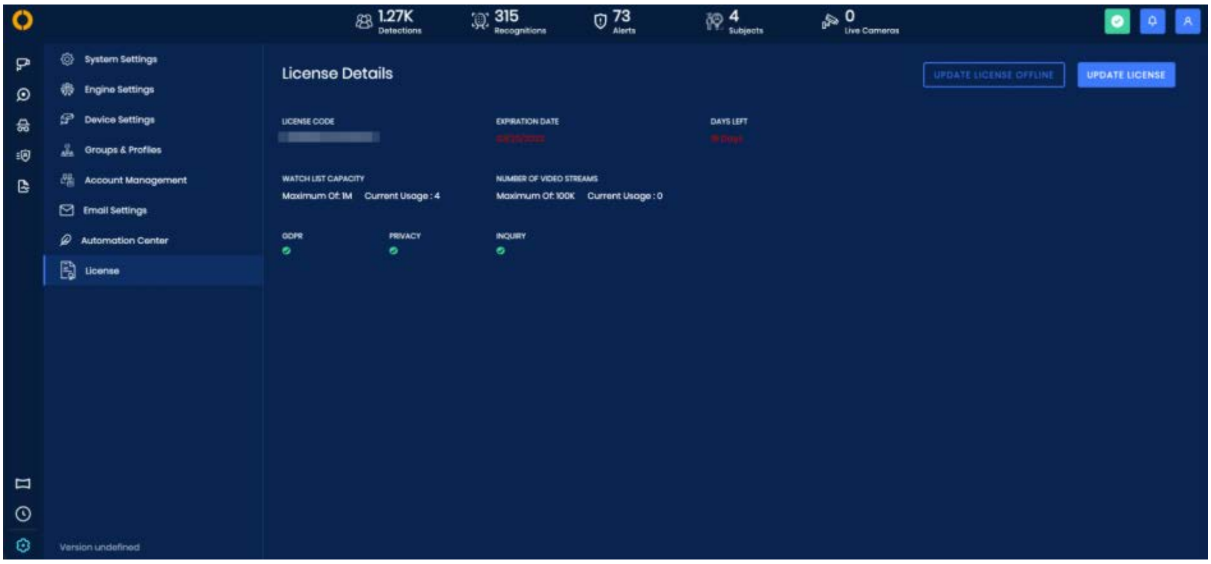
You can see when each rule was created - and a number assigned to the Rule - at the bottom left of the rule's row.

Easily disable or enable a rule using the toggle displayed on the bottom right of the rule's row.

License

Activating Your License Online

1. To activate your license, select the **Settings** tab from the left-side navigation pane.
2. Click on **License**.
3. Insert your 18 digit license code, provided to you by Oosto.



License Details

LICENSE CODE [redacted]

EXPIRATION DATE [redacted]

DAYS LEFT [redacted]

WATCH LIST CAPACITY
Maximum Of: 1M Current Usage : 4

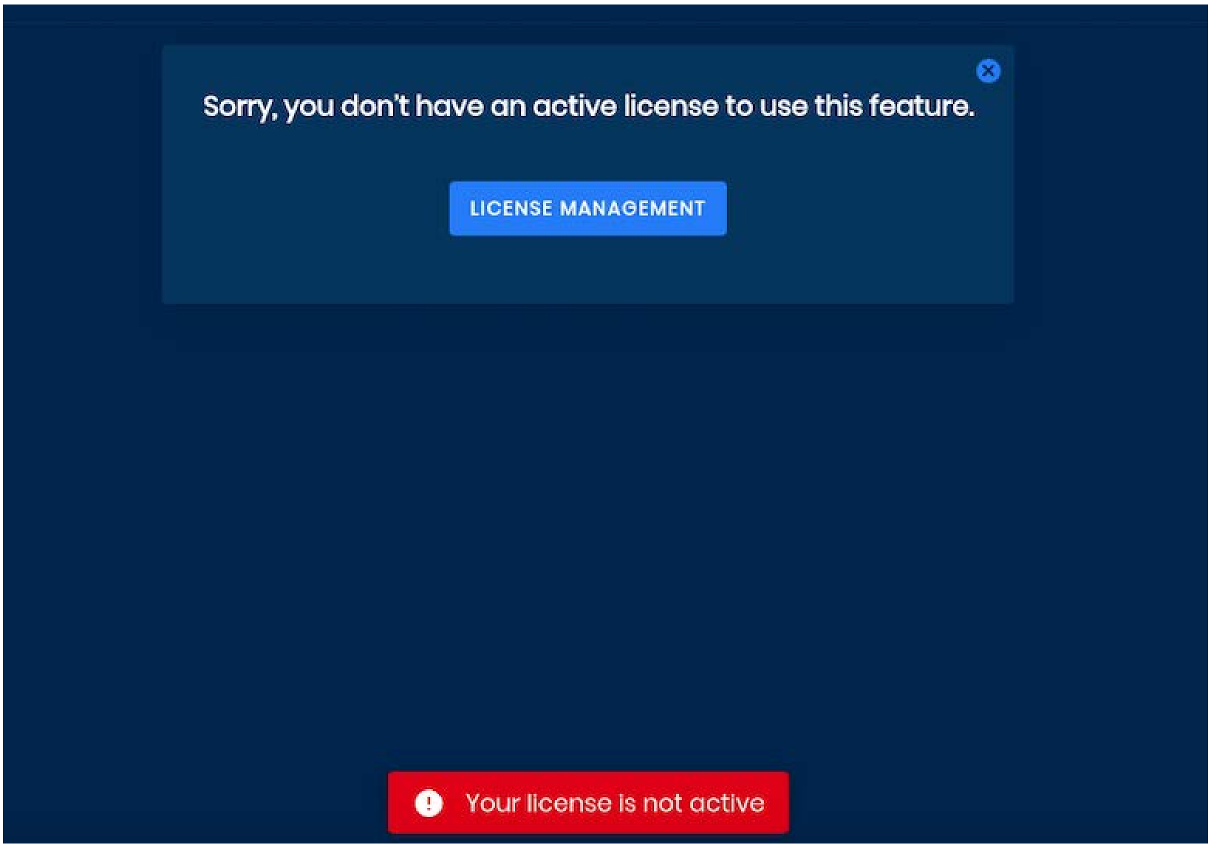
NUMBER OF VIDEO STREAMS
Maximum Of: 100K Current Usage : 0

GDPR ✓ PRIVACY ✓ INQUIRY ✓

Update Your Expired License Online

> 👍 **Use a DMZ Server for More Security**
>
> You can activate your license online with the highest level of security using a DMZ server.

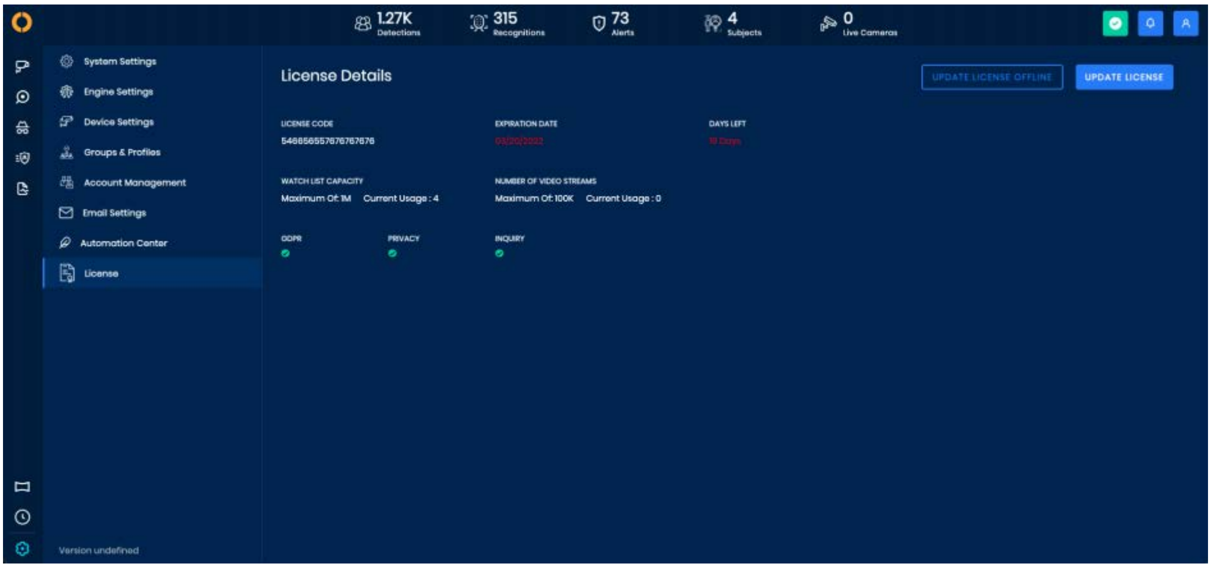
Once your license expires, the system will notify you to update your license. You can update your license by clicking on **License Management** in the pop-up or by navigating to the *License* section of the *Settings* tab.



Sorry, you don't have an active license to use this feature.

Your license is not active

1. Within the *License* page in *Settings*, click on **Update License**.



License Details

LICENSE CODE: 546656557676767676

EXPIRATION DATE: 03/20/2022

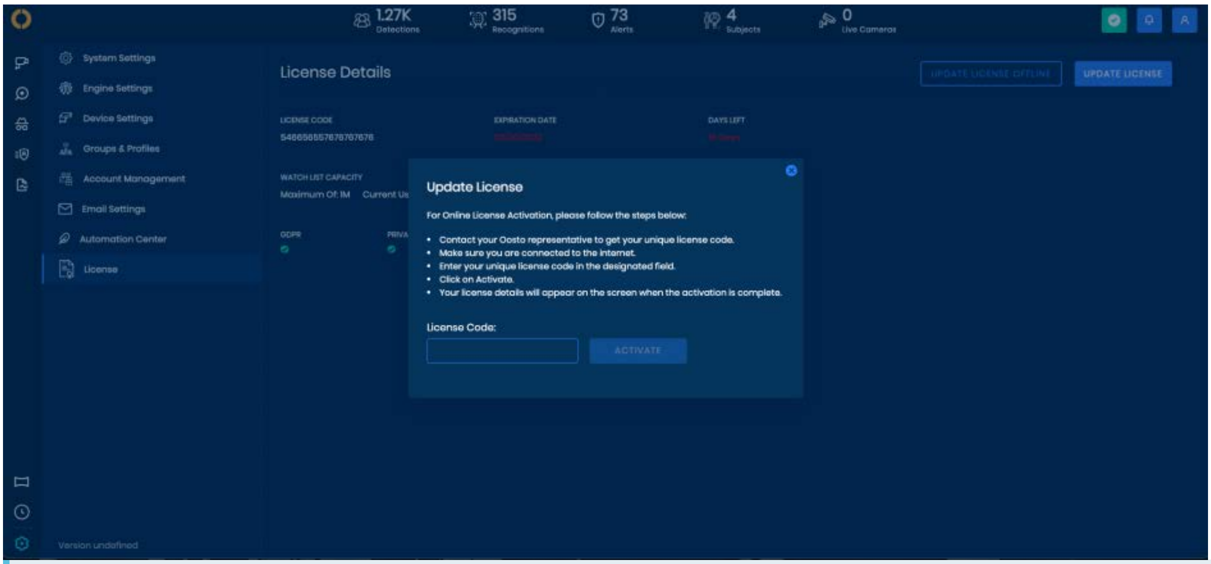
DAYS LEFT: 10 Days

WATCH LIST CAPACITY: Maximum Of: 1M Current Usage : 4

NUMBER OF VIDEO STREAMS: Maximum Of: 100K Current Usage : 0

GDPR ✓ PRIVACY ✓ INQUIRY ✓

2. Input your new license code in the pop-up that appears.



Update License

For Online License Activation, please follow the steps below:

- Contact your Oosto representative to get your unique license code.
- Make sure you are connected to the internet.
- Enter your unique license code in the designated field.
- Click on Activate.
- Your license details will appear on the screen when the activation is complete.

License Code:

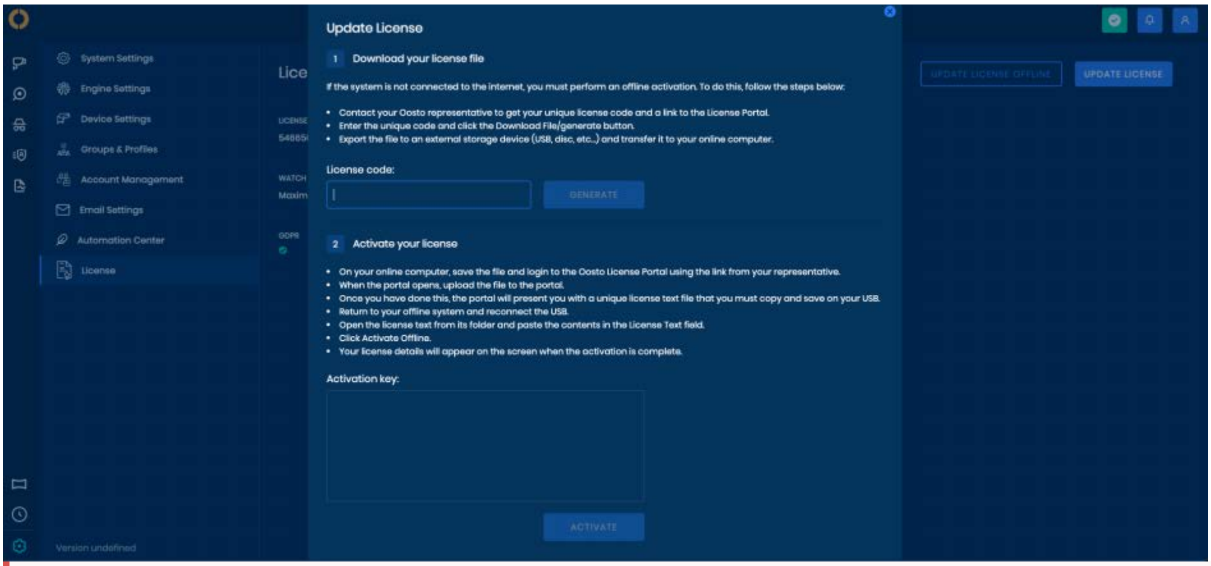
Need a New License Code?

Contact your Oosto representative or contact Support at support@oosto.com

Activate or Update Your License Offline

You can activate or update your OnWatch license within the *License* section of the *Settings* tab. Simply click on **Activate License** or **Update License** and follow the instructions presented.

At the beginning of the offline activation process, you will be prompted to download a file from your offline machine and save it on an external drive. This file is then used to validate and activate your license as if you were online.



Update License

1 Download your license file

If the system is not connected to the internet, you must perform an offline activation. To do this, follow the steps below:

- Contact your Oosto representative to get your unique license code and a link to the License Portal.
- Enter the unique code and click the Download File/generate button.
- Export the file to an external storage device (USB, disc, etc..) and transfer it to your online computer.

License code:

GENERATE

2 Activate your license

- On your online computer, save the file and login to the Oosto License Portal using the link from your representative.
- When the portal opens, upload the file to the portal.
- Once you have done this, the portal will present you with a unique license text file that you must copy and save on your USB.
- Return to your offline system and reconnect the USB.
- Open the license text from its folder and paste the contents in the License Text field.
- Click Activate Offline.
- Your license details will appear on the screen when the activation is complete.

Activation key:

ACTIVATE

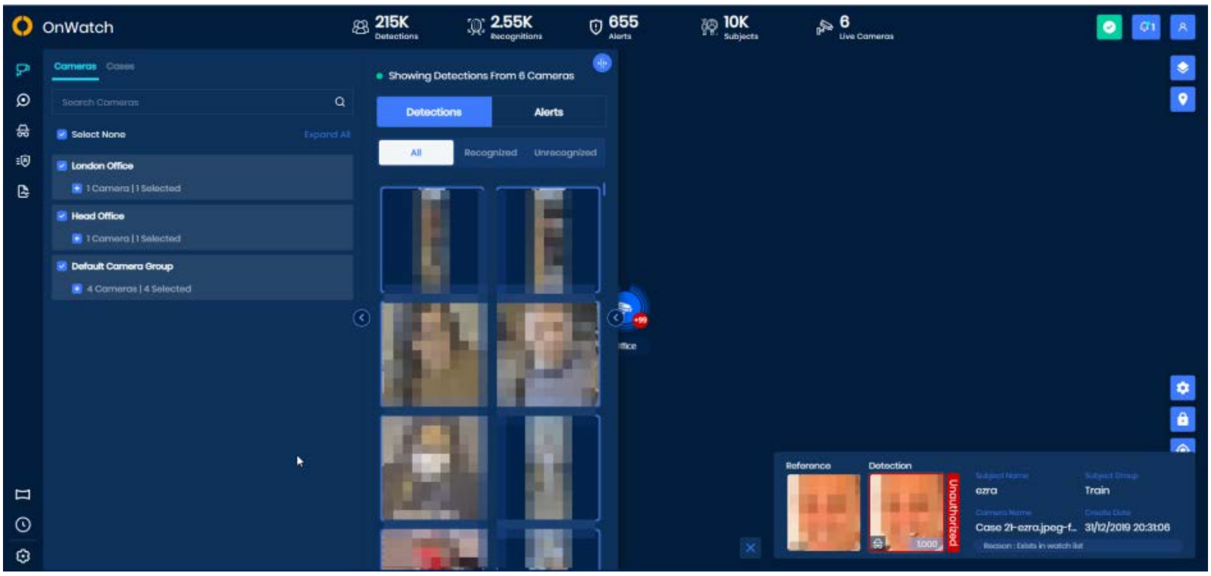
! All Cameras Are Disabled When Your License Expires

Once your license expires, the system will no longer search for detections and recognitions from your cameras and the live stream will cease.

Alerts

Alerts are designed to let you know when the OnWatch system has met a rule configured in the system, such as authorized and unauthorized, known or unknown people.

By editing predefined groups in the Watch List, you can configure the notifications type (sounds and pop-ups can be set) depending on the urgency of the group. Configurations can be set in *Settings* under *Groups & Profiles*.



Subject Name: ezra

Subject Group: Train

Camera Name: Case 21-ezra.jpeg-f...

Create Date: 31/12/2019 20:31:06

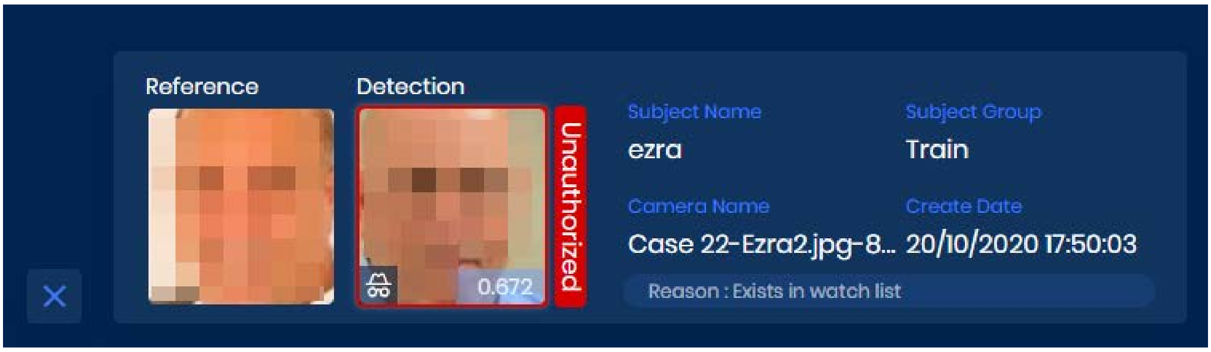
Reason : Exists in watch list

By default, the notification will include the subject's reference image and detection image. The number on the detection image indicates the score, which is the numerical strength of the match on a scale of 0 to 1.

The color and authorization status next to the detection image will reflect your settings for that subject group.

If multiple frames were captured for one detection, this will be accounted for as a small number on the bottom of the reference image (see below, the number in purple reflects this).

A reason will be given for the Alert allowing different types of Alerts to be shown depending on the system rules. Additionally, an icon will be shown for Inquiry when the alert was generated via n inquiry processed case



Subject Name
ezra

Subject Group
Train

Camera Name
Case 22-Ezra2.jpg-8...

Create Date
20/10/2020 17:50:03

Reason : Exists in watch list

The alert itself will include the *Subject Name*, the *Subject Group*, the *Camera Name/Case Name* of whichever camera/case provided the detection with the *Reason* for the alert *Create Date* with time and date when the subject was detected.

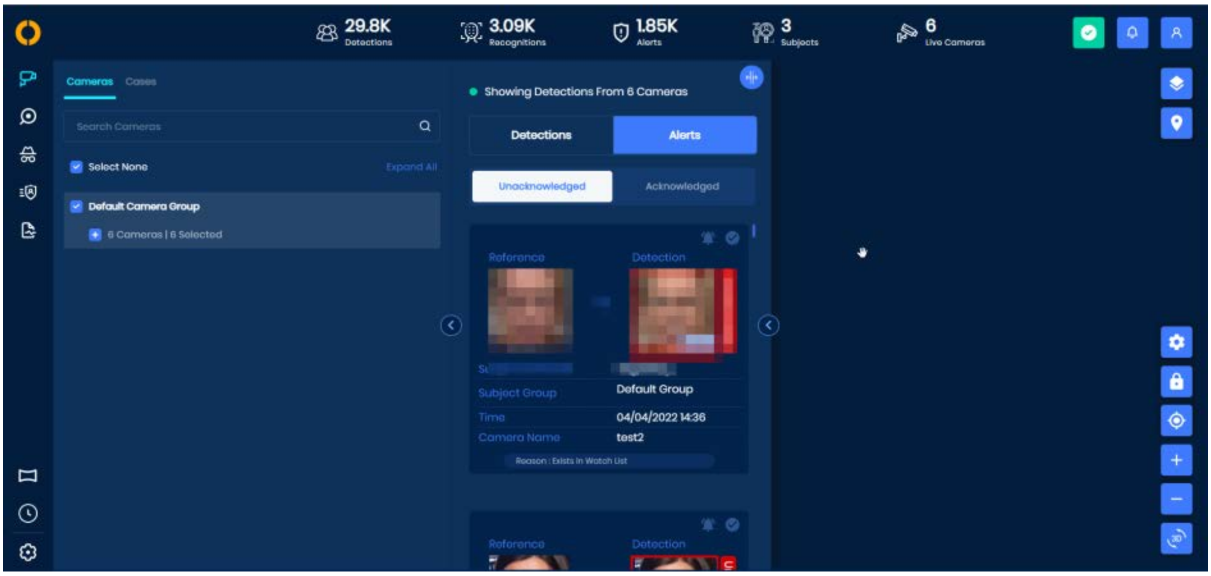
For more information on how to configure your notifications and alerts in Settings, navigate to the *Groups & Profiles* page in *Settings by Super Admin*.

How To

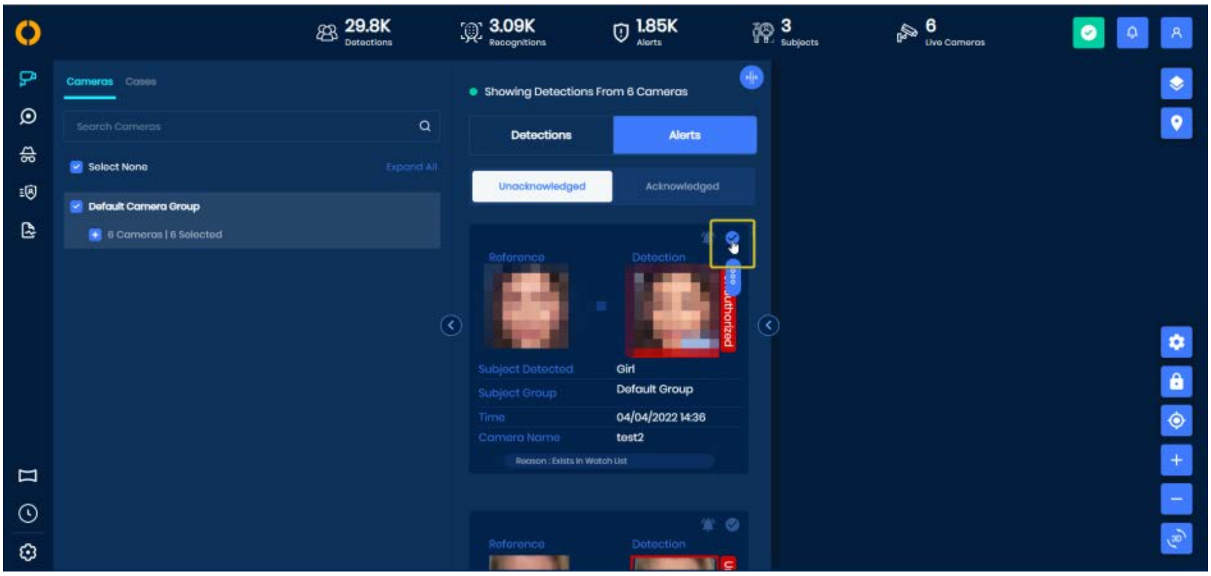
How To Summary

Acknowledge an Alert

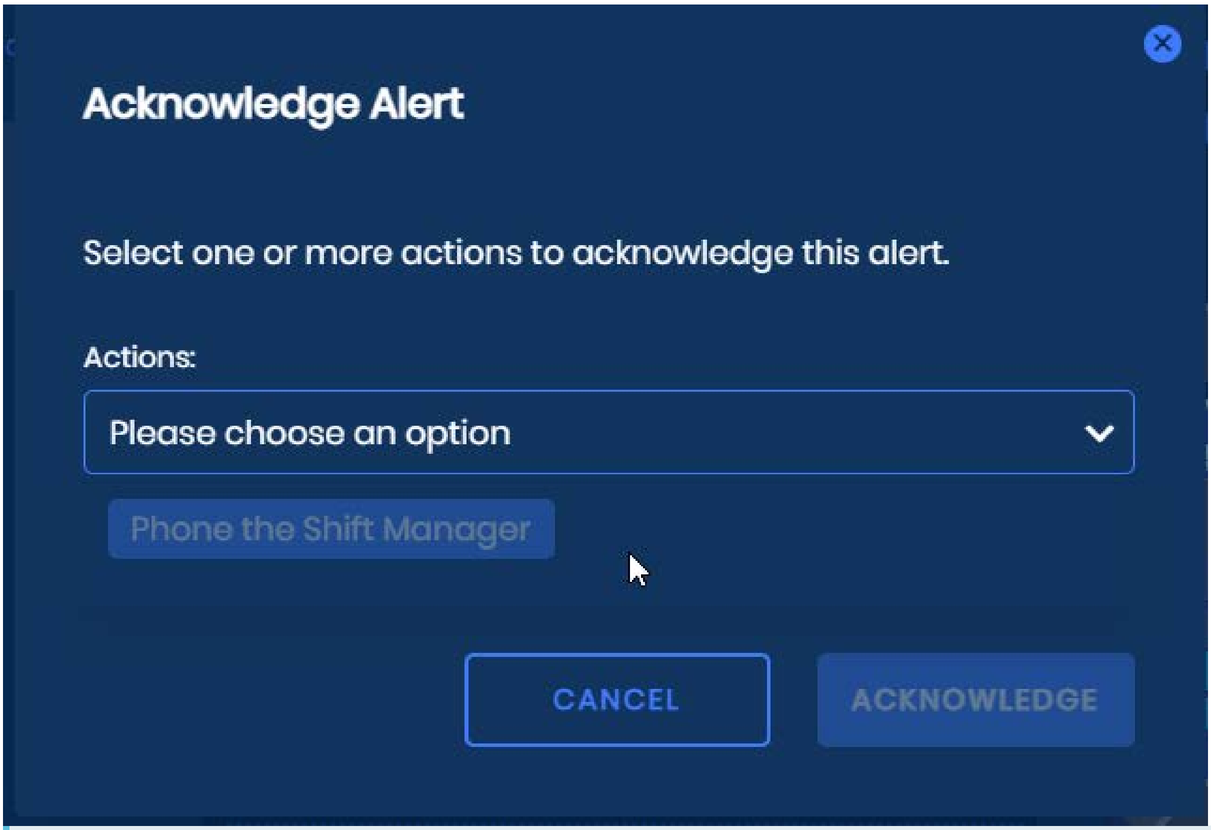
1. Click on the **Alerts** button to view all the acknowledged and unacknowledged alerts. By default, once the Alert button is pressed, all the unacknowledged alerts are displayed.



2. Click on the **checkmark** that appears in the circle icon next to the alert you would like to acknowledge.



3. Select the **Action** you would like to classify this alert under. You can choose multiple actions if desired



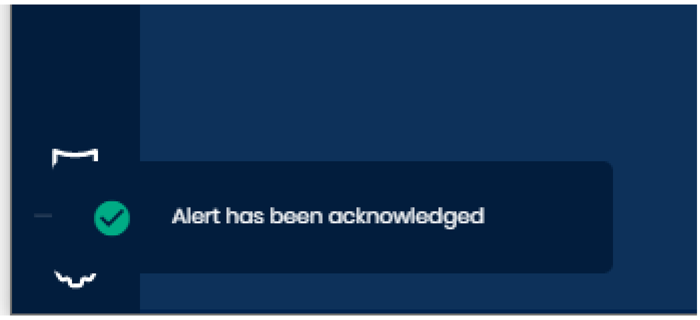
Acknowledge Alert

Select one or more actions to acknowledge this alert.

Actions:

> Actions are predefined and are set in the Settings tab.

6. If necessary, check the box labelled "Apply for all alerts of this subject".
7. Select **Acknowledge**.
8. On the bottom left-hand corner of the dashboard will be a notification that the selected alerts have been acknowledged and moved to the acknowledged tab.



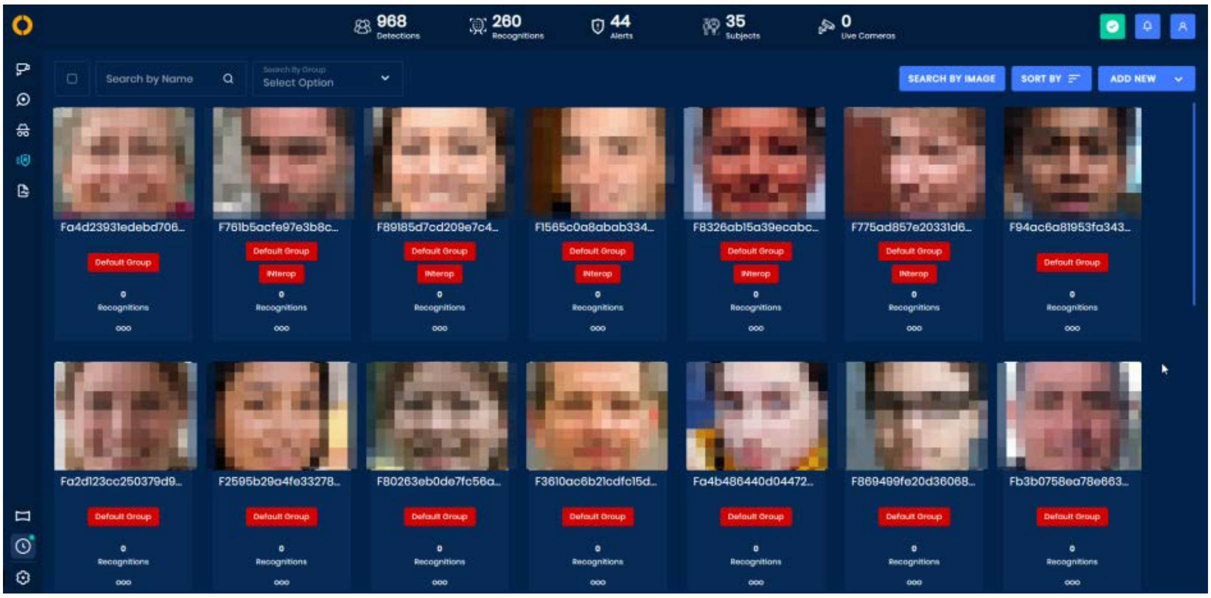
Alert has been acknowledged

Add, Edit, Delete, Move Subjects

How to Add Subjects to the Watch List

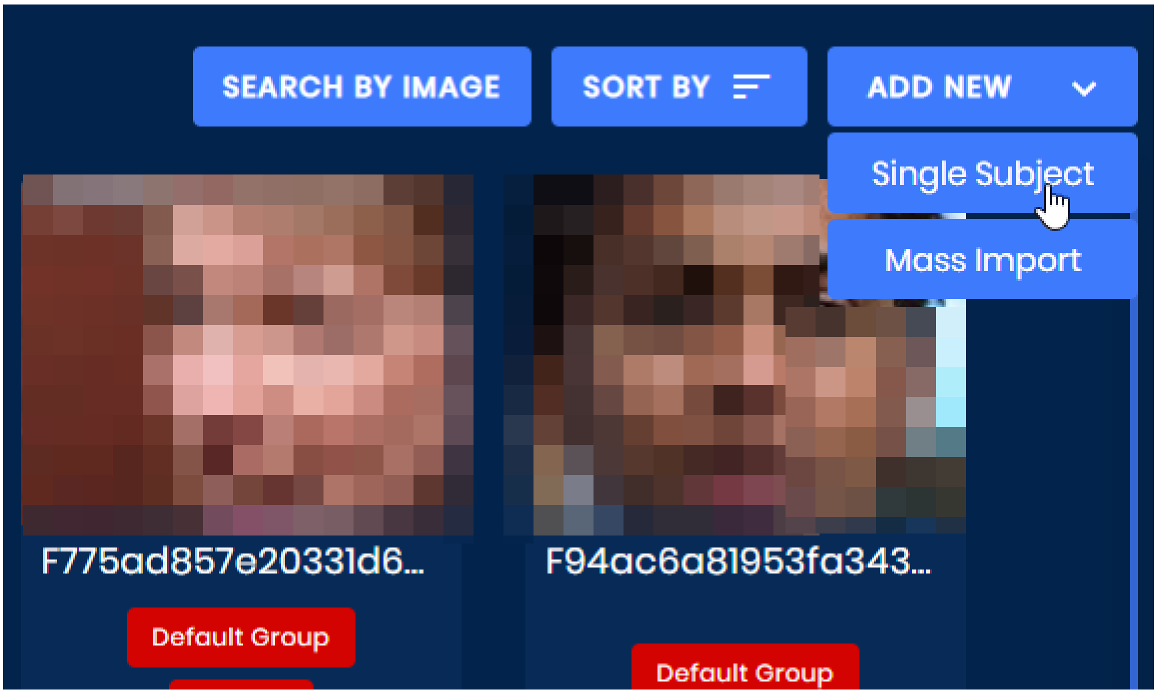
Within OnWatch, you can add a single subject to the watch list or add multiple subjects at a time through mass import.

A subject can be added to the watch list from the Watch List tab or the View Sources tab if the person was previously captured on one of your cameras and was detected by the system.



Add a Single Subject to the Watch List from the Watch List Tab

1. Click **Add New** and select **Single Subject** from the displayed dropdown.



2. Upload a photo of the subject. This photo will be used as a reference image for the system and can be an image of the subject's face, body, or both.

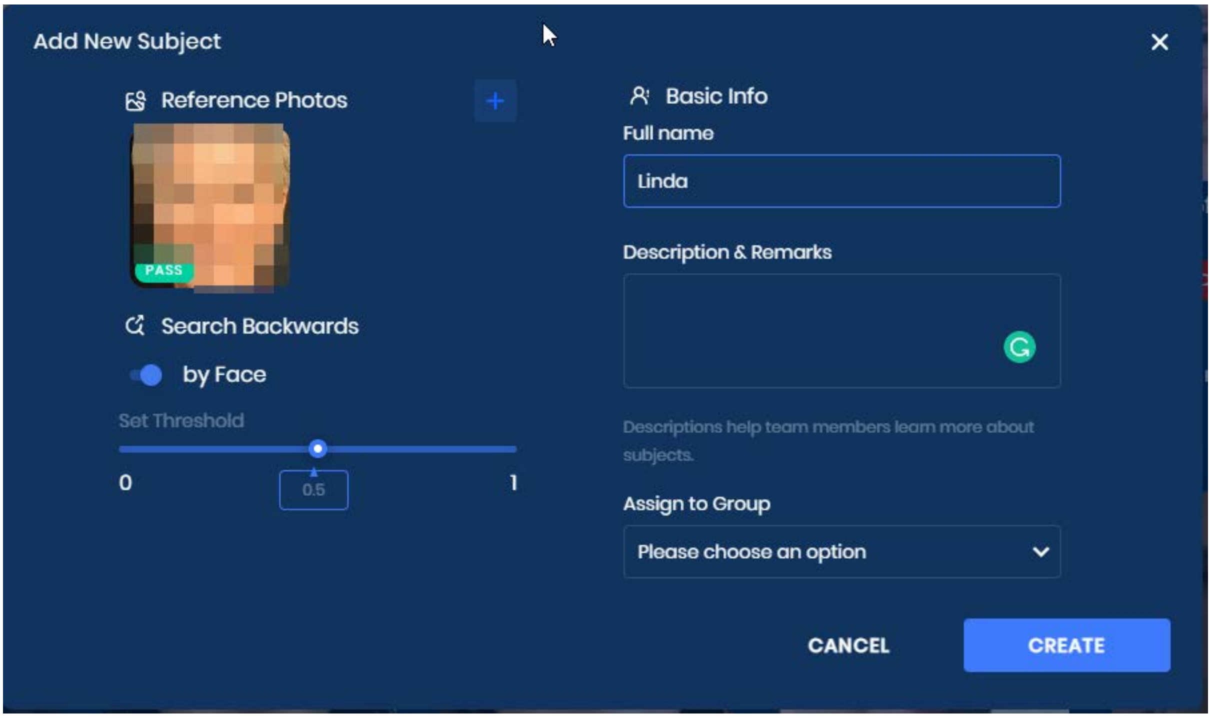
Only images that include a person's body can be saved as a body reference image. (The system will recognize everything from the neck down as body.) If the image of the subject includes their face and body, you will have the opportunity to save the image as both a reference for the face and for the body. However, if the image you are uploading is just of a face, it will not recognize a body too.

🚧 Face and Body Reference Images from a Photo with Multiple People

If the uploaded photo of the subject includes other people, you will need to select which person in the image should be added to the watch list.

The other people in the image will not be saved or added to the watch list. You will need to repeat the process to add another person from the same image.

3. Once the image is uploaded, you will immediately see if the photo is suitable to be a reference image. If a *Pass* icon is shown, the photo can be used. If the photo has a *Poor* icon, please upload a new image for the subject.



by Face

Set Threshold 0 0.5 1

Full name Linda

4. Add details about the subject, including their name, subject description, subject group, and threshold for recognition.
5. Click **Create**.

🚧 Subject Already Exists in the Watch List

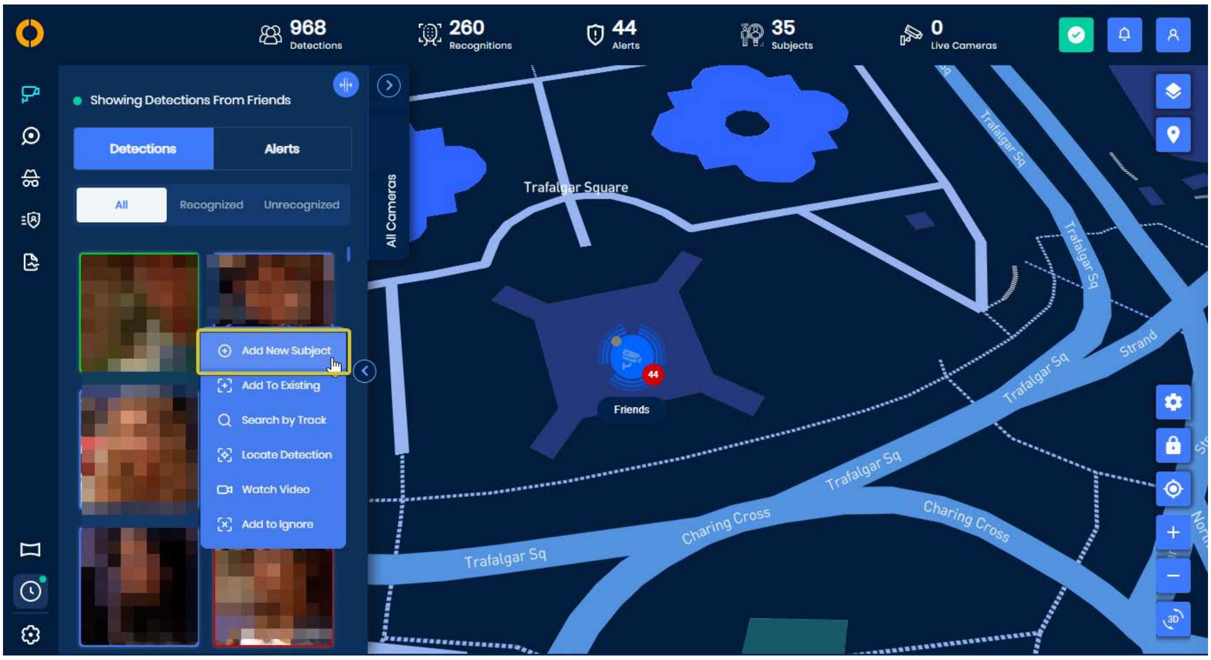
If the system detects that the new image you have uploaded matches someone else that is already in the system, it will allow you to assign it to that subject.

You can choose to add that person as a new subject as well, if you'd like.

Add a Subject to the Watch List from the View Sources Tab

A detection made by the system can be used as a reference image for a subject added to the Watch List from the View Sources tab. To do so:

1. Right-click on the detection image of the subject you would like to add to the Watch List and select **Add New Subject**.

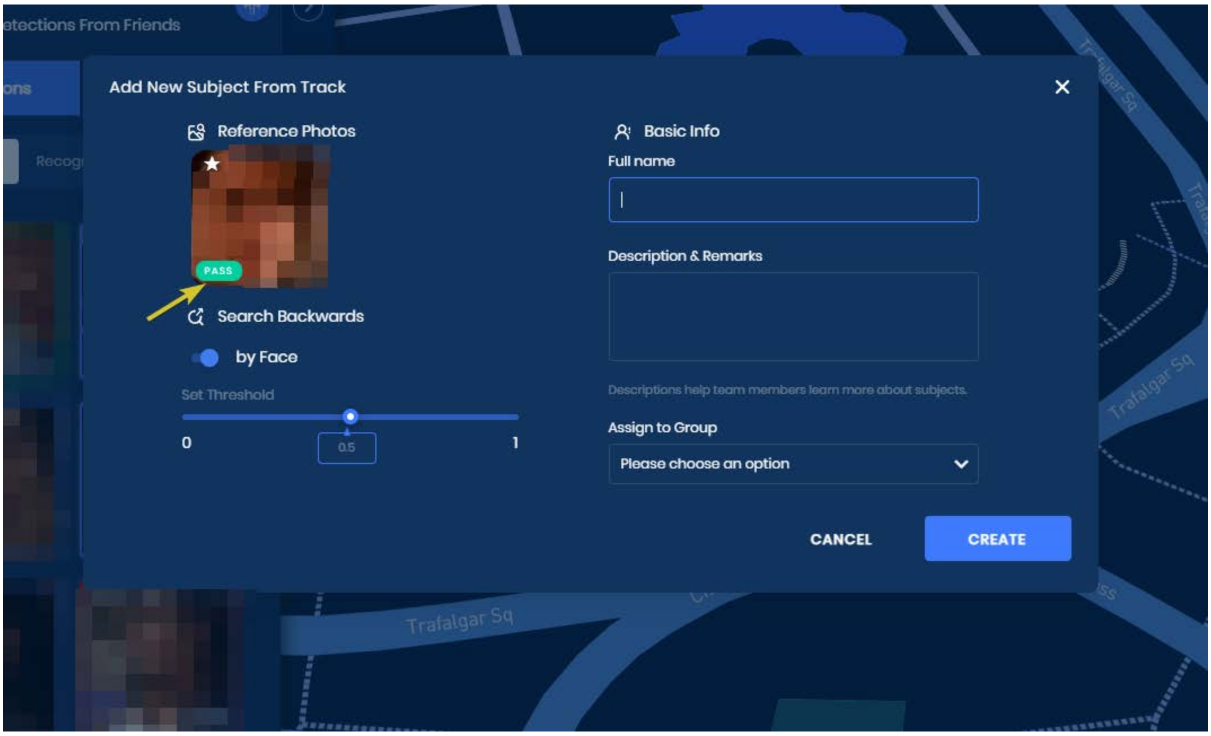


2. A popup will appear you can add details about the subject, including their name, subject description, subject group, and threshold for recognition.

🚧 Be Mindful of the Image Quality

When adding a photo from the View Sources tab as a subject's reference image, you will notice the system provides you with an indication on whether this is a good or poor image to use. If the image is good quality, it will be marked as pass.

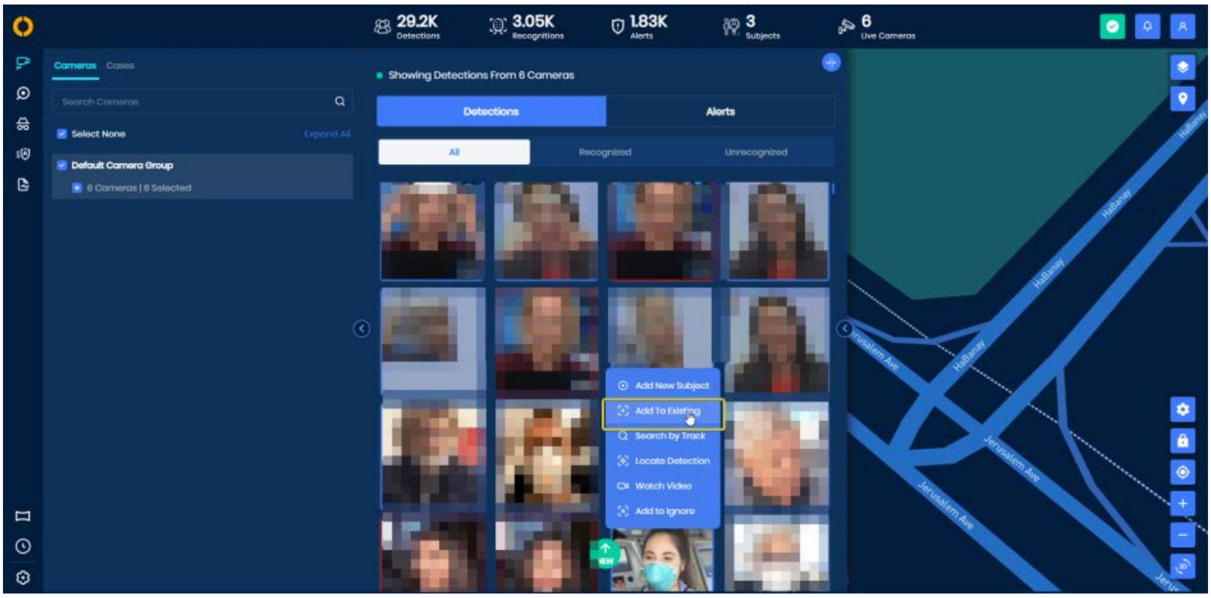
Please note that if the image is marked as poor, we suggest using a different reference image.



3. Use the toggle next to **by Face** to indicate that the system should use this reference when searching backwards.
4. Click **Create**.

Add to Existing

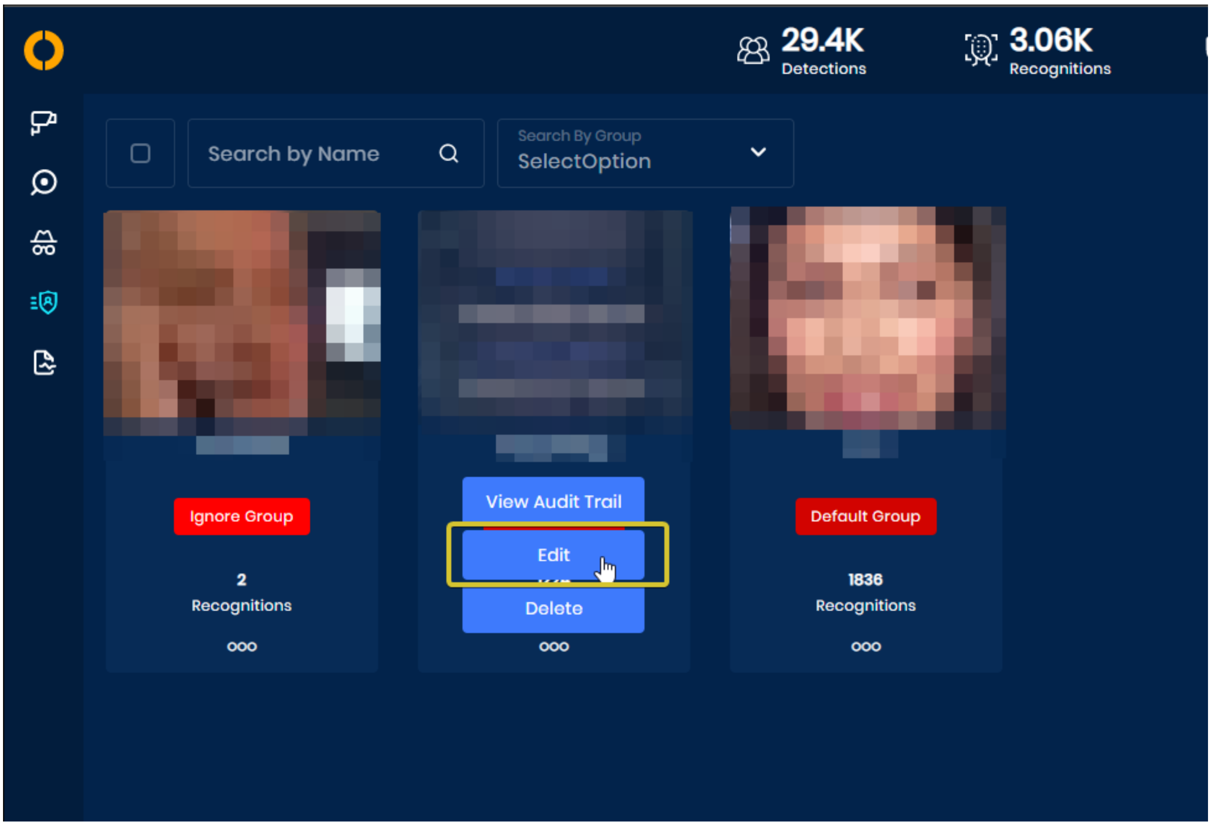
You can also use this process to add a reference image from the View Sources tab to an existing subject by selecting **Add to Existing** from the dropdown available.



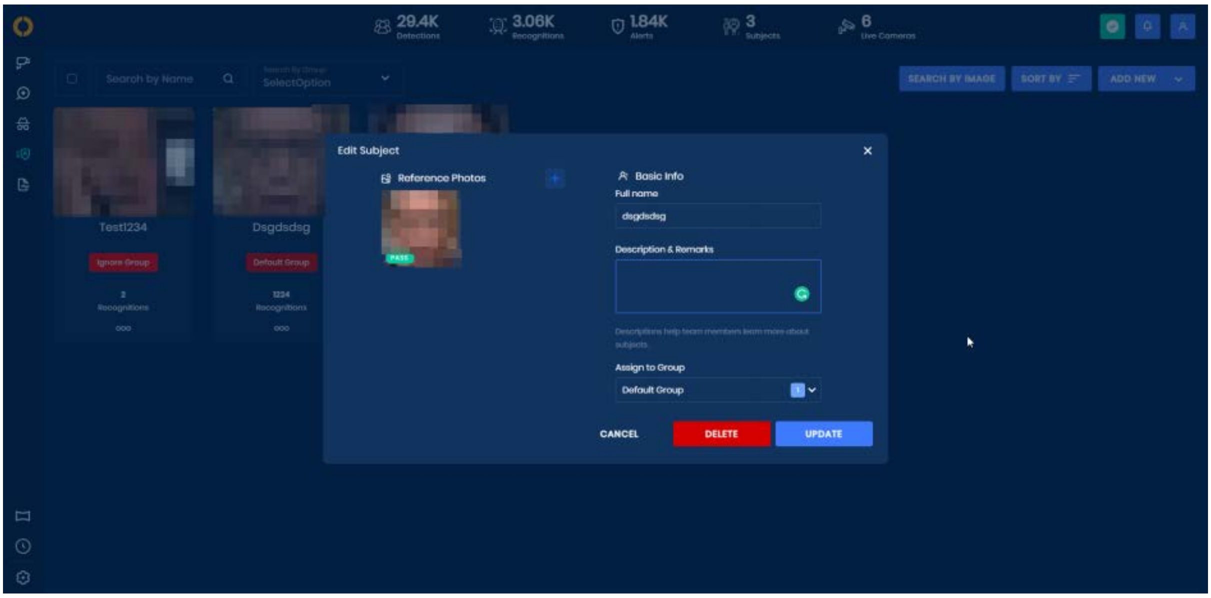
How to Edit a Subject's Profile

You can update and change the profile details of subjects in the watch list or recognitions from any location. You can also use this option to add more images of a subject manually.

1. From the Watch List tab, click on the menu button (3-dotted icon) on the subject's image.
2. Choose **Edit** from the dropdown.



3. Here you can add or remove images and change the subject's name, description, or group.



Edit Subject

Basic Info

Full name: dsgdsdsg

Description & Remarks

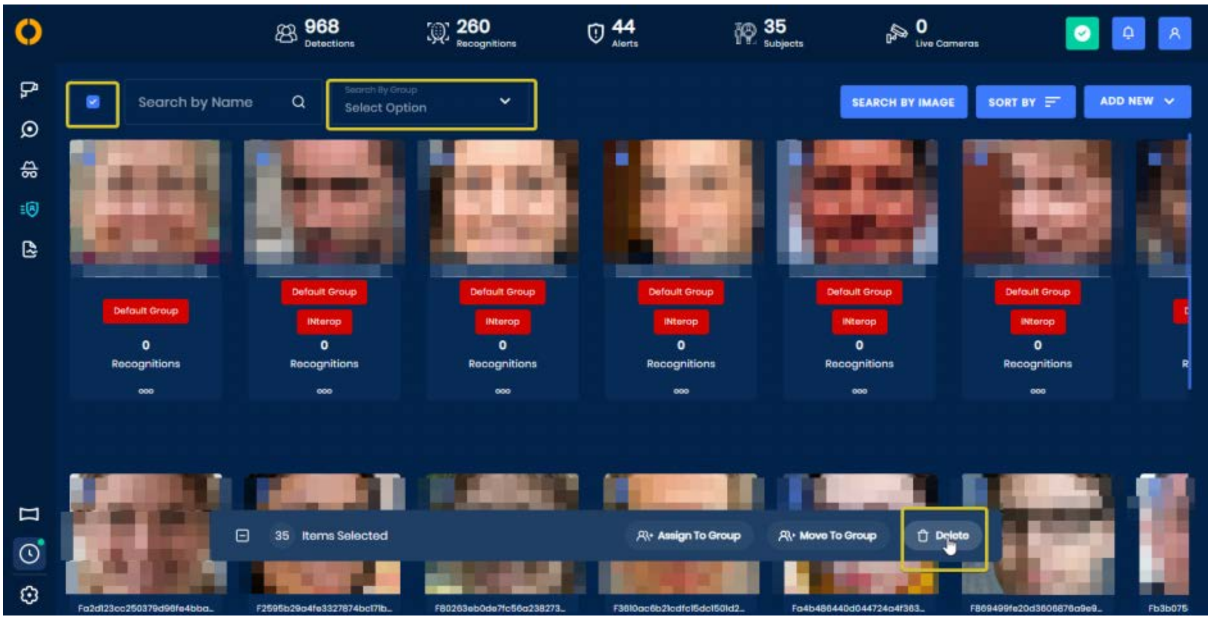
Descriptions help team members learn more about subjects

Assign to Group: Default Group

4. Click **Save**.

How to Delete a Subject from the Watch List

1. Select the Watch List tab from the main dashboard.
2. Select the subjects you would like to delete by adding a checkmark on the top, left corner of the subject's reference image. You may select more than one subject at a time or select bulk subjects with the select all check box in the top left corner.



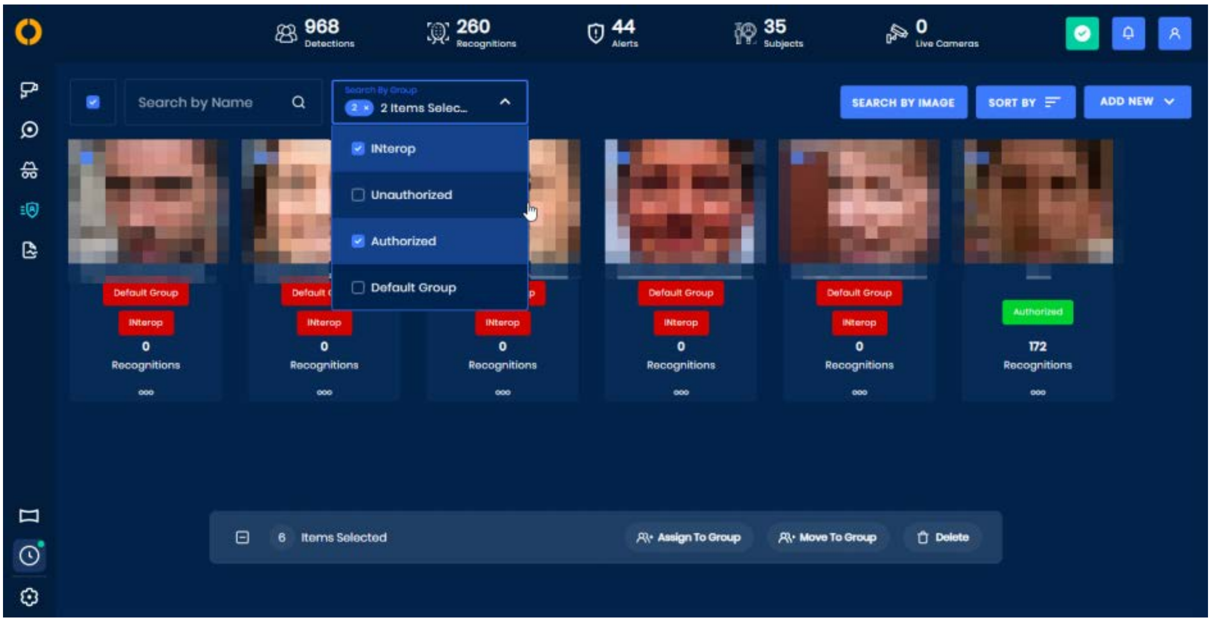
3. Press **Delete** on the pop up multi-action tool bar.

4. You will be prompted to confirm that you are interested in deleting a subject(s). Press **Delete**.

You can also delete a single subject by pressing the 3-dotted icon on the subject's image and select **Delete** from the dropdown.

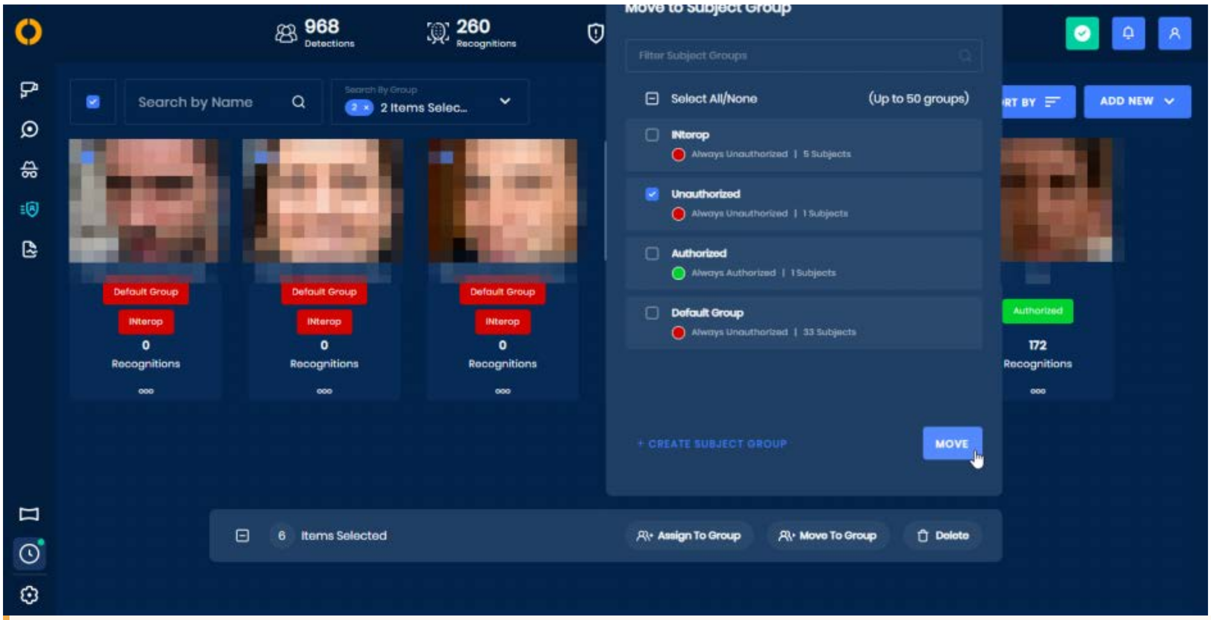
How to Move / Add a subject to Multiple Subject Lists

1. Goto the "Watchlist" tab
2. Select one or more subjects, you can also filter by one or more groups when doing this selection



3. A Bulk job toolbar will appear that can be used to

- Delete in bulk - Deleted all the subjects
- Assign in bulk - Adds the selected subjects to additional subject groups
- Move-in bulk - Moves all the subjects from their existing group/s to the newly selected ones



🚧 Note

A maximum of 50 groups can be used with bulk jobs

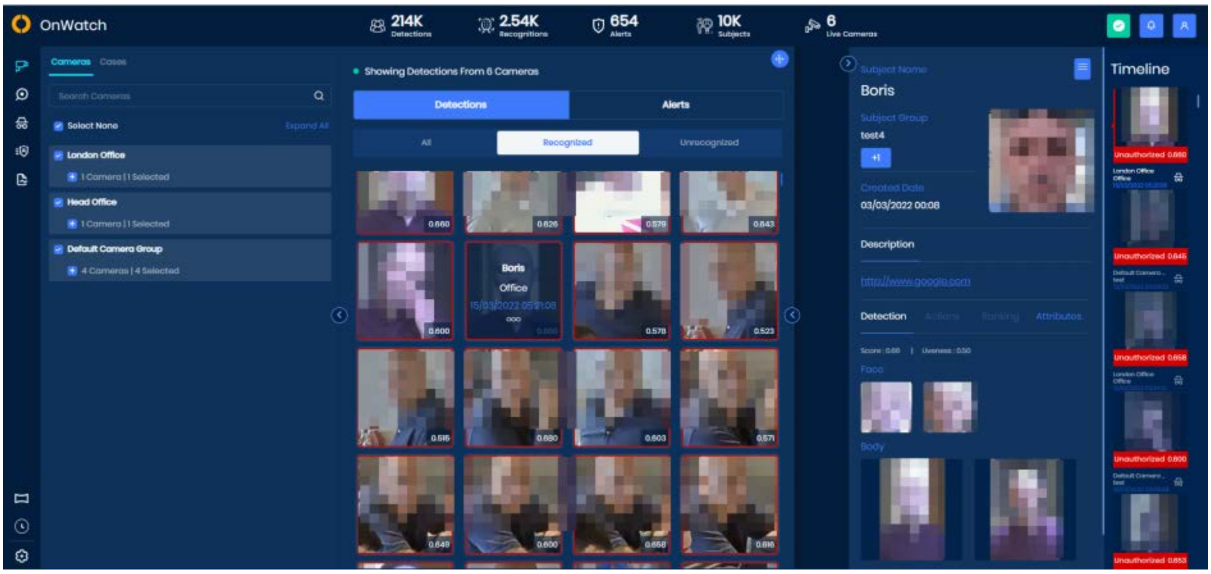
When selecting the assign or move action it is also possible to create a subject group on the fly

View a Subject's Detection Timeline

See a subject's detection history in their **Timeline**

How To View the Detection Timeline From Live Cameras

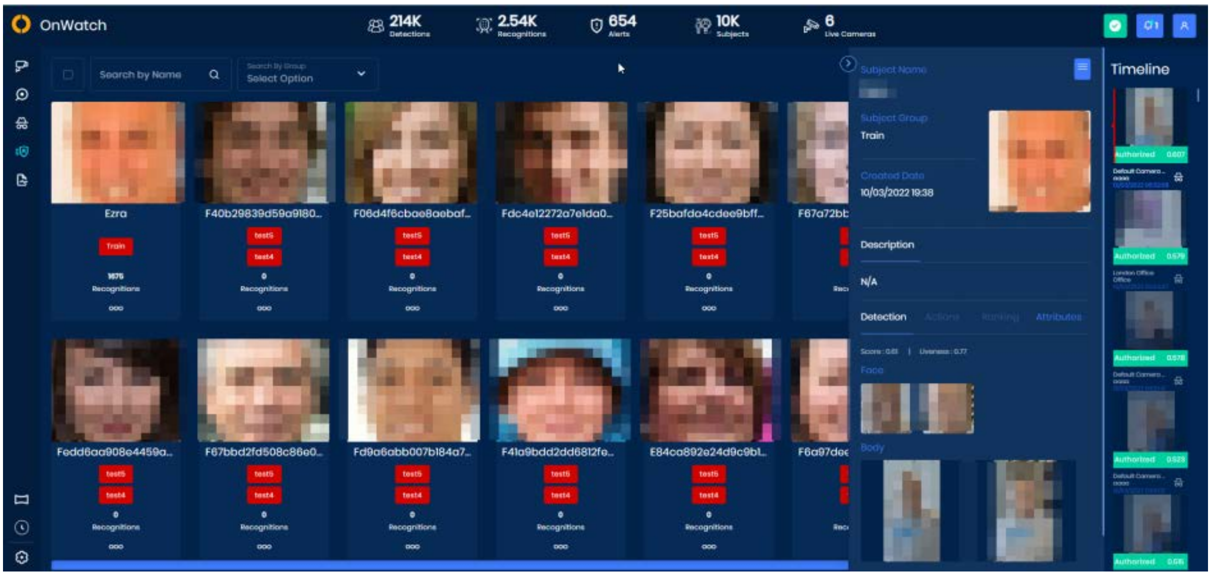
1. Click on an image of a detected subject within the View Sources tab.
2. View the timeline on the far right of the screen.



You can scroll down the timeline to view all detections of that subject. If a person detected is not saved on the watch list, you will only see a list of images from the current detection within its camera group and if we have less than 90-second gaps between detections tracks.

How To View the Detection Timeline From the Watch List

1. Click anywhere on a subject's image from the Watch List tab.
2. View the timeline on the far right of the screen.



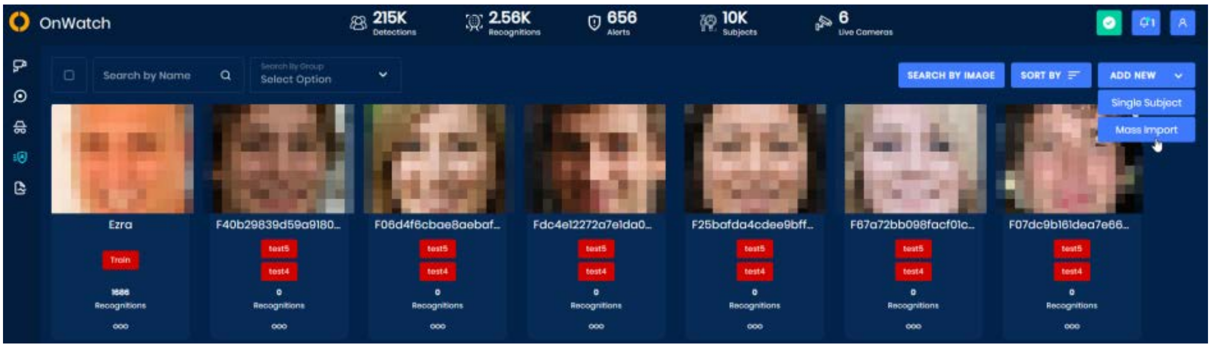
You can scroll down the timeline to view all detections. If a subject on a watch list has no recognitions yet, no timeline will appear. Instead, you will see a message **The subject has no recognitions** at the bottom left of the screen.

The subject has no recognitions

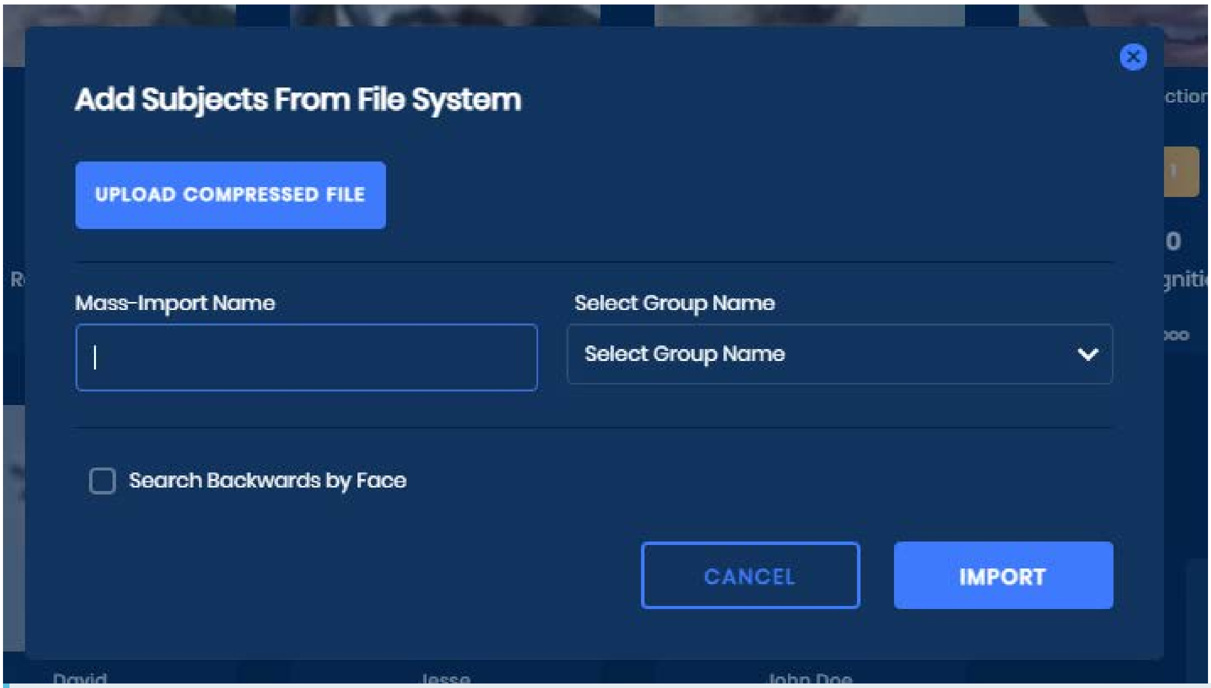
Add Subjects via Mass Import

Add Multiple Subjects to the Watch List Through Mass Import

1. From the *Watch List* tab, click **Add New**.



2. Select **Mass Import** from the displayed drop-down.
3. Click on **Upload Compressed File** and select the desired file.



📘 Subject Images Must be Inputted as a Compressed File

OnWatch only accepts compressed files as input for mass import. You can upload a compressed file that includes a single image per subject, or you can upload a compressed file that consists of numerous folders, each with a few images per subject.

Images of subjects within the compressed folder must be in JPEG or PNG format.

Learn more on how you can compress a folder with images or compress a folder of images with other folders.

4. Fill in the **Mass Import Name**.
5. Select the **Subject Group** you would like the subjects to be added to within the Watch List.

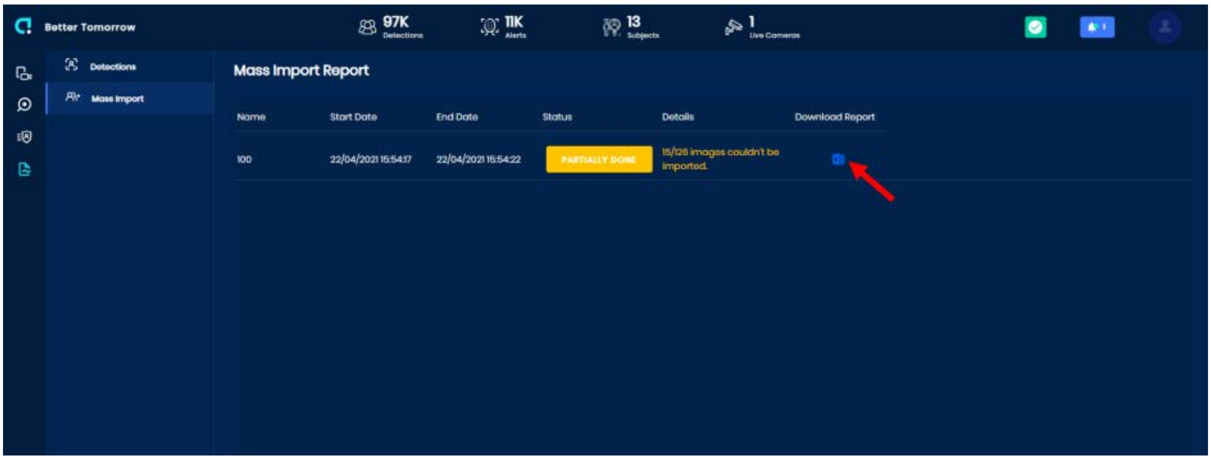
🚧 Subjects from a Mass Import Can Be Added to Only One Subject Group

For every mass import conducted, you can only add the subjects from the mass import to a single subject group.

6. Check off the **Search Backwards** box if you'd like OnWatch to locate all previous appearances (detections) of the subjects you are uploading.
7. Select **Import.** A message confirming your file is loading will appear in the upper right-hand corner.
8. You will then start to see the images from the file loading onto the Watch List. Once the file has been uploaded, you will see the status marked as **Done.**

Download Mass Import Report

> ### Want to Know the Status of Your Mass Import?
>
> If you want to monitor the progression of the mass import, check out the mass import progress bar on the **Reports** page. Once the import is complete, you'll have the option to download an external CSV report that showcases whether or not each subject was added to the system. For all subjects that were not added, you can view the exact reason why within the CSV report.
>
> For more information on mass import reports, click here!



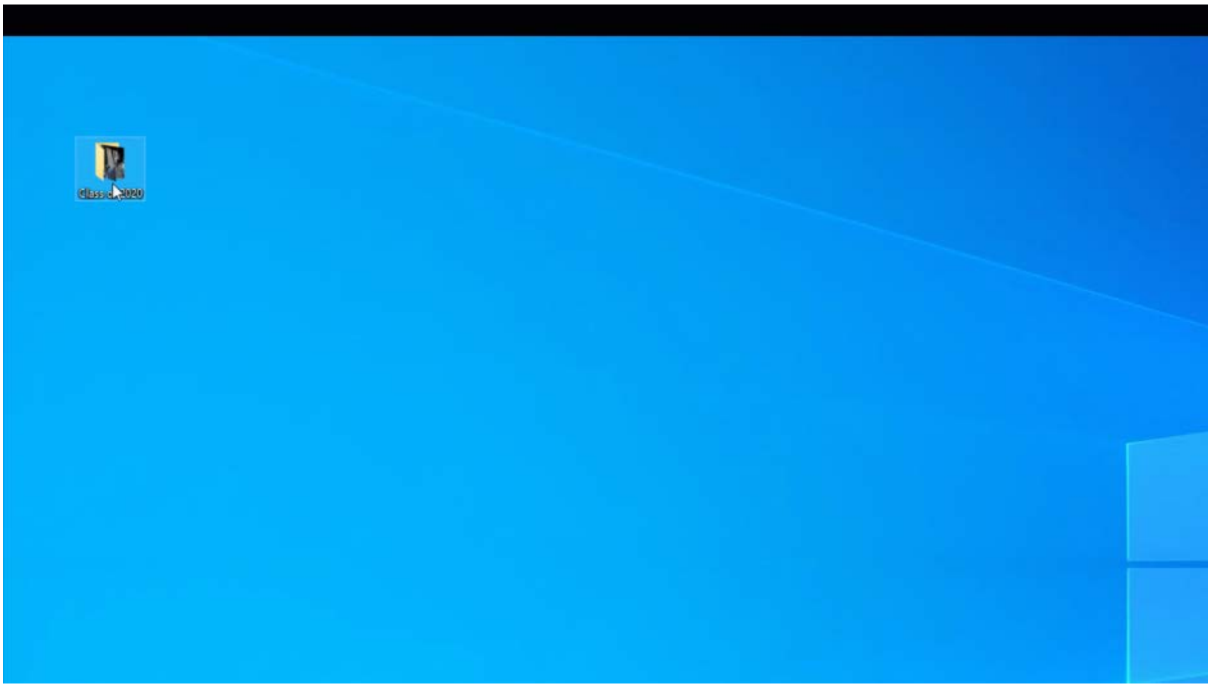
Mass Import Report

Name	Start Date	End Date	Status	Details	Download Report
100	22/04/2021 15:54:17	22/04/2021 15:54:22	PARTIALLY DONE	15/126 images couldn't be imported.	

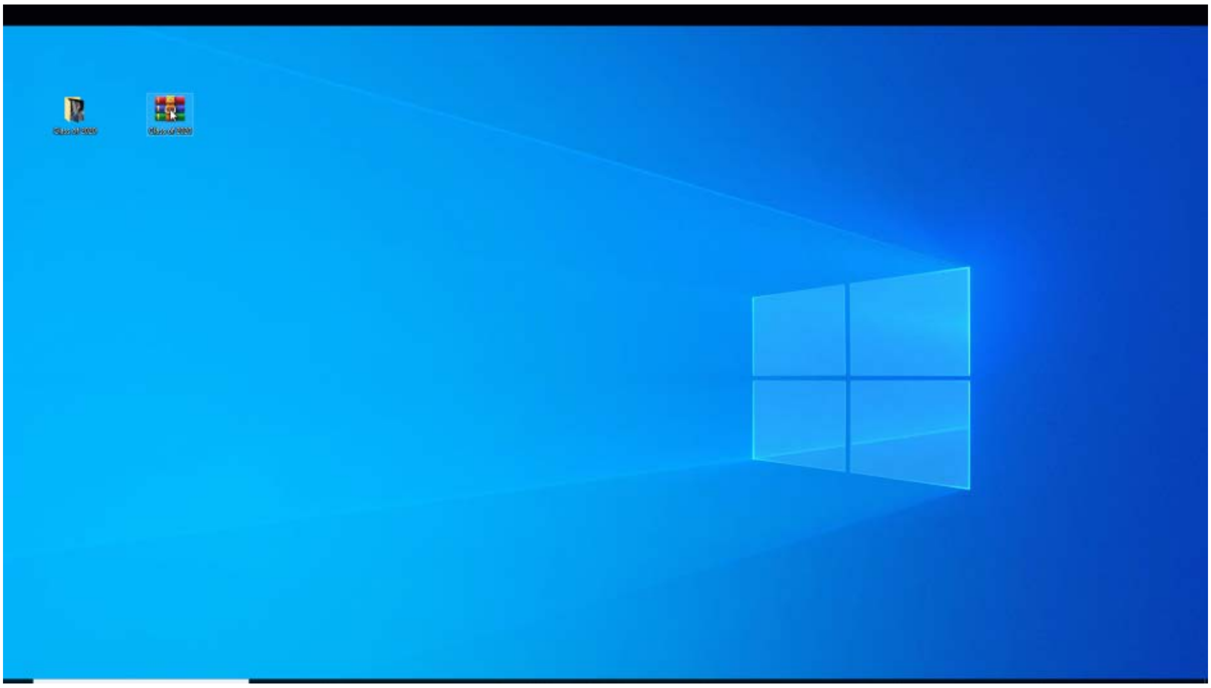
Compress a Folder with Images

1. Highlight the folder you want to compress (make sure that the folder only contains images).

2. Right-click on your mouse, scroll down to **Send To** and select **Compressed Zip Folder**



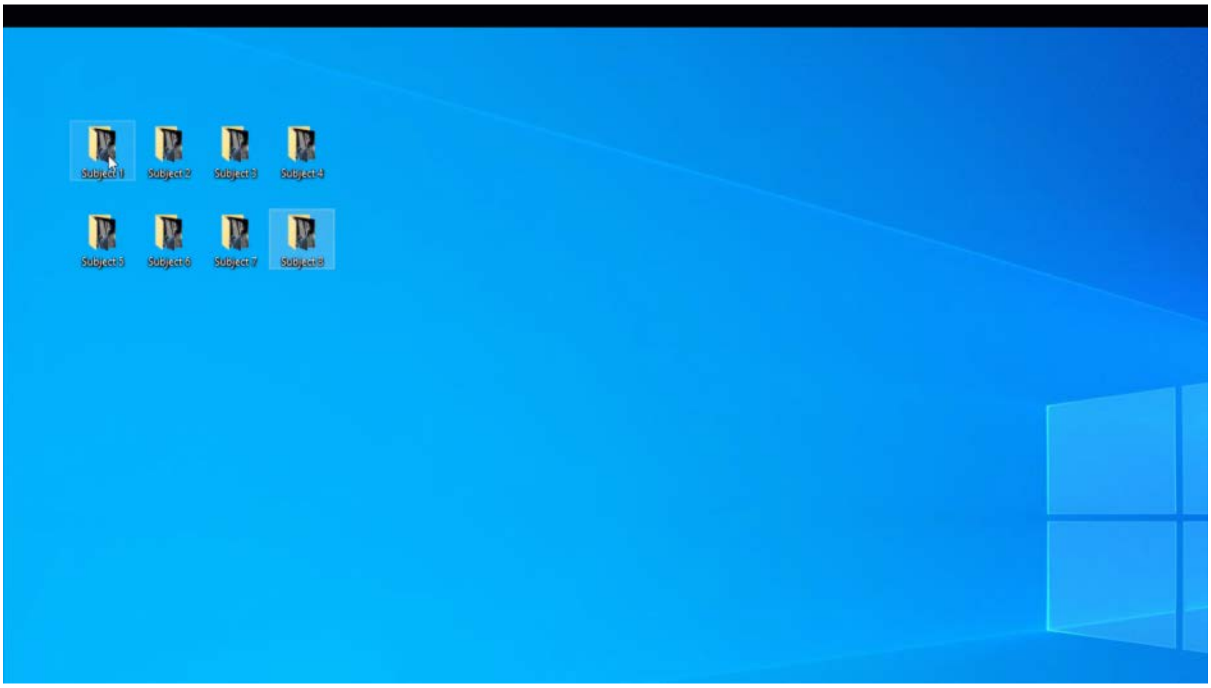
The compressed file will appear on your screen. Inside the file will be your folder, along with the images.



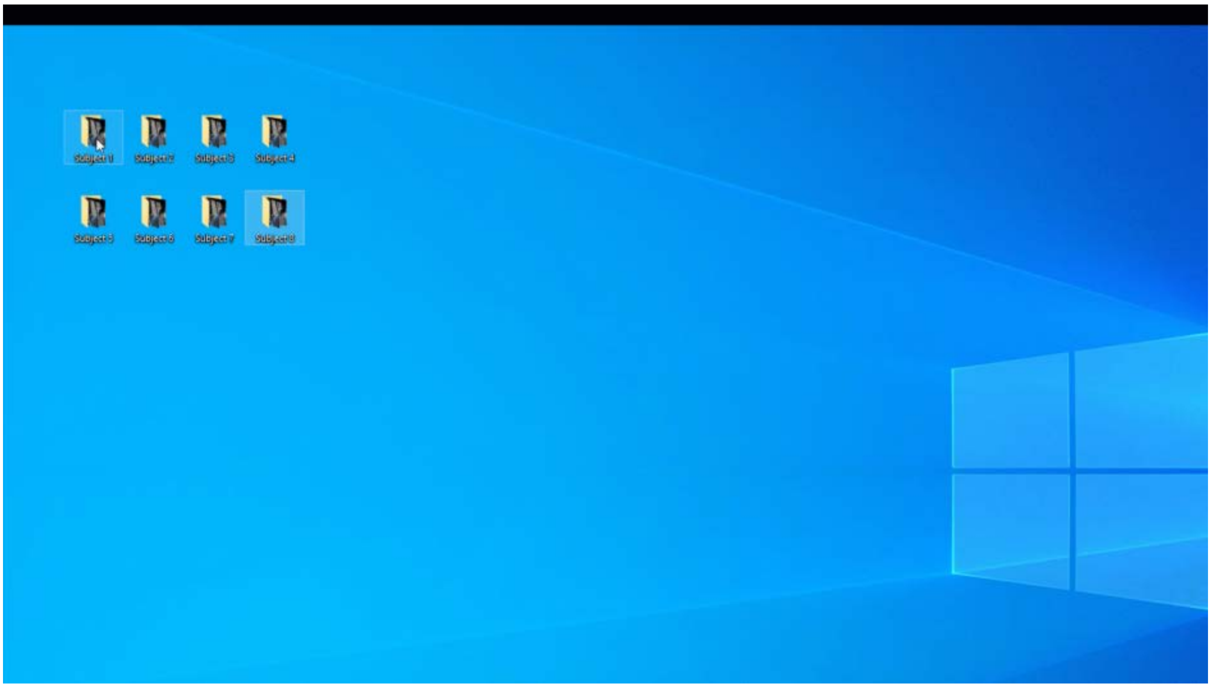
Compress a Folder with Other Folders

1. Highlight the folders you want to import.

> 🚧 **Each Folder Represents 1 Subject**
>
> We allow 15 images per subject.



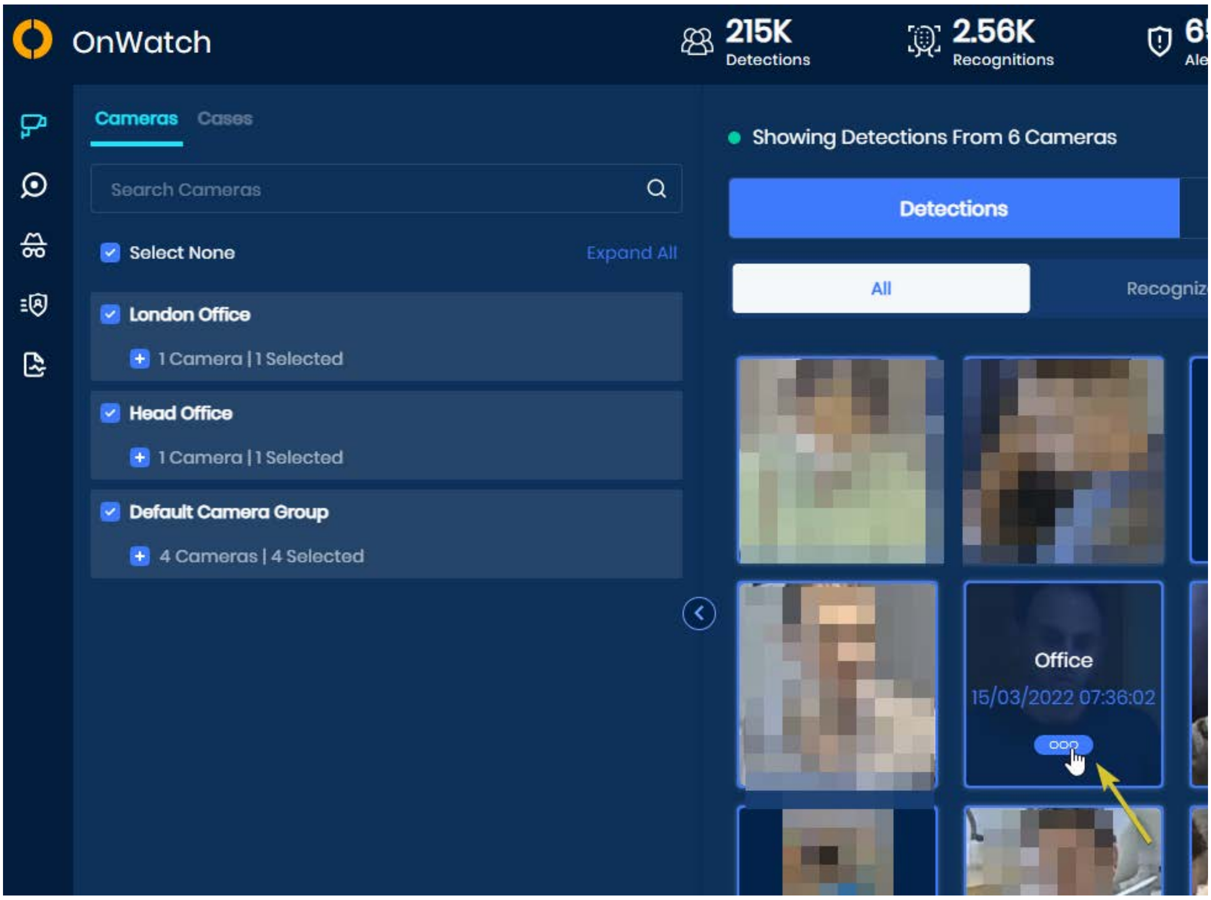
2. Right-click on your mouse, scroll down to **Send To** and select **Compressed Zip Folder**.



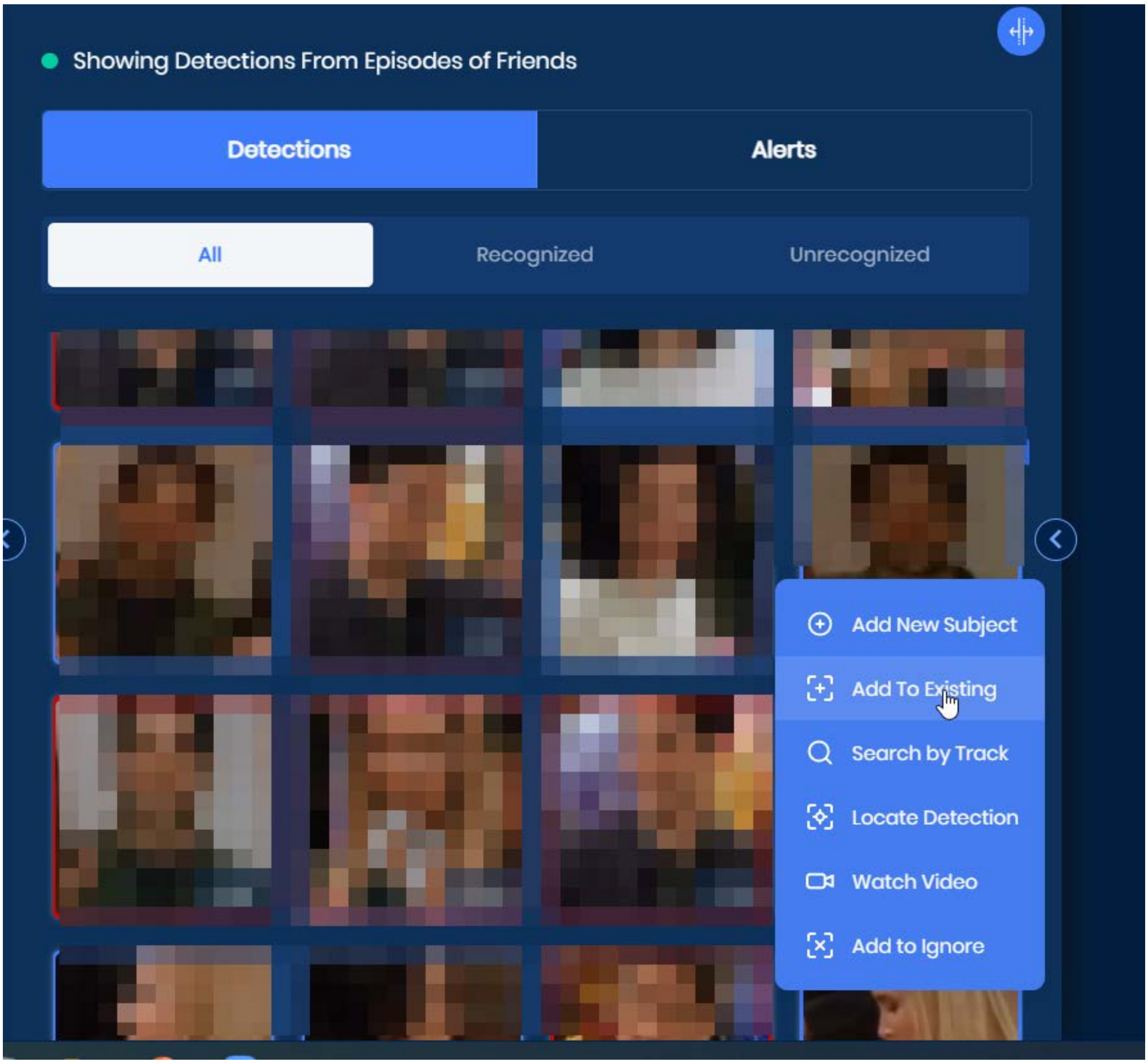
The compressed file will appear on your screen. Inside the file will be your folders, along with the images.

Add a Detection to an Existing Subject's Profile

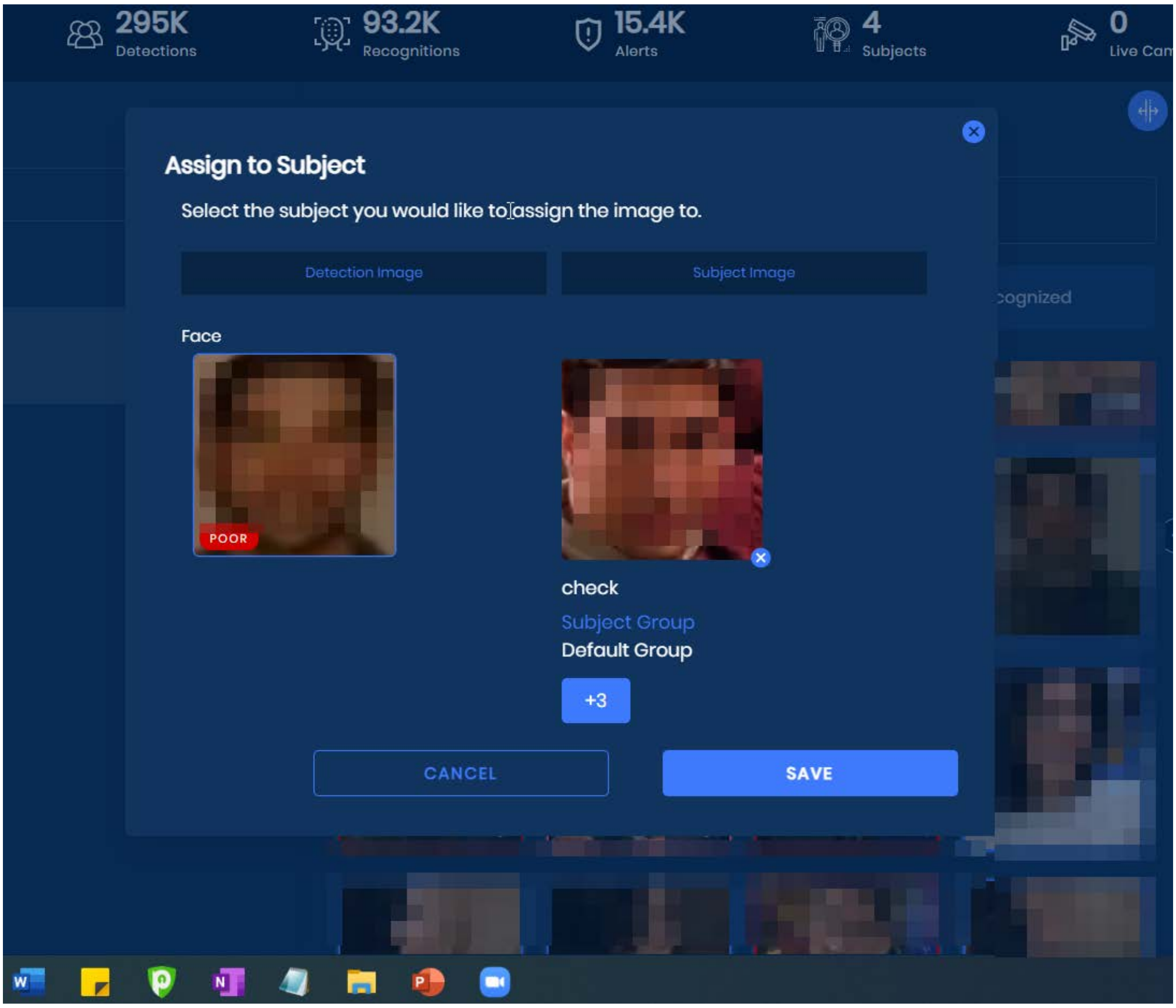
1. Hover over a detection image in the Detections & Recognitions panel and click on the **three-dotted menu icon**



2. Choose **Add To Existing** from the drop-down.



3. Search the subject list for the subject you wish to assign this image to.



Assign to Subject

Select the subject you would like to assign the image to.

check

Subject Group

Default Group

4. Click **Save**.

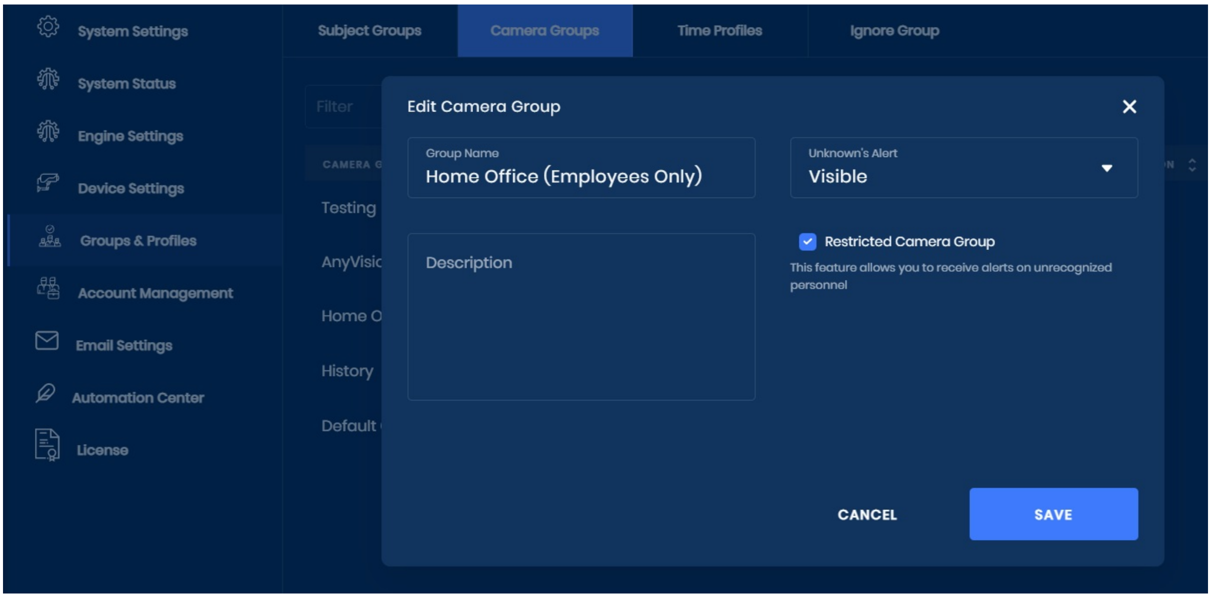
Receive Alerts on Unknown Individuals - Restricted Area

1. Add known individuals to a watchlist that are allowed to be in a specific area.

> ## 📘 Adding Known Individuals
>
> These individuals can be added manually via the upload mechanism Click here or imported automatically via our API.
> Additionally: Oosto has some pre-existing integrations that can be set up to import individuals from an access control system periodically. Click for API. Please contact Oosto Support to assist with this one-time configuration for existing plugins as listed below

Access Control	Version
Avigilon ACM	5.2
Bosch BIS	4.8 & 4.9
C-CURE 9000	2.7, 2.8
Genetec Synergis	5.7, 5.8
Genetec Synergis	5.9.4
Honeywell ProWatch	4.3.5, 4.5, 5.03
Lenel S2	7.6
Nedap Aeos	2020.1
RS2 Access It!	7.3.3

2. Add and edit a camera group to be enabled for Restricted Area



Edit Camera Group

Group Name: Home Office (Employees Only)

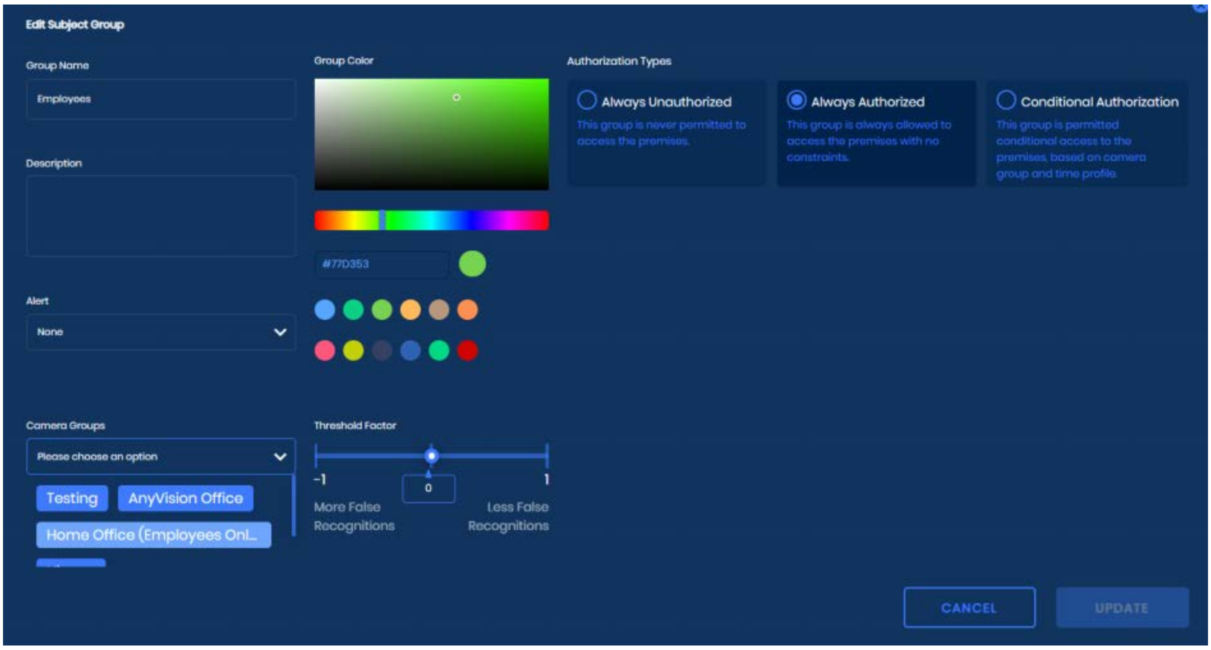
Unknown's Alert: Visible

Description

☑ Restricted Camera Group

This feature allows you to receive alerts on unrecognized personnel

3. Relate the specific known individual watchlist or watchlist to the relevant camera groups without alerting



Edit Subject Group

Group Name: Employees

Description

Alert: None

Group Color: #77D353

Authorization Types

○ Always Unauthorized
This group is never permitted to access the premisas.

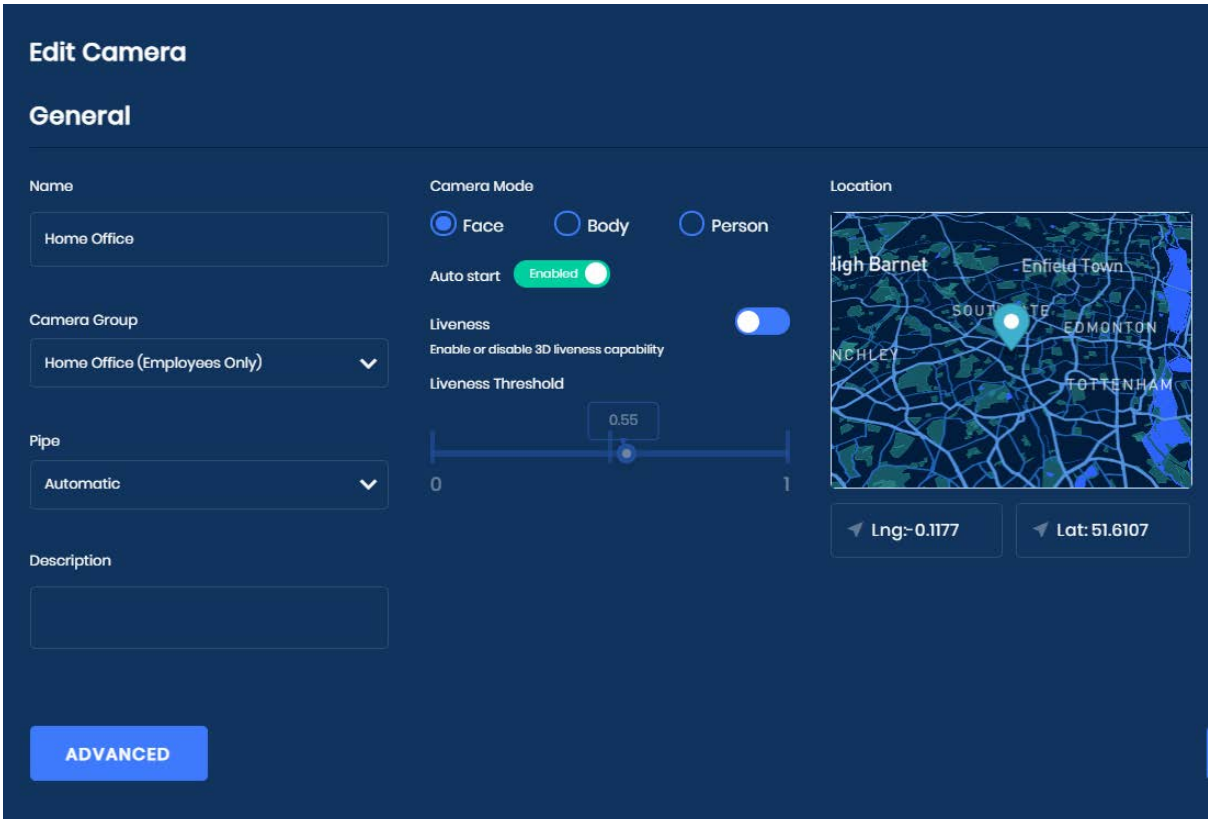
● Always Authorized
This group is always allowed to access the premisas with no constraints.

○ Conditional Authorization
This group is permitted conditional access to the premises, based on camera group and time profile.

Camera Groups: Please choose an option
Testing
AnyVision Office
Home Office (Employees Onl...

Threshold Factor: 0

4. Add the specific camera/cameras to the relevant restricted area camera groups Edit Camera



Edit Camera

General

Name: Home Office

Camera Group: Home Office (Employees Only)

Pipe: Automatic

Description:

Camera Mode: ● Face ○ Body ○ Person

Auto start: Enabled

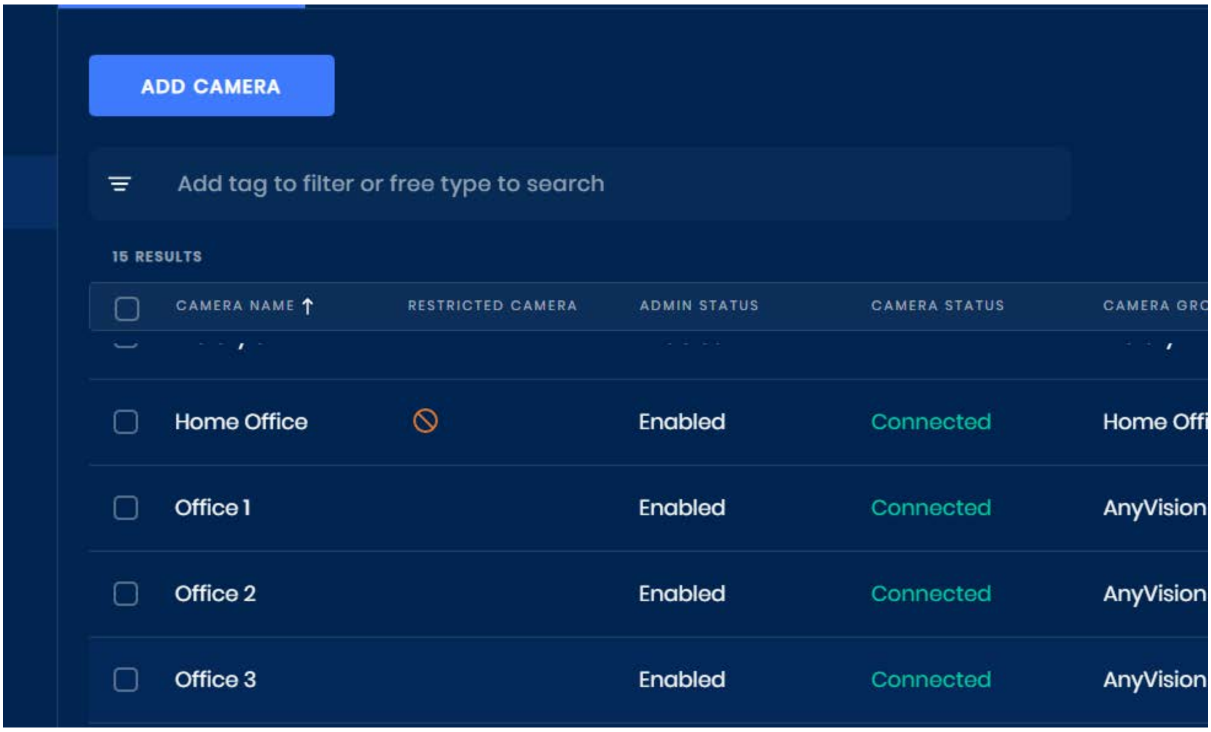
Liveness
Enable or disable 3D liveness capability

Liveness Threshold: 0.55

Location

Lng:-0.1177 Lat: 51.6107

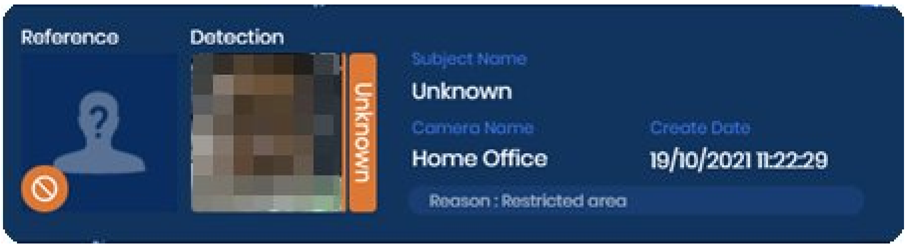
The camera will be marked as a restricted area camera in the devices list



15 RESULTS

□	CAMERA NAME ↑	RESTRICTED CAMERA	ADMIN STATUS	CAMERA STATUS	CAMERA GRO
□	Home Office	🚫	Enabled	Connected	Home Offi
□	Office 1		Enabled	Connected	AnyVision
□	Office 2		Enabled	Connected	AnyVision
□	Office 3		Enabled	Connected	AnyVision

4. Now when someone is not on the watchlist is detected an unknown alert will be shown without a reference but with the detection of the individual. This can then be used to review the timeline, view the playback or even add the individual to a temporarily allowed watchlist.



Subject Name: Unknown

Camera Name: Home Office

Create Date: 19/10/2021 11:22:29

Reason : Restricted area

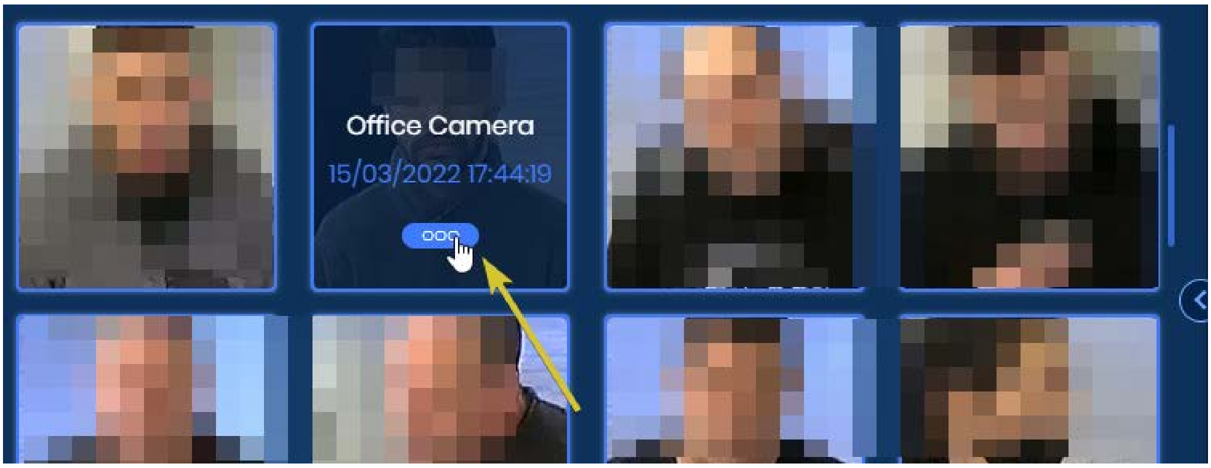
Alerts Timing

By default, alerts have now been configured to have a 1-minute delay between alerts for the same individual. This can be configured within the administrative Consul. Please contact Oosto support if this is required, to adjust the second for "trackAggregationSec"

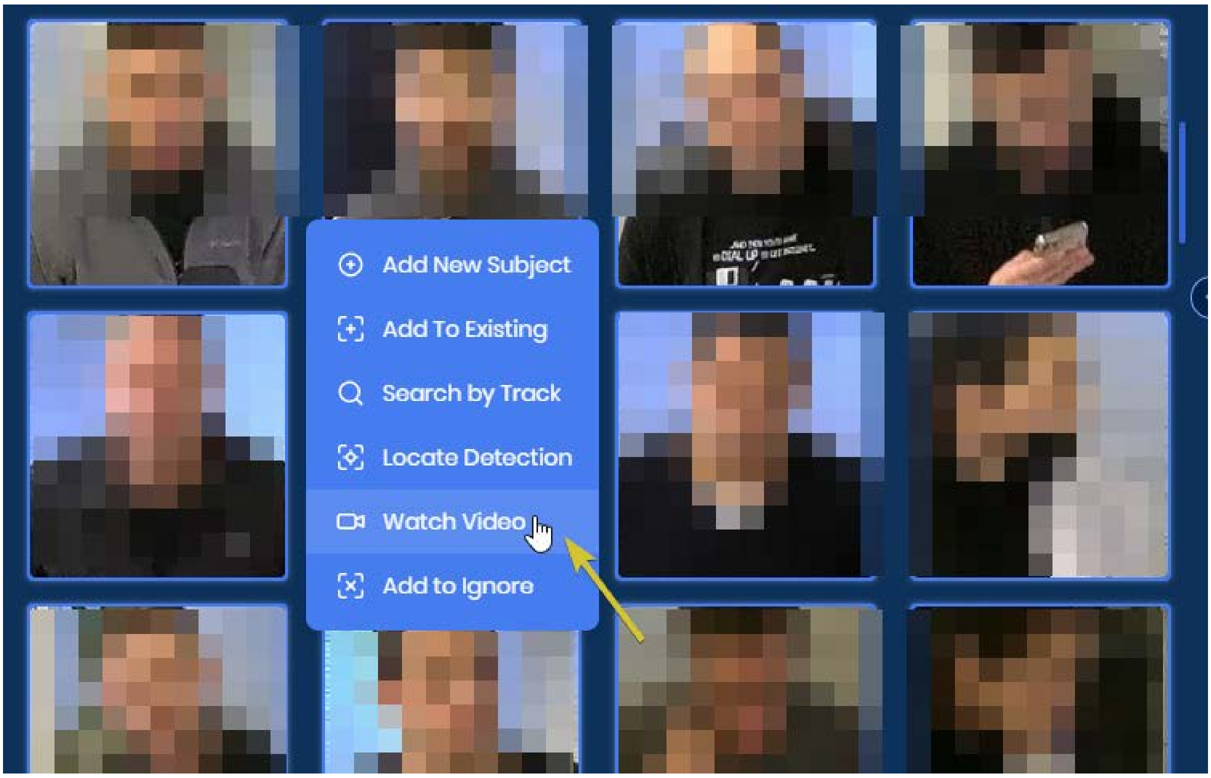
Download a Detection Video or Image

Download a Detection Video

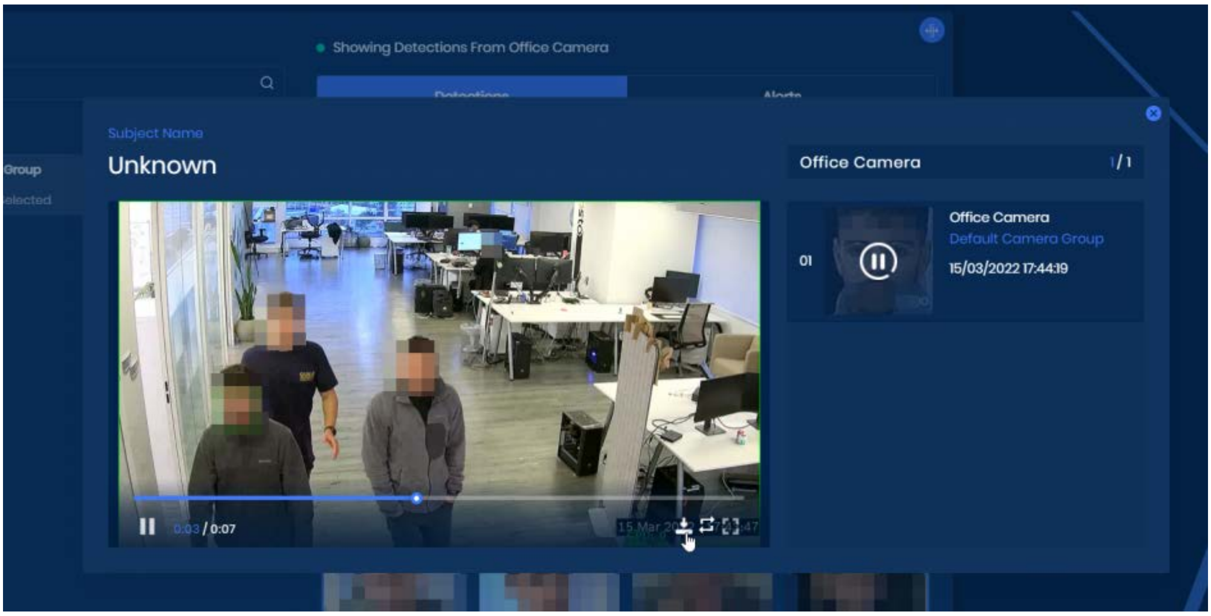
1. Select and click on a detection image that you would like to see a video for.



2. From the right-side pane that appears, click on the **hamburger icon** and select **Watch Video** from the dropdown.



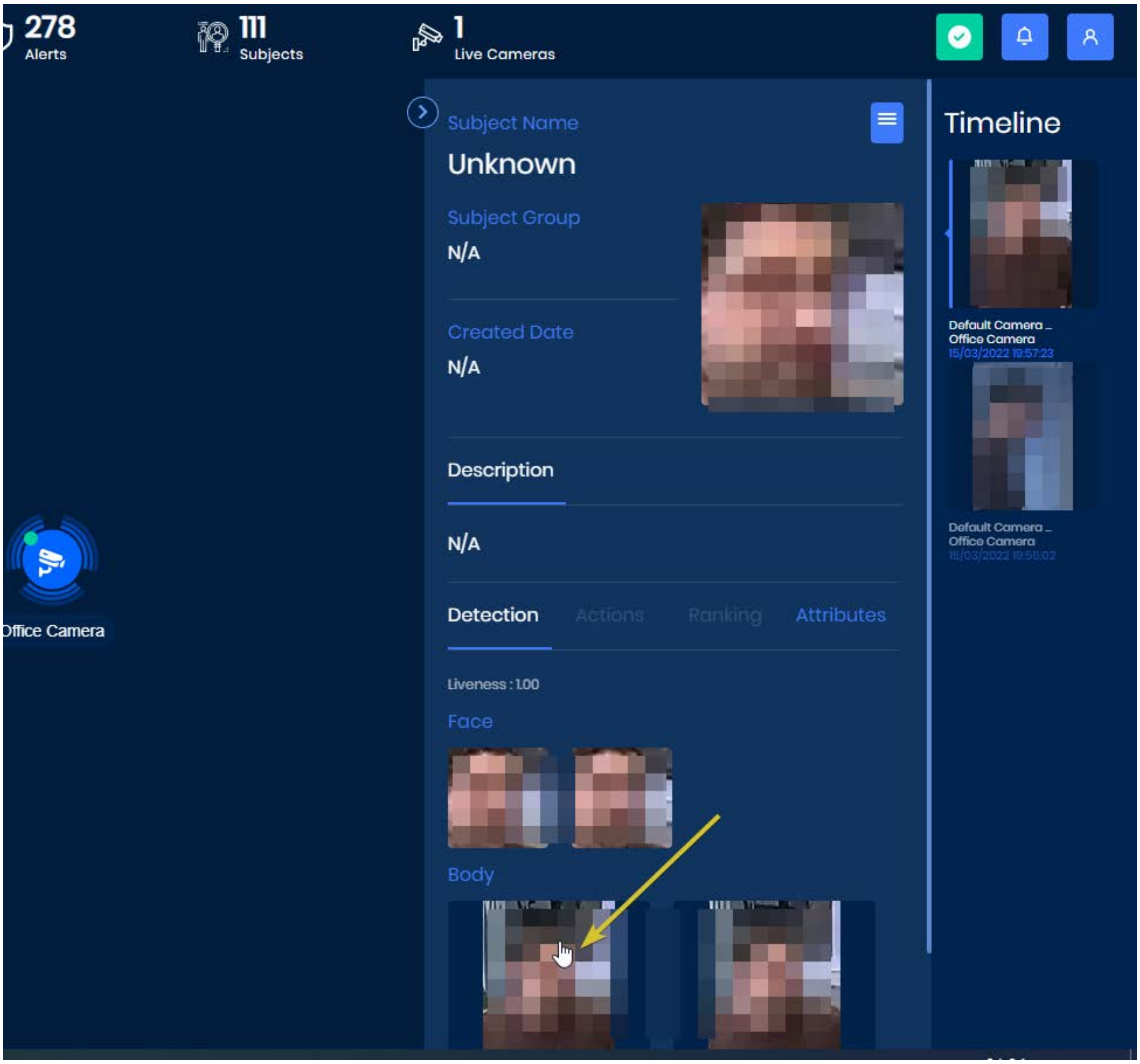
3. Within the subject detection video, tap the **download button**.



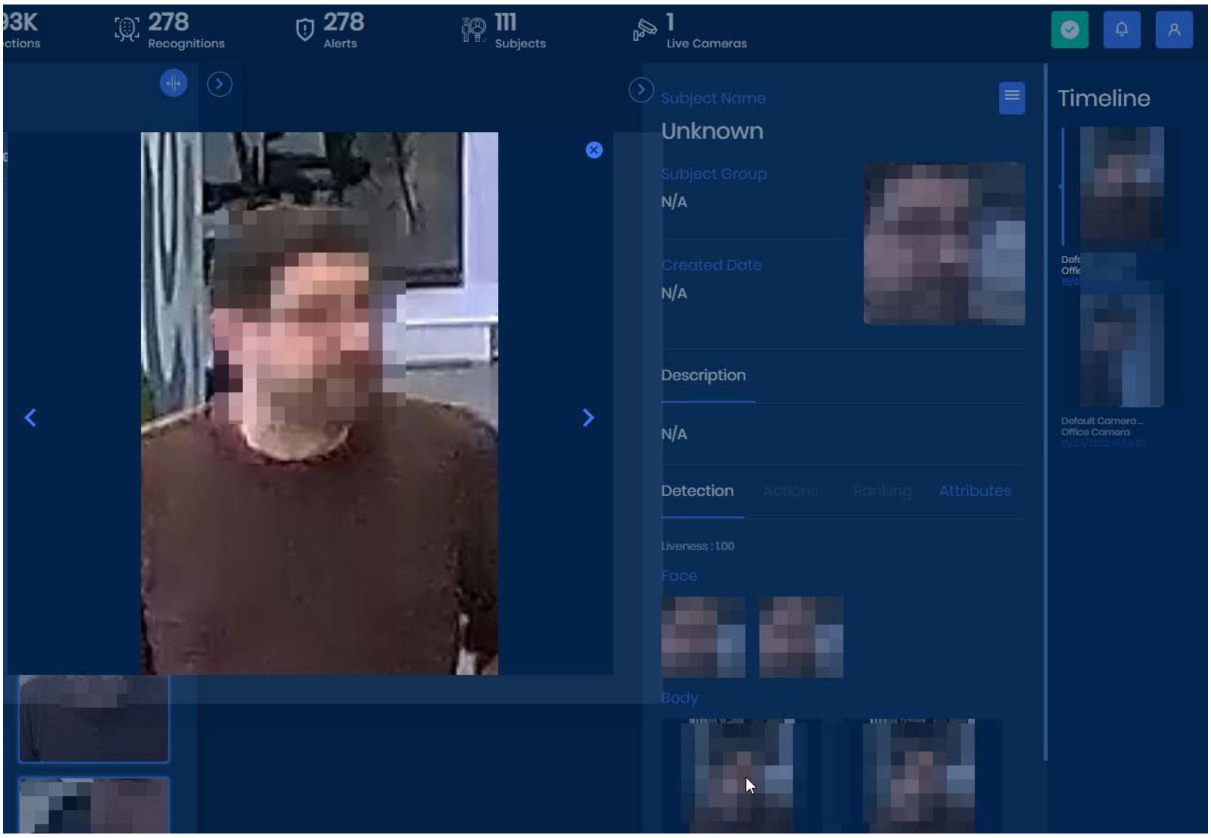
4. The video will now open in your computer's video player.

Download a Detection Image

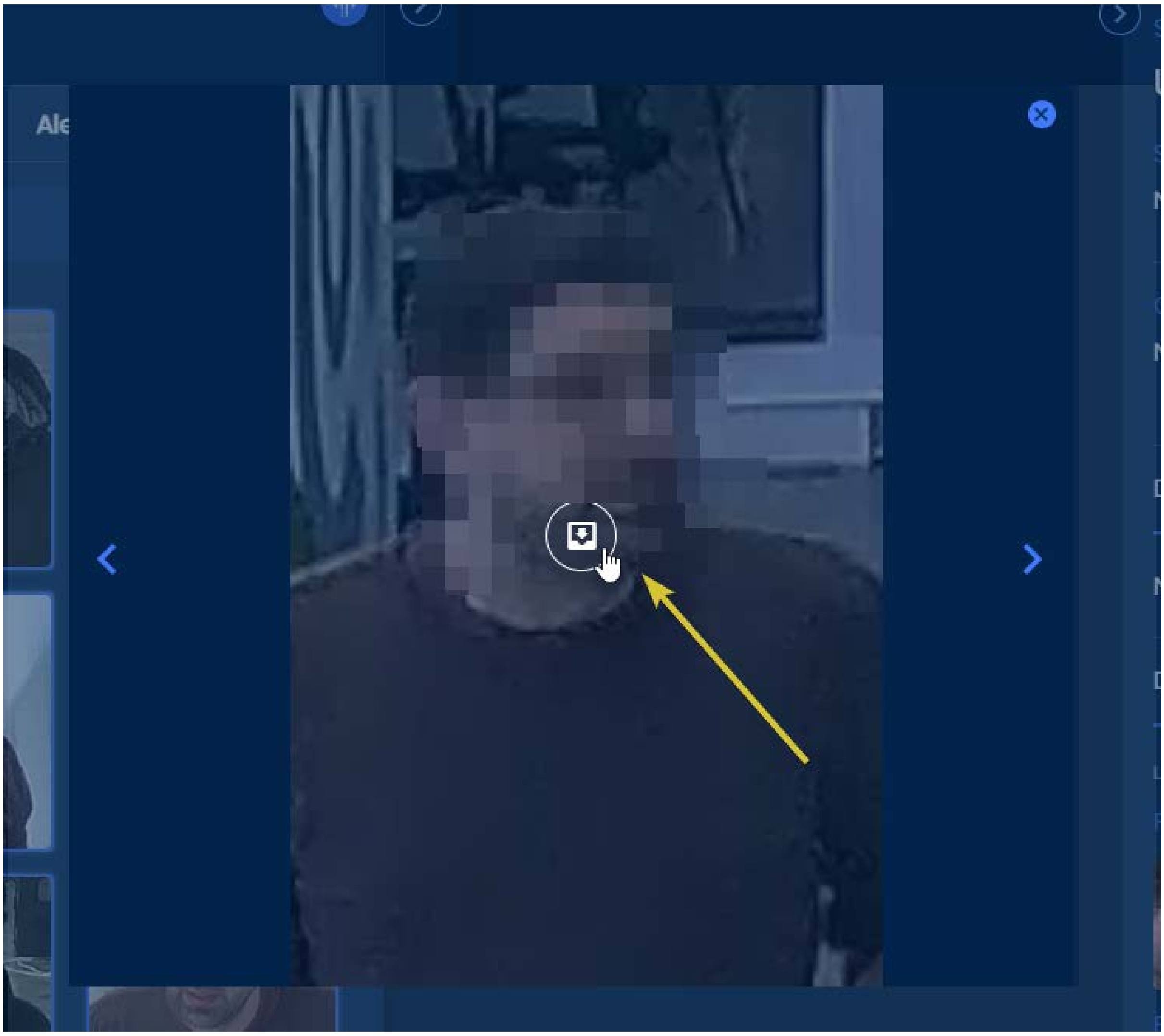
1. Click on the **detection image** you want to download.
2. The image will now appear in the subject's information box within the right-side pane.



3. Tap the **image** to open it.



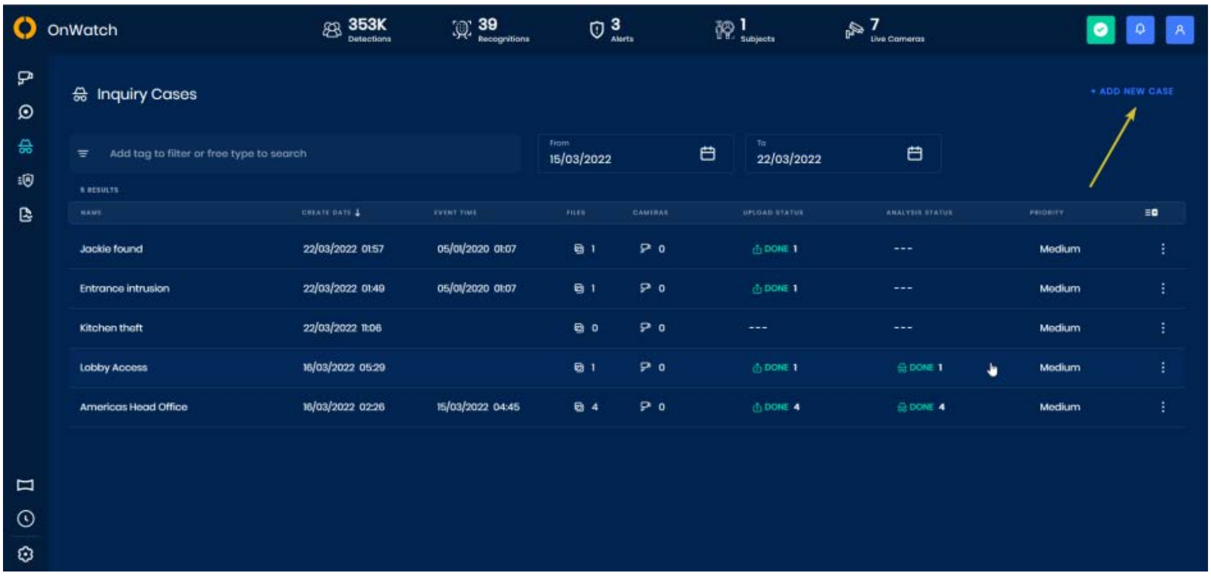
4. Click the **download button** in the center of the image to download it.



Open and Manage Inquiry Case

How to Create a New Inquiry

1. Navigate to the **Inquiry** tab and select **Add New Case**.



From 15/03/2022

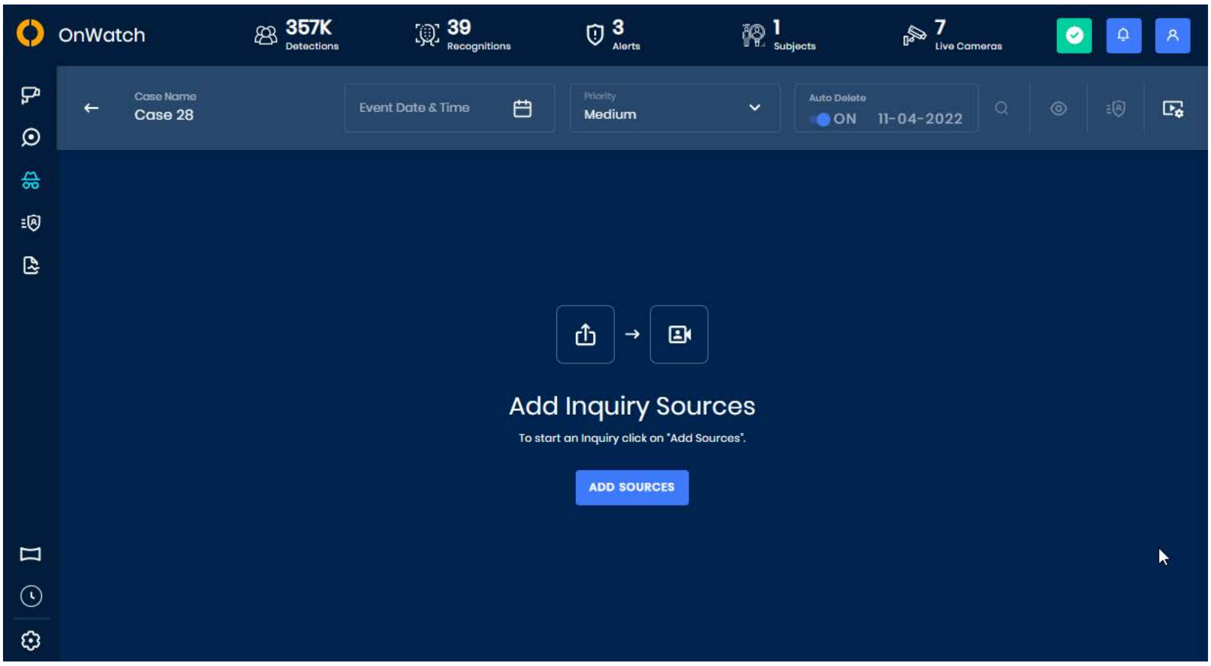
To 22/03/2022

5 RESULTS

NAME	CREATE DATE ↓	EVENT TIME	FILES	CAMERAS	UPLOAD STATUS	ANALYSIS STATUS	PRIORITY
Jackie found	22/03/2022 01:57	05/01/2020 01:07	1	0	DONE 1	---	Medium
Entrance intrusion	22/03/2022 01:49	05/01/2020 01:07	1	0	DONE 1	---	Medium
Kitchen theft	22/03/2022 11:06		0	0	---	---	Medium
Lobby Access	16/03/2022 05:29		1	0	DONE 1	DONE 1	Medium
Americas Head Office	16/03/2022 02:26	15/03/2022 04:45	4	0	DONE 4	DONE 4	Medium

2. The case will be provided with a default name that can be altered, when opening the case it defaults to the following settings.

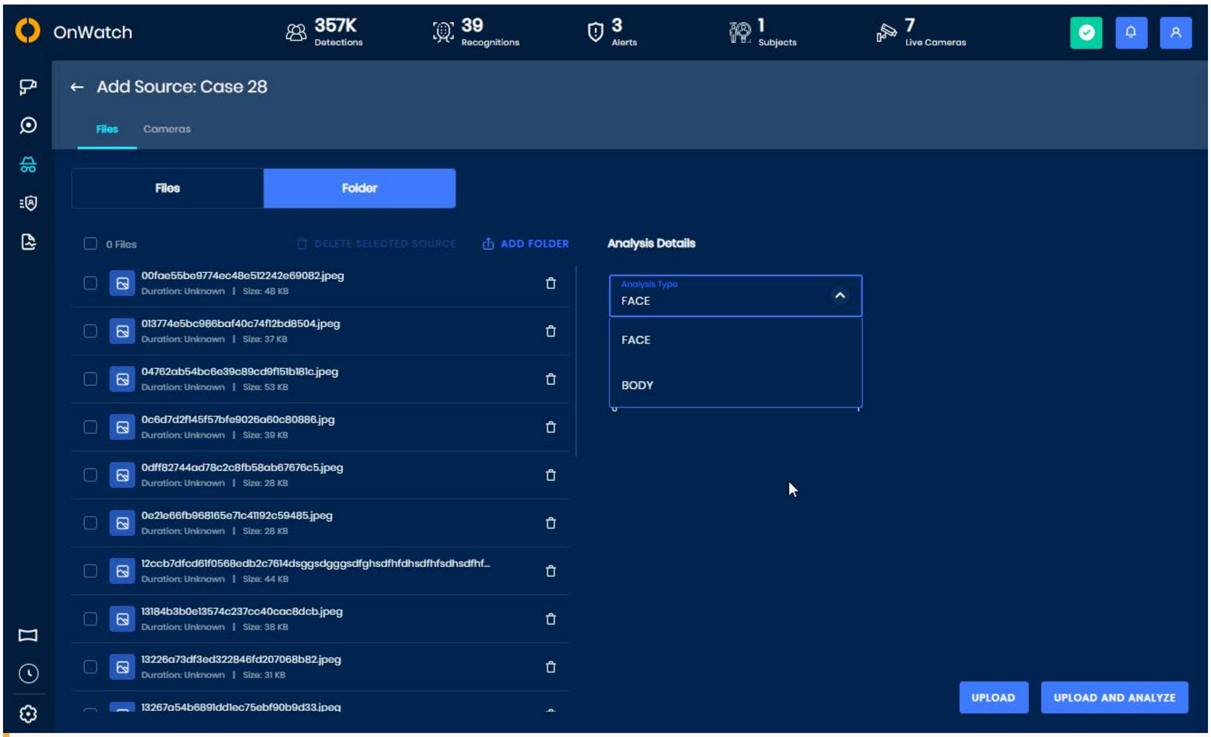
- **Empty** - No event date time (this is used to allow a specific time for when the incident happened, allowing the search page to take this into account for cases)
- **Priority** - Provides the system with the ability to prioritize between currently processing video files. This setting is set per case. When you have reached your maximum concurrent inquiry streams the next stream processed will be chosen by the highest priority cases
- **Auto deletion** - This indicated when the case and all its content will be deleted automatically by the system based on the system retention time, it can also be used to remove this auto-deletion overriding the system for important long term cases
- **Analysis Defaults** - These are the default file analysis settings set per case, once set the next uploaded files will have these settings, they can be overridden per case at a later stage



Case Name: Case 28
Priority: Medium
Auto Delete: ON 11-04-2022

To start an Inquiry click on "Add Sources".

At this stage, you can add sources to your case These include video files or images in bulk or by folder as well as allowing you to associate cameras to the case. Files or folders can be dragged into the window or a selection dialogue will appear by choosing the select files/folders option.



Analysis Type: FACE

00fae55be9774ec48e512242e69082.jpeg
Duration: Unknown | Size: 48 KB

013774e5bc986baf40c74f12bd8504.jpeg
Duration: Unknown | Size: 37 KB

04762ab54bc6e39c89cd9f151b181c.jpeg
Duration: Unknown | Size: 53 KB

0c6d7d2f145f57bfe9026a60c80886.jpg
Duration: Unknown | Size: 39 KB

0dff82744ad78c2c8fb58ab67676c5.jpeg
Duration: Unknown | Size: 28 KB

0e21e66fb968165e71c41192c59485.jpeg
Duration: Unknown | Size: 28 KB

12ccb7dfcd61f0568edb2c7614dsggsdgggsdfghsdfhfdhsdfhfsdhsdfhf...
Duration: Unknown | Size: 44 KB

13184b3b0e13574c237cc40cac8dcb.jpeg
Duration: Unknown | Size: 38 KB

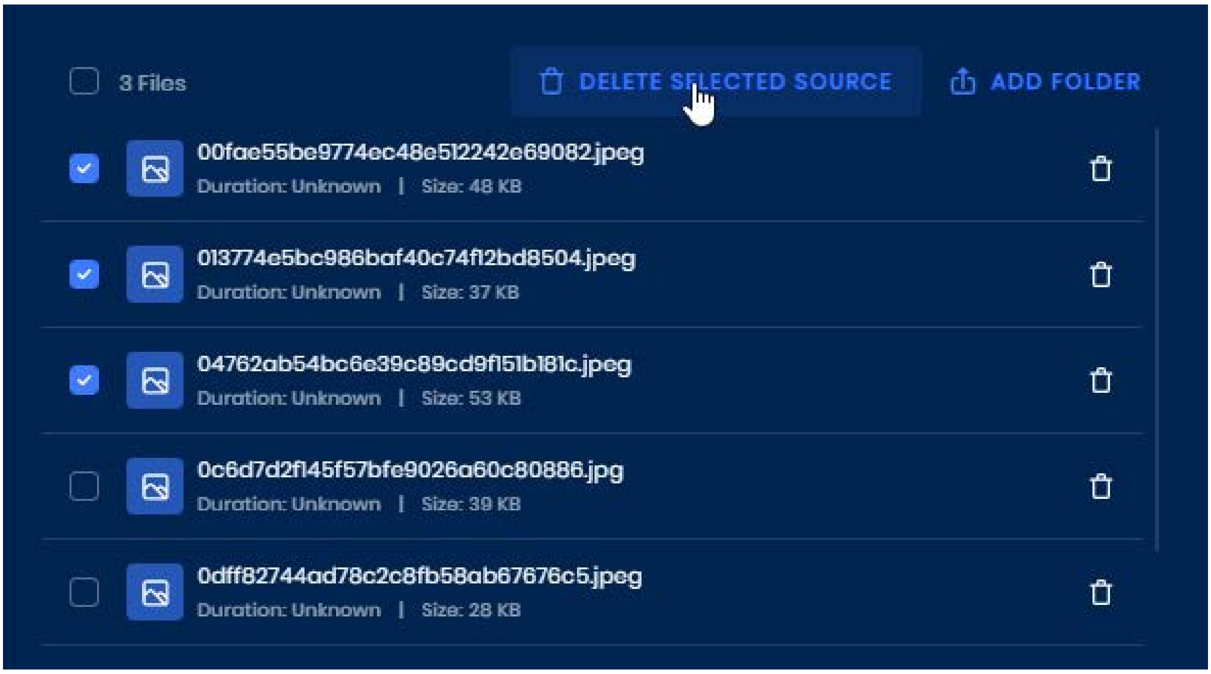
13226a73df3ed322846fd207068b82.jpeg
Duration: Unknown | Size: 31 KB

13267a54b6891dd1ec75ebf90b9d33.jpeg

🚧 Note

Up to 999 files can be uploaded at one time based on browser capabilities
When using the API to upload this is not a limitation

It is possible to add select files individually or in bulk and delete them at this stage or add files or more folder



□ 3 Files

☑ 00fae55be9774ec48e512242e69082.jpeg
Duration: Unknown | Size: 48 KB

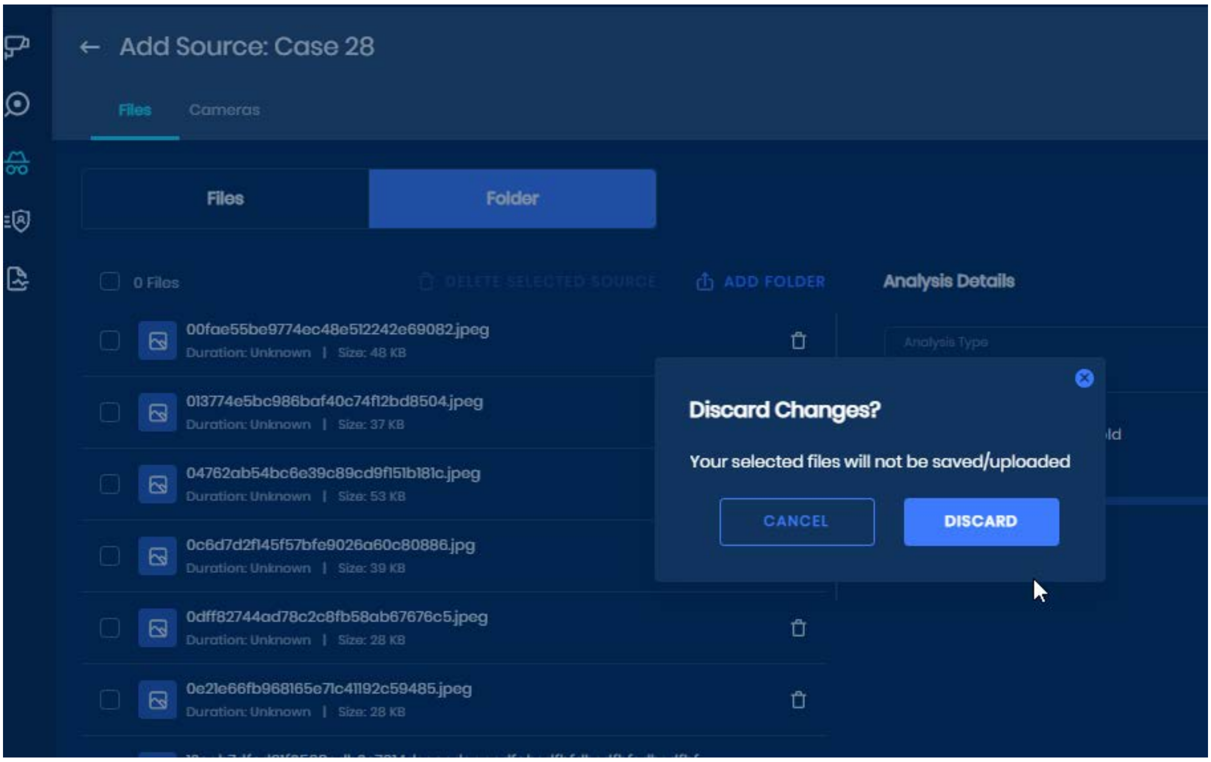
☑ 013774e5bc986baf40c74f12bd8504.jpeg
Duration: Unknown | Size: 37 KB

☑ 04762ab54bc6e39c89cd9f151b181c.jpeg
Duration: Unknown | Size: 53 KB

□ 0c6d7d2f145f57bfe9026a60c80886.jpg
Duration: Unknown | Size: 39 KB

□ 0dff82744ad78c2c8fb58ab67676c5.jpeg
Duration: Unknown | Size: 28 KB

If you decide to switch to the cameras or file/folder tab that you are not currently using before you upload/analyze the files the system will discard the currently selected files



← Add Source: Case 28

□ 0 Files

□ 00fae55be9774ec48e512242e69082.jpeg
Duration: Unknown | Size: 48 KB

□ 013774e5bc986baf40c74f12bd8504.jpeg
Duration: Unknown | Size: 37 KB

□ 04762ab54bc6e39c89cd9f151b181c.jpeg
Duration: Unknown | Size: 53 KB

□ 0c6d7d2f145f57bfe9026a60c80886.jpg
Duration: Unknown | Size: 39 KB

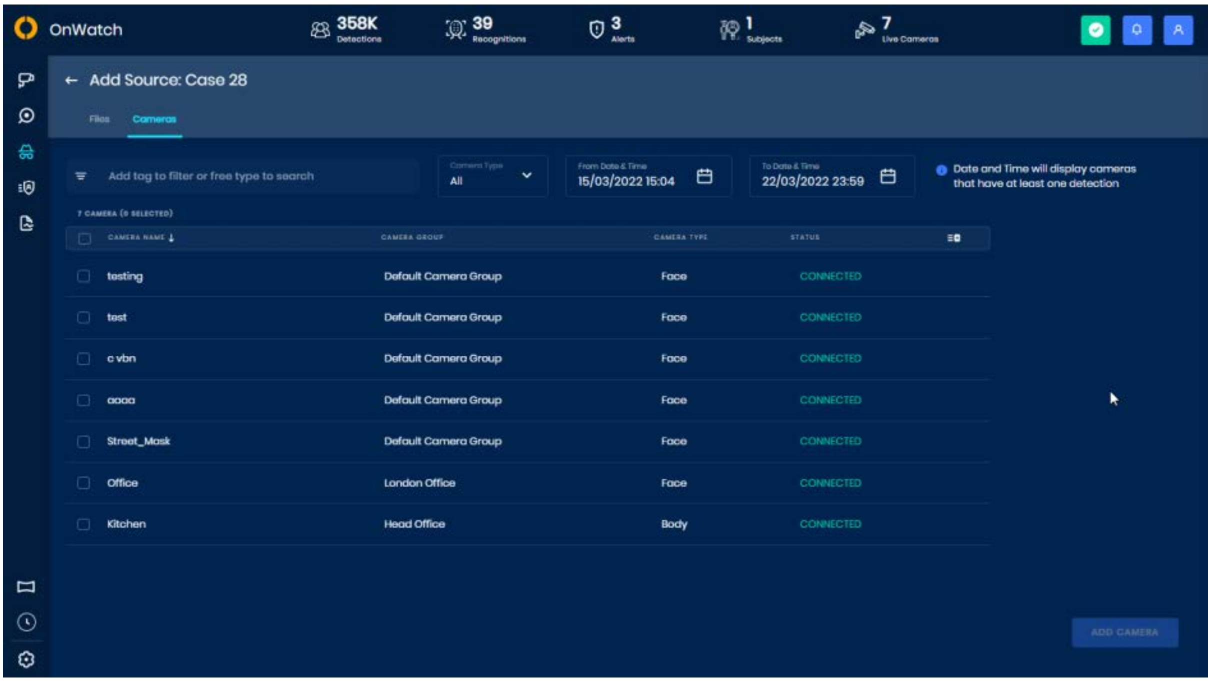
□ 0dff82744ad78c2c8fb58ab67676c5.jpeg
Duration: Unknown | Size: 28 KB

□ 0e21e66fb968165e71c41192c59485.jpeg
Duration: Unknown | Size: 28 KB

Discard Changes?

Your selected files will not be saved/uploaded

It is possible to add cameras to a case so that the detections between a timeframe can be used for that investigation. When selecting the cameras tab you can search for a camera by name, type, and connection status and then you have the ability to filter between dates/times. This filter will only show you cameras that had detections between that date/time range, which is relevant to your cases.



← Add Source: Case 28

Add tag to filter or free type to search

Camera Type: All

From Date & Time: 15/03/2022 15:04

To Date & Time: 22/03/2022 23:59

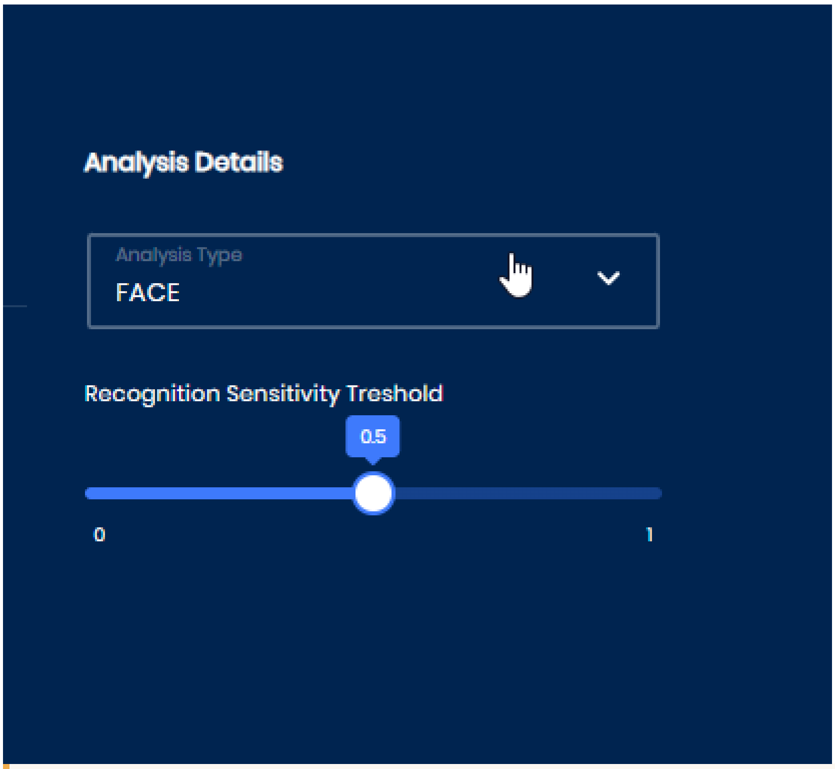
Date and Time will display cameras that have at least one detection

7 CAMERA (0 SELECTED)

	CAMERA NAME ↓	CAMERA GROUP	CAMERA TYPE	STATUS
□	testing	Default Camera Group	Face	CONNECTED
□	test	Default Camera Group	Face	CONNECTED
□	c vbn	Default Camera Group	Face	CONNECTED
□	aaaa	Default Camera Group	Face	CONNECTED
□	Street_Mask	Default Camera Group	Face	CONNECTED
□	Office	London Office	Face	CONNECTED
□	Kitchen	Head Office	Body	CONNECTED

At this stage, you can choose to upload or upload and analyse in a single action. If you plan on adjusting the default analysis setting per file you should choose the upload only route.

When uploading or uploading and analyzing you should choose Face, Body or person options and the threshold. These will be applied at the analysis stage. *Face* refers to only recognizing individuals by their face, *Body* refers to only recognizing people by their body attributes, and *Person* refers to both face and body.



Analysis Details

Analysis Type: FACE

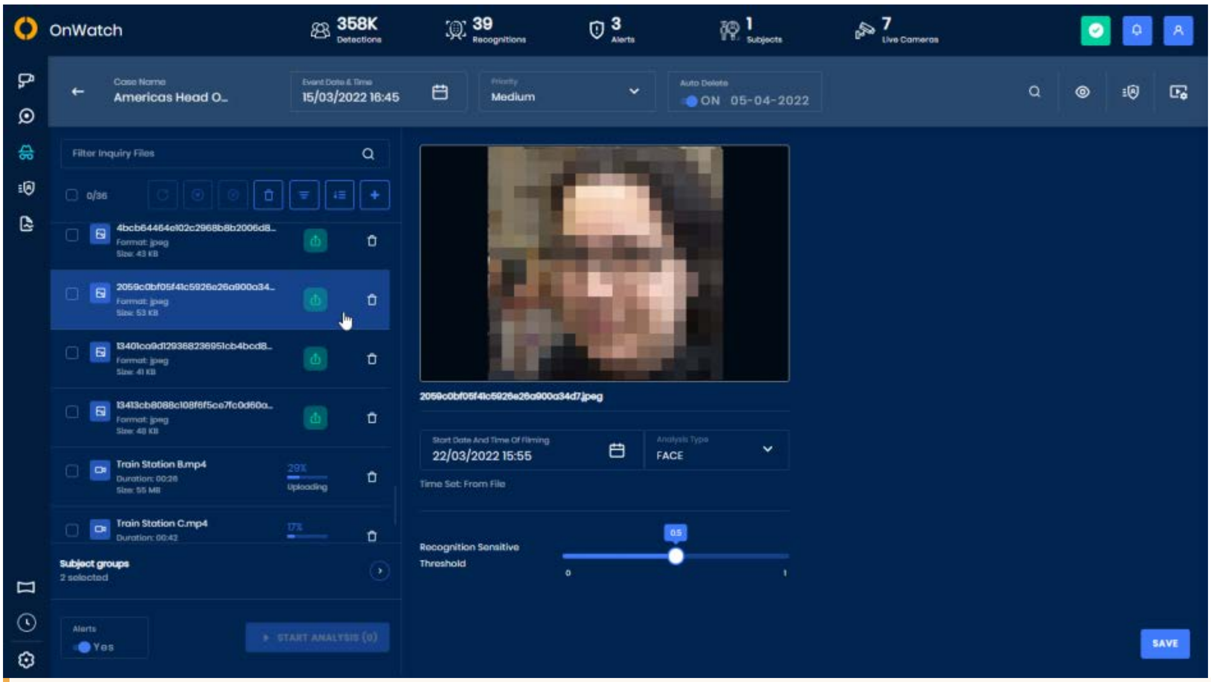
Recognition Sensitivity Treshold: 0.5

🚧 Note

When uploading files and selecting the default analysis type **Person** will only appear as an option at this stage if all file types are video

Once upload or upload and analyze is selected you will be shown the main case edit window. From this window you can easily manage all your content including:

- Search, filter, sort and view the files
- View each files state and analysis settings
- Manipulate each file individually or in bulk
- Select the case subject groups
- Select if alerts are required or not according to subject groups
- Initiate analysis/reanalysis
- Open case content in sources or search views



Case Name: Americas Head O...
Event Date & Time: 15/03/2022 16:45
Priority: Medium
Auto Delete: ON 05-04-2022

4bcb64464e102c2968b8b2006d8... Format: jpeg Size: 43 KB
2059c0bf05f41c5926e26a900a34... Format: jpeg Size: 53 KB
13401ca9d12936823695Icb4bcd8... Format: jpeg Size: 41 KB
13413cb8088c108f6f5ce7fc0d60a... Format: jpeg Size: 48 KB
Train Station B.mp4 Duration: 00:26 Size: 55 MB 29% Uploading
Train Station C.mp4 Duration: 00:42 17%

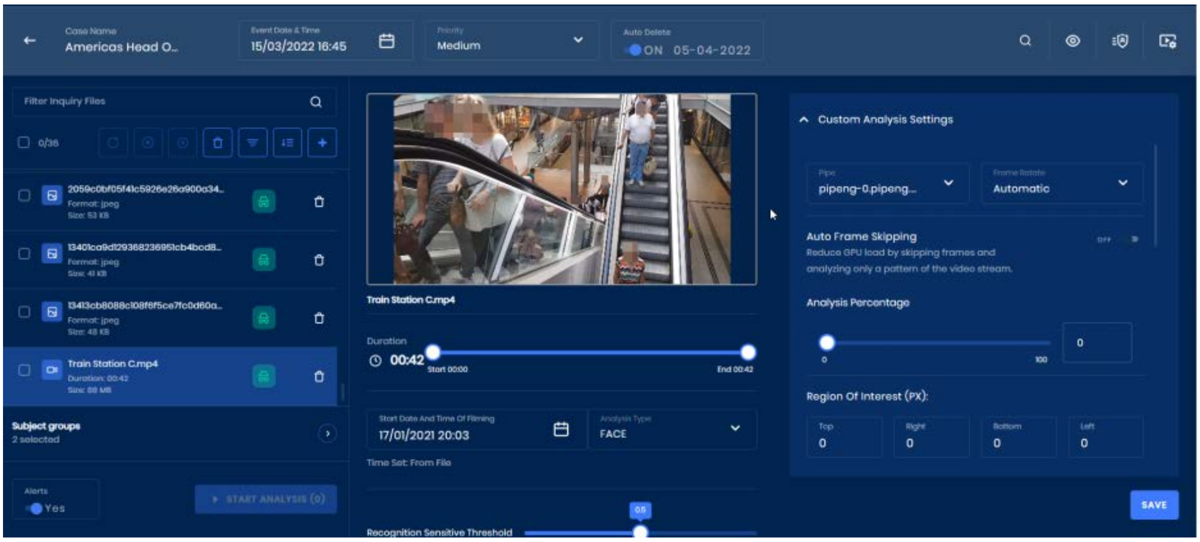
Subject groups: 2 selected
Alerts: Yes

2059c0bf05f41c5926e26a900a34d7.jpeg
Start Date And Time Of Filming: 22/03/2022 15:55
Analysis Type: FACE
Time Set: From File
Recognition Sensitive Threshold: 0.5 (0 – 1)

Note

The system will automatically **inherit** the date/time from the files being uploaded, if no date/time is detected the system will set **now** as the default date/time. Either one of these can be overridden **manually**

When clicking on a specific file the uploading content will show a file preview. whilst analysing video content the preview will change to the analysis stream with bounding boxes of the progressing source.



Case Name: Americas Head O...
Event Date & Time: 15/03/2022 16:45
Priority: Medium
Auto Delete: ON 05-04-2022

2059c0bf05f41c5926e26a900a34... Format: jpeg Size: 53 KB
13401ca9d12936823695Icb4bcd8... Format: jpeg Size: 41 KB
13413cb8088c108f6f5ce7fc0d60a... Format: jpeg Size: 48 KB
Train Station C.mp4 Duration: 00:42 Size: 88 MB

Subject groups: 2 selected
Alerts: Yes

Train Station C.mp4
Duration: 00:42 Start 00:00 End 00:42
Start Date And Time Of Filming: 17/01/2021 20:03
Analysis Type: FACE
Time Set: From File
Recognition Sensitive Threshold: 0.5

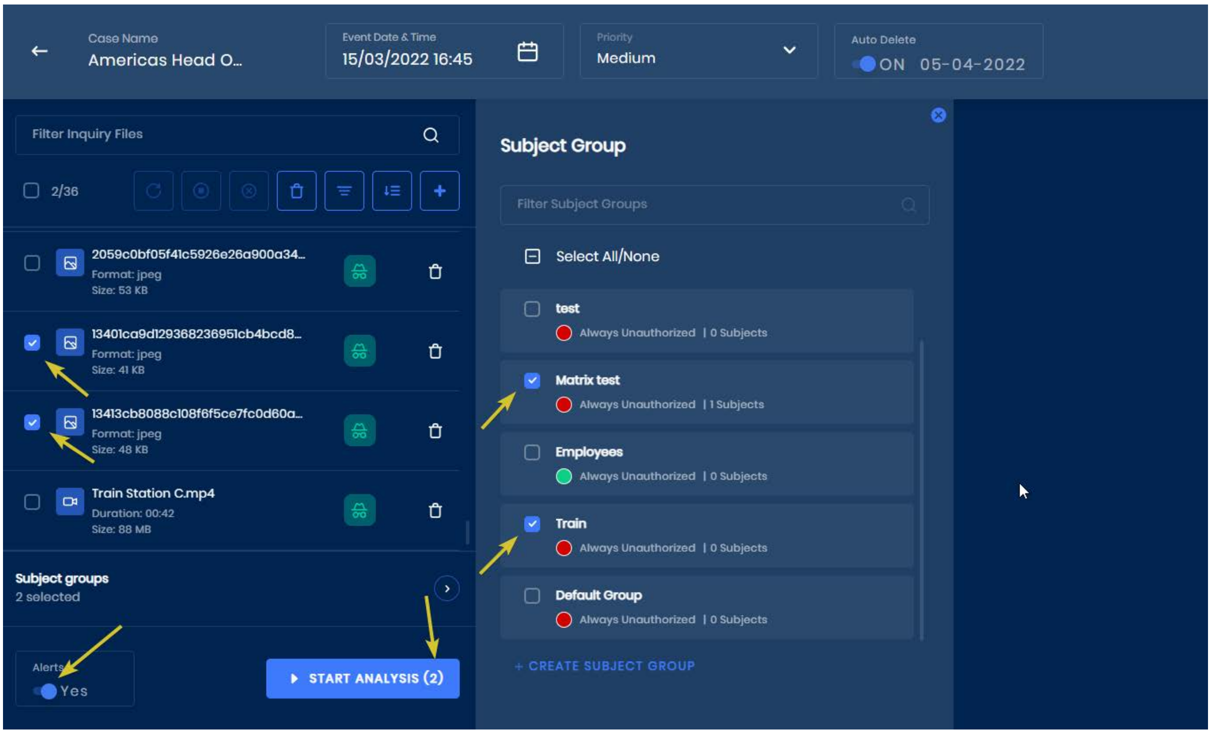
Custom Analysis Settings
Pipe: pipeng-0.pipeng...
Frame Rotate: Automatic
Auto Frame Skipping: OFF
Reduce GPU load by skipping frames and analyzing only a pattern of the video stream.
Analysis Percentage: 0 (0 – 100)
Region Of Interest (PX):
Top: 0 Right: 0 Bottom: 0 Left: 0

🚧 Note

AVI file preview will not show the upload preview due to browser constraints but will be shown after analysis

3. Each file can be chosen and settings changed, when these are saved the old analysis information (if previously analysed) will be removed from the system and the file will be ready for re-analysis
By selecting one or more files individually or selecting all items, the count of all items that are ready to be processed or reprocessed will show in the "Start Analysis". By clicking the "Start analysis" these files will start to be analysed.

The analysis will take place against all the watchlists but it is also possible to set up if you would like to receive alerts when recognition is detected, the alerts can also be set to specific groups.



Case Name: Americas Head O...
Event Date & Time: 15/03/2022 16:45
Priority: Medium
Auto Delete: ● ON 05-04-2022

Filter Inquiry Files

□ 2/36

	File	
□	2059c0bf05f41c5926e26a900a34... Format: jpeg Size: 53 KB	
☑	13401ca9d129368236951cb4bcd8... Format: jpeg Size: 41 KB	
☑	13413cb8088c108f6f5ce7fc0d60a... Format: jpeg Size: 48 KB	
□	Train Station C.mp4 Duration: 00:42 Size: 88 MB	

Subject groups
2 selected

Alerts: ● Yes

▶ START ANALYSIS (2)

Subject Group

Filter Subject Groups

□ Select All/None

- □ test — 🟥 Always Unauthorized | 0 Subjects
- ☑ Matrix test — 🟥 Always Unauthorized | 1 Subjects
- □ Employees — 🟩 Always Unauthorized | 0 Subjects
- ☑ Train — 🟥 Always Unauthorized | 0 Subjects
- □ Default Group — 🟥 Always Unauthorized | 0 Subjects

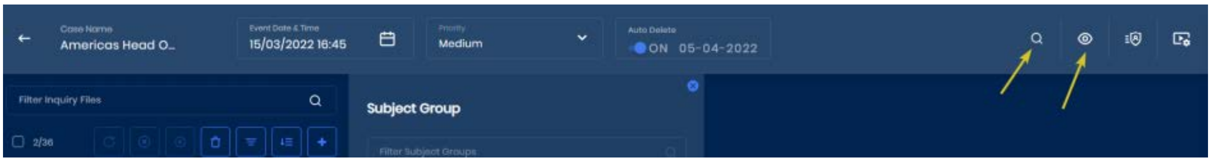
+ CREATE SUBJECT GROUP

The above shows two specifically selected files, ready to be analysed (medium) priority, with alerts, enabled against two specific subject groups.

Results

Once analysis is completed results can be seen in the view sources and search results components, these can be selected from the following menu within the inquiry cases.

View Sources
Search



Case Name: Americas Head O...
Event Date & Time: 15/03/2022 16:45
Priority: Medium
Auto Delete: ● ON 05-04-2022

Filter Inquiry Files

□ 2/36

Subject Group

Filter Subject Groups

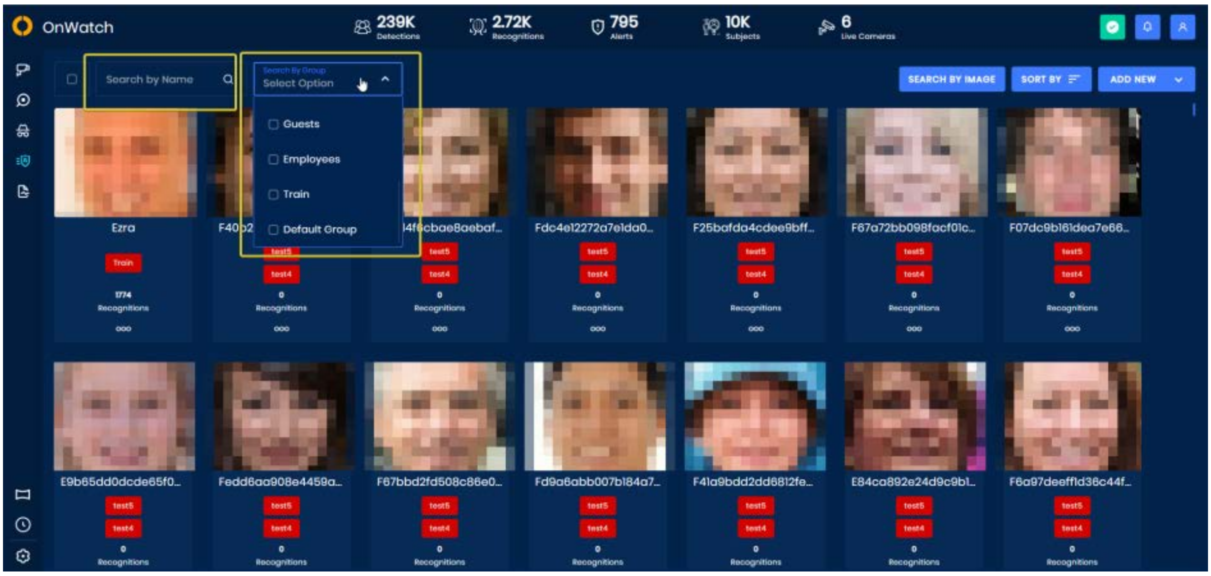
Search and Sort Subjects in the Watch List

There are a few ways to search for a subject in the watch list. You can:

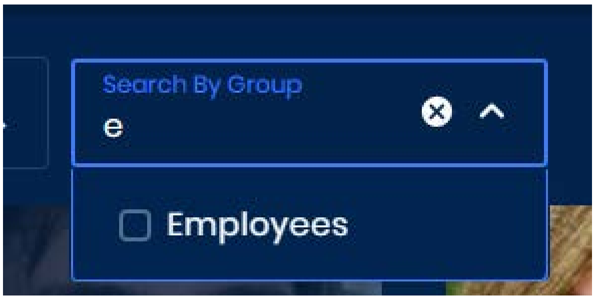
- Type the subject's name in the search bar
- Search for a subject based on the subject group their in through **Search by Group**
- Search for a subject using an uploaded image through **Search by Image**

Search by Group

1. In the Watch List tab, click Search by Group.

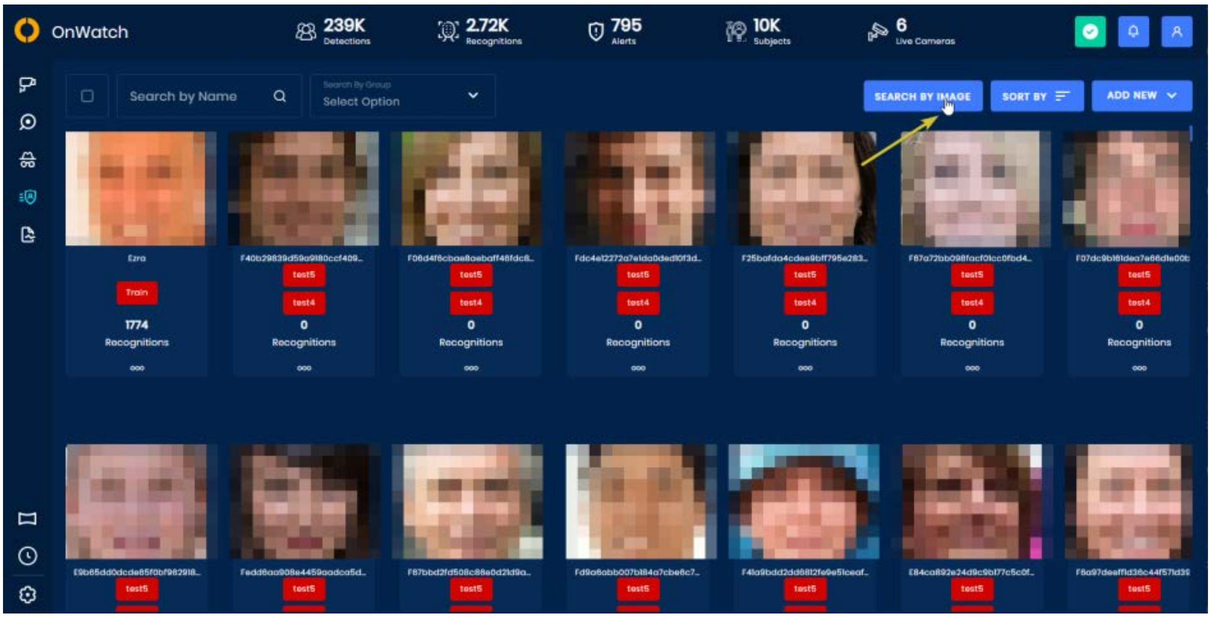


2. From the dropdown presented, select/search which group(s) you're searching for.
3. The system will display everyone in that subject group.

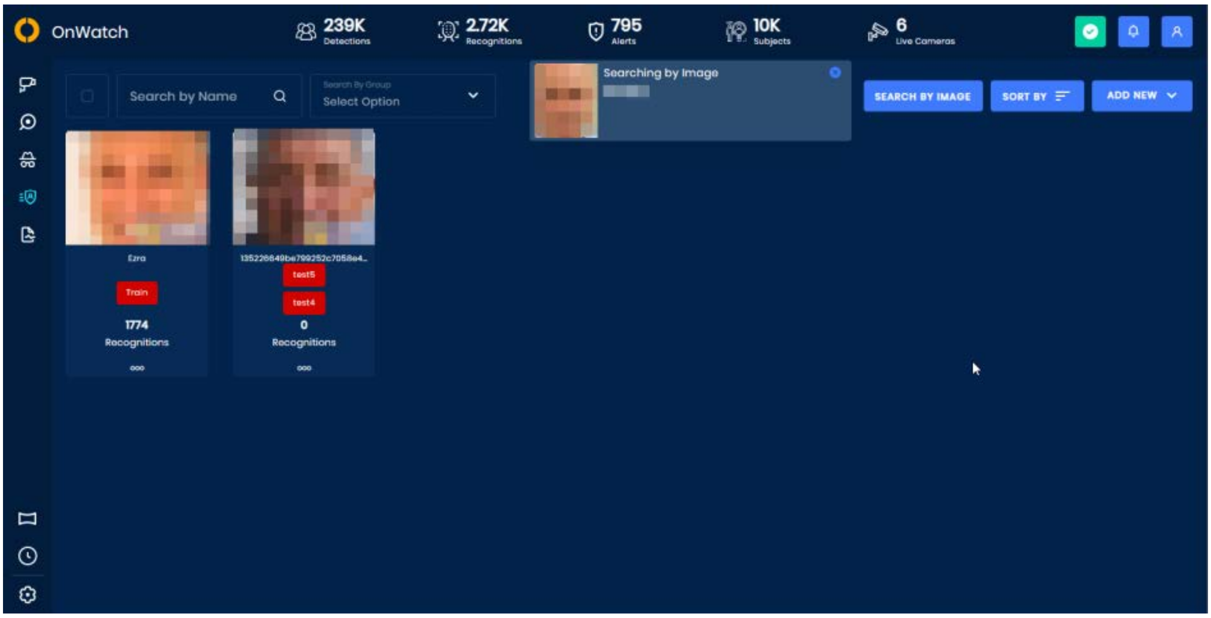


Search by Image

1. In the Watch List tab, click **Search by Image**.



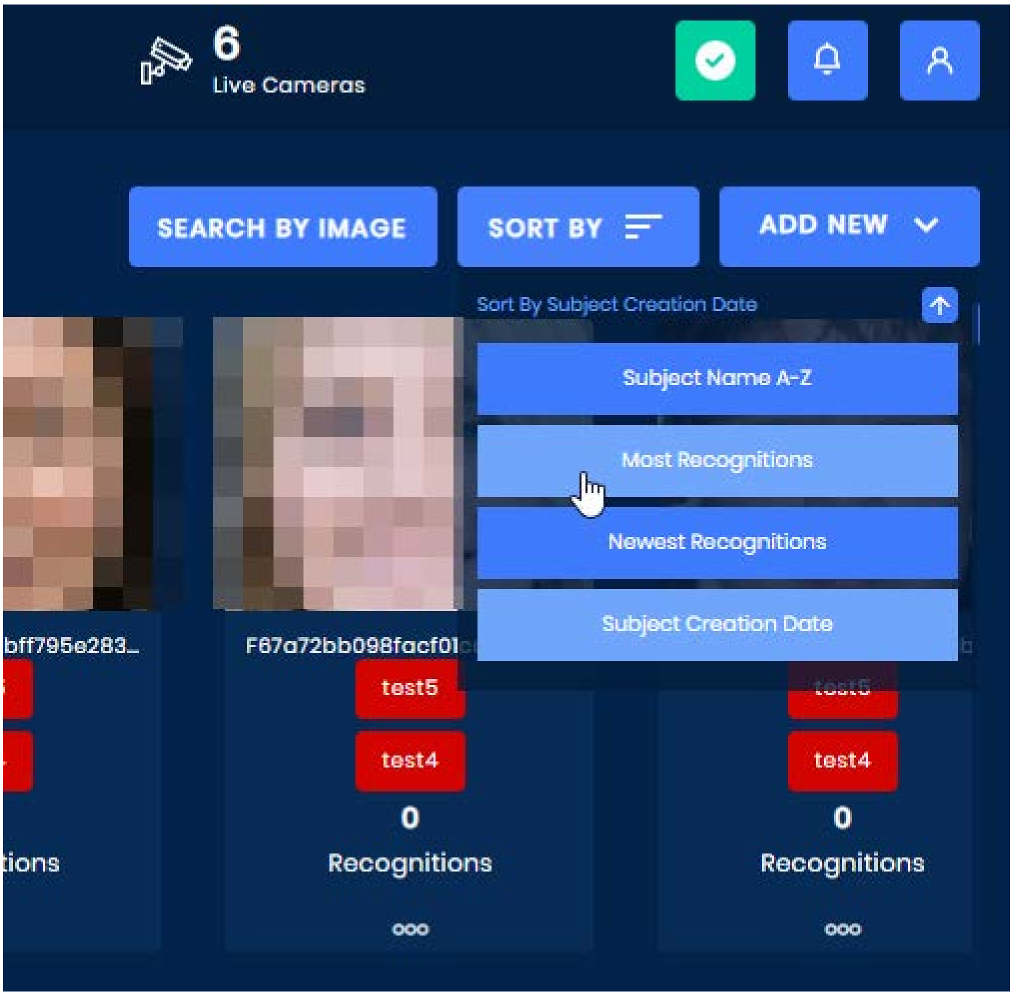
2. You will be requested to upload an image of the subject you are searching for.
3. The system automatically search and find the subject who matches the uploaded image. If there is no person that matches the uploaded image, you can add that person as a new subject.



Sort Subjects

Click **Sort By** to sort subjects by:

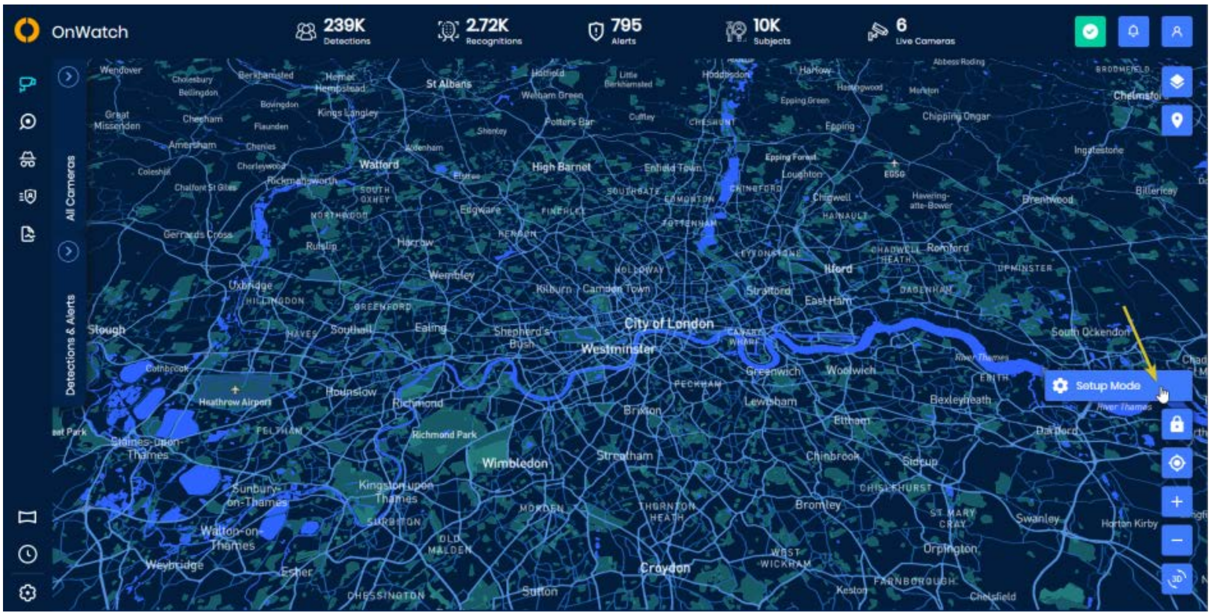
- Subject Name
- Most Recognitions
- Newest Recognitions
- Subject Creation Date



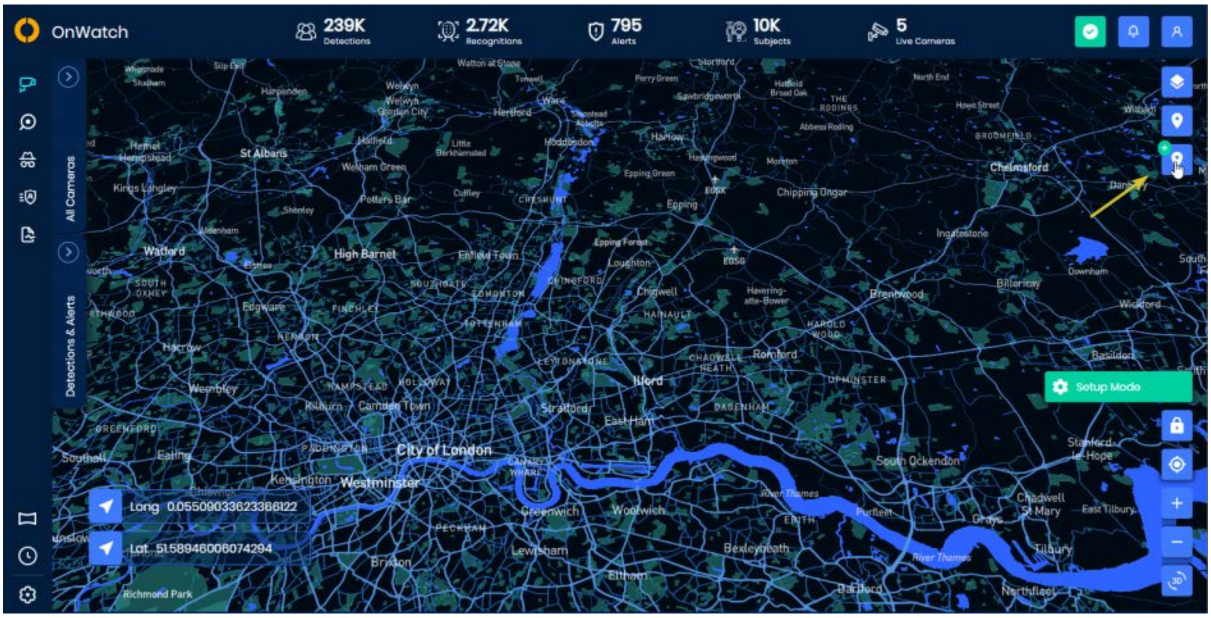
Set Up Zones on the Map

You can divide your cameras by zones. Set up zones from the **Live Cameras** map.

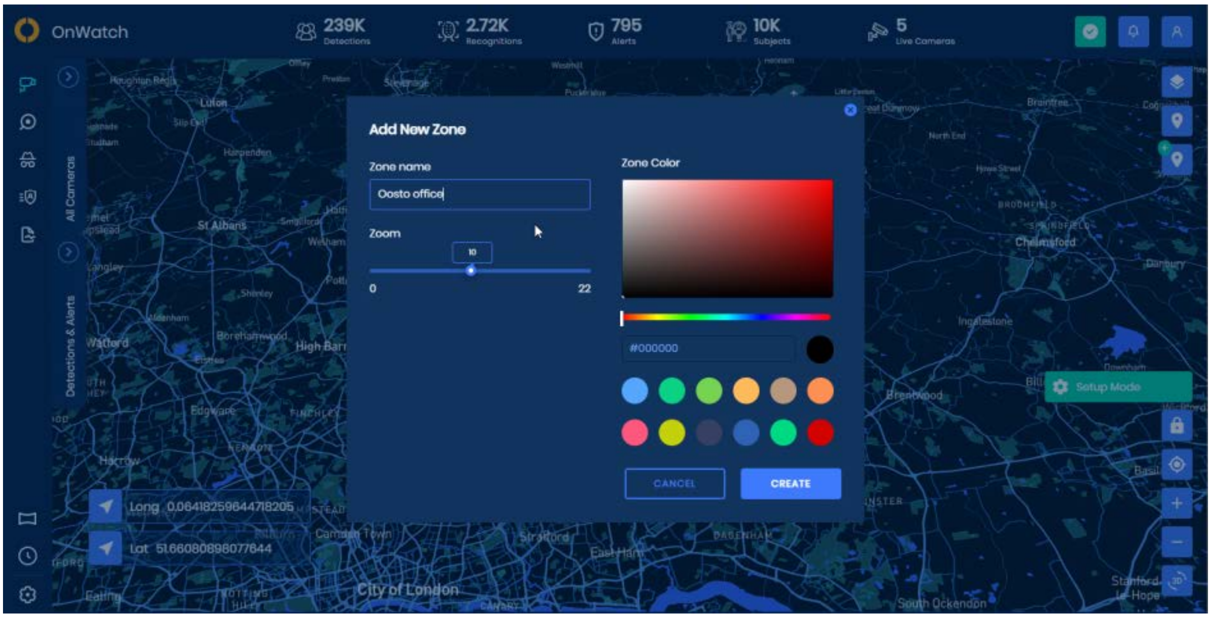
1. Click the **Setup** button to enter Setup Mode.



2. Tap the **Add Zones** button to create a new zone



3. Define a zone by clicking on the map by clicking on a specific location with your mouse.
4. Give the new zone a name, choose a color to define it, and click **Create**.


Add New Zone

Zone name: Oosto office

Zoom: 10 (0–22)

Zone Color: #000000

The new zone will appear on the map. You can move around zones by clicking the Zones button and choosing the zone you want to go to.

Track Real-Time or Historical Routes

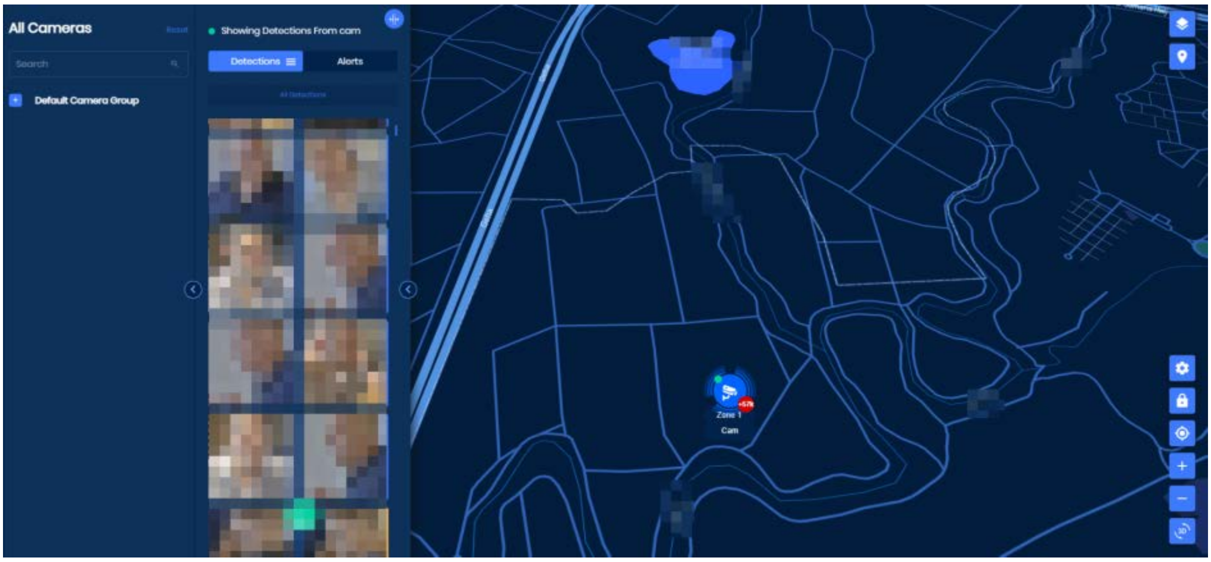
Follow a subject’s route to see where they came from, or where they went to next.

Real-time route - If a subject is currently being tracked by the cameras, you can see where they are now.
Historical route - See the routes a subject took during the last 24 hours.

> 🚧 You can only track the route of a subject who has been recognized by the system.

How to Track a Realtime Route

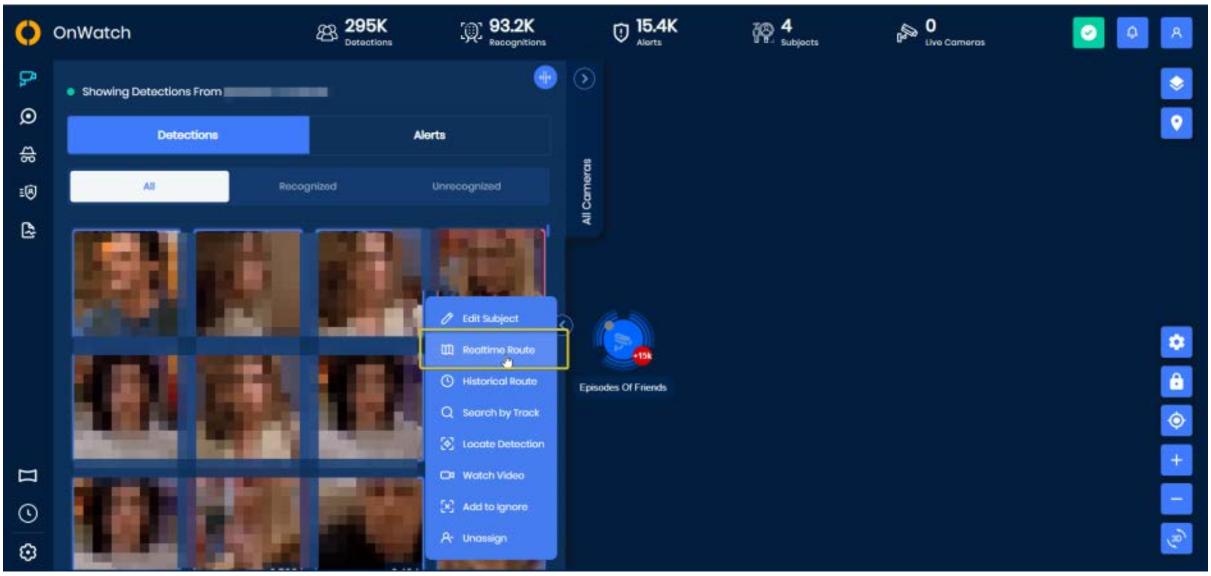
1. Navigate to the **Live Cameras** tab.



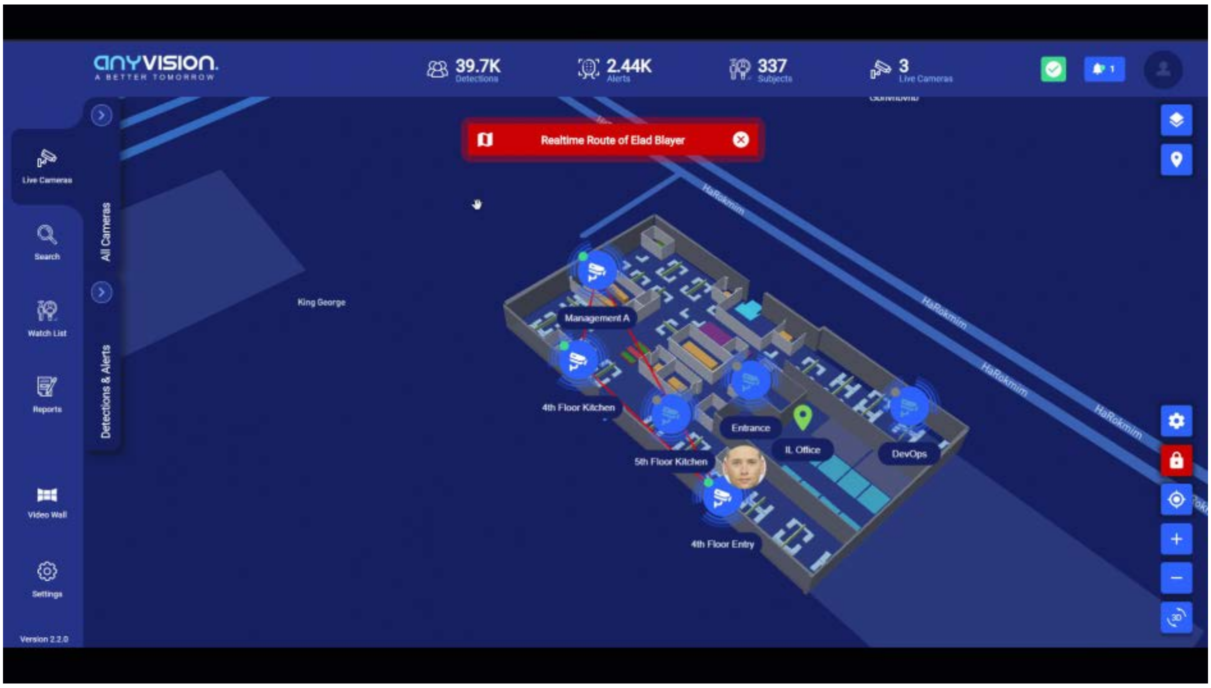
2. Hover over an image of a recognized subject in the *Detections & Recognitions* panel.

3. Click on the **three-dotted menu icon**.

4. Select **Realtime Route** from the drop-down list.

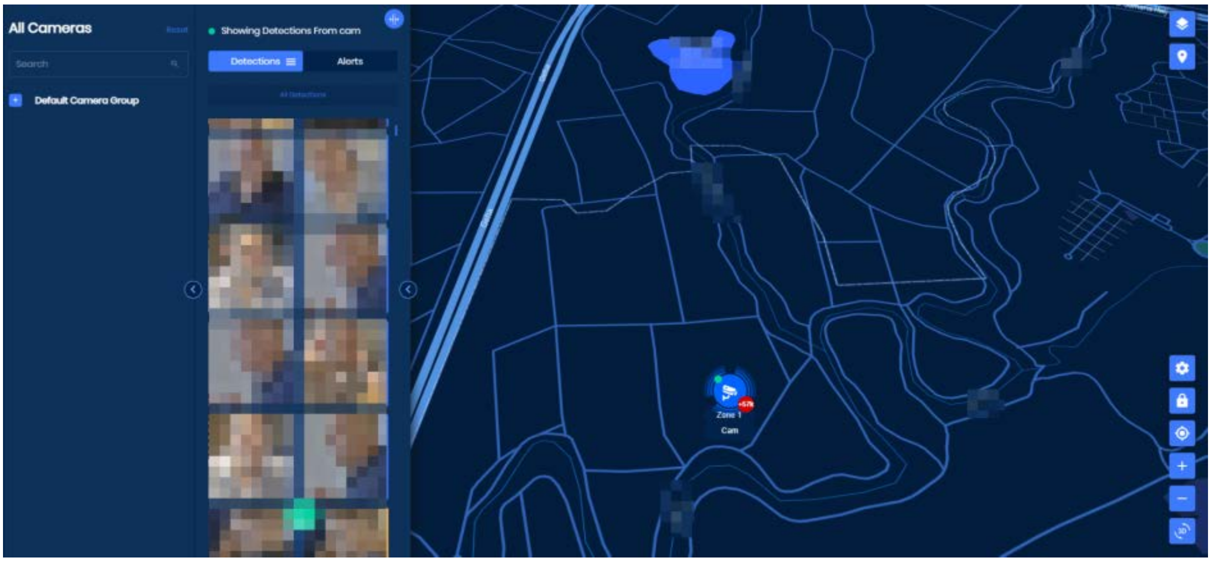


5. You will now see the route the subject is currently heading in as they move and are recognized by your cameras.

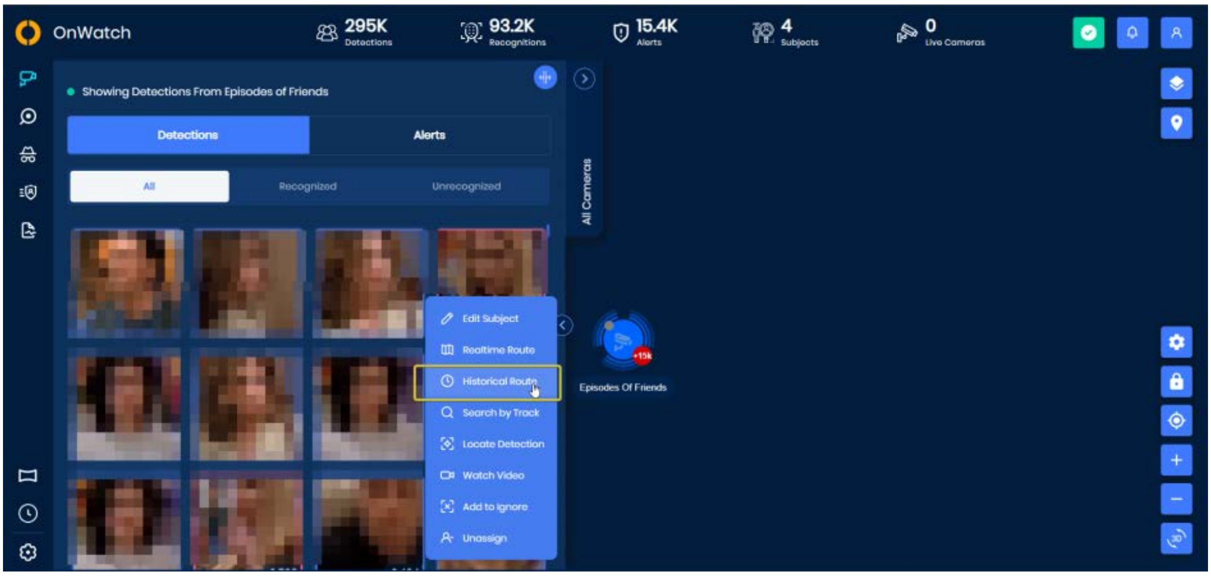


How to Track a Historical Route

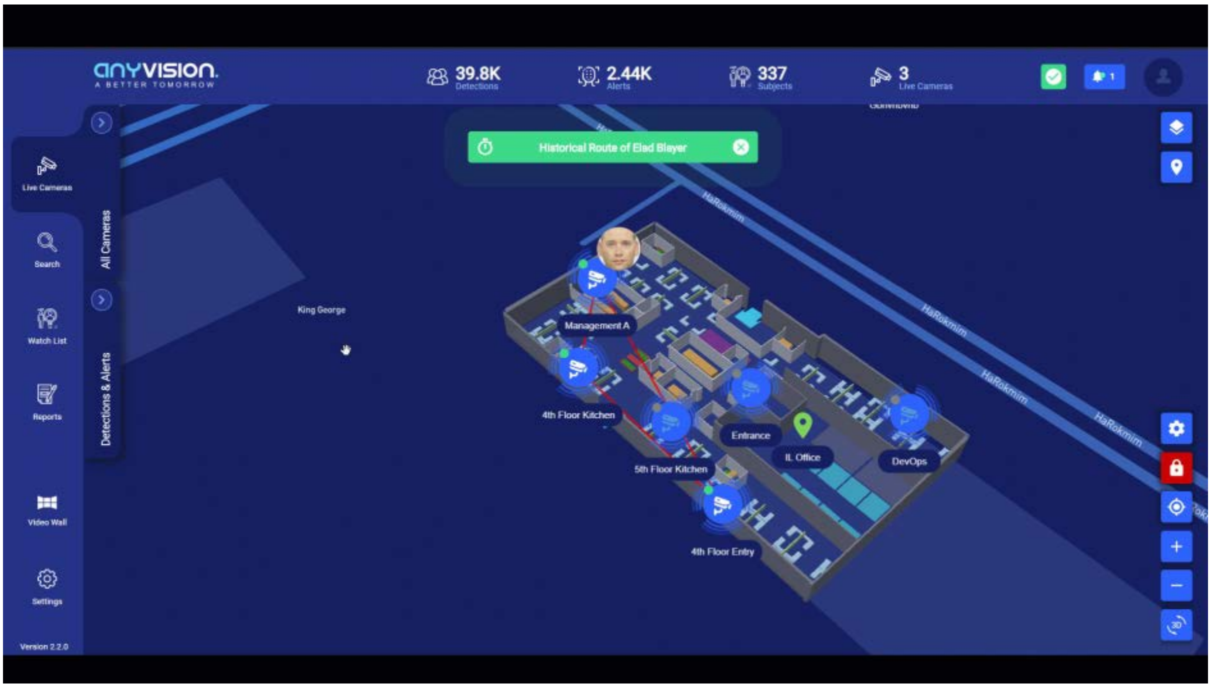
1. Navigate to the **Live Cameras** tab.



2. Hover over an image of a recognized subject in the *Detections & Recognitions* panel.
3. Click on the **three-dotted menu icon**.
4. Select **Historical Route** from the drop-down list.

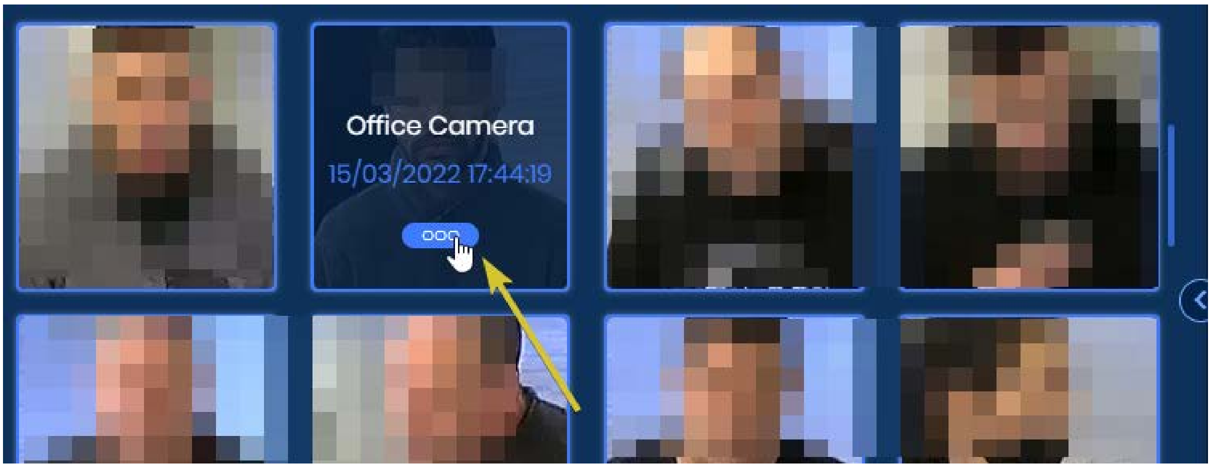


5. You will see now see the route the subject is taking now, in real-time, as captured by the cameras.

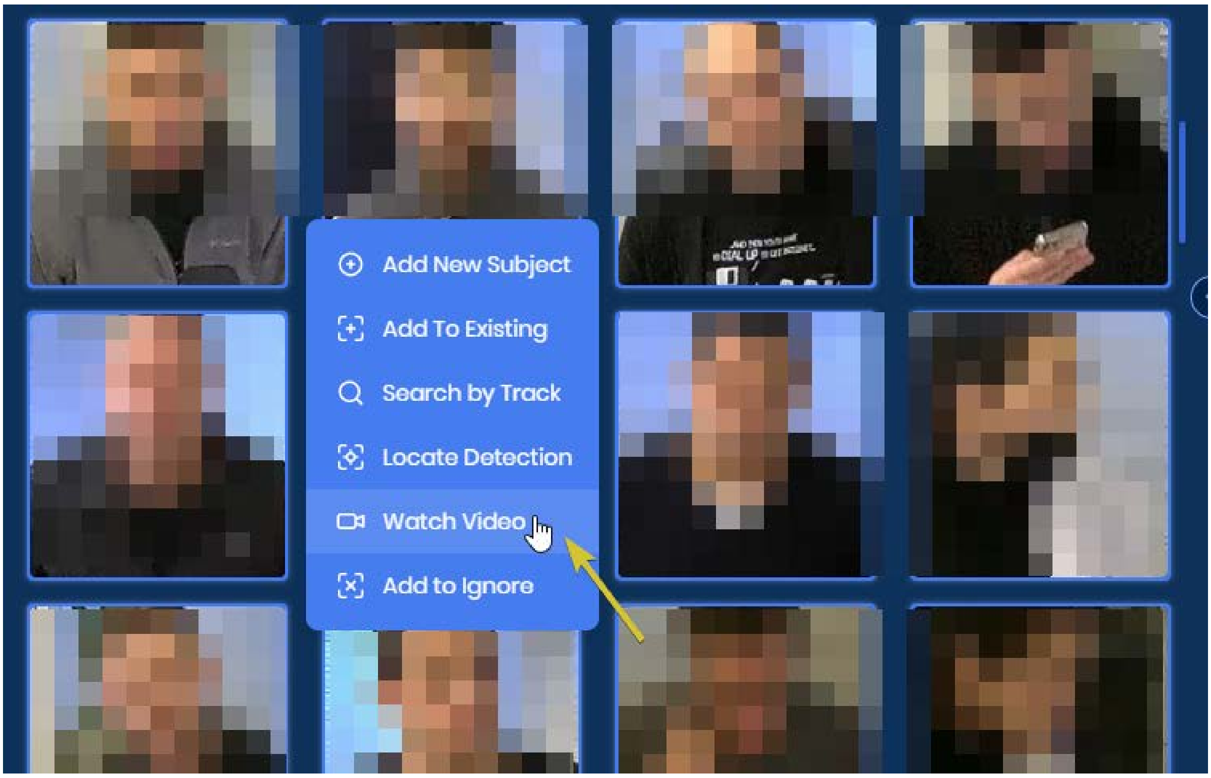


View a Detection Video

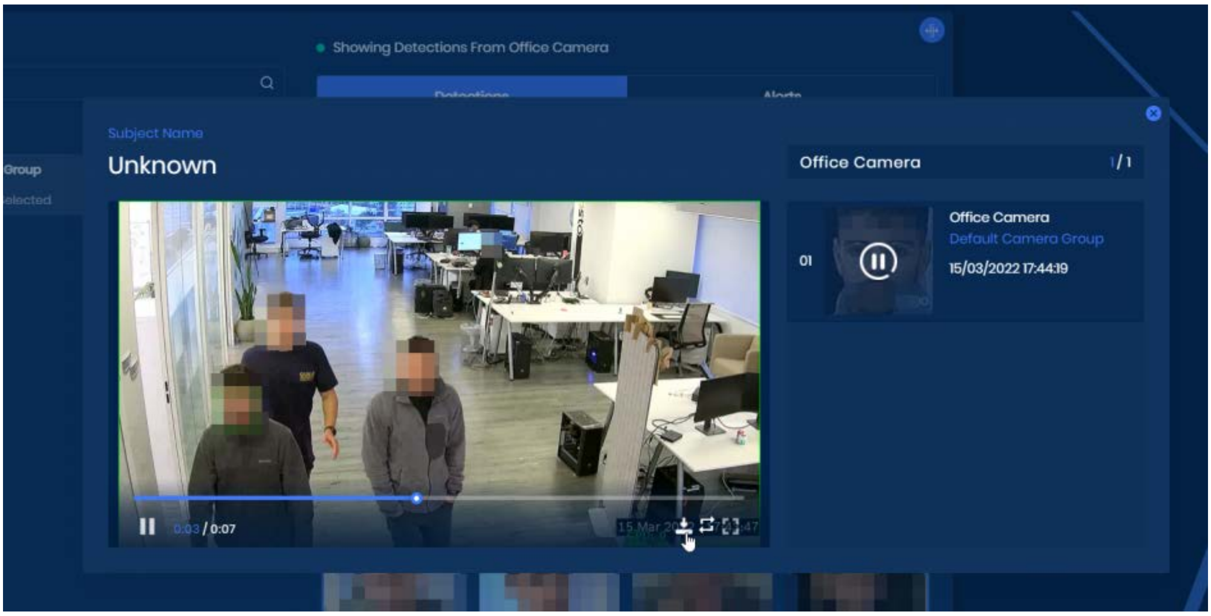
1. From the Live Cameras tab, hover over an image and click the **three-dotted menu** icon.



2. Choose **Watch Video**.



3. You can now view the playback for the specific detection and watch other related video playbacks of the same subject.



When a subject is detected, a square will show around their face. If there is more than one person in the video, only the face of the detected subject will have a square around it.

> **! Privacy**
>
> If GDPR mode is on, the faces of everyone other than the detected subject will be hidden. To enable privacy modes, navigate to *System Settings*.

VMS integrations

Overview

Customers want fewer interfaces, more information, and quick actions/responses in their control rooms.

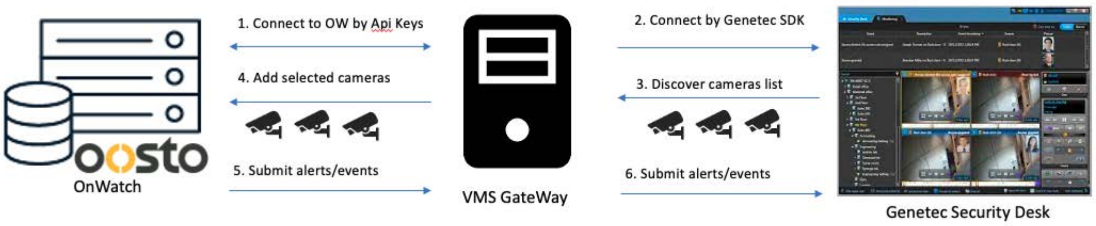
Many of our customers are already using Video Management Systems (VMS) for their security requirements. Almost every camera on the premise is connected via VMS systems allowing for easy management and centralized security policies.

It is possible to utilize Ootos VMS GateWay integration via the Oosto Api to communicate with the existing video security solution to configure and enhance it with AI analytics.

Integration support

Vendor	Product Name	Version	OnWatch API version	Plugin Creator
Genetec	Security Center	5.10	2.5.1, 2.6, 2.6.1	oosto
Genetec	Security Center	5.9	2.5.1, 2.6, 2.6.1	oosto

High Level Flow Diagram



Step 1
The VMS Gateway is connected to OnWatch with a defined account API

Step 2
The VMS gateway connects to Genetec via the Genetec SDK (see Genetec integration Guide)

Step 3
Discover the VMS cameras

Step 4
Choose which cameras to import into OnWatch to analyze the video stream

Step 5
OnWatch sends events and alarms with metadata to the VMS Gateway base on the imported cameras

Step 6
The VMS Gateway send events and alarm with metadata to Genetec

Genetec integration Guide

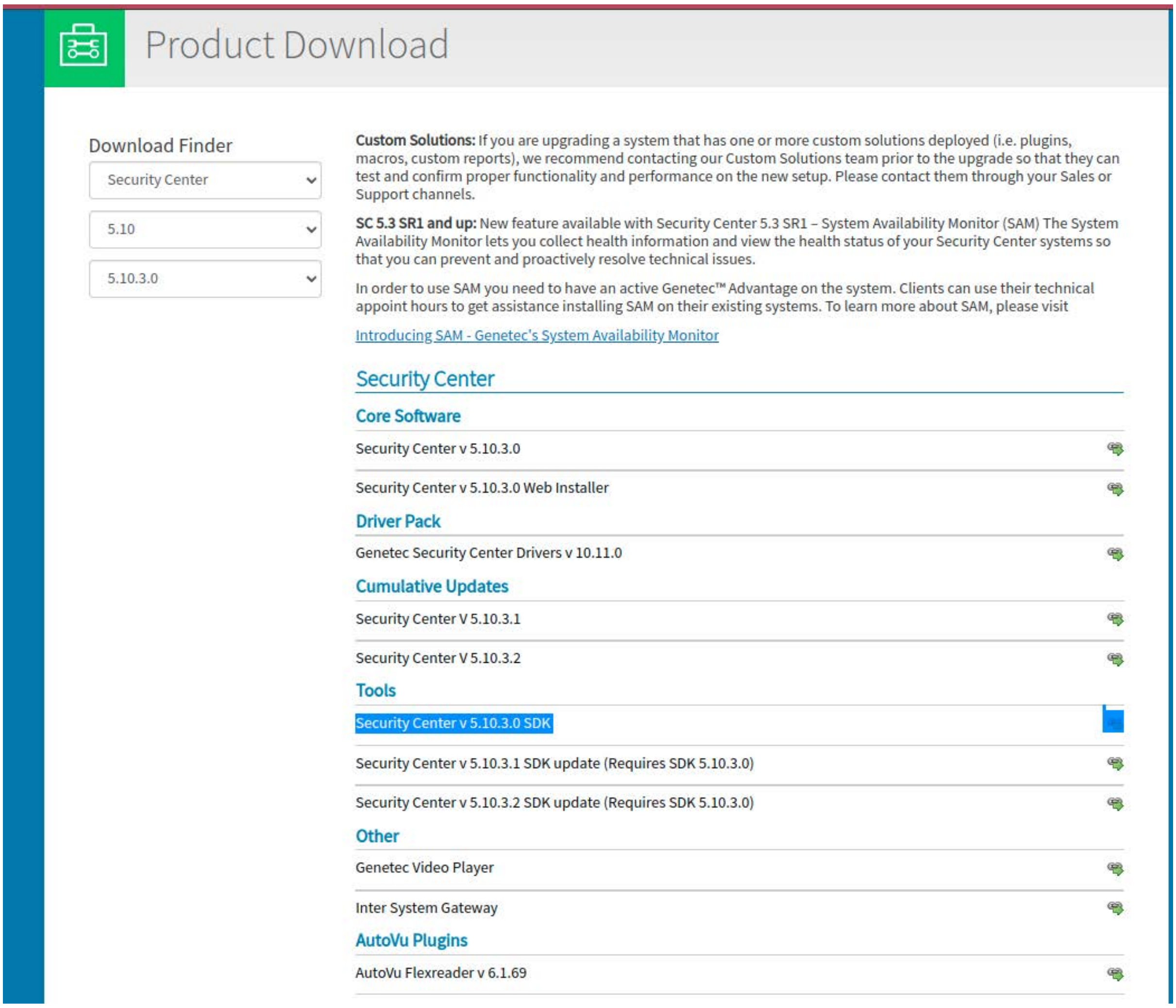
Pre-requirements -

On the GW server (Dev-windows machine)

- Windows OS

Install Genetec SDK with the relevant version

- Download from Genetec download center



Product Download

Download Finder

Security Center

5.10

5.10.3.0

Custom Solutions: If you are upgrading a system that has one or more custom solutions deployed (i.e. plugins, macros, custom reports), we recommend contacting our Custom Solutions team prior to the upgrade so that they can test and confirm proper functionality and performance on the new setup. Please contact them through your Sales or Support channels.

SC 5.3 SR1 and up: New feature available with Security Center 5.3 SR1 – System Availability Monitor (SAM) The System Availability Monitor lets you collect health information and view the health status of your Security Center systems so that you can prevent and proactively resolve technical issues.

In order to use SAM you need to have an active Genetec™ Advantage on the system. Clients can use their technical appoint hours to get assistance installing SAM on their existing systems. To learn more about SAM, please visit

Introducing SAM - Genetec's System Availability Monitor

Security Center

Core Software

Security Center v 5.10.3.0

Security Center v 5.10.3.0 Web Installer

Driver Pack

Genetec Security Center Drivers v 10.11.0

Cumulative Updates

Security Center V 5.10.3.1

Security Center V 5.10.3.2

Tools

Security Center v 5.10.3.0 SDK

Security Center v 5.10.3.1 SDK update (Requires SDK 5.10.3.0)

Security Center v 5.10.3.2 SDK update (Requires SDK 5.10.3.0)

Other

Genetec Video Player

Inter System Gateway

AutoVu Plugins

AutoVu Flexreader v 6.1.69

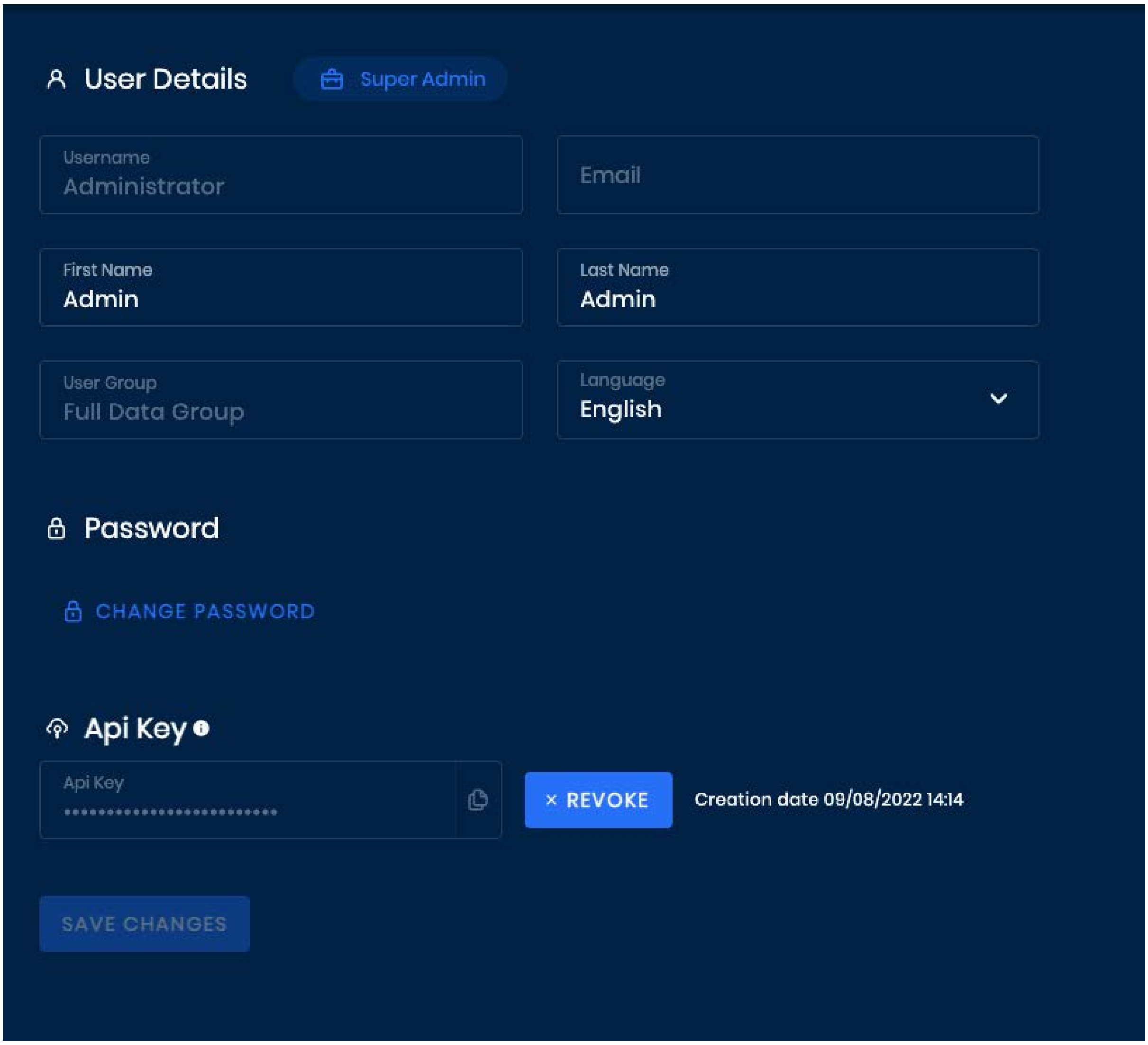
Install VMS GW
- Download vms gw

- Select “Genetec” for the plugin
- Note that the system will need to be rebooted after installation is complete

Download postman collection - Need Link

Setup flow

- Generate API keys from OnWatch (profile settings of Super Admin)



Username
Administrator

Email

First Name
Admin

Last Name
Admin

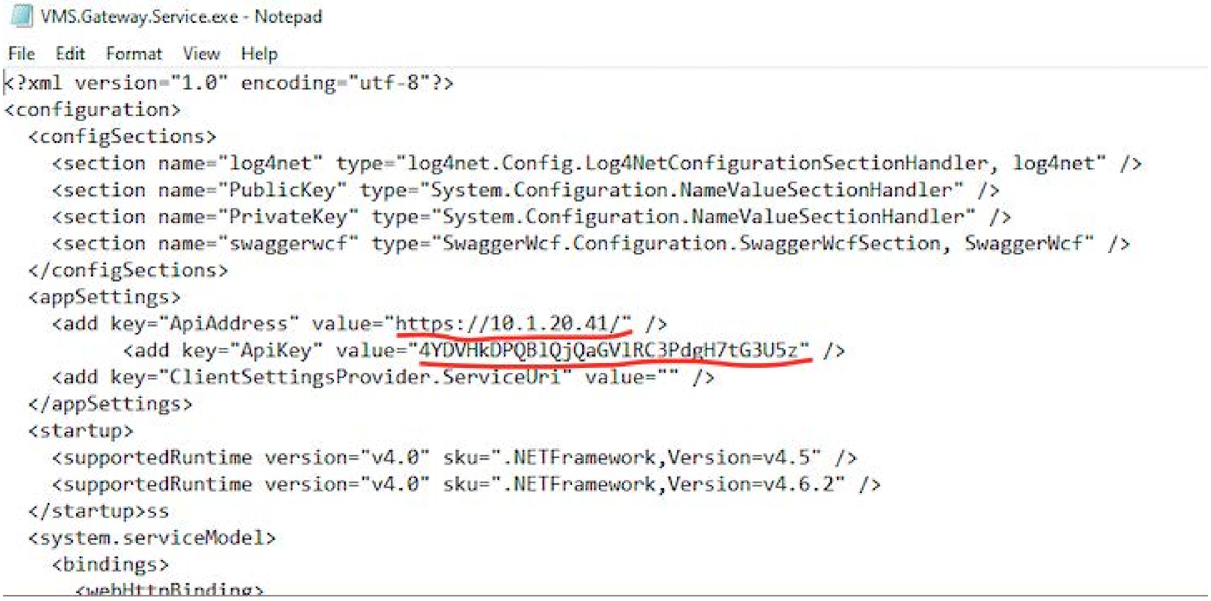
User Group
Full Data Group

Language
English

Api Key
••••••••••••••••••••••••

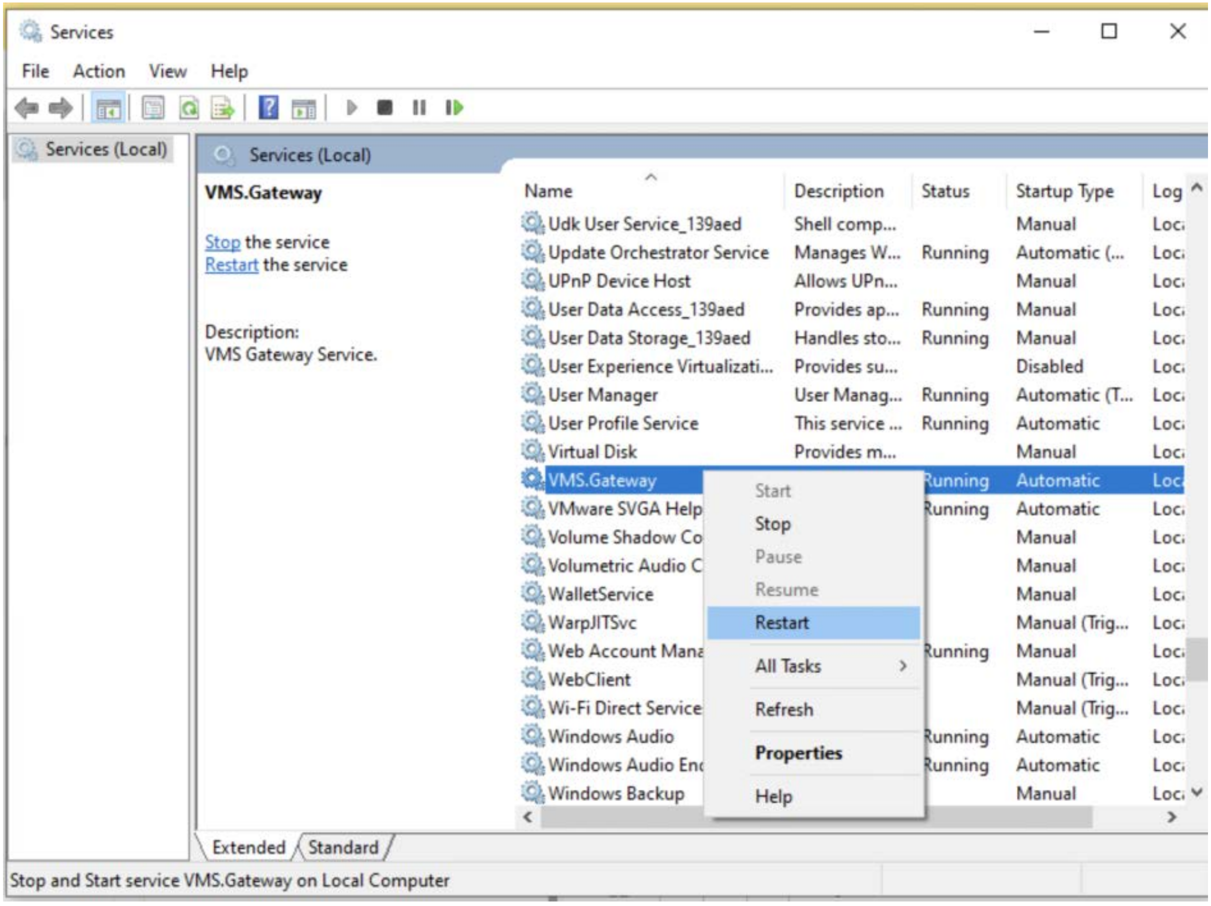
Creation date 09/08/2022 14:14

- Insert on the C:/programfiles(X86)/VMS/VMS.Gateway/VMS.Gateway.Service.exe.config the OnWatch IP + API Key
- Edit as an administrator via notepad



```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <section name="log4net" type="log4net.Config.Log4NetConfigurationSectionHandler, log4net" />
    <section name="PublicKey" type="System.Configuration.NameValueSectionHandler" />
    <section name="PrivateKey" type="System.Configuration.NameValueSectionHandler" />
    <section name="swaggerwcf" type="SwaggerWcf.Configuration.SwaggerWcfSection, SwaggerWcf" />
  </configSections>
  <appSettings>
    <add key="ApiAddress" value="https://10.1.20.41/" />
          <add key="ApiKey" value="4YDVHkDPQB1QjQaGV1RC3PdgH7tG3U5z" />
    <add key="ClientSettingsProvider.ServiceUri" value="" />
  </appSettings>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5" />
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.6.2" />
  </startup>ss
  <system.serviceModel>
    <bindings>
      <webHttpBinding>
```

- Restart VMS.Gateway service



VMS.Gateway

Stop the service
Restart the service

Description:
VMS Gateway Service.

Name	Description	Status	Startup Type	Log
Udk User Service_139aed	Shell comp...		Manual	Loc
Update Orchestrator Service	Manages W...	Running	Automatic (...	Loc
UPnP Device Host	Allows UPn...		Manual	Loc
User Data Access_139aed	Provides ap...	Running	Manual	Loc
User Data Storage_139aed	Handles sto...	Running	Manual	Loc
User Experience Virtualizati...	Provides su...		Disabled	Loc
User Manager	User Manag...	Running	Automatic (T...	Loc
User Profile Service	This service ...	Running	Automatic	Loc
Virtual Disk	Provides m...		Manual	Loc
VMS.Gateway		Running	Automatic	Loc
VMware SVGA Help		Running	Automatic	Loc
Volume Shadow Co			Manual	Loc
Volumetric Audio C			Manual	Loc
WalletService			Manual	Loc
WarpJITSvc			Manual (Trig...	Loc
Web Account Mana		Running	Manual	Loc
WebClient			Manual (Trig...	Loc
Wi-Fi Direct Service			Manual (Trig...	Loc
Windows Audio		Running	Automatic	Loc
Windows Audio Enc		Running	Automatic	Loc
Windows Backup			Manual	Loc

Stop and Start service VMS.Gateway on Local Computer

- To create the integration need to run a few Postman commands.

Import the attached postman collection to postman
To login to the OnWatch API -

- Run 'login'
- Copy and save Token from the response

To get the installed plugin information into the VMS GW service data -

- Run 'GetPlugins'
- add a token to the header
- The response should be 'Genetec'

If you want to Add/Update/Delete VMS information-
Add -

- Run 'Add VMS'
- add a token to the header
- Add the relevant server information
- The 'Name' should be 'Genetec'

Configuration options -
EventFilter- Filter of which event show at Genetec machine.

- 0- none
- 1- recognized event
- 2- unrecognized event
- 3 - all event (default)

Update -

- Run ‘Update VMS’
- add a token to the header
- Update the relevant VMS information on the body

Delete -

- Run ‘Delete VMS’
- add a token to the header
- add VMS id from ‘Get vms list’ response to the command

To get the current VMS information on the VMS GW service -

- Run ‘Get vms list’
- add a token to the header
- The response should be VMS details
- in case there is no VMS, need to add VMS by ‘add vms’

To connect the GW to the VMS system

- Run ‘connect’
- add a token to the header
- add VMS id from ‘Get vms list’ response to the command
- The response should be '1'

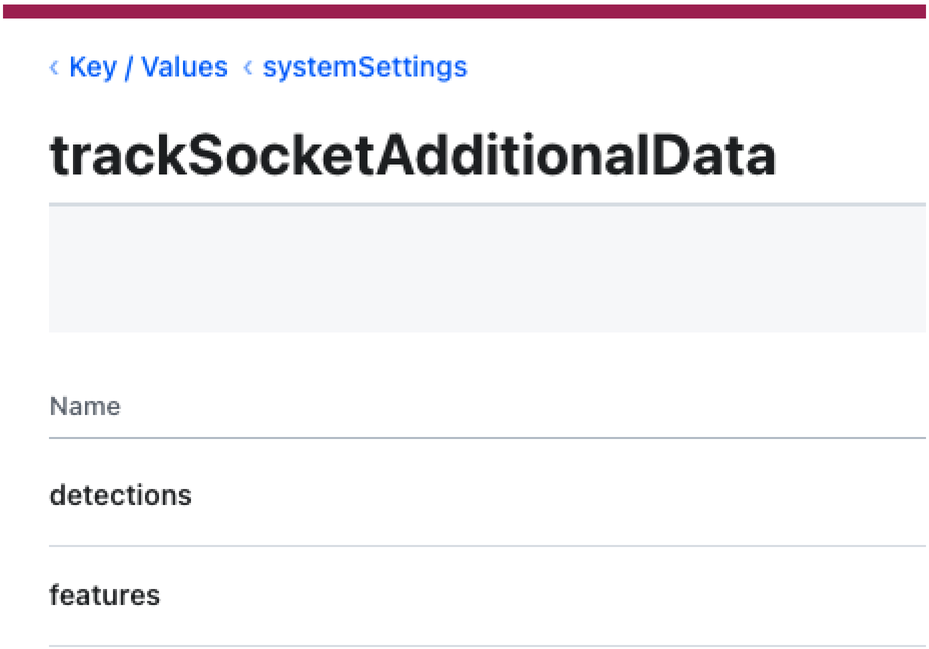
To get the VMS cameras list

- Run ‘get camera list’
- add token to the header
- add vms id from ‘Get vms list’ response to the command
- The response should be the list of the VMS cameras
- ‘IsImported’ attribute indicates if the camera is already been imported to the OW via the GW.

To add the cameras to the OW server

- Run ‘add cameras’
- add token to the header
- add vms id from ‘Get vms list’ response to the command
- add cameras details from ‘get cameras list' response
- The response should be 200 with output like success: list of cameras....”
- Cameras will be added immediately to the OnWatch server

##OnWatch side -
For a better playback and detections stream quality add to the camera collaboration -
rtsp_transport=tcp
change on consul to true -



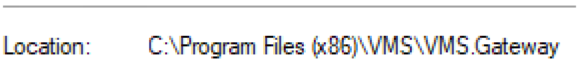
trackSocketAdditionalData

Name
detections
features

Events should appear on the Genetec VMS

Debug tools -

-postman error responses
-Logger file



Location: C:\Program Files (x86)\VMS\VMS.Gateway

Resources

User Roles & Groups Breakdown

Within OnWatch, **Roles** determine the functions a user can do within the system, while **User Groups** determines what data users can see.

User Groups

Within an organization, members of different teams may need different viewing access within the system. For each new user group, define access permissions to specific camera groups and subject lists.

The user groups distinguish between what users can see. For example, a security staff group at a casino may need to see only known criminals, while another team needs to see VIPs. User groups channel the data to the appropriate audience.

By default, the system comes with a "Full Data Group", meaning everyone can see everything.

User Roles

Different user roles allow for different levels of activity within an organization. Establish roles and permissions for users by categorizing each one as either a Viewer, Operator, Super Operator, Admin, or Super Admin when creating an account for each user. These options are intended to provide flexibility for the user - there is no need to use all of them, although you can.

Because system users can have different access permissions for the data they see and the actions they can take, it's important to understand the differences between each role.

Viewer

Viewers have the lowest permission level they can view system information but cannot perform actions in the system. For example, lower-level security guards or people on marketing teams who may want to view information may be logged in as viewers.

Viewers also do not have any Settings permissions, and can only view the System's Status in Settings. If a viewer attempts to act as the system, and they do not have permission to do so, they will immediately be logged out of the system.

Operator

Operators can't make changes to the watchlist, pull reports, add subjects, but they can perform other actions in the system, like searching.

Super Operator

Super Operators can perform all actions except those within *Admin Settings*. A super operator might be a general manager.

Sub Admin

Sub Admins have derived rights to different cameras and subject groups like Super Operators but they have some additional administrative abilities such as adding/removing cameras. This role was added to allow customers to continue to add entities without gaining access to the system installer's or integrator's full capabilities whilst still being limited to

specific content.
As part of 2.6 release, super-operators in 2.5 and below are migrated to be sub-admin

Admin

Admins can create users and perform all actions in the system. They have the highest level of access aside from the system's single Super Admin.

Super Admin

Super Admins have the highest permission level. They are owners of the system and are in charge of setting up OnWatch. Only one person within an organization can be the Super Admin, whereas all other roles can have unlimited members. Super Admins create and manage all accounts, and oversee all activity.

User Roles Chart

Location	Function	Viewer	Operator	Super Operator	Sub Admin	Admin	Supe Admi
Live Cameras	View Detections	✓	✓	✓	✓	✓	✓
Live Cameras	View POI	✓	✓	✓	✓	✓	✓
Live Cameras	View Timeline	✓	✓	✓	✓	✓	✓
Live Cameras	View Recognition Color	✓	✓	✓	✓	✓	✓
Live Cameras	View New Alerts	✓	✓	✓	✓	✓	✓
Live Cameras	Select / Deselect Cameras	✓	✓	✓	✓	✓	✓
Live Cameras	Download Timeline		✓	✓	✓	✓	✓
Live Cameras	Watch Video from Timeline		✓	✓	✓	✓	✓
Live Cameras	Search by Track		✓	✓	✓	✓	✓
Live Cameras	Watch Video		✓	✓	✓	✓	✓
Live Cameras	Route View		✓	✓	✓	✓	✓
Live Cameras	Add to Ignore			✓	✓	✓	✓
Live Cameras	Add New Subject			✓	✓	✓	✓
Live Cameras	Add to Existing			✓	✓	✓	✓
Live Cameras	Tracking			✓	✓	✓	✓
Live Cameras	Acknowledge Alert			✓	✓	✓	✓
Search	Search by	✓	✓	✓	✓	✓	✓

Location	Function	Viewer	Operator	Super Operator	Sub Admin	Admin	Supe Admi
	Gender						
Search	Search by Date	✓	✓	✓	✓	✓	✓
Search	Search In	✓	✓	✓	✓	✓	✓
Search	Filter By	✓	✓	✓	✓	✓	✓
Search	Search by Threshold	✓	✓	✓	✓	✓	✓
Search	Inquiry Cases	✓	✓	✓	✓	✓	✓
Search	Search by Image		✓	✓	✓	✓	✓
Watch List	Sort Watch List	✓	✓	✓	✓	✓	✓
Watch List	Search by Group	✓	✓	✓	✓	✓	✓
Watch List	Search by Name	✓	✓	✓	✓	✓	✓
Watch List	Search by Image		✓	✓	✓	✓	✓
Watch List	Add New			✓	✓	✓	✓
Watch List	Mass Import			✓	✓	✓	✓
Watch List	Delete			✓	✓	✓	✓
Watch List	Edit			✓	✓	✓	✓
Inquiry	Create, Edit, Delete Case			✓	✓	✓	✓
Settings	Access System Settings				• Acknowledge Actions	✓	✓
Settings	Access Engine Settings					✓	✓
Settings	Access Device				• Camera Settings	✓	✓

Location	Function	Viewer	Operator	Super Operator	Sub Admin	Admin	Supe Admi
	Settings						
Settings	Access Groups & Profiles				✓	✓	✓
Settings	Manage Accounts					✓	✓
Settings	Create Admin Accounts						✓

- = Partial Access

The Concept of Collate

This guide goes over what collate is and lists the OnWatch features that require collate.

What is a Collate?

Collate is a concept in OnWatch that combines two or more tracks of a specific person that occur within 30 seconds of each other (the time frame is configurable). The objective of this feature - and the reasoning behind combining these tracks - is to ensure the system recognizes the same face from separate tracks as one person.

Whenever multiple tracks are combined or are collated, a unique collate ID is given to represent that group of tracks.

Let's say, for example, that a subject is captured by the system, and a track is therefore created. 30 seconds later, the subject is captured again, but this time, the subject and the track received a low recognition score (one below the threshold). After a few more seconds, the subject is captured again with a high score.

For the system to include that second track - the one with the low score - as a recognition of the subject, the system will collate these tracks together, providing them with a single collate ID.

API Use Cases

VMS Integration

Overview

The OnWatch API allows organizations that utilize video management systems to integrate with OnWatch to subscribe to specific events. The integration works by live-streaming camera footage from a video management system, analyzing the footage in real-time, and generating metadata whenever a face or body is captured within the camera's field of view.

These occurrences are called events. Whenever a subscribed occurrence takes place, an event is sent out to the socket.

The following events are available for subscription. You can subscribe to all events or just to specific events that are relevant to your use case.

WebSocket	Description
track:created	A detection of an unknown person took place
recognition:created	A recognition of a subject took place
camera:changed	One or more parameters of a camera were changed
camera:deleted	A camera was deleted from OnWatch

For example, if you subscribe to track:created, whenever an unknown person is captured on one of your connected cameras, you will receive a push notification.

Integration Process

Integrate your VMS with OnWatch by:

1. Streaming live cameras from your VMS, and
2. Subscribing to WebSockets.

> 👍 **Default Base URL**
>
> Remember, the default base URL for the OnWatch API is https://kong.tls.ai. However, based on your use case, it might change. Please speak to your system administrator for more information.

Stream Cameras in OnWatch

Use the POST /bt/api/cameras route to stream your VMS camera and include relevant camera parameters within the request body.

Default values will be used for all parameters that are not provided within the request body.

> ### 🚧 Assign the Camera to a Camera Group
>
> You'll need to associate the camera with a Camera Group. Get a list of all your Camera Groups using the GET /bt/api/cameras/groups route. To learn more on how to create a Camera Group, click here.

Here is an example request body:

JSON

```json
{
    "title":"string",
    "description":"",
    "cameraGroupId":"00000000-0200-4c1b-4e12-1ba74bff4a4b",
    "restriction":false,
    "isEnabled":true,
    "location":[34.855499,32.109333],
    "videoUrl":"rtsp://username:password@210.12.23.32/camera",
    "threshold":0.55,
    "configuration":{
        "preview":false,
        "frameRotation":-1,
        "webRTC":false,
        "ffmpegOptions":"",
        "trackMinLength":4,
        "trackMaxLength":200,
        "frameSkip":{
            "autoSkipEnabled":true,
            "percent":0
        },
        "trackerSeekTimeOut":45,
        "cameraMode":[1]
    },
    "pipe":"",
    "isLoadBalancingEnabled":true,
    "isAlternativeThresholdEnabled":false,
    "alternativeThreshold": null,
    "timeProfileId":null
}
```

The response body of the API call will display the newly added camera's details.

Subscribe to Events

Subscribe to All Events

Use the connect socket to subscribe to all events, including the recognition of a subject and the detection of an unknown person.

Subscribe to Specific Events Only

To subscribe to track:created, click here.
To subscribe to recognition:created, click here.
To subscribe to camera:changed, click here.
To subscribe to camera:deleted, click here.

API Docs

Activate License

You can activate your OnWatch license using the POST /bt/api/bt-licensing/activation/online/activate route and providing your license code (given by Oosto) within the request body of the API call.

Example Request Body:

JSON

```
{
  "licenseCode": "0123456789876543 21"
}
```

Within the response of the request, receive your system license details, including when your license expires, how many cameras can be connected, and even how many members can be added to your watch list.

Add Cameras

Connect cameras to OnWatch to analyze the video stream and detect subjects in real-time. Every camera needs to be associated with a Camera Group, so we suggest creating all your groups first.

Camera Groups allow you to better search and access information from the system. For example, if I have 5 cameras in the lobby of a building, I may want to group those cameras to get a better idea of what is going on there. Because of that, we suggest grouping your cameras based on their purpose and location.

In addition, Camera Groups can be used to configure access permissions for certain users of the system. For example, under Account Management in *Settings*, you can create User Groups where each group is allowed to view recognition data only from the cameras in certain Camera Groups.

Create New Camera Groups

The POST /bt/api/cameras/groups route can be used to create a new Camera Group.

You'll need to provide a title for the Camera Group within the request body. It's **optional** to also include a description of the group and the IDs of any camera you may already have connected to the system.

JSON

```
{
    "title":"Large Meeting Room",
    "description": "All cameras that are currently active in the large meeting room."
}
```

When you finish creating all your groups, you'll want to run the GET /bt/api/cameras/groups route. This will display all the groups you have created in the system and what their respective ID number is. Use the ID in the next route to associate the newly connected camera to your group of choice.

Add Camera to the System

Use the POST /bt/api/cameras route to create a camera in the system and include relevant camera parameters within the request body.

Default values will be used for all parameters that are not provided within the request body.

Here is an example request:

JSON

```json
{
    "title":"string",
    "description":"",
    "cameraGroupId":"00000000-0200-4c1b-4e12-1ba74bff4a4b",
    "restriction":false,
    "isEnabled":true,
    "location":[34.855499,32.109333],
    "videoUrl":"rtsp://username:password@210.12.23.32/camera",
    "threshold":0.55,
    "configuration":{
        "preview":false,
        "frameRotation":-1,
        "webRTC":false,
        "ffmpegOptions":"",
        "trackMinLength":4,
        "trackMaxLength":200,
        "frameSkip":{
            "autoSkipEnabled":true,
            "percent":0
        },
        "trackerSeekTimeOut":45,
        "cameraMode":[1]
    },
    "pipe":"",
    "isLoadBalancingEnabled":true,
    "isAlternativeThresholdEnabled":false,
    "alternativeThreshold": null,
    "timeProfileId":null
}
```

The response body of the API call will display the newly added camera's details.

Possible Errors

Error	HTTP Status
`ERR_ROUTE_SCHEMA_VALIDATION`	400
`ERR_CAMERA_TITLE_IS_INVALID`	400
`ERR_DELETE_DEFAULT_CAMERA_NOT_ALLOWED`	400
`ERR_ERR_GROUP_IN_USE`	400
`ERR_GROUP_HAS_CAMERAS`	400
`ERR_CAMERA_NOT_FOUND`	404
`ERR_REGION_NOT_FOUND`	404
`ERR_CAMERA_GROUPS_NOT_FOUND`	404
`ERR_CAMERA_ALREADY_EXISTS`	409
`ERR_REGIONS_ALREADY_EXISTS`	409
`ERR_CAMERA_GROUP_ALREADY_EXISTS`	409
`ERR_CAMERA_IS_NOT_CONNECTED`	412
`ERR_CAMERA_ALREADY_CONNECTED`	412
`ERR_STOP_CAMERA_SERVER_ERROR`	500
`ERR_START_CAMERA_SERVER_ERROR`	500
`ERR_DELETE_CAMERA_SERVER_ERROR`	500
`ERR_FAILED_TO_GET_CAMERA_DEFAULT_SETTINGS`	503
`ERR_NO_AVAILABLE_BACKEND`	503

Manage Users

Add Users to the System

The POST /bt/api/users route allows you to add new users to the OnWatch system via API. We suggest creating a user account for every team member who will have access to OnWatch.

Here is an example request:

JSON

```json
{
  "username": "johnDough",
  "password": "string",
  "email": "email@mail.com",
  "firstName": "John",
  "lastName": "Dough",
  "roleId": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "userGroupId": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "isActive": true,
  "isMobileAccessEnabled": true,
  "avatarUrl": "avatar-uri/avatarPicture.jpeg",
  "description": "string",
  "location": [
    31,
    31
  ],
  "phoneNumber": "string",
  "timezone": "Asia/Jerusalem",
  "locale": "en_us"
}
```

The response of the API call will include confirmation that the new user was added and will display the user's details based on what was provided in the request.

Delete a User from the System

The DELETE /bt/api/users/{id} route allows you to delete a user from the system. Input the ID number of the user as a path parameter within the request.

If you don't know the ID number of the user, you can use the GET /bt/api/users route. Within the response of the route, you will get a list of all active users and their ID numbers.

Add Subjects to the Watchlist

Upload a New Subject to the Watch List

Before you can add a subject to the watch list using an external image, you will need to extract the facial features of the subject and create a cropped image using the POST /bt/api/external-functions/extract-faces-from-image route.

Once you finish extracting the facial features, the response of the API call will provide you with an array of features (in numbers) and an internal URL for the cropped image.

Use the response from the previous step to add the subject to the watchlist using the POST /bt/api/subjects route and include the subject's details within the request body.

Add a New Subject to the Watch List from a Track

You can also add an unknown detected individual as a subject in the watchlist using the POST /bt/api/subjects/from-track route.

Add Multiple Subjects via Mass Import

Click here to learn more on how to add subjects to the watchlist via mass import API.

Mass Import Subjects via API

OnWatch allows users to add numerous subjects to the system at once by uploading a compressed file that includes the name of each subject that should be added, as well as one or more reference images for each new subject.

The process is comprised of 4 main steps:
Step 1: Prepare the mass import by providing metadata.
Step 2: Copy the metadata into a folder.
Step 3: Compress the folder into a file.
Step 4: Upload the compressed file for the mass import.
Step 5: Check the status of the entire mass import process.
Step 6: Run a report to check if every subject was added successfully.

The default base URL for the OnWatch API is https://kong.tls.ai unless configured otherwise. If you did configure the base URL, you will need to conduct a server connection.

Before you can conduct a mass import, make sure you are logged in.

Prepare the Mass Import

Step 1: Prepare the mass import using the POST /bt/api/upload/prepare/mass-import route. The request body should include the following:

- Name of the mass import.
- The ID of the subject group(s) you would like to add the subjects too. You can find the ID of your subject groups using the GET /bt/api/groups route.
- Whether or not you would like the system to "search backwards" and locate the new subjects within historic video footage (true or false).
- What the recognition threshold should be. (Only required when `isSearchBackwards` is true.)

> 👍 **Default Threshold in OnWatch**
>
> The threshold in OnWatch is a value between 0.0 to 1 and represents whether a detection with a certain score is considered a recognition of a subject.
>
> The default threshold is 0.55.

Here is an example request body for your reference:

JSON

```
{
  "name": "Mass Import",
  "subjectGroups": [
    "n934t03c-cb48rx", "{SubjectGroupID}"
  ],
  "isSearchBackwards": true,
  "threshold": 0.55
}
```

Once you make the API call, you will receive an `uploadID` value within the response of the request. The `uploadID` represents a unique ID for this mass import and will be displayed as a string.

Use the `uploadID` in the next step, but make sure to be quick as the ID is **valid for only two minutes**.

Upload the Compressed File

Step 2: Copy the metadata into a folder.
Step 3: Compress the folder into a file.

> ### Using a Compressed File for Mass Import
>
> OnWatch only accepts compressed files as input for mass import (either **.zip** or **.tar**). You can upload a compressed file that includes a single image per subject, or you can upload a compressed file that consists of numerous folders, each with a few images per subject.
>
> Make sure the name of the folder of images, or the images themselves, are labeled as the subject's name. Images of subjects within the compressed folder must be in JPEG or PNG format. In addition, up to 15 images can be added per subject.
>
> Learn more on how you can compress a folder with images or compress a folder of images with other folders.

Step 4: Use the POST /bt/api/upload/extract/id to upload the compressed file of subjects. Input your `uploadID` as the {id} value within the route request and include the compressed file's path/location within the request body.

Here is an example request body for your reference:

JSON

```
{
  "file":"{PATH_TO_FILE}"
}
```

Once you make the API call, you should receive a 200- `OK` value within the response of the request. The compressed file will be extracted and uploaded to the OnWatch system.

Check the Status of the Entire Mass Import Process

Step 5: Check the status of your mass import using the GET /bt/api/mass-import/id route. Input your `uploadID` as the {id} value within the route request.

The response of the API call will display the metadata of the mass import, including the status. The status can be either: started, uploading, extracting, processing, done, or failed.

Here is an example response for your reference:

JSON

```json
{
  "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "jobId": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "name": "johnDough",
  "mappedName": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "subjectFolderName": "johnDough",
  "clientRelativePath": "string",
  "storagePath": "string",
  "status": "done",
  "metadata": {},
  "createdDate": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
}
```

> ### Did Your Mass Import Fail?
>
> Learn more on what may have caused your entire mass import to fail.

Run a Report to Check if Each Subject was Added Successfully

Step 6: Review the mass import report using the /bt/api/mass-import/stream/id route. Input your `uploadID` as the {id} value within the route request.

It's important to verify that each subject from the mass import was successfully uploaded to the system. The mass import report summarizes this information and lets you know the specific status of each added subject.

If a subject was not successfully added to OnWatch when conducting a mass import of subjects, an error code will appear on that subject's row within the downloaded report. This will tell you exactly what went wrong so that you can try again.

> ### Were Some Subjects Not Added?
>
> Learn more on what may have caused certain subjects to fail within the mass import.

Subscribe to Event Socket

The OnWatch API allows organizations to connect their live stream cameras, analyze the video footage in real-time, and generate metadata whenever an occurrence takes place, such as a face or body being captured within the camera's field of view.

These occurrences are called events. Whenever a subscribed occurrence takes place, an event is sent out to the socket. The following events are available for subscription. You can subscribe to all events or just to specific events that are relevant to your use case.

WebSocket	Description
track:created	A detection of an unknown person took place
recognition:created	A recognition of a subject took place
camera:changed	One or more parameters of a camera was changed
camera:deleted	A camera was deleted from OnWatch

When you subscribe to an event, you will immediately get notified whenever that event takes place.

Subscribe to All Events

Use the connect socket to subscribe to all events, including the recognition of a subject and the detection of an unknown person.

Subscribe to Specific Events Only

To subscribe to track:created, click here.
To subscribe to recognition:created, click here.
To subscribe to camera:changed, click here.
To subscribe to camera:deleted, click here.

API Keys

The system supports api keys which enables integration with third party applications.

It is important to understand the distinction between api-keys and api-tokens since the two are often mistakingly used interchangeably.

Api Tokens

api tokens are used to identify and authenticate a user - the person - that is using the app or site

Api Keys

API keys identify the calling project — the application or site — making the call to an API.

How to Get/Revoke/Delete

Retrieval
Retrieval through the api:
Request:

HTTP

```
GET /bt/api/api-keys?username=<username> HTTP/1.1
Host: <HOST>
Cookie: <USER_AUTH_TOKEN>
```

Response:

JSON

```
{
    "items": [
        {
            "id": "c27ff648-e0cd-4093-88ea-40f59c1055fe",
            "createdAt": "2022-06-08T06:23:18.000Z"
        }
    ]
}
```

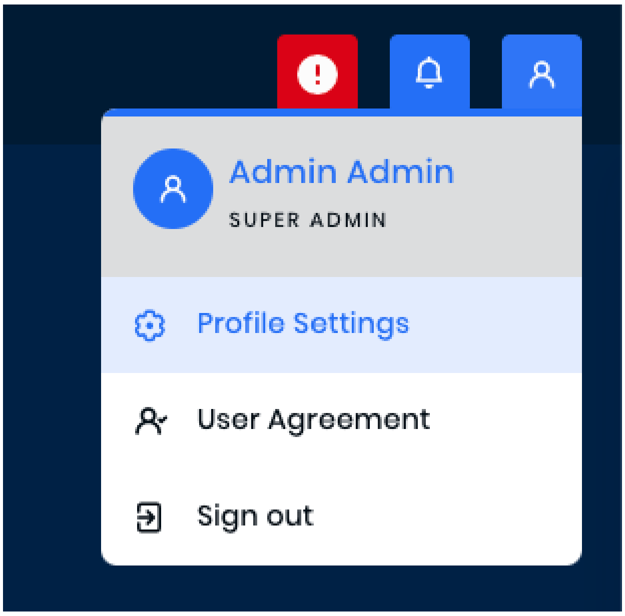
> 📘 **NOTICE**
>
> Due to security reasons, the api key is not included in the response payload.
> This request is mainly used to retrieve the api key id so that it can later be revoked if necessary.

Rules:
Only higher roles can make a fetch request to get a lower role's api key response. This rule does not apply when a user tries to get their own api key id.

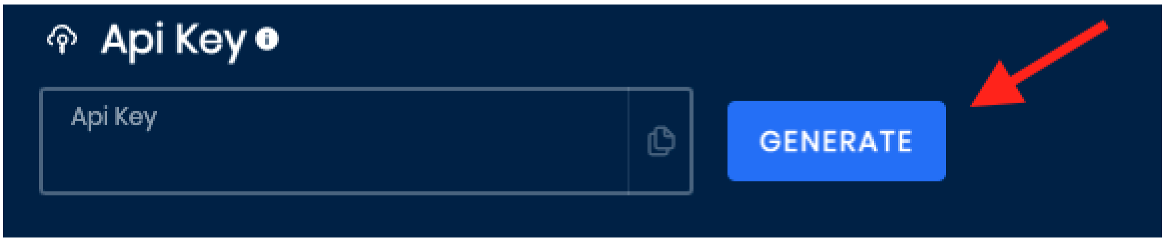
Creation

- how to

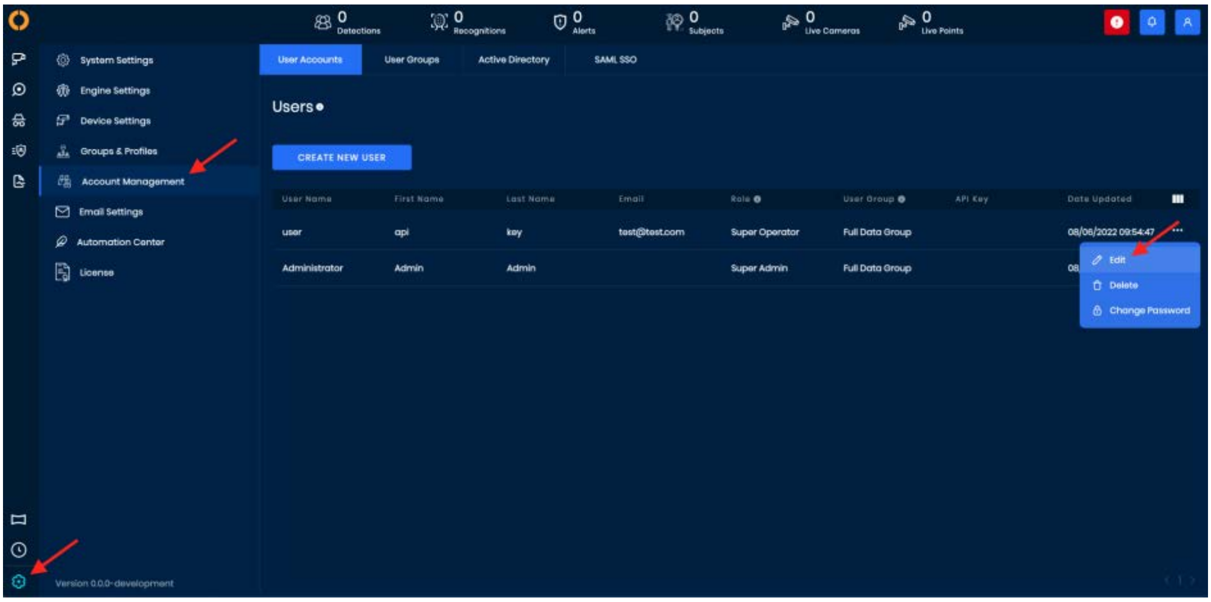
- Dashboard
  Creating a user for oneself:
  Go to user profile by clicking on the right corner and selecting "Profile Settings"



Click on "Generate" at the api key section



Creating a user for other users:



User Name	First Name	Last Name	Email	Role	User Group	API Key	Date Updated
user	api	key	test@test.com	Super Operator	Full Data Group		08/08/2022 09:54:47
Administrator	Admin	Admin		Super Admin	Full Data Group		08

API

HTTP

```
POST /bt/api/api-keys HTTP/1.1
Host: kong.tls.ai
Cookie: <Token>
Content-Type: application/json
Content-Length: 35

{
    "username": "<username>"
}
```

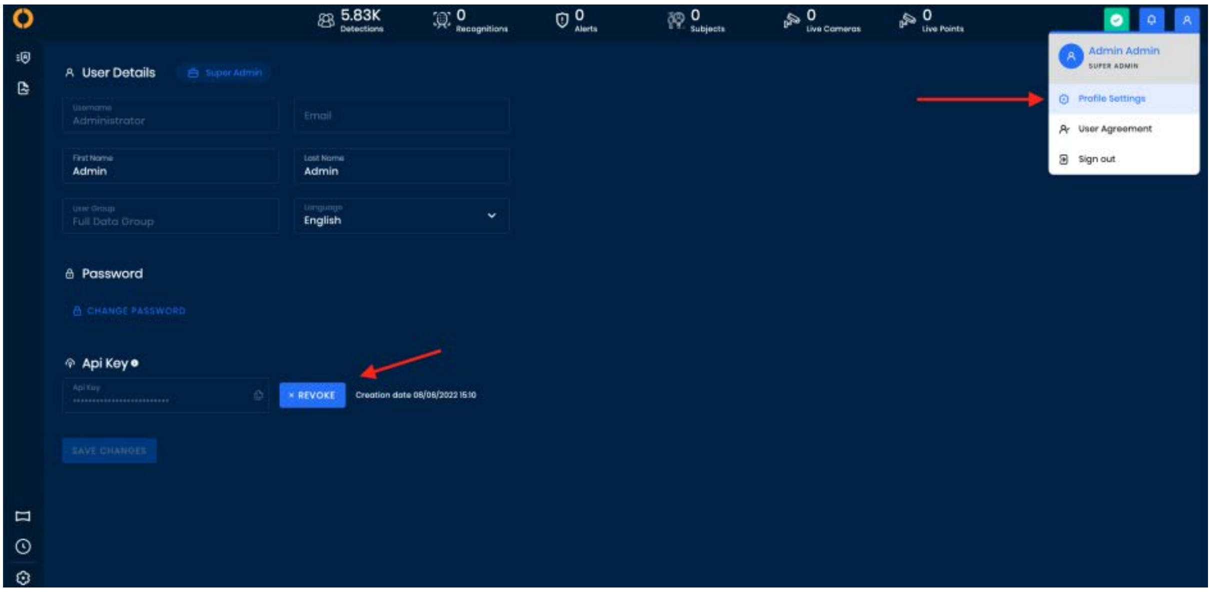
NOTICE

Api keys do not have an expiration. Therefore to remove an api key a user must do it manually.

- Rules
  Role weight
  Only higher roles can make a post request to get a lower role's api key.
  Each user may only have one api key at a time

Revoke

UI



User Details

Username: Administrator

Email

First Name: Admin

Last Name: Admin

User Group: Full Data Group

Language: English

Password

Api Key

Api Key: ························

Creation date 08/06/2022 15:10

API

```HTTP
POST /bt/api/api-keys/revoke/<api_key_id> HTTP/1.1
Host: kong.tls.ai
Content-Type: application/json
Content-Length: 35

{
    "username": "<username>"
}
```

Rules
Only higher roles can revoke lower role's api key. This rule does not apply when a user tries to revoke their own api key.

Restrictions

Api keys do not work on the following services:

- app licensing
- auth service
- users-service
- permission-management-service

How to use an api key

Using an api key is simple. All one must do is add the `api-key` header to a request, and put the api key for the value. For example (using Node.js with Axios):

JavaScript

```
var axios = require('axios');

var config = {
  method: 'post',
  url: '<host>/bt/api/cameras',
  headers: {
    'api-key': '<api_key>'
  }
};

axios(config)
.then(function (response) {
  console.log(JSON.stringify(response.data));
})
.catch(function (error) {
  console.log(error);
});
```

Download API Documentation

Oosto 2.6.2 API is available to download from the Oosto Knowledge portal in PDF format

403

Forbidden

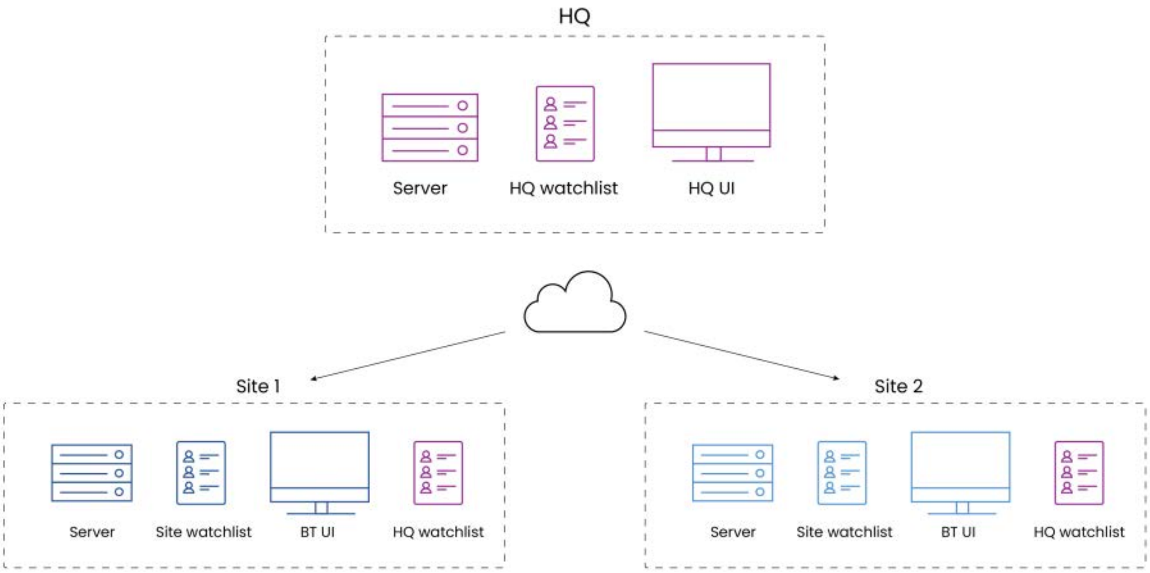
Access to this resource on the server is denied!

HQ Overview

> 📘 **HQ Is An Additional On-Demand Feature**
>
> If you are interested in purchasing and using HQ, please contact your Oosto representative.

HQ Distributed Architecture

OnWatch HQ enables system administrators to define subjects and subject groups which are automatically distributed to all the connected sites. In addition, site system administrators can define new subjects and request that specific subject be added to the OnWatch HQ watchlist. The HQ system will then automatically distribute the subject to all sites if they were approved.



OnWatch Site Servers

In the OnWatch system, a site is a specific location at which a OnWatch server is installed. The server is connected to the live camera feeds at that site.

An organization may have multiple OnWatch sites, each of which a OnWatch server is installed.

OnWatch HQ Server

The OnWatch HQ (Headquarters) server is typically installed at an organization’s headquarters or monitoring center. The HQ server is connected to the OnWatch site servers (described above) using an internet connection in order to provide a central, aggregated web portal from which to monitor and control the detections and recognitions at all or any of the sites.

OnWatch HQ Web Client

The HQ Client connects to the OnWatch HQ server from a standard web browser. The HQ Client enables you to actually view the detection and recognition data collected from multiple OnWatch sites. The HQ Client (which is sometimes referred to as the Master) also enables you to manage, monitor, administrate and configure OnWatch settings.

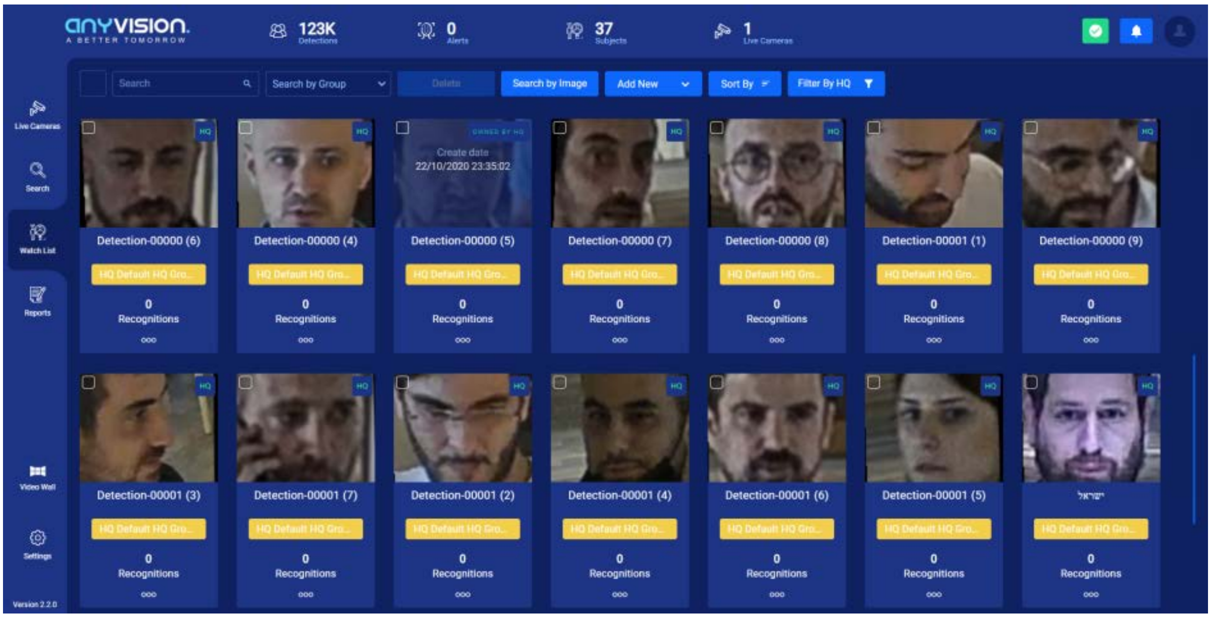
OnWatch HQ Subject Hierarchy

What is the difference between an HQ subject and a site subject?

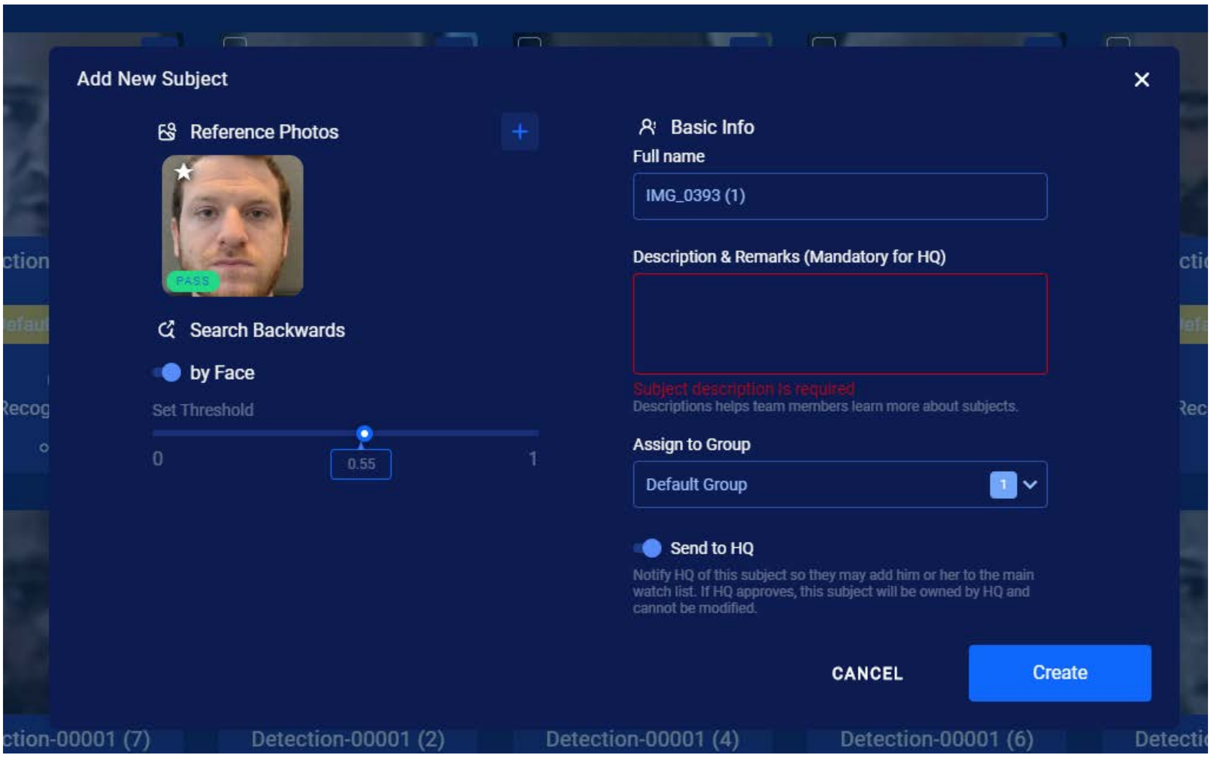
All subjects defined in OnWatch HQ are automatically distributed to all the OnWatch sites that are connected. From the site dashboard, you can see all the HQ subjects that were added to the site's watchlist.

OnWatch site administrators cannot edit or delete subjects that were defined on the HQ system and HQ administrators cannot edit or delete subjects directly on the site's end.

When a OnWatch HQ user removes a subject that was created on the HQ system, then this subject will automatically be removed from all OnWatch sites.



When a new subject is defined in the OnWatch site's watchlist, an optional toggle (**Send to HQ**, as seen in the image below) is provided at the bottom of the window, enabling the system administrator to request that the subject also be added to the OnWatch HQ watchlist. This means that the OnWatch HQ system will receive a request to add this subject to the watchlist, and will include the name of the subject and a short description on them. If the HQ system administrator authorizes this request, then the subject will be distributed to all the sites connected to HQ.



Search Backwards

by Face

Set Threshold: 0.55 (0 – 1)

Basic Info

Full name: IMG_0393 (1)

Description & Remarks (Mandatory for HQ)

Subject description is required

Descriptions helps team members learn more about subjects.

Assign to Group: Default Group 1

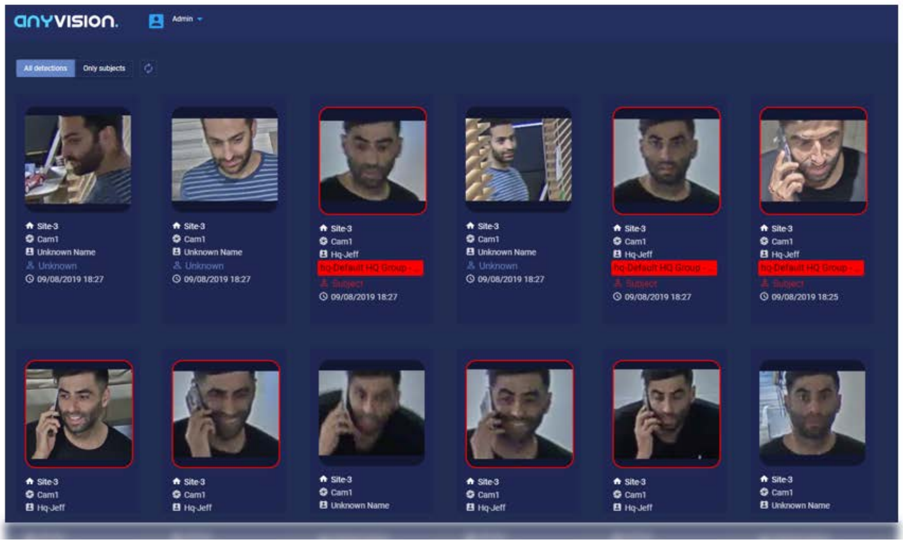
Send to HQ

Notify HQ of this subject so they may add him or her to the main watch list. If HQ approves, this subject will be owned by HQ and cannot be modified.

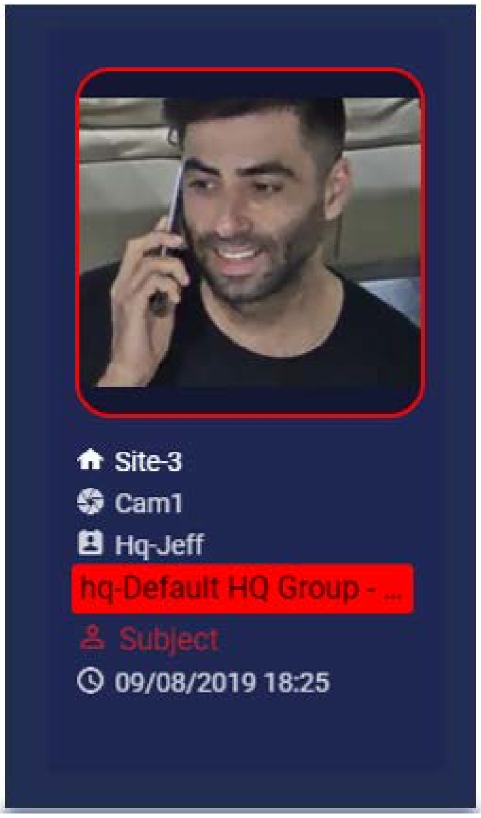
HQ Gallery

Gallery Overview

The OnWatch HQ Gallery shows the latest detections of all unknown faces and all the recognitions of subjects defined in the OnWatch HQ watchlist.



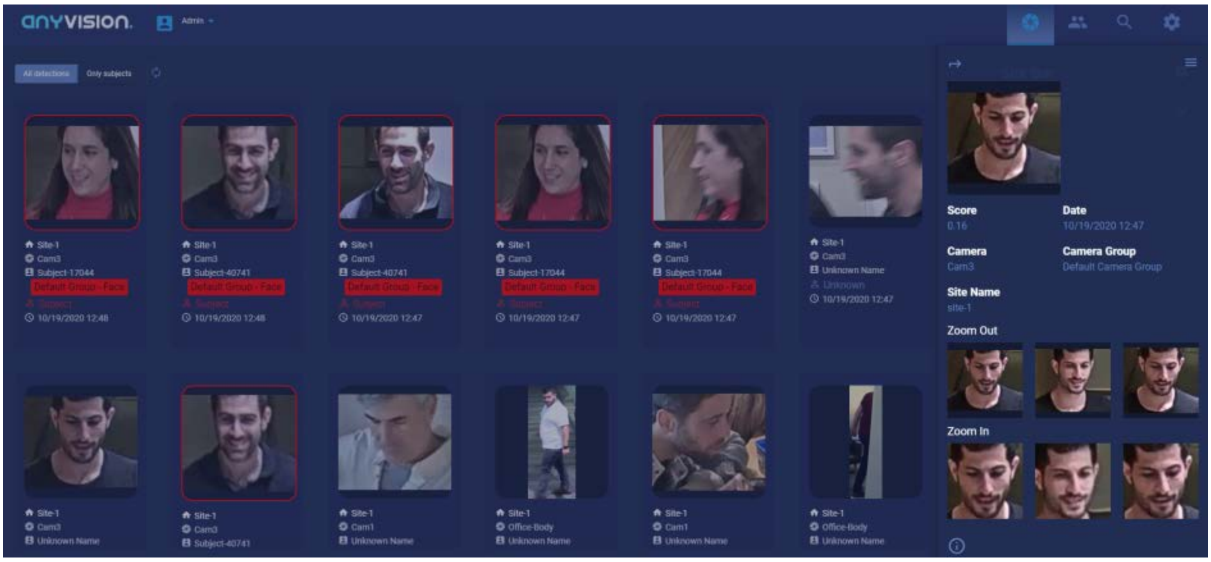
The system will specify the site, camera name, subject name, subject group, type and time of the detection. It also specifies whether the person is unknown or is a subject in the watchlist by placing a colored box around the cropped image.



Site-3
Cam1
Hq-Jeff
hq-Default HQ Group - ...
Subject
09/08/2019 18:25

In addition, a score is shown, specifying how close a match there is between the detected image and the reference image that was added when the subject was added to the watchlist. If this is an unknown person, then the score indicates how close the detected image is to the most similar image in the OnWatch HQ database.

By clicking on any detection image, more information pertaining to the detection appears. You can zoom in or out of the detected image, can get a wider view of when the detection took place, and you can even download the detection images from here.



Score
0.16

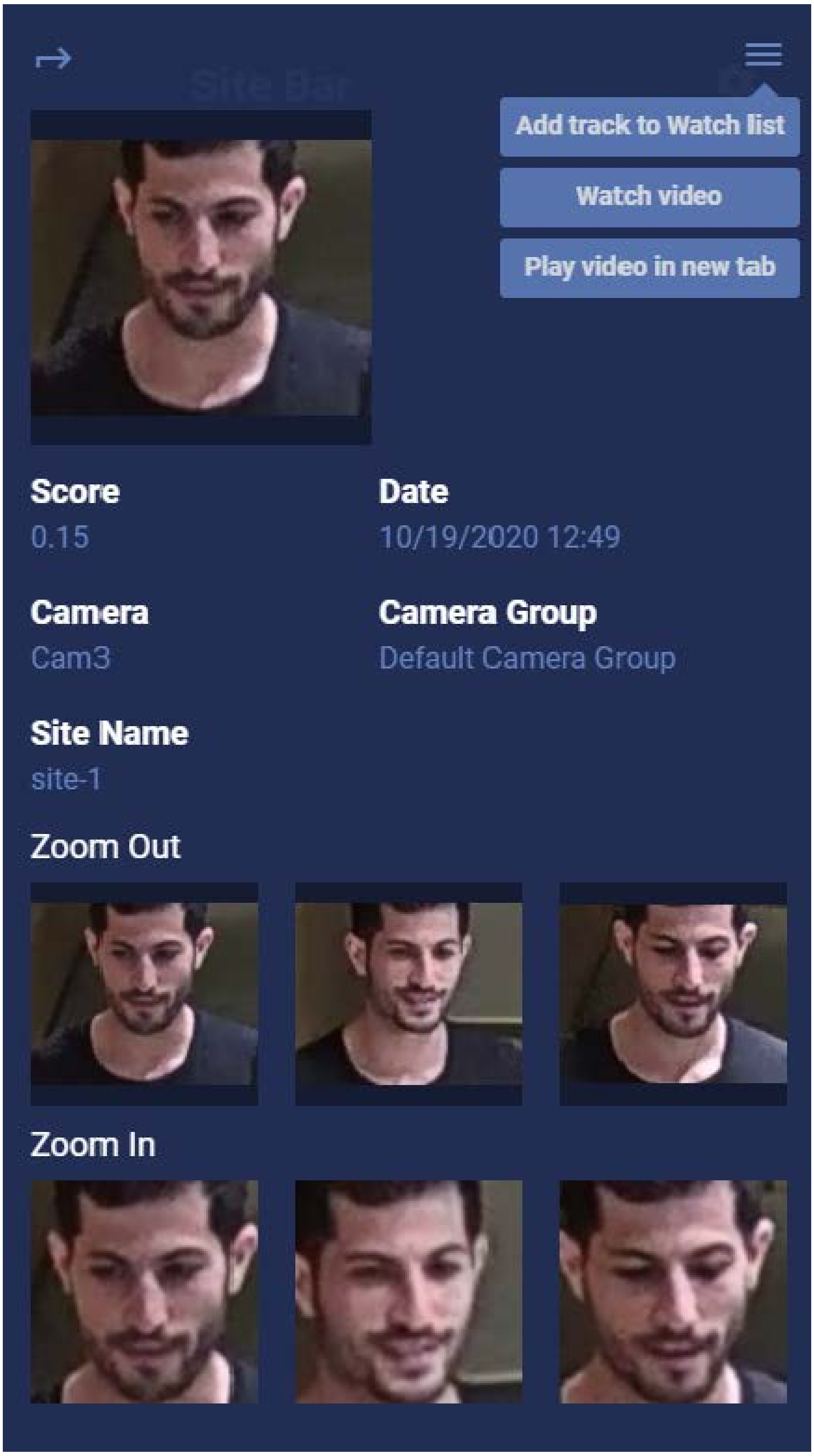
Date
10/19/2020 12:47

Camera
Cam3

Camera Group
Default Camera Group

Site Name
site-1

Clicking on the hamburger icon on this screen displays additional options for what you can do with this detection.



Score
0.15

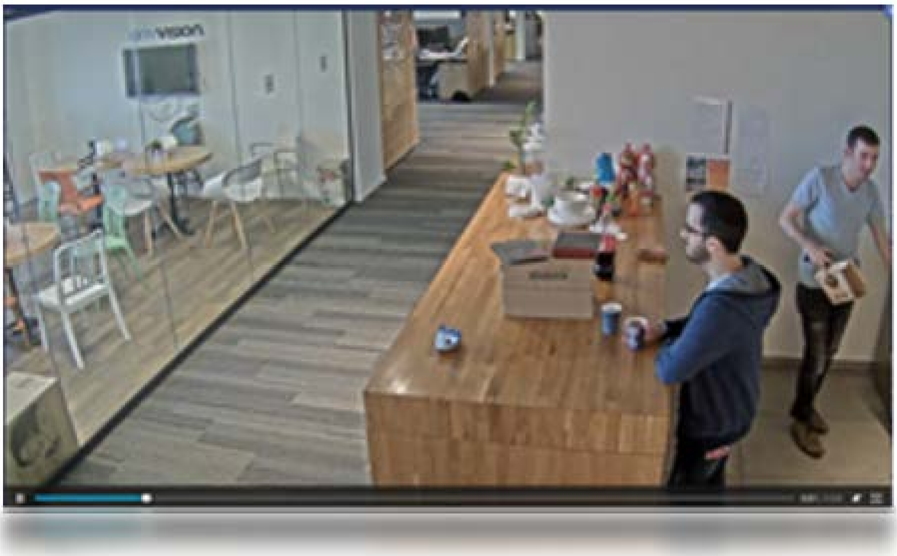
Date
10/19/2020 12:49

Camera
Cam3

Camera Group
Default Camera Group

Site Name
site-1

- **Add track to Watchlist**: If this person is unknown (meaning not in the watchlist already), then this option enables you to add the person detected as a subject.
- **Watch Video**: This option displays a few seconds of a full view of the video in which the person was detected (a few seconds before the person was detected, and a few seconds after.)
- **Play Video In New Tab**: This option displays the same video in a separate tab. In addition, the **Download Video** button enables you to download the few relevant seconds of this video.

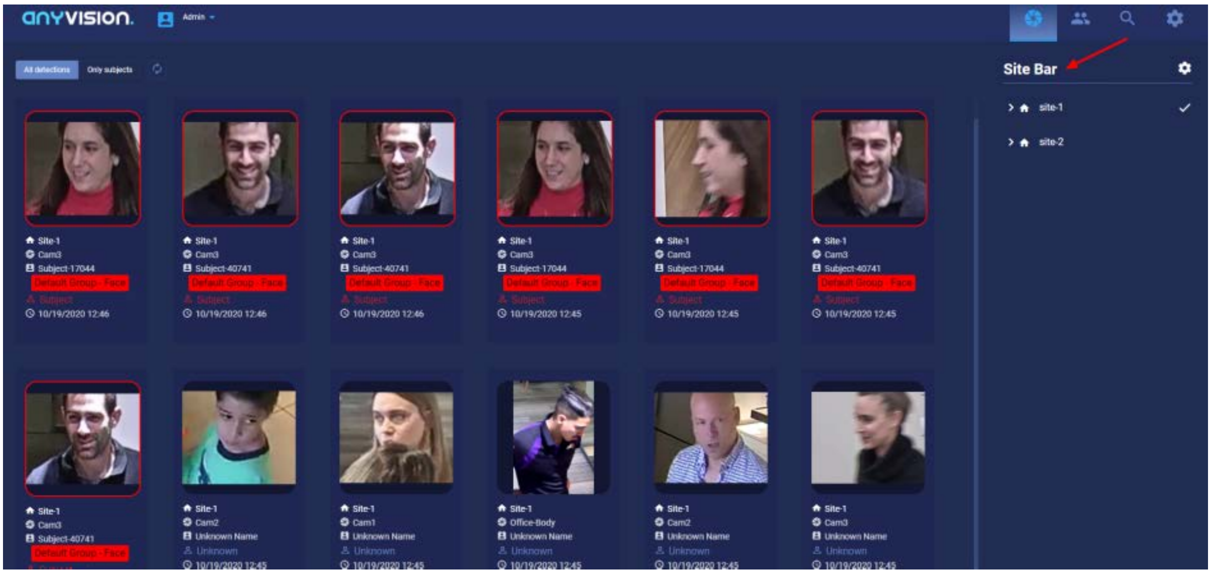


Filtering the Gallery

The following options are provided for filtering the faces and information displayed in the Gallery.

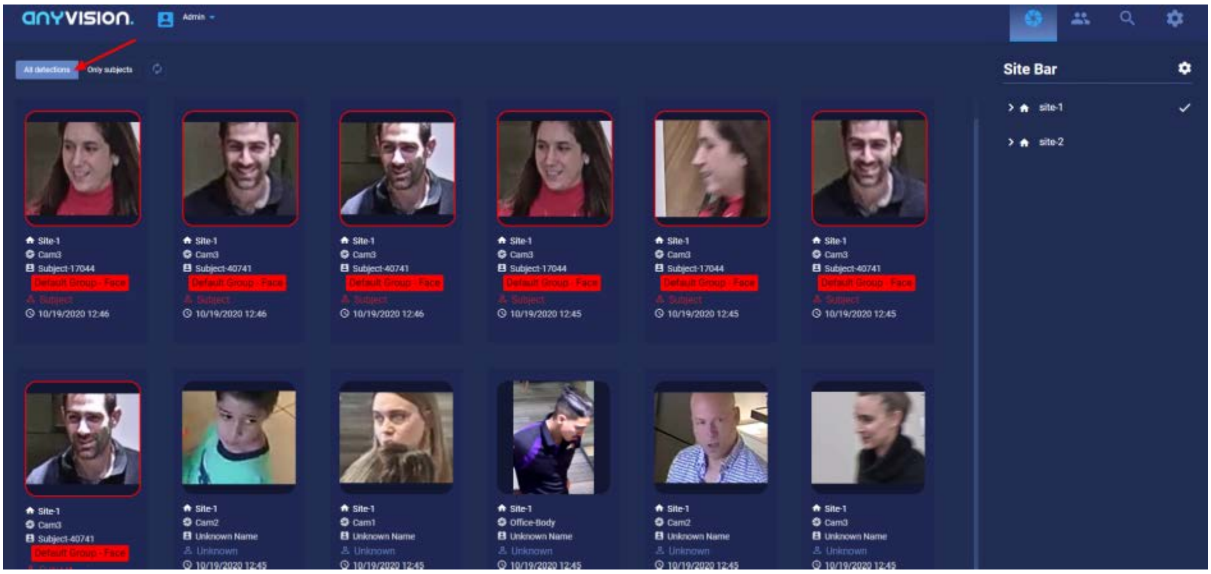
By Site

In the sidebar on the top left of the window, you can select if you want to view the detections and recognitions of all your sites or just of specific sites. The detections displayed will be filtered accordingly.



By All Detections or Only Subjects

You can select whether you are interested in viewing **All Detections**, meaning the faces of unknown persons as well as known subjects from the watchlist, or you can select **Only Recognitions**, which will condense the display of the Gallery to only showcase when a subject from the watchlist was captured.

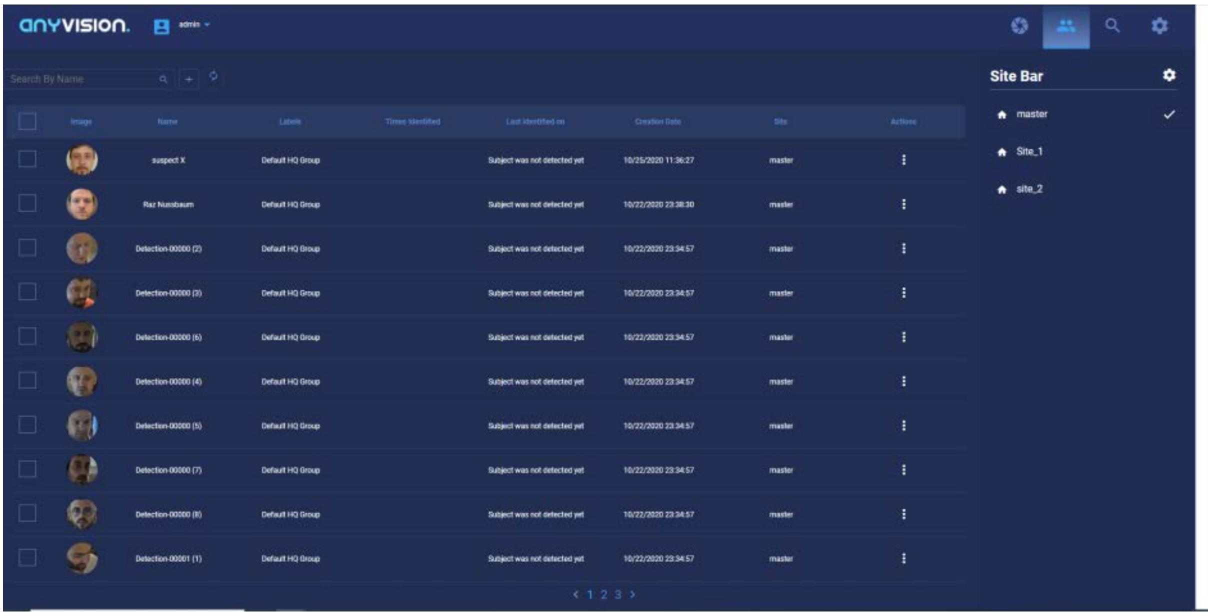


HQ Watchlist

HQ Watchlist Overview

The **Watchlist** section enables users to manage the subjects that have been added to the OnWatch HQ system. The watchlist itself is a library of all subjects defined in the system (either added directly into the HQ system or has been added by a site).

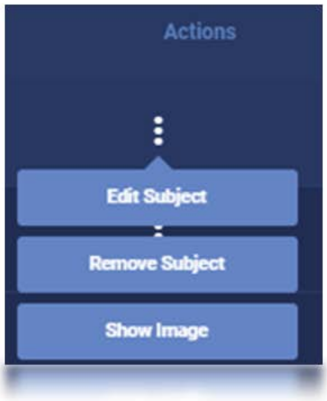
Click the **Watchlist icon** to display the watchlist. You will see the following columns of information about each subject that was added to the system.



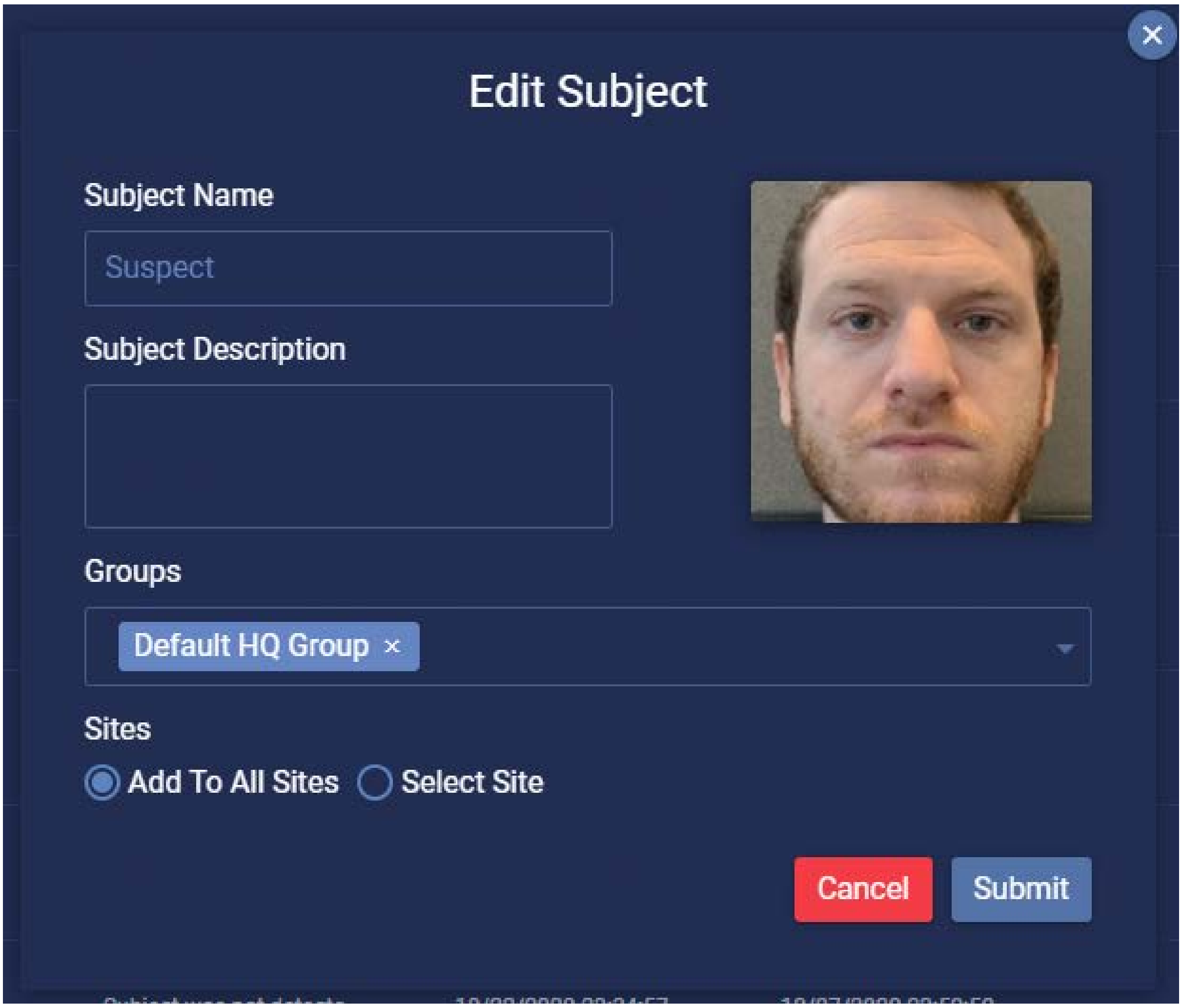
□	Image	Name	Labels	Times Identified	Last Identified on	Creation Date	Site	Actions
□		suspect X	Default HQ Group		Subject was not detected yet	10/25/2020 11:36:27	master	⋮
□		Raz Nussbaum	Default HQ Group		Subject was not detected yet	10/22/2020 23:38:30	master	⋮
□		Detection-00000 (2)	Default HQ Group		Subject was not detected yet	10/22/2020 23:34:57	master	⋮
□		Detection-00000 (3)	Default HQ Group		Subject was not detected yet	10/22/2020 23:34:57	master	⋮
□		Detection-00000 (6)	Default HQ Group		Subject was not detected yet	10/22/2020 23:34:57	master	⋮
□		Detection-00000 (4)	Default HQ Group		Subject was not detected yet	10/22/2020 23:34:57	master	⋮
□		Detection-00000 (5)	Default HQ Group		Subject was not detected yet	10/22/2020 23:34:57	master	⋮
□		Detection-00000 (7)	Default HQ Group		Subject was not detected yet	10/22/2020 23:34:57	master	⋮
□		Detection-00000 (8)	Default HQ Group		Subject was not detected yet	10/22/2020 23:34:57	master	⋮
□		Detection-00001 (1)	Default HQ Group		Subject was not detected yet	10/22/2020 23:34:57	master	⋮

- **Image**: Shows the image of the subject that was added when the subject was created. This is called the reference image.
- **Name**: Specifies the name of the subject.
- **Labels**: Specifies one or more group that the subject is assigned to.
- **Times Identified**: Specifies the number of times the subject was recognized in all the data stored in OnWatch.
- **Last Identified**: Specifies the last date on which the subject was recognized.
- **Creation Date**: Specifies the date when the subject was added.

- **Actions**: Clicking the **three dotted icon** displays a menu of options that enable you to perform the following actions for a subject in the watchlist. These actions are not available for subjects that were created on a specific OnWatch site and not added to OnWatch HQ.



- **Edit Subject**: Enables you to change the profile aspects of a subject. The HQ system automatically distributes this new definition to all the sites during its ongoing background processes.



Edit Subject

Subject Name

Suspect

Subject Description

Groups

Default HQ Group ×

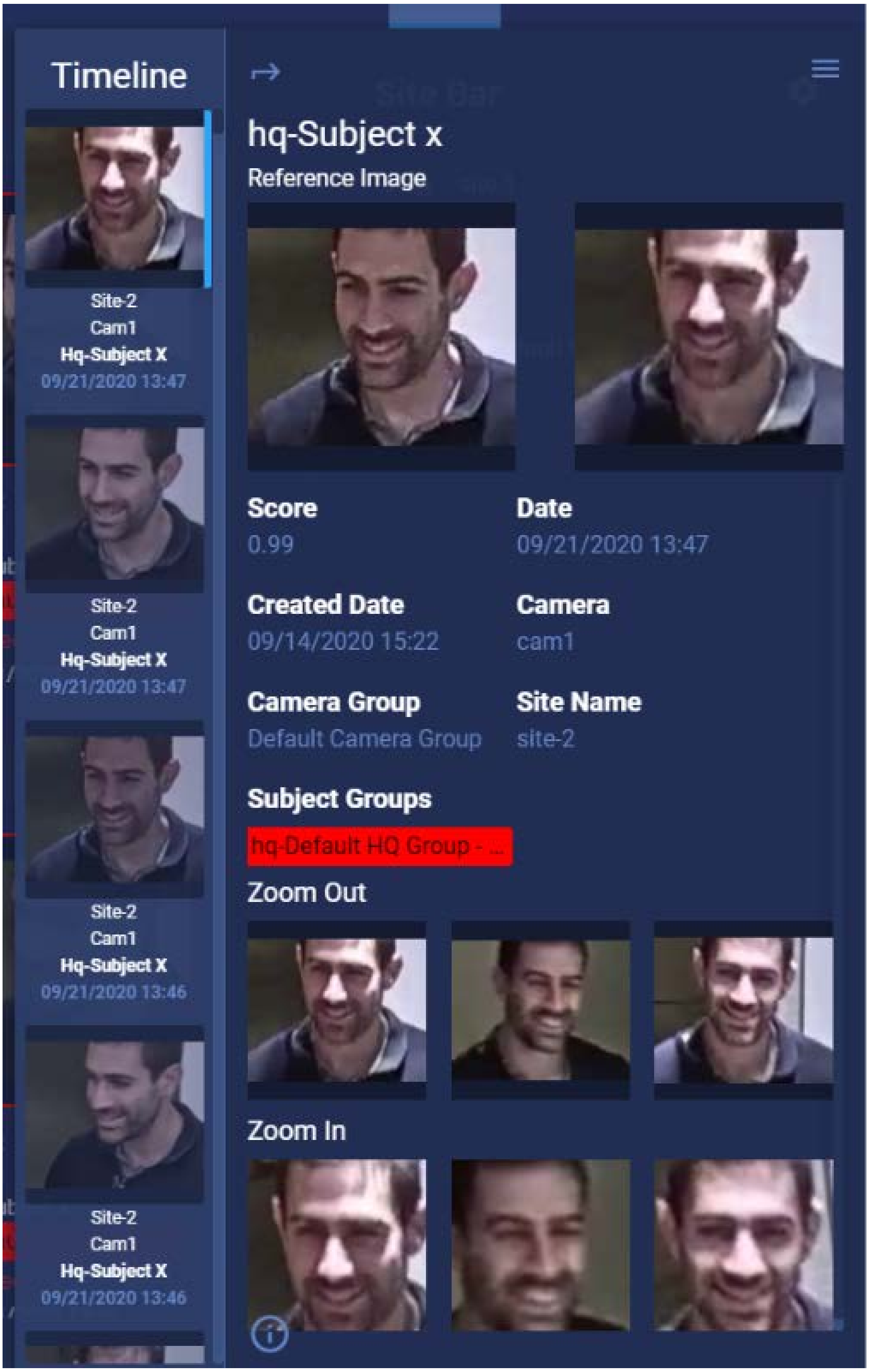
Sites

● Add To All Sites ○ Select Site

- **Remove Subject**: Enables you to remove a subject from the watchlist. The HQ system automatically removes this subject from all the sites during its ongoing background processes.
- **Show Image**: Displays the reference image of this subject, meaning the image that was added when this subject was added to the watchlist.

View a Subject's Timeline

You can view a subject's timeline simply by clicking on the row of the specific subject. The timeline showcases all the times the subject was spotted by the system in the past.



Timeline

Site-2
Cam1
Hq-Subject X
09/21/2020 13:47

Site-2
Cam1
Hq-Subject X
09/21/2020 13:47

Site-2
Cam1
Hq-Subject X
09/21/2020 13:46

Site-2
Cam1
Hq-Subject X
09/21/2020 13:46

hq-Subject x

Reference Image

Score
0.99

Date
09/21/2020 13:47

Created Date
09/14/2020 15:22

Camera
cam1

Camera Group
Default Camera Group

Site Name
site-2

Subject Groups
hq-Default HQ Group - ...

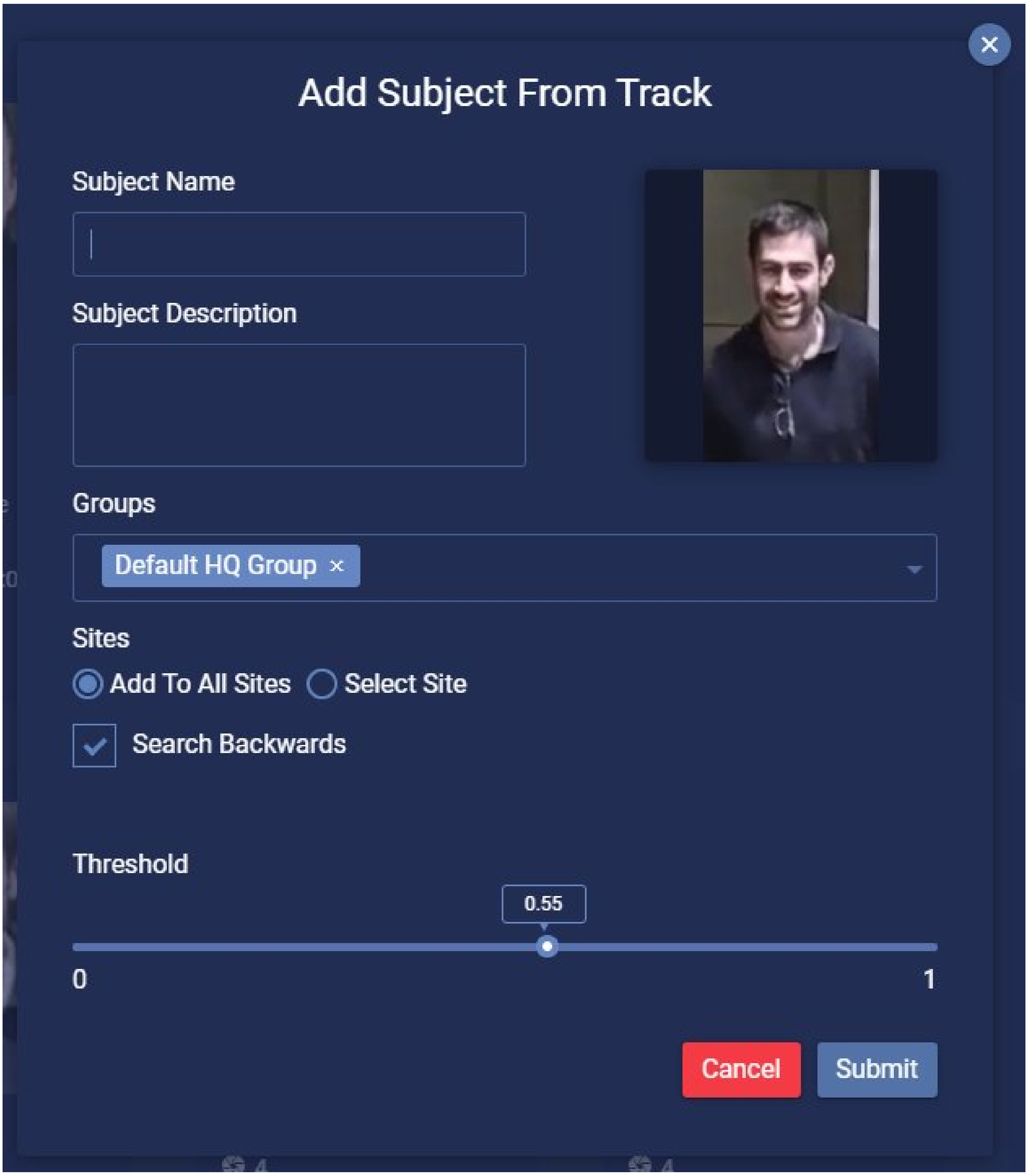
Zoom Out

Zoom In

The following information is also displayed in the subject's timeline.

- **Score**: Specifies how close a match there is between the detected image and the reference image of the subject.
- **Date**: The timestamp of the detection.
- **Camera**: The name of the camera that detected the person.
- **Camera Group**: The group to which the camera that detected this person belongs.
- **Site name**: The site at which this person was detected.
- **Subject groups**: The group to which the subject belongs.

- **Zoom Out**: Additional detected images of the same person.
- **Zoom in**: The same images as in the Zoom Out area, but zoomed in.



Add Subject From Track

Subject Name

Subject Description

Groups

Default HQ Group ×

Sites

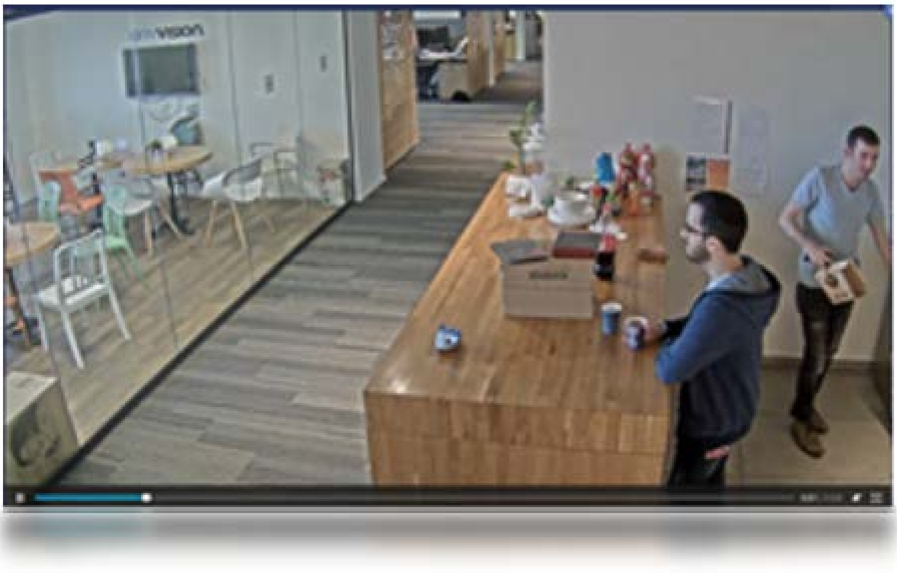
● Add To All Sites ○ Select Site

☑ Search Backwards

Threshold

0.55

0 1



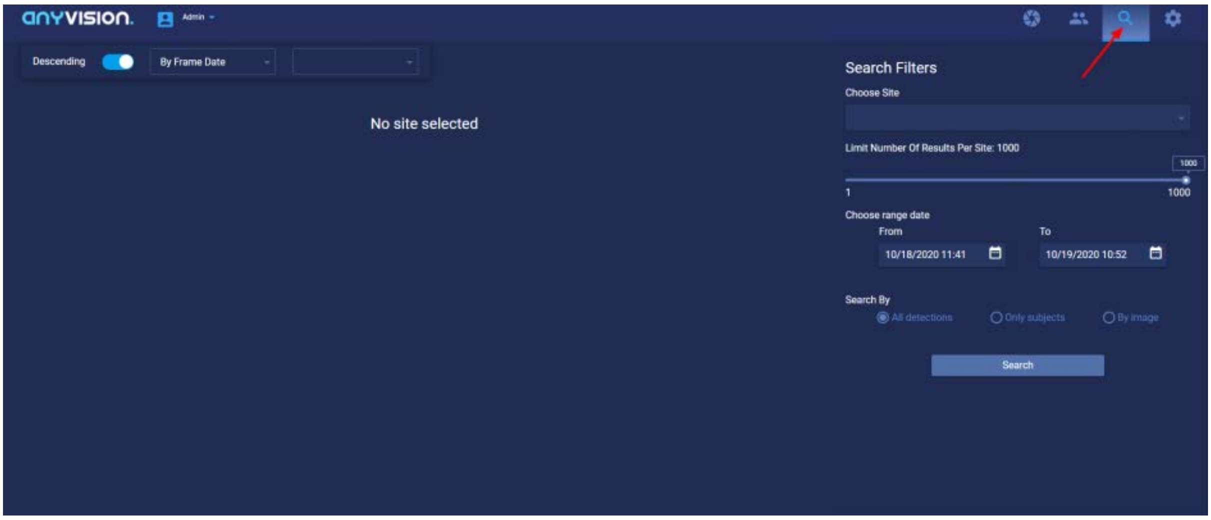
HQ Search

Search Overview

The *Search* section of the HQ system enables you to retroactively search through video and image detections and recognitions that were previously analyzed. For example, you can check whether a certain subject was in your building during a specific time period or upload an image of an individual and see if that person was ever-present in your facility.

One of the main benefits of searching on HQ is that you can identify if a subject was spotted on more than one of your sites. By default, when you perform a search in HQ, the system retrieves the latest detections/recognitions from all the OnWatch sites that are connected. You can also pick and choose which detections you want to see based on specific sites that you select.

You can access the Search section by clicking on the **magnifying glass icon** at the top of the page.



Search Filters

Choose Site

Limit Number Of Results Per Site: 1000

1 — 1000

Choose range date

From 10/18/2020 11:41

To 10/19/2020 10:52

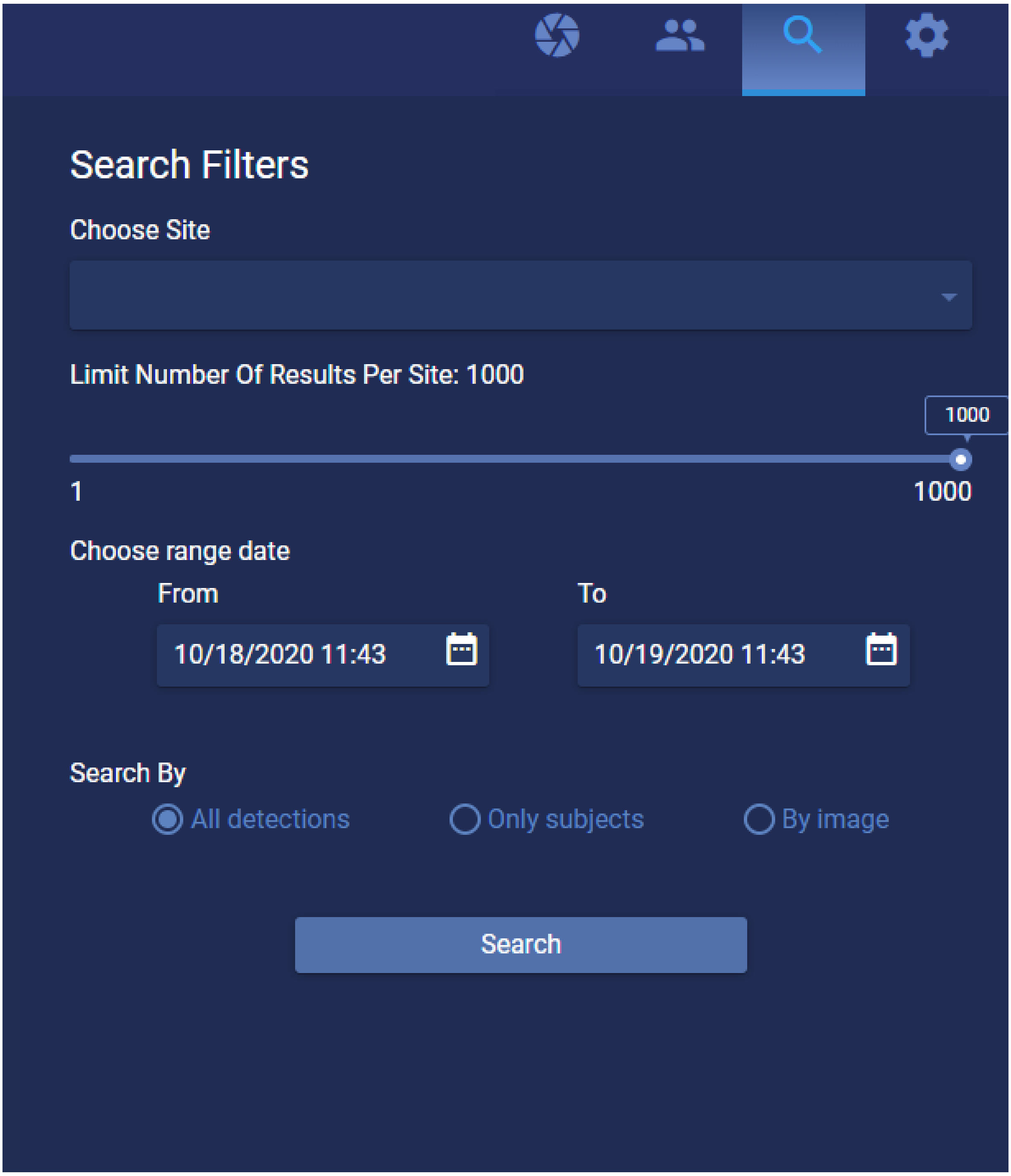
Search By

● All detections ○ Only subjects ○ By image

How to Search in OnWatch HQ

1. You can determine if you would like to search for a specific subject in all of your sites or just specific sites using the **Choose Site** dropdown.

2. Next, determine the maximum number of results that should display from your search.



Search Filters

Choose Site

Limit Number Of Results Per Site: 1000

Choose range date

From: 10/18/2020 11:43

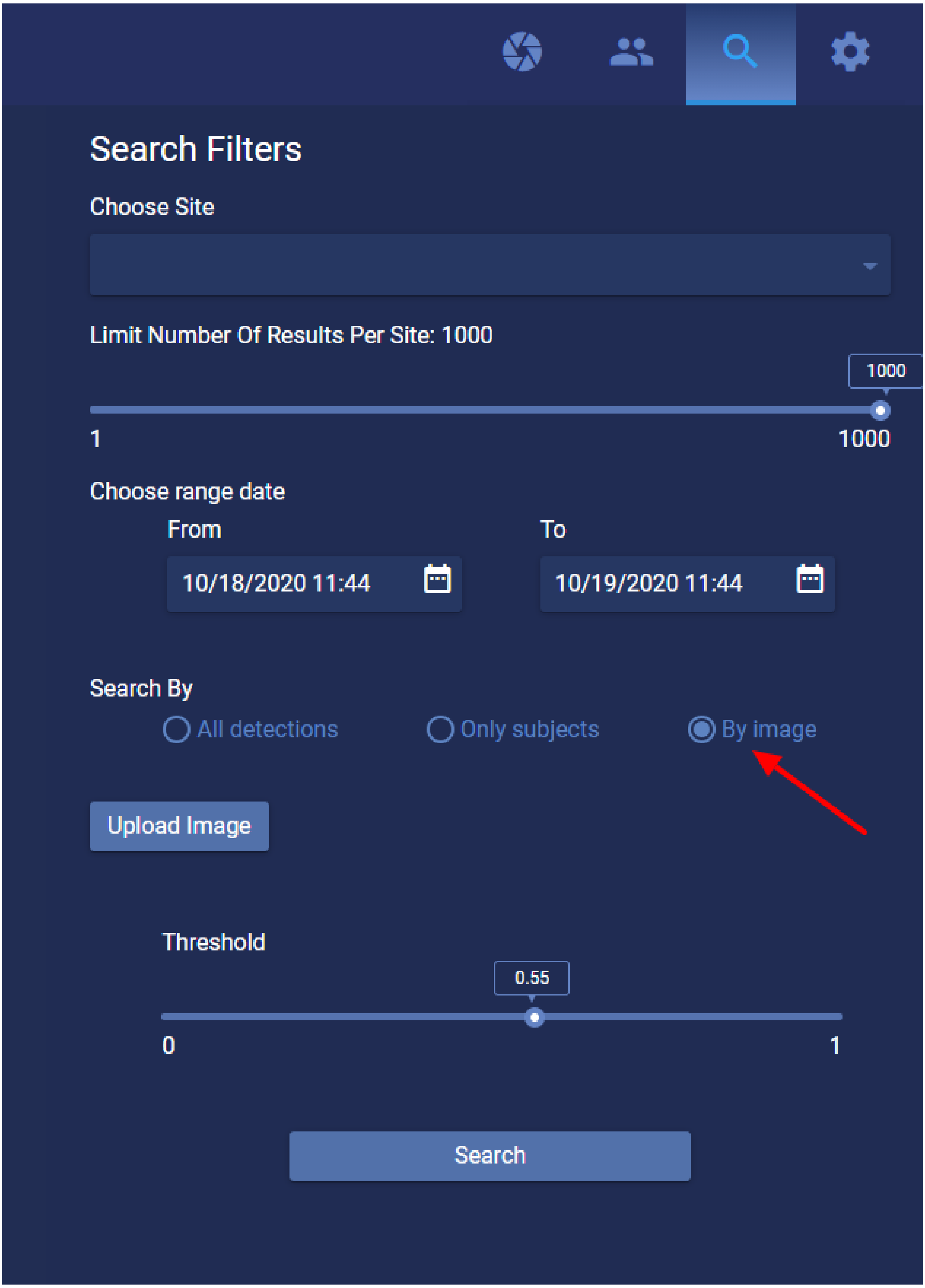
To: 10/19/2020 11:43

Search By

● All detections ○ Only subjects ○ By image

3. Select a date range for the search. The system will only look for detections and recognitions that occurred within that time period.
4. Select how you would like to search under *Search By.*

If you select **All detections**, you will be searching through all of the data in the system.
If you select **Only subjects**, you will be searching through all the images of recognized subjects from the HQ watchlist.
If you select **By image**, you will be requested to upload an image and the system will search for any detection or recognition that matches the face of the person you uploaded, according to the threshold (which you determine in the next step).



Search Filters

Choose Site

Limit Number Of Results Per Site: 1000

1000

1 1000

Choose range date

From 10/18/2020 11:44

To 10/19/2020 11:44

Search By

○ All detections ○ Only subjects ● By image

Threshold

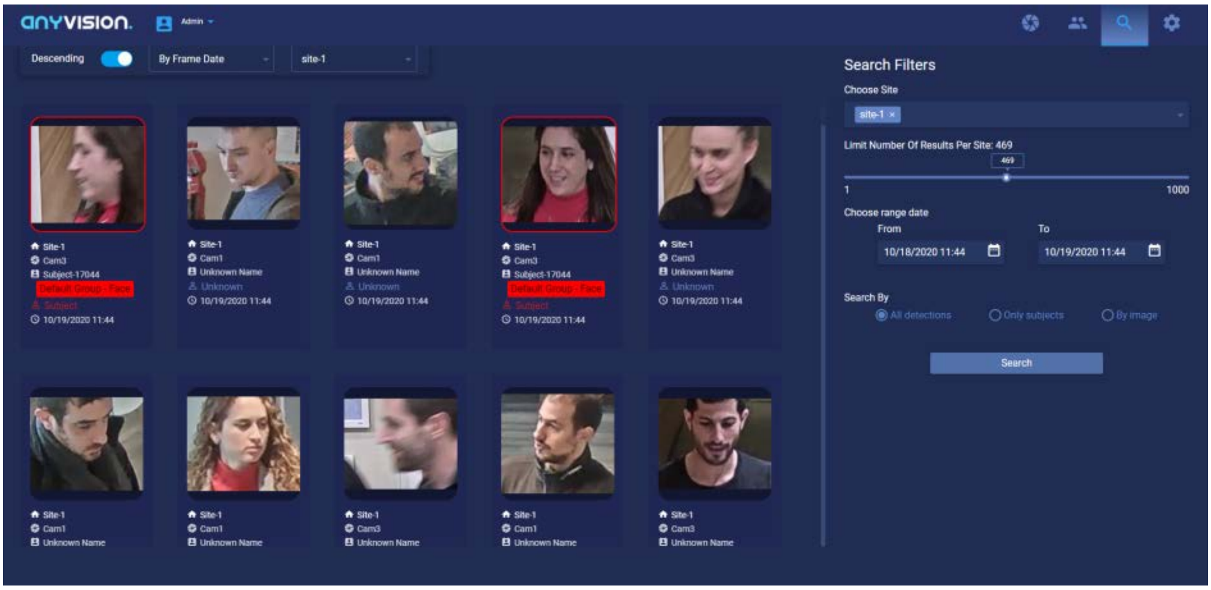
0.55

0 1

5. Set the threshold for the search. (This section only appears when searching by image).

6. Press **Search**.

7. The system will automatically display the search results, if there are any.



Descending ● By Frame Date site-1

Search Filters

Choose Site: site-1 ×

Limit Number Of Results Per Site: 469 (1 – 1000)

Choose range date
From 10/18/2020 11:44 To 10/19/2020 11:44

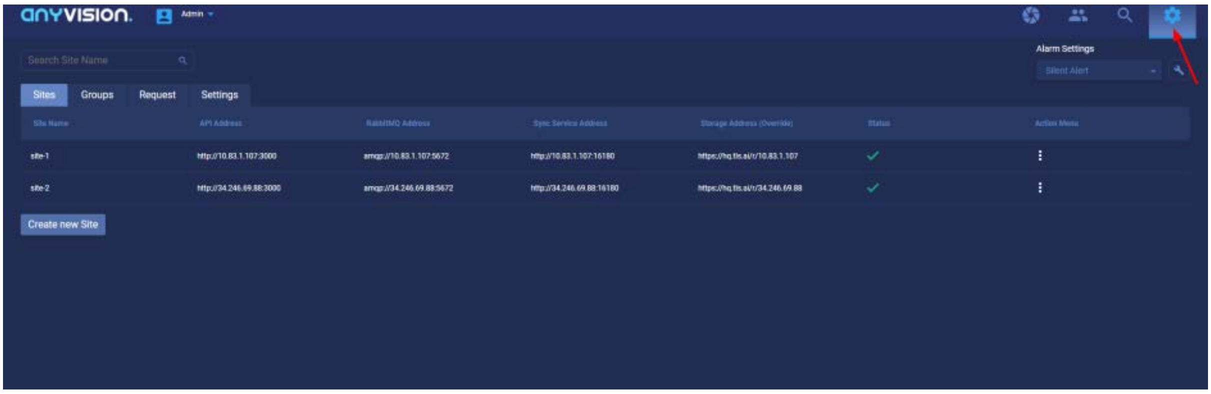
Search By
● All detections ○ Only subjects ○ By image

Search

HQ Settings

Settings Overview

The *Settings* section of the OnWatch HQ system is comprised of 4 tabs. You can access the *Settings* section by clicking on the **Settings icon** on the top corner of the screen.



Alarm Settings: Silent Alert

Site Name	API Address	RabbitMQ Address	Sync Service Address	Storage Address (Override)	Status	Action Menu
site-1	http://10.83.1.107:3000	amqp://10.83.1.107:5672	http://10.83.1.107:16180	https://hq.tls.ai/r/10.83.1.107	✓	⋮
site-2	http://34.246.69.88:3000	amqp://34.246.69.88:5672	http://34.246.69.88:16180	https://hq.tls.ai/r/34.246.69.88	✓	⋮

Settings will automatically open to the first tab, called *Sites*, but you can navigate to any other tab simply by clicking its name. From this section, you will be able to:

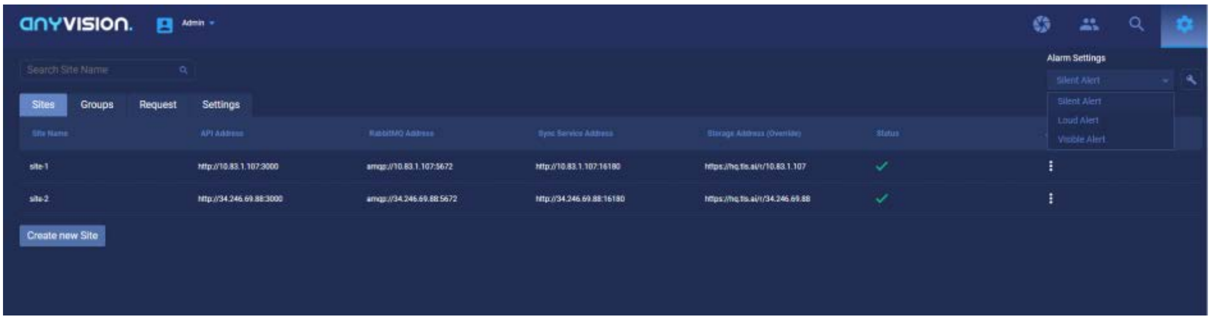
- Configure the system according to your use case
- Add a new site to the HQ system
- Approve or reject subject submissions from your sites.
- View setting configurations
- & more.

Alarm Settings & Basic Configuration

From the main screen, you can configure several aspects of the system. Update the **Alarm Settings**, which determines how the system should notify you when a subject is recognized, by clicking on the dropdown menu and selecting either:

- **Silent Alert**: The system will not generate any noise or popup message, but a detection snapshot will appear in the Alerts tab.

- **Loud Alert**: The system will generate an audible noise and popup message when subjects are identified, and will show a detection snapshot in the Alerts tab in Live Cameras.
- **Visible Alert**: The system will not generate any noise, but will apply a popup messages and show a detection snapshot in Alerts.



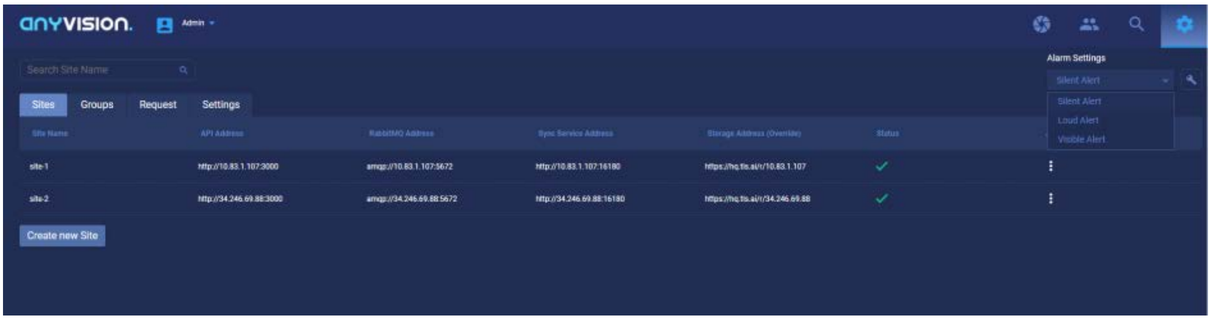
Site Name	API Address	RabbitMQ Address	Sync Service Address	Storage Address (Override)	Status
site-1	http://10.83.1.107:3000	amqp://10.83.1.107:5672	http://10.83.1.107:16180	https://hq.tls.ai/r/10.83.1.107	✓
site-2	http://34.246.69.88:3000	amqp://34.246.69.88:5672	http://34.246.69.88:16180	https://hq.tls.ai/r/34.246.69.88	✓

Settings Tabs

Sites

The Sites tab lists all sites that you have added to the OnWatch HQ. These are the sites that are being monitored by the HQ system. This list displays the name and connection properties of each site in addition to the following:

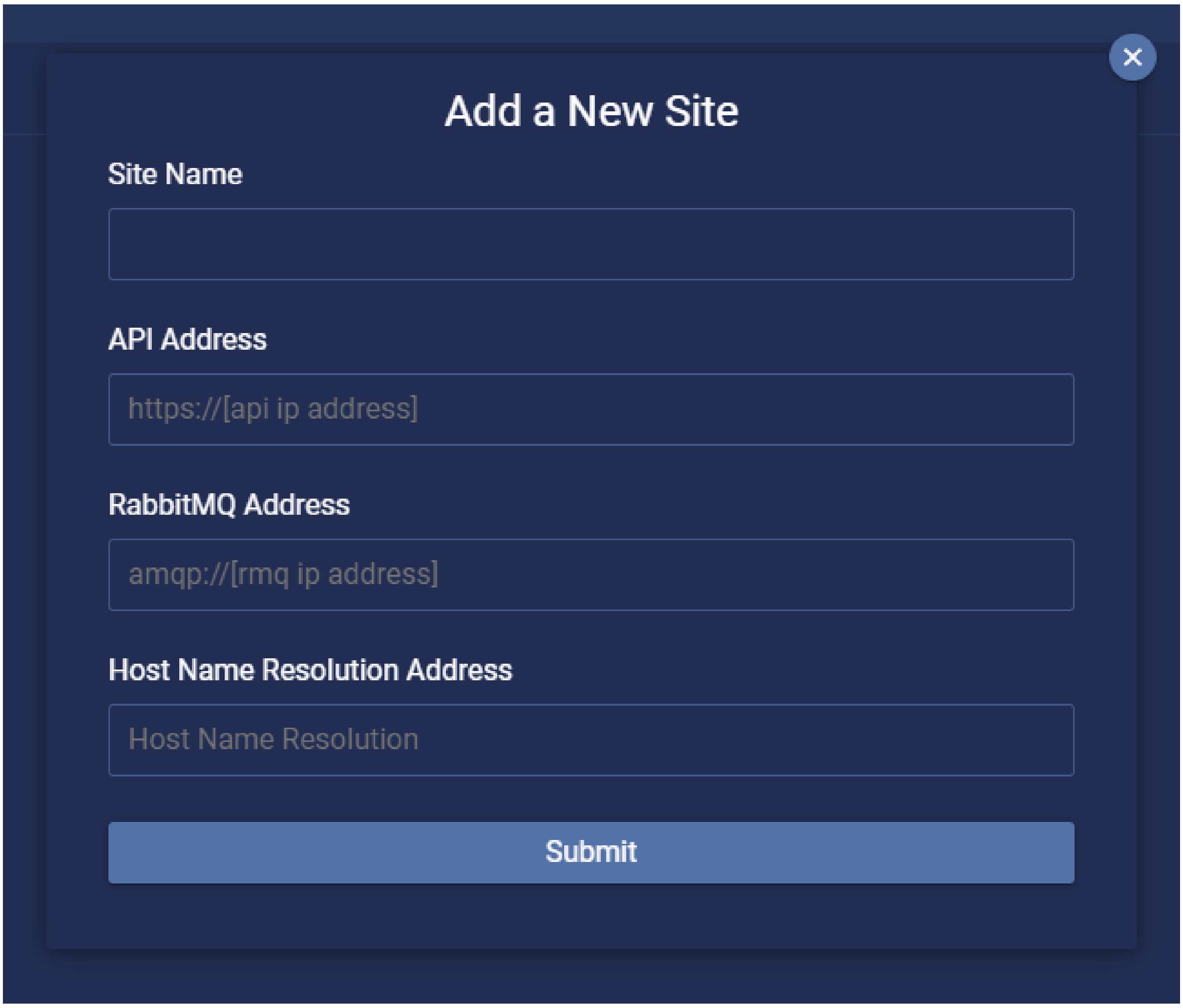
- **Status**: After a site is added, the detections and recognitions from all the site's servers are available for viewing in the dashboard. A green checkmark indicates that the site is connected and is showing all the latest data (detections and recognitions) of this site.
- **Action Menu**: The Action menu provides a variety of actions that you can perform on the site in that row.


Site Name	API Address	RabbitMQ Address	Sync Service Address	Storage Address (Override)	Status
site-1	http://10.83.1.107:3000	amqp://10.83.1.107:5672	http://10.83.1.107:16180	https://hq.tls.ai/r/10.83.1.107	✓
site-2	http://34.246.69.88:3000	amqp://34.246.69.88:5672	http://34.246.69.88:16180	https://hq.tls.ai/r/34.246.69.88	✓

Add a Site

1. Click **Create New Site** to connect one of your sites to the HQ system.
2. A popup will display where you must provide the server details of the machine carrying OnWatch for that specific site, including the:

- **Site Name**: The name you would like to call the site (we recommend naming based on location).
- **API Address**: https://<IP Address of Site Server (ex: https://193.170.21.187)
- **RabbitMQ Address**: amqp://:5672
- **Host Name Resolution Address**:



Add a New Site

Site Name

API Address

https://[api ip address]

RabbitMQ Address

amqp://[rmq ip address]

Host Name Resolution Address

Host Name Resolution

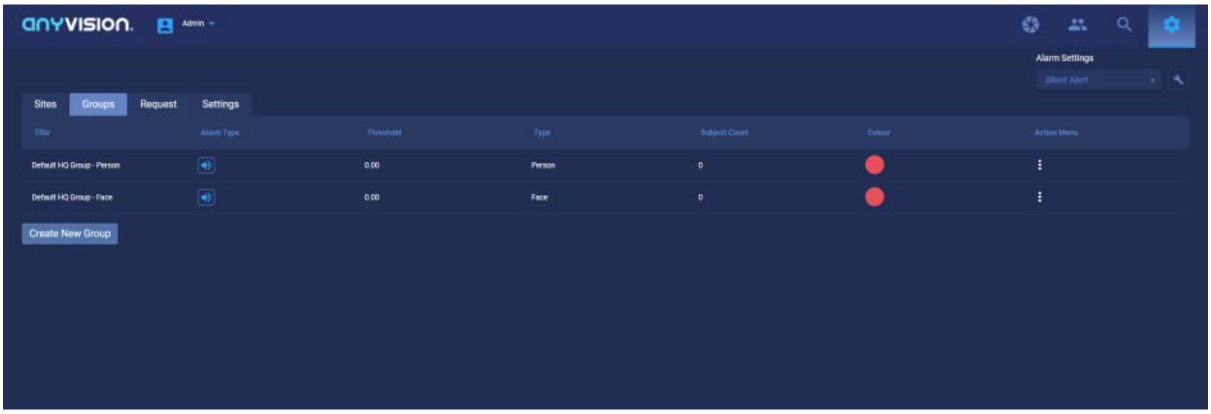
3. Click **submit** when finished. The new site will appear in the Site List once you finish.

At this point, detections and recognitions from the newly connected site will already begin streaming so long as the Status of the site has a green checkmark.

Groups

Groups can be used to categorize subjects according to your organization's use case. For example, you might assign main suspects to one group and their known associates to another group.

All groups that are created in the system will be displayed here. What's cool about groups is that you can determine the specific alarm type you would like for that specific group and determine a recognition threshold just for those predefined subjects. This ensures that very dangerous persons - or persons of high risk - will always be recognized and never missed.



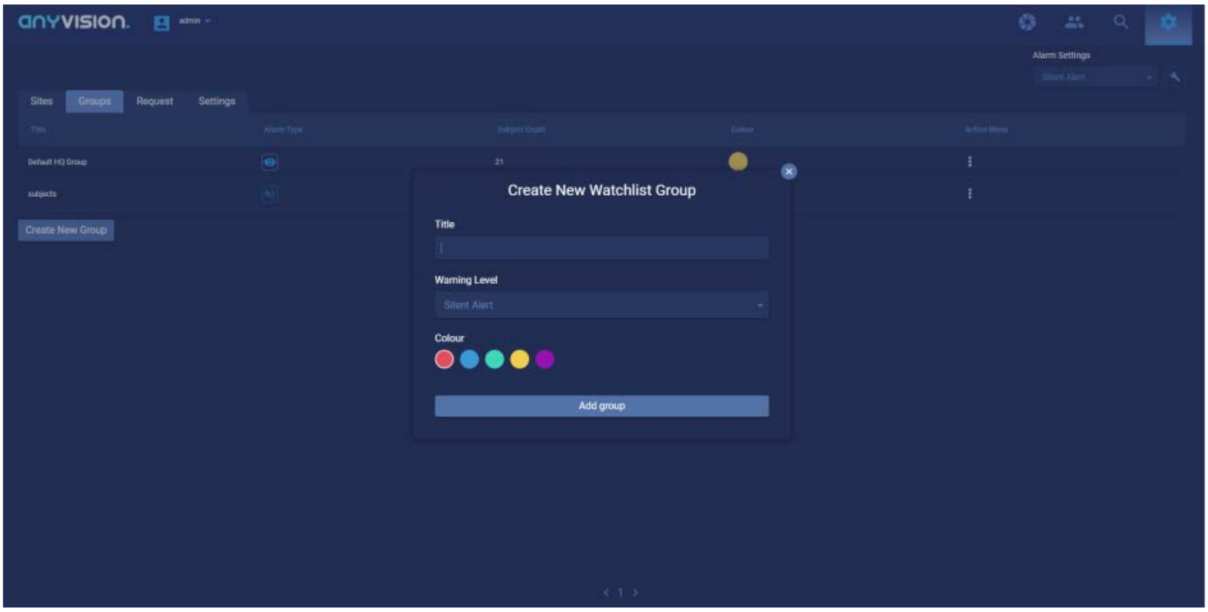
Alarm Settings

Silent Alert

Title	Alarm Type	Threshold	Type	Subject Count	Colour	Action Menu
Default HQ Group - Person	🔊	0.00	Person	0	●	⋮
Default HQ Group - Face	🔊	0.00	Face	0	●	⋮

Add a Group

1. To add new groups in the system, select Create New Group.
2. A popup will appear, where you can input the *Group Title*, *Warning Level* (Alarm Settings), and assign a specific color to the group. This color will be seen as a bounding box around the cropped image of a detected subject from a known group.



Title	Alarm Type	Subject Count	Colour	Action Menu
Default HQ Group		21	●	⋮
subjects				⋮

Create New Watchlist Group

Title

Warning Level: Silent Alert

Colour: ● ● ● ● ●

Add group

3. Click **Add Group** when finished. The new group will appear in the Group List.

You can known assign subjects to this group.

Requests

While subjects can be added to the HQ system directly from the HQ Watchlist tab by system administrators, there may be instances where a subject from a specific site needs to be added to the HQ Watchlist as well.

This is handled by the discretion of site system administrators, who can send a subject request to HQ directly from the site's OnWatch dashboard. Once they submit a request, it will appear on this screen and you can choose to approve the request (which will add the site subject to the HQ watchlist) or reject the request (which will not add the site subject to the HQ watchlist but the subject will still be present on a site level).

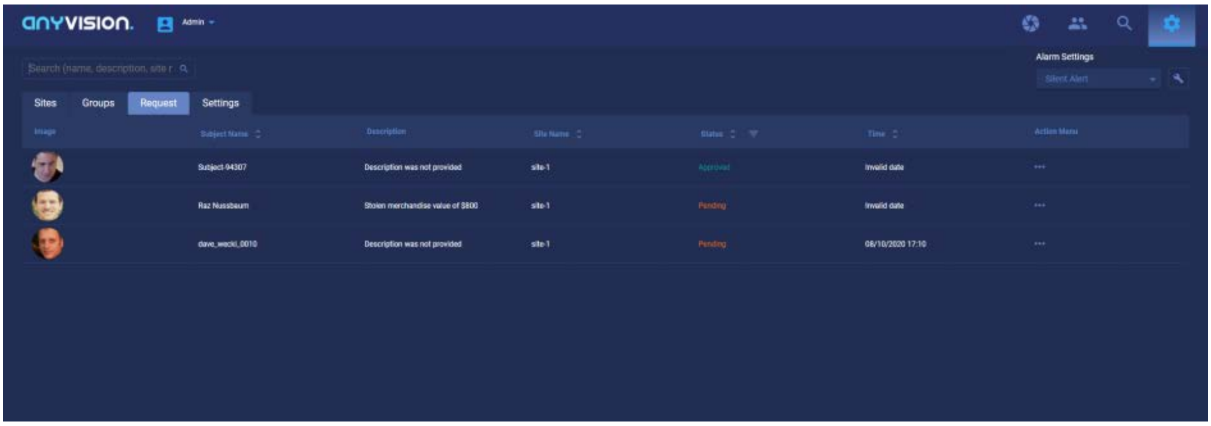


Image	Subject Name	Description	Site Name	Status	Time	Action Menu
	Subject-94307	Description was not provided	site-1	Approved	Invalid date	•••
	Raz Nussbaum	Stolen merchandise value of $800	site-1	Pending	Invalid date	•••
	dave_wecki_0010	Description was not provided	site-1	Pending	08/10/2020 17:10	•••

To approve or reject a request, simply click on the row of the request you would like to review. You can also click on the **three dotted icon** under *Actions Menu* and select **View** or **Remove**.

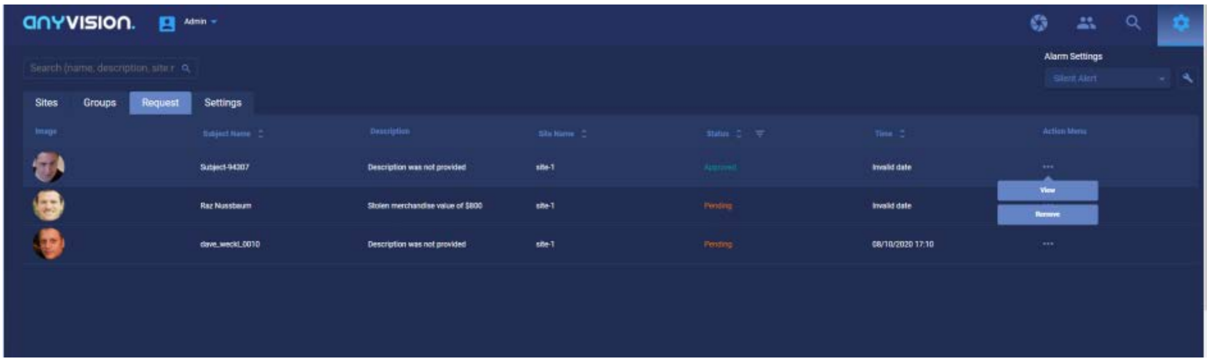
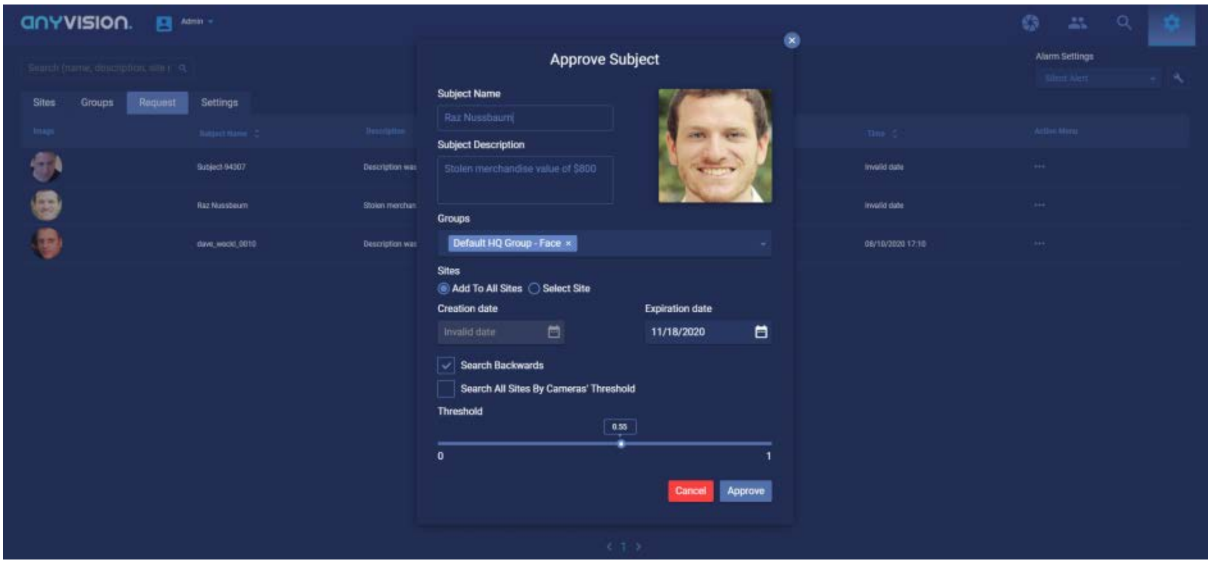


Image	Subject Name	Description	Site Name	Status	Time	Action Menu
	Subject-94307	Description was not provided	site-1	Approved	Invalid date	•••
	Raz Nussbaum	Stolen merchandise value of $800	site-1	Pending	Invalid date	
	dave_weckl_0010	Description was not provided	site-1	Pending	08/10/2020 17:10	•••

Information on the subject will be displayed to provide you with more information. You can make some basic edits to the subject's profile here as well. Click **Approved** when finished.



Approve Subject

Subject Name: Raz Nussbaum

Subject Description: Stolen merchandise value of $800

Groups: Default HQ Group - Face ×

Sites: ● Add To All Sites ○ Select Site

Creation date: Invalid date

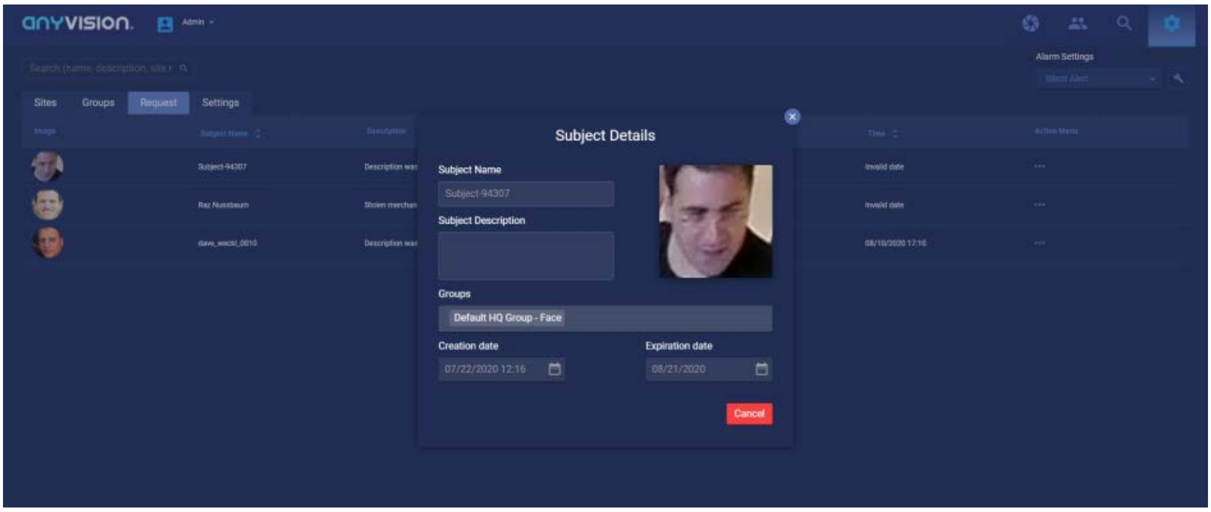
Expiration date: 11/18/2020

☑ Search Backwards

☐ Search All Sites By Cameras' Threshold

Threshold: 0.55 (0 – 1)

Subjects that are already approved will remain on the list as well and their information can be viewed by clicking on that subject's row.



Subject Details

Subject Name: Subject-94307

Subject Description:

Groups: Default HQ Group - Face

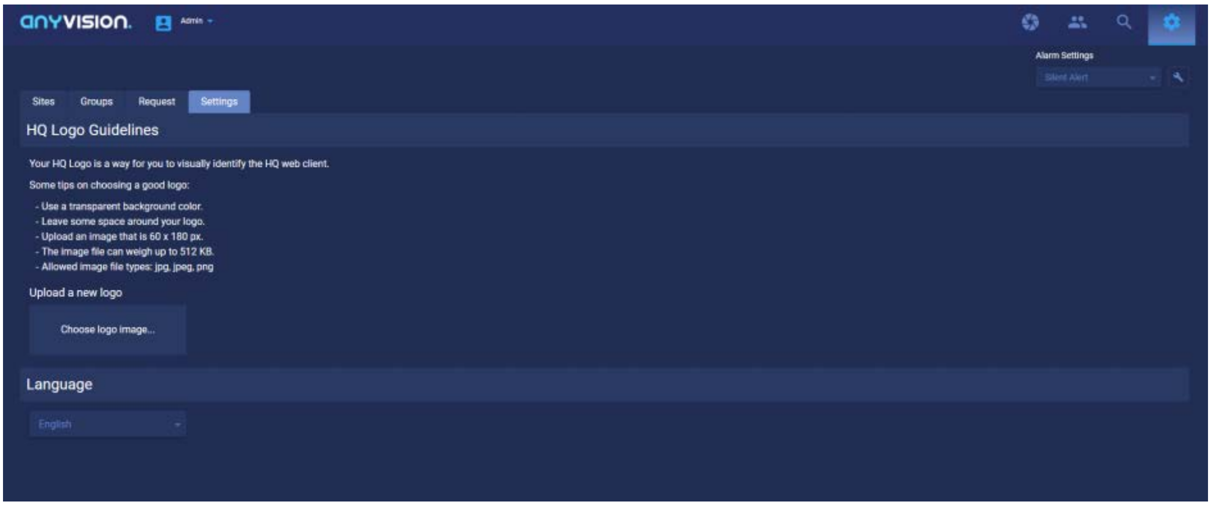
Creation date: 07/22/2020 12:16

Expiration date: 08/21/2020

All subjects that are approved can be viewed and will appear in the HQ Watchlist section of the system.

Settings

The **Settings** tab in *Settings* allows you to upload your company logo to the system to personalize the dashboard. You can also choose a different language for the system (currently only Spanish and English are available).



HQ Logo Guidelines

Your HQ Logo is a way for you to visually identify the HQ web client.

Some tips on choosing a good logo:

- Use a transparent background color.
- Leave some space around your logo.
- Upload an image that is 60 x 180 px.
- The image file can weigh up to 512 KB.
- Allowed image file types: jpg, jpeg, png

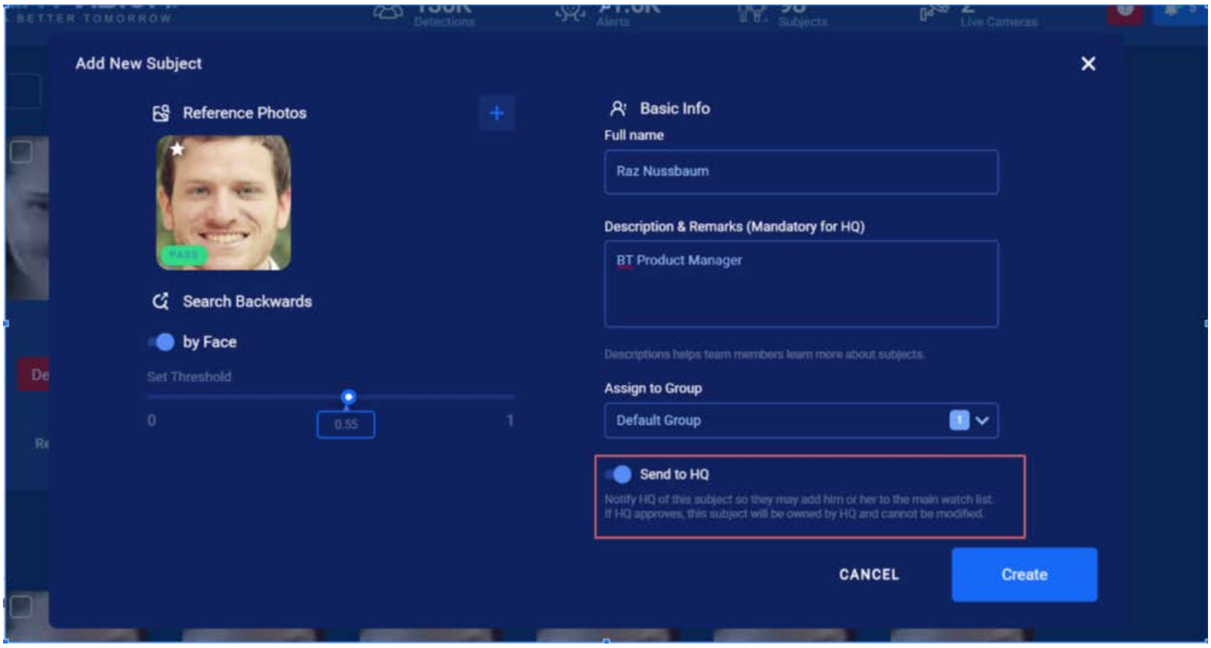
Upload a new logo

Language

English

Add Subject from Site to HQ Watchlist

When adding a subject to a site's watchlist, you will have the option to "Send to HQ". When turned on, this toggle indicates that the subject should be sent to the HQ dashboard for a system administrator to review and potentially add to the HQ's own watchlist.



Full name: Raz Nussbaum

Description & Remarks (Mandatory for HQ): BT Product Manager

Descriptions helps team members learn more about subjects.

Assign to Group: Default Group

Send to HQ

Notify HQ of this subject so they may add him or her to the main watch list. If HQ approves, this subject will be owned by HQ and cannot be modified.

When sending a subject to HQ, you will need to add:

- a description of the subject to assist the system administrator in assessing whether this specific subject should be approved or rejected.
- a single facial reference photo for the subject (only one image can be sent to HQ and it cannot be a body reference image)

Want to learn more?

For more information on how subjects can be sent from a site to HQ, check out the Overview section of HQ User Manual.

OnPatrol Remote

iOS Installation Guide

> 📘 **Remote Is An Additional On-Demand Feature**
>
> If you are interested in purchasing and using Remote, please contact your Oosto representative.

Overview

Oosto's On Patrol application sends alerts to a user's mobile phone whenever a real-time recognition occurs. With this application, security personnel can monitor, track, and detain subjects or dangerous persons that enter a place of business, restricted area, or any other public or private location.

The application must be installed on a user’s phone in order to receive push notifications. This guide describes how to install the application.

OnWatch Preparation

Before beginning the installation process, please confirm the following:

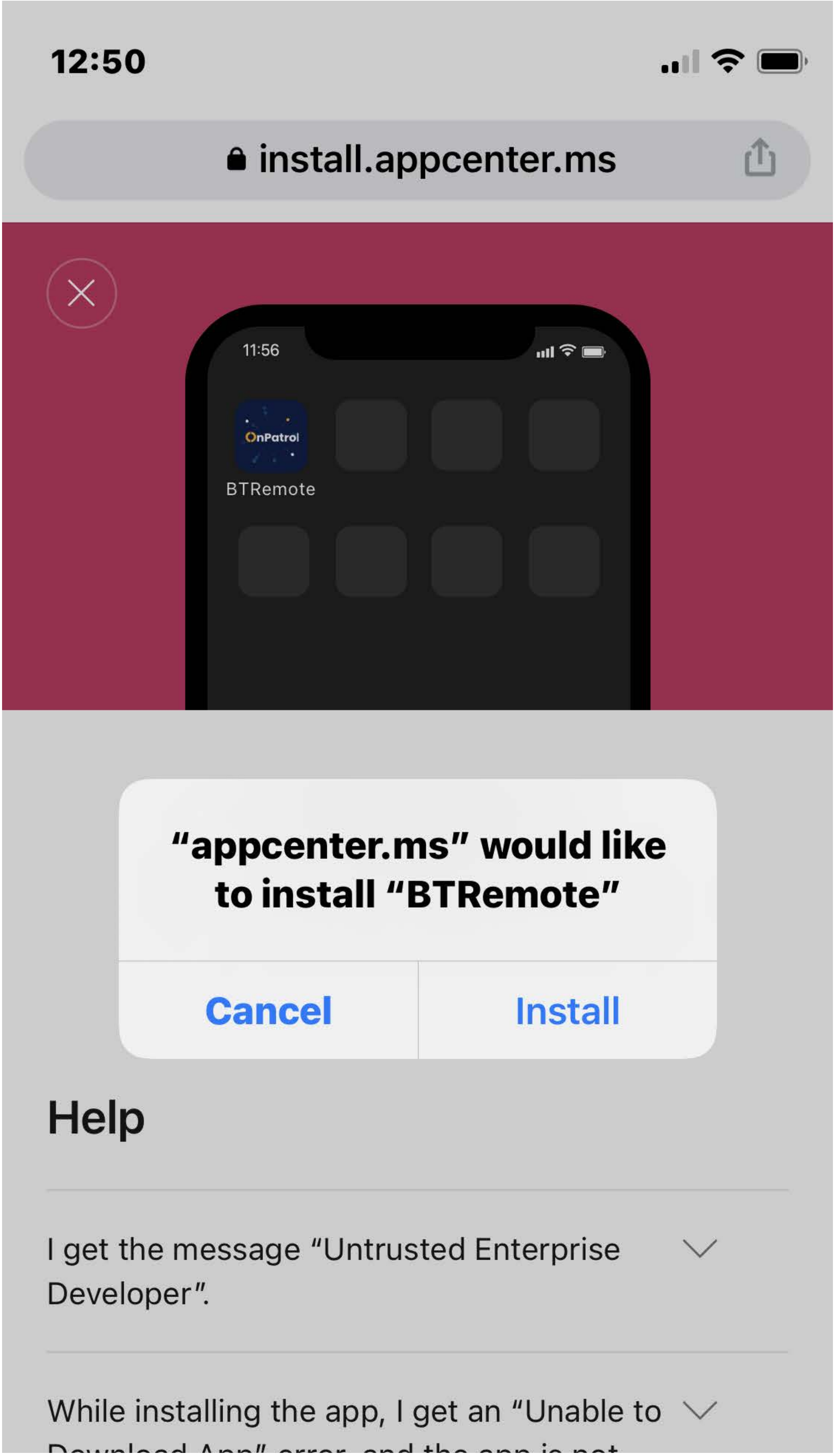
1. Both the mobile device and the OnWatch server have internet access. The mobile notifications feature is internet-based so a shared network without internet access won’t be enough. The easiest way to secure an internet connection for both applications is to open a “Mobile Hotspot” on your own phone and connect both devices to the Hotspot network.
2. The OnWatch version is 2.x
3. The supported devices and operating systems are iOS 12 or higher.
4. Verify the OnWatch server has proper firewall configuration rules. Incoming port (Ingress) number 443 should be open to external internet networks and Outgoing ports (Egress) should have no restrictions. Nevertheless, if you’d like to restrict certain ports, make sure that the following Egress ports always remain open: 5228, 5229, 5230. This will allow proper connection from Firebase to enable the push notifications feature.

Installing On Patrol on an iOS Phone

> 👍 **Remote Mobile Application**
>
> The following steps should be conducted on your phone.

To install the On Patrol *application* on a mobile device:

1. Click here to install the application.
2. Press **Download**.
3. The “App-Center” will request permission to install the application. Tap **Install**.
4. A popup will appear requesting permission to send notifications to the device. Press **Allow**.
5. After approving the requested permissions, you will have the option to log in.

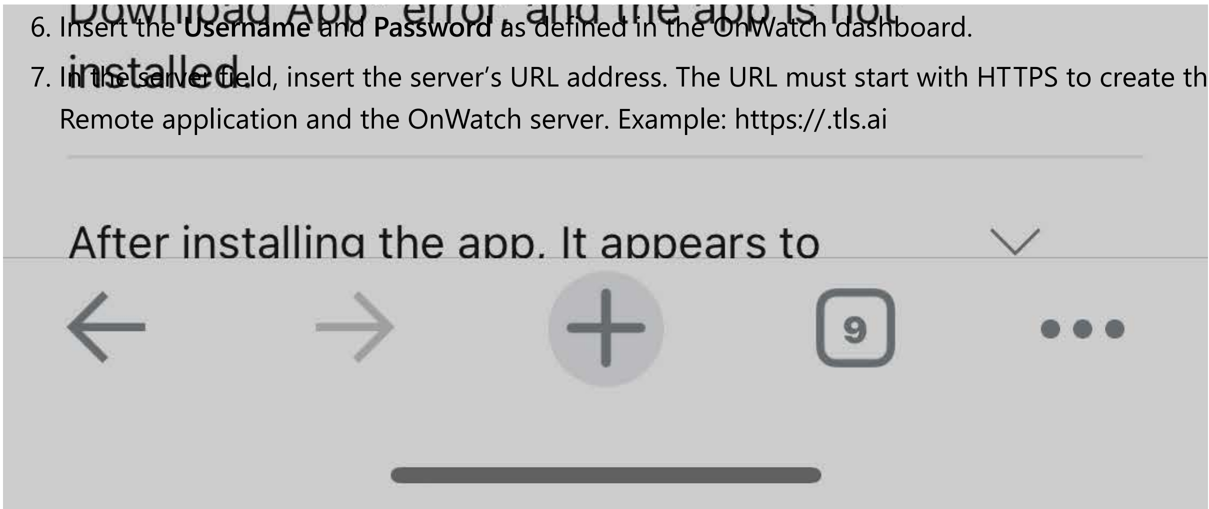


"appcenter.ms" would like to install "BTRemote"

Help

I get the message "Untrusted Enterprise Developer".

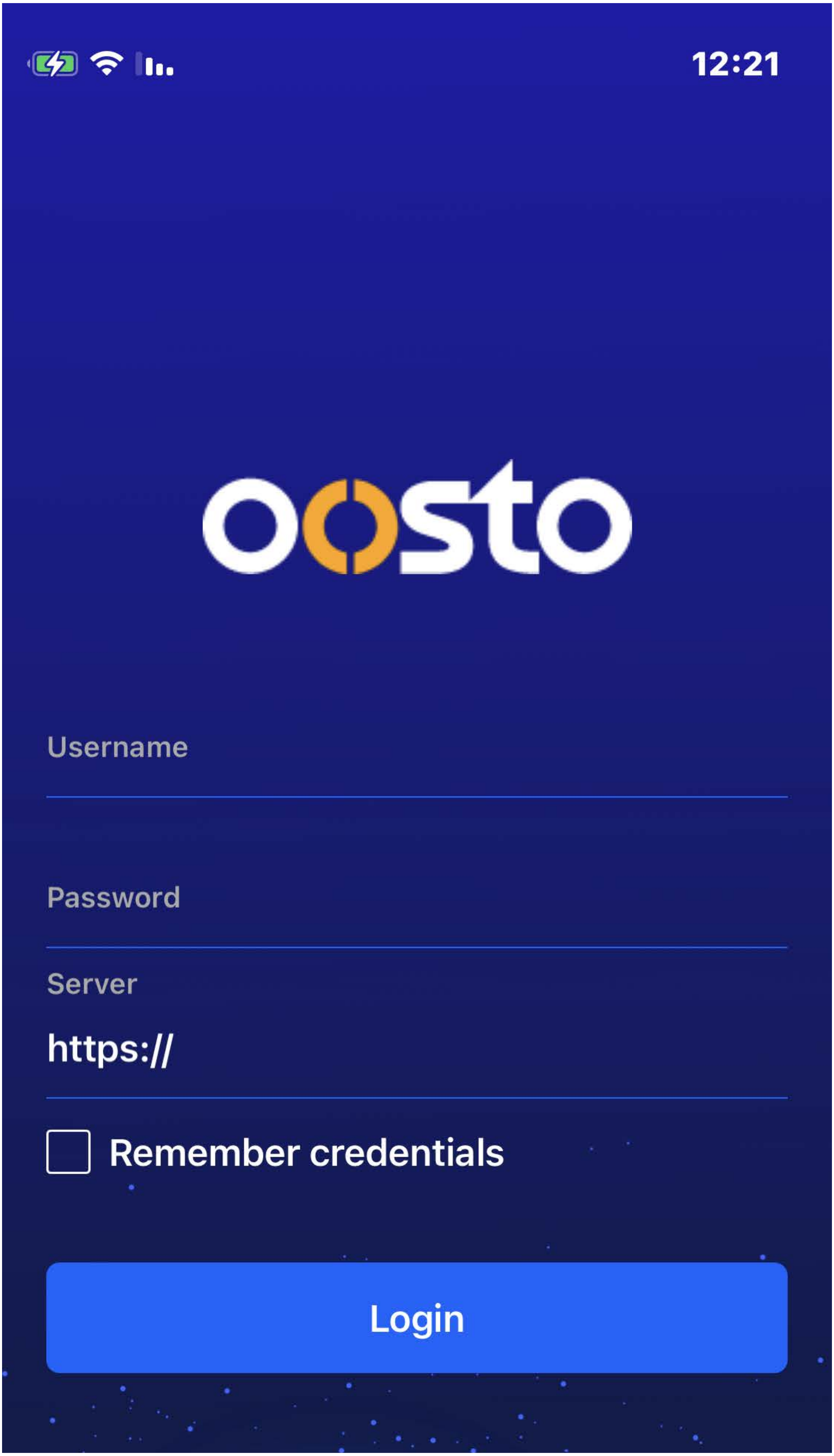
While installing the app, I get an "Unable to Download App" error, and the app is not



Download App" error, and the app is not installed.

After installing the app. It appears to

6. Insert the **Username** and **Password** as defined in the OnWatch dashboard.
7. In the server field, insert the server's URL address. The URL must start with HTTPS to create the link between the Remote application and the OnWatch server. Example: https://.tls.ai



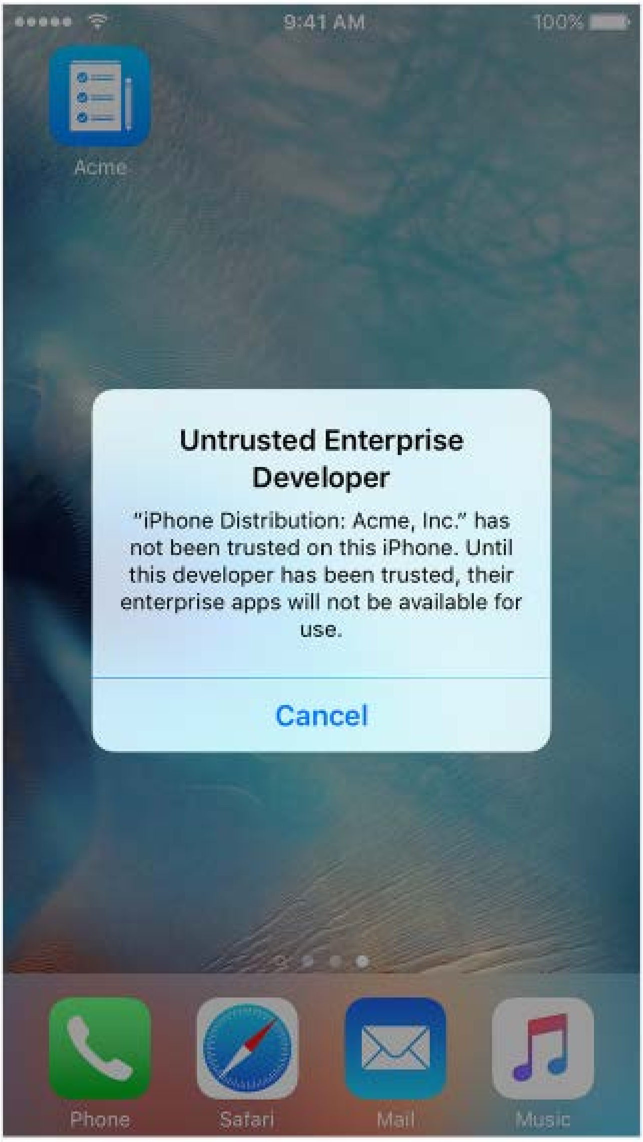
12:21
oosto
Username
Password
Server
https://
□ Remember credentials
Login

Congratulations! The On Patrol application is installed and ready to use.

🚧 iOS Installation Note - Trusted Developer Application

When you first open an enterprise app that you've manually installed, you see a notification that the developer of the app isn't trusted on your device. You can dismiss this message, but then you can't open the application.

Should the following image pop up when you try to open the app, follow the steps below to address this issue:



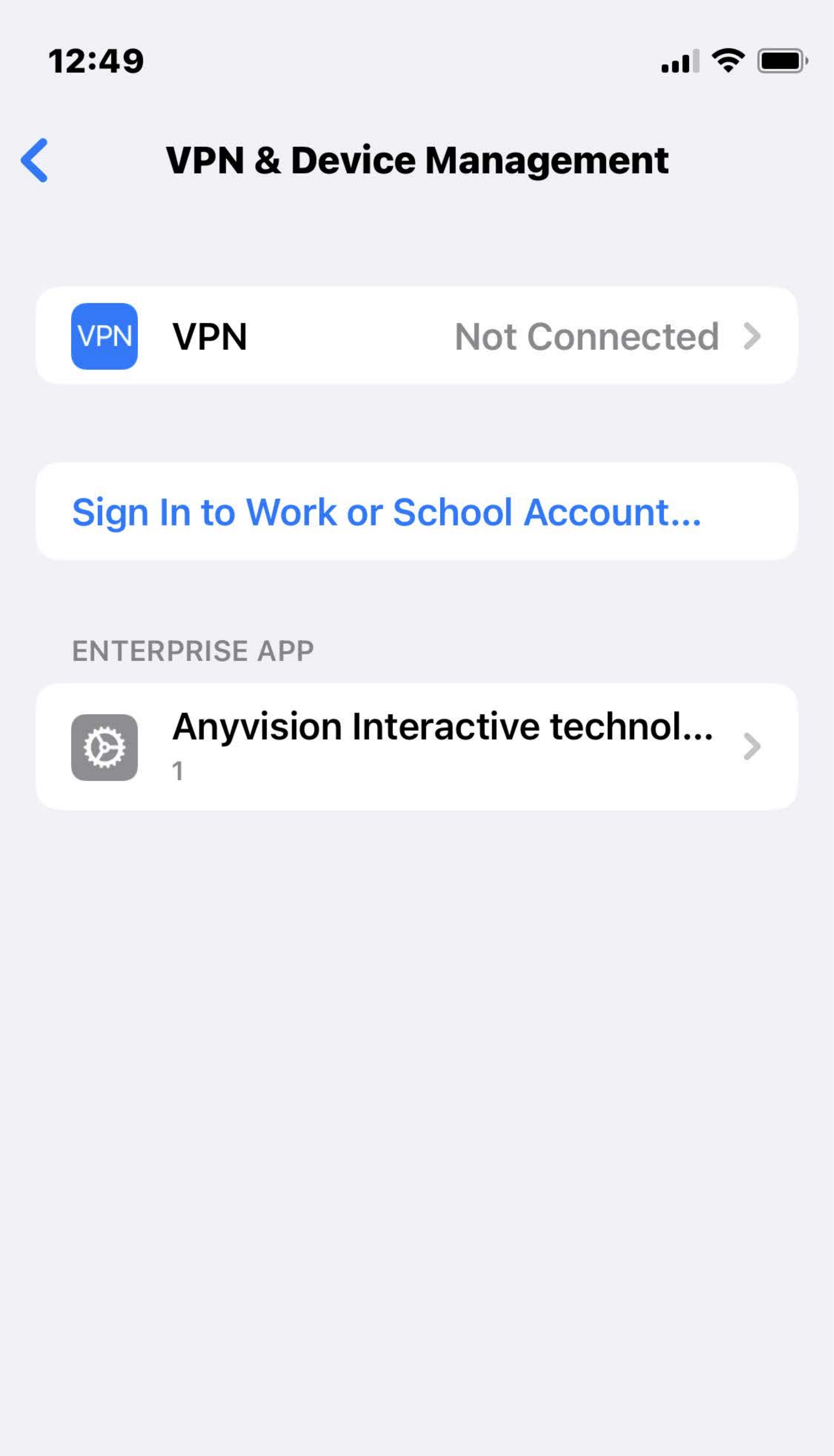
Untrusted Enterprise Developer

"iPhone Distribution: Acme, Inc." has not been trusted on this iPhone. Until this developer has been trusted, their enterprise apps will not be available for use.

Cancel

After you dismiss this message, you can establish trust for the app developer. Tap **Settings** > **General** > **Manage devices & VPN**.

Tap the name of the developer profile under the *Enterprise App* heading to establish trust for this developer.



12:49

VPN & Device Management

VPN — Not Connected

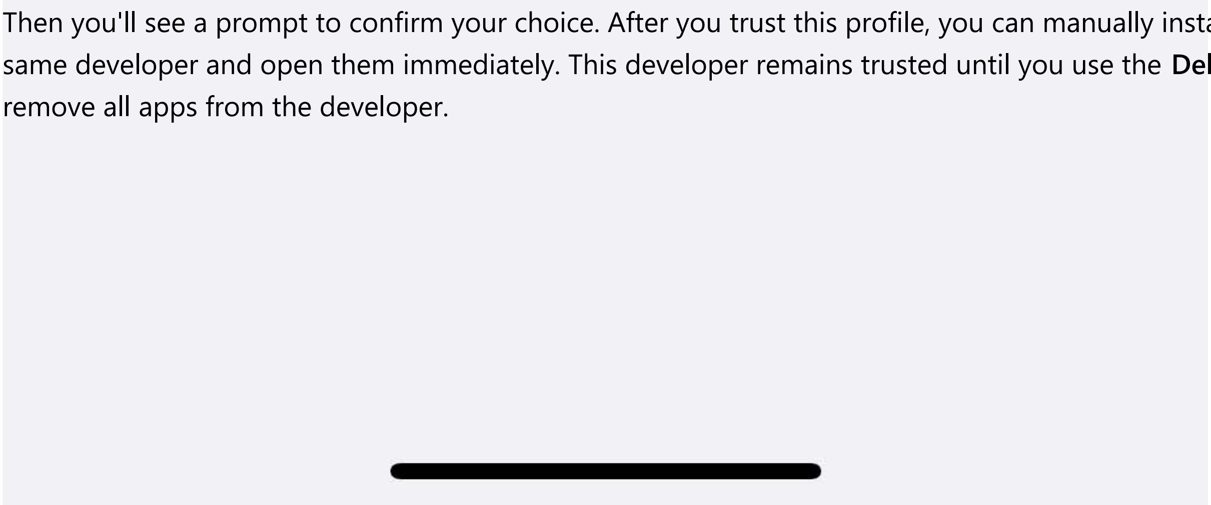
Sign In to Work or School Account...

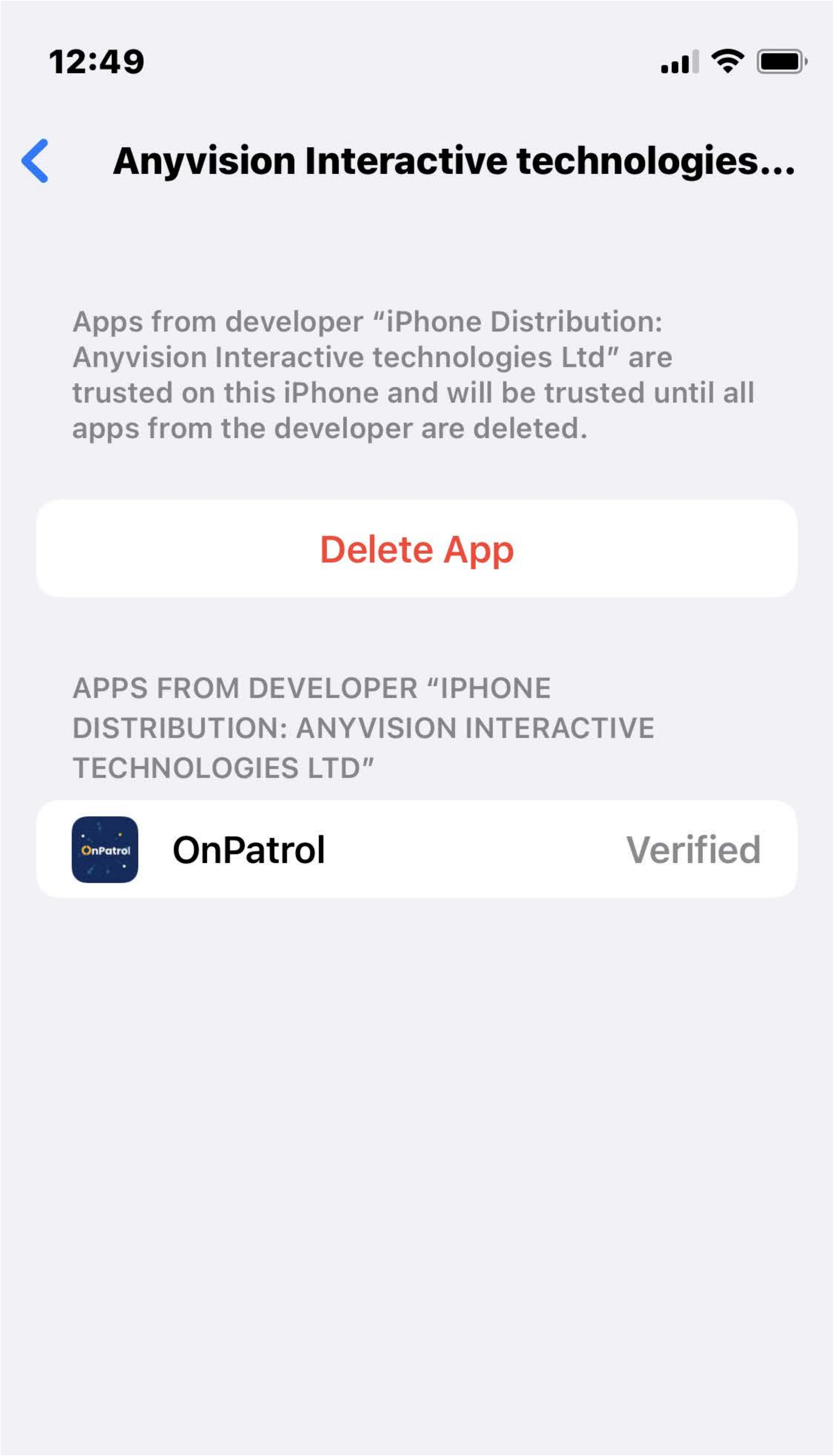
ENTERPRISE APP

Anyvision Interactive technol...

1

Then you'll see a prompt to confirm your choice. After you trust this profile, you can manually install other apps from the same developer and open them immediately. This developer remains trusted until you use the **Delete App** button to remove all apps from the developer.





Anyvision Interactive technologies...

Apps from developer “iPhone Distribution: Anyvision Interactive technologies Ltd” are trusted on this iPhone and will be trusted until all apps from the developer are deleted.

APPS FROM DEVELOPER “IPHONE DISTRIBUTION: ANYVISION INTERACTIVE TECHNOLOGIES LTD”

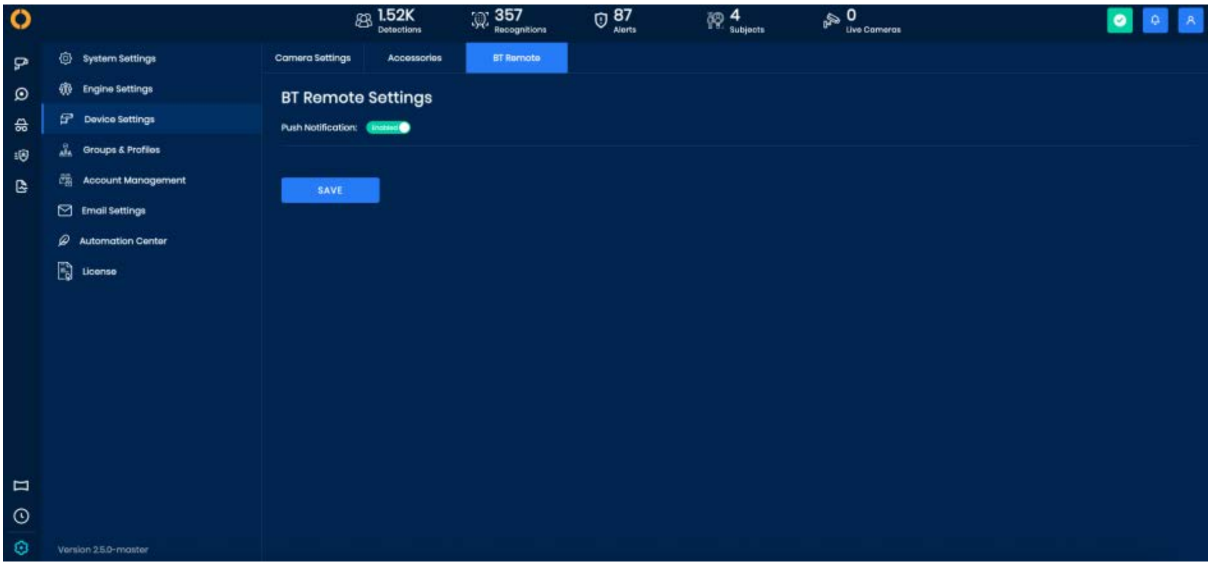
OnPatrol Verified

You must be connected to the Internet to verify the app developer's certificate when establishing trust. If you're behind a firewall, make sure that it's configured to allow connections to https://ppq.apple.com. If you aren't connected to the Internet when you trust an app, the device displays "Not Verified" instead. To use the app, connect to the Internet and tap the Verify App button.

After you verify an app for the first time, your iPhone, iPad, or iPod touch must reverify the app developer's certificate periodically to maintain trust. If you can't reverify, you may see a message that verification will expire soon. To maintain trust, connect your device to the Internet, then tap the Verify App button or launch the app.

Enable Remote on the OnWatch Dashboard

In order to utilize Better Tomorr[redacted]hin the Better Tomorrow dashboard. Simply navigate to the *Device Settings* section of the *Settings* menu and switch the **Push Notification** toggle to on.



BT Remote Settings

Push Notification: Enabled

Android Installation Guide

> ### Remote Is An Additional On-Demand Feature
>
> If you are interested in purchasing and using Remote, please contact your Oosto representative.

Overview

Oosto's OnPatrol Remote application sends alerts to a user's mobile phone whenever a real-time recognition occurs. With this application, security personnel can manage, monitor, track, and detain subjects or dangerous persons that enter a place of business, restricted area, or any other public or private location.
The application installed on a user’s phone in order to receive push notifications. This guide describes how to install the application.

OnPatrol Remote Preparation

Before beginning the installation process, please confirm the following:

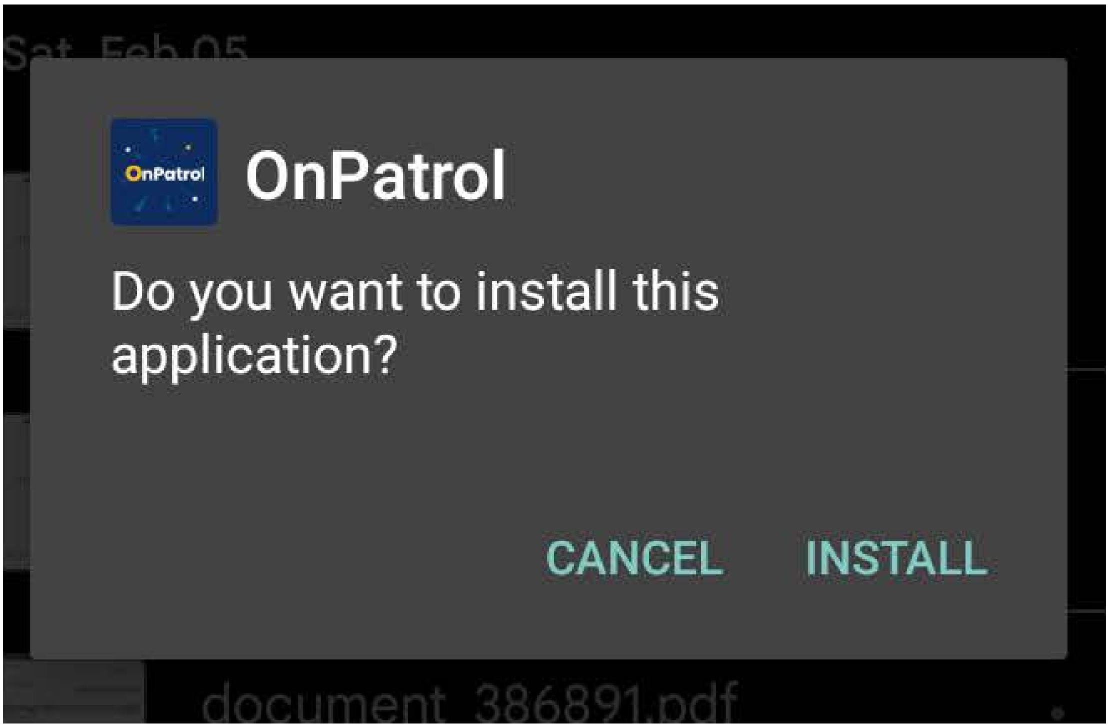
1. Both the mobile device and the OnPatrol server have internet access. The mobile notifications feature is internet-based so a shared network without internet access won't be enough. The easiest way to secure internet connection for both applications is to open a "Mobile Hotspot" on your own phone and connect both devices to the Hotspot network.
2. The OnWatch version is 2.x
3. The supported devices and operating systems are Android 6 or higher.
4. Verify the OW server has proper firewall configuration rules. Incoming port (Ingress) number 443 should be open to external internet networks and Outgoing ports (Egress) should have no restrictions. Nevertheless, if you'd like to restrict certain ports, make sure that the following Egress ports always remain open: 5228, 5229, 5230. This will allow proper connection from Firebase to enable the push notifications feature.

Installing OnPatrol on an Android Device

> 👍 **Remote Mobile Application**
>
> The following steps should be conducted on your mobile phone.

To install the OnPatrol application on a mobile device:

1. Click here to open and download the OnPatrol file.
2. Once the application is downloaded, a screen will appear. Tap **Install**. If the installation process fails, turn off Google Play Protect.
3. After the installation is complete, open the application by tapping the **Open** button.

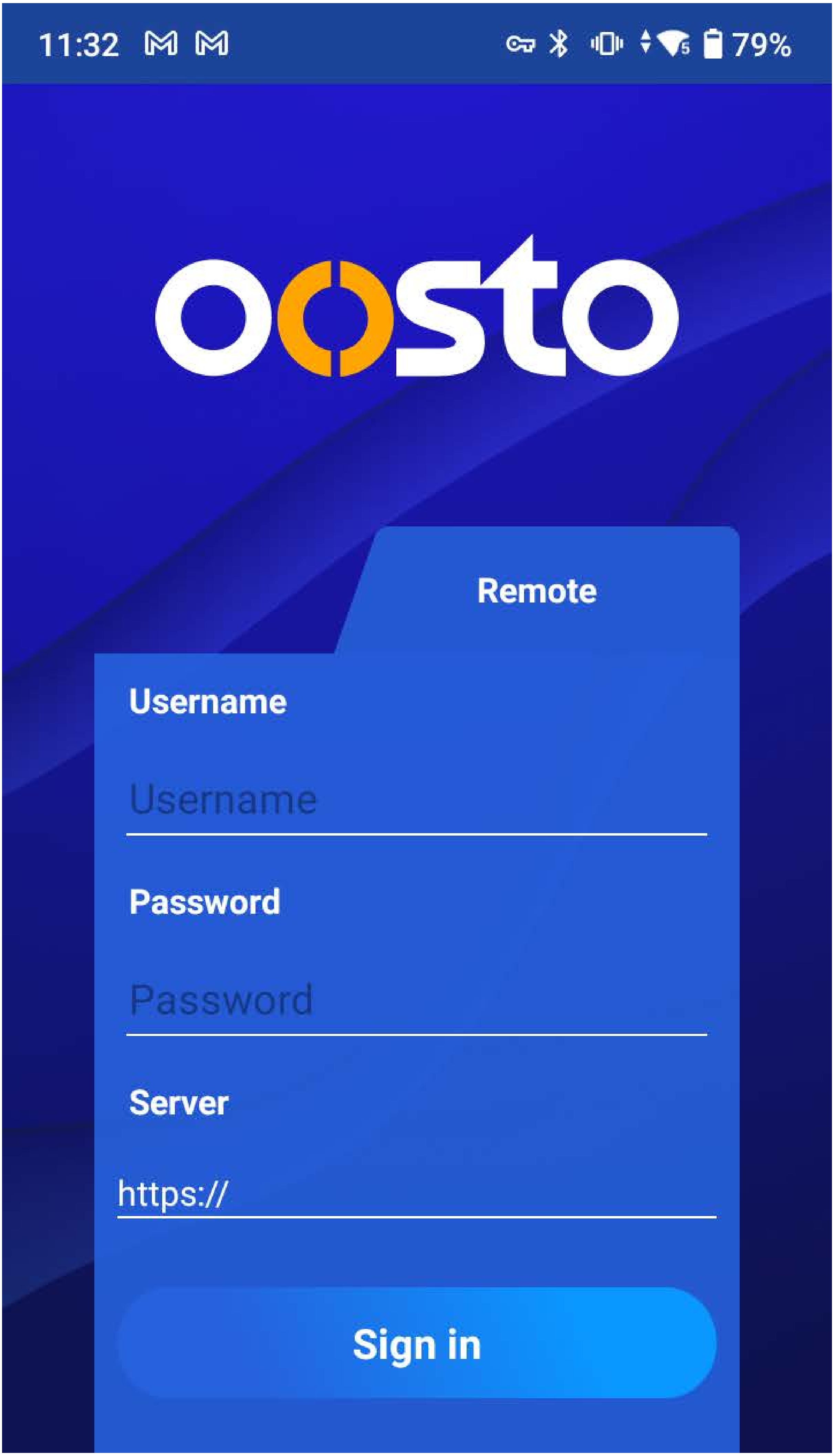


OnPatrol

Do you want to install this application?

5. You can now log in using your user credentials. Insert the **Username** and **Password** as defined in the OnPatrol dashboard.

6. In the server field, insert the server's URL address. The URL must start with HTTPS to create the link between the Remote application and the OnPatrol server. Example: https://.tls.ai



11:32 79%

oosto

Remote

Username

Username

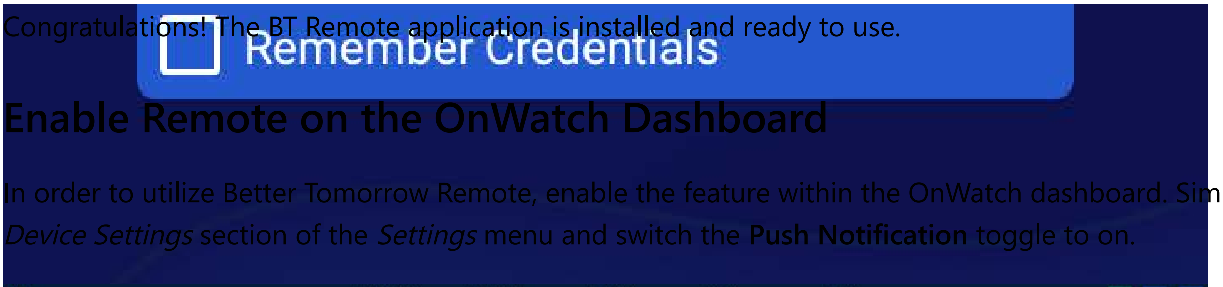
Password

Password

Server

https://

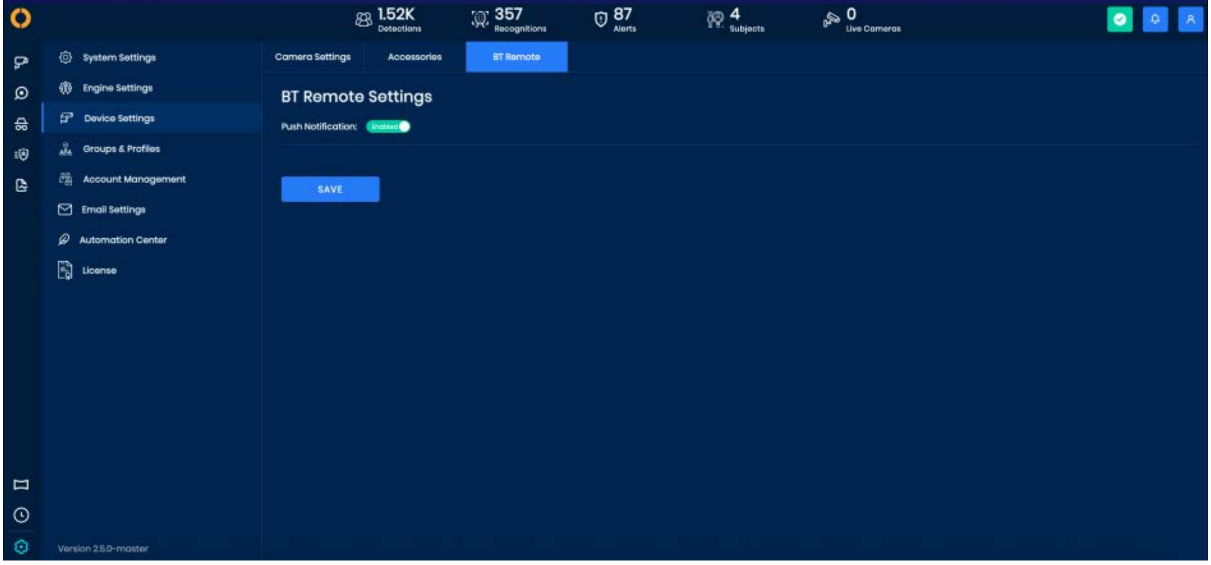
Sign in



Congratulations! The BT Remote application is installed and ready to use.

Enable Remote on the OnWatch Dashboard

In order to utilize Better Tomorrow Remote, enable the feature within the OnWatch dashboard. Simply navigate to the *Device Settings* section of the *Settings* menu and switch the **Push Notification** toggle to on.



BT Remote Settings

Push Notification: Enabled

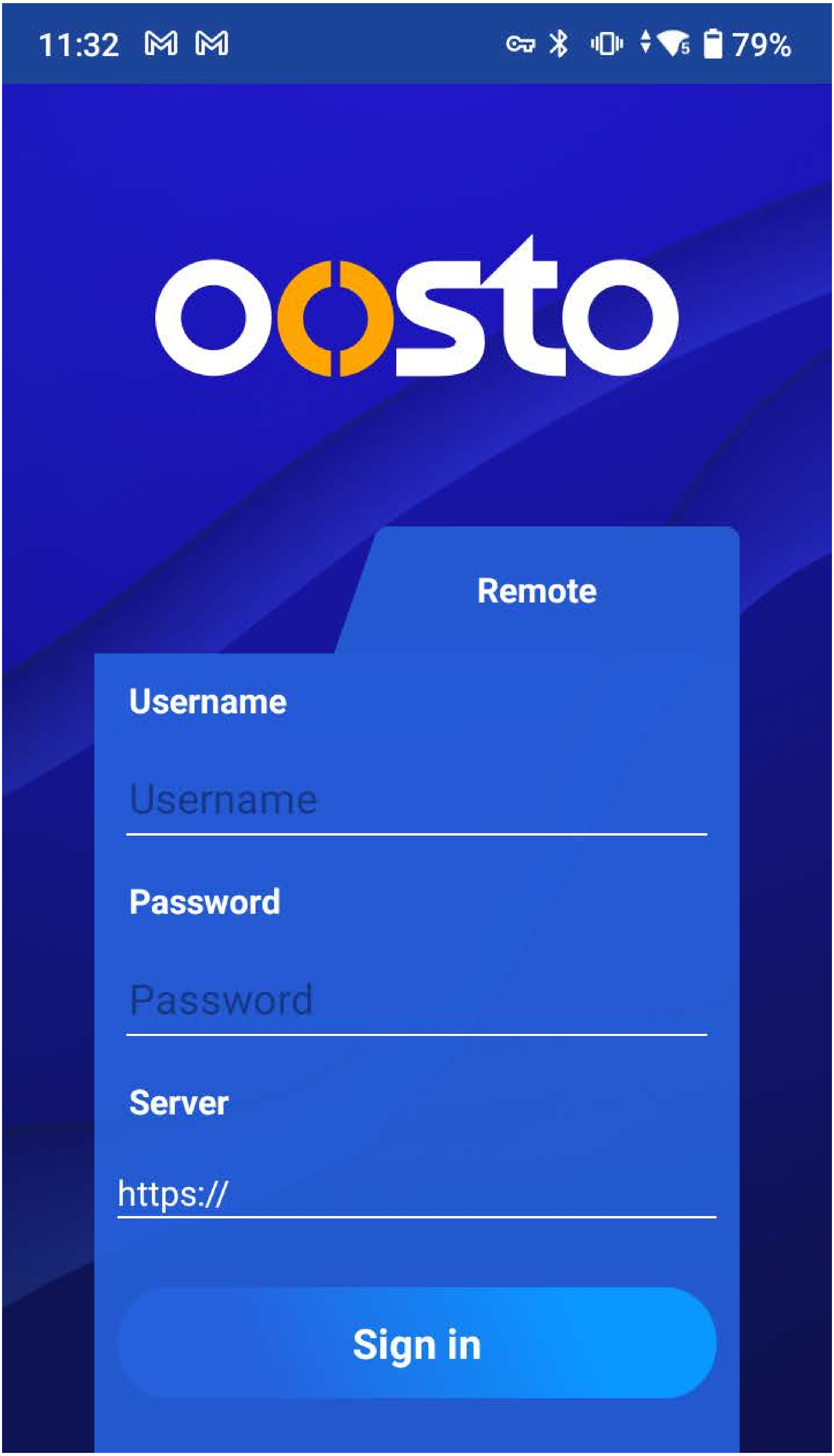
OnPatrol Remote Overview

Oosto's OnPatrol Remote application is a mobile client of the OnWatch system, it sends alerts to a user's mobile phone whenever a real-time recognition occurs. With this application, security personnel can manage, monitor, track, and detain subjects or dangerous persons that enter a place of business, restricted area, or any other public or private location. The application is installed on a user’s phone(Android or iOS) to receive push notifications.

Login

User will perform "Login" and register to an OnWatch server through the mobile app. From this point onwards, until the user manually logs out or the identification token is deactivated, he should receive a real-time push notification upon a POI recognition.

> 🚧 Limitation
>
> To receive notification the phone must be connected to the Internet.



11:32 79%

Remote

Username

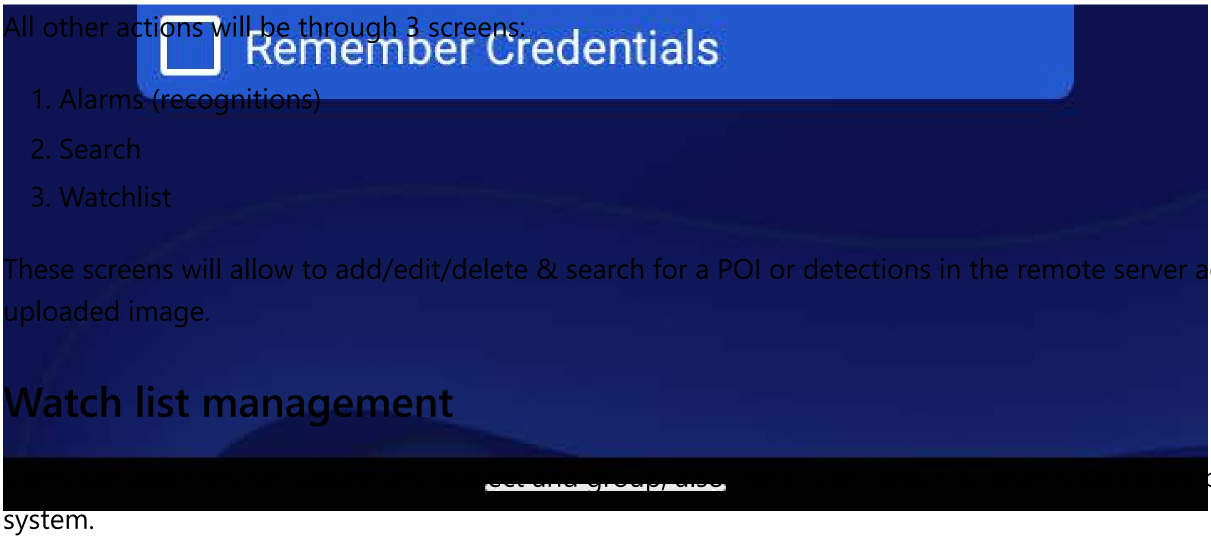
Username

Password

Password

Server

https://



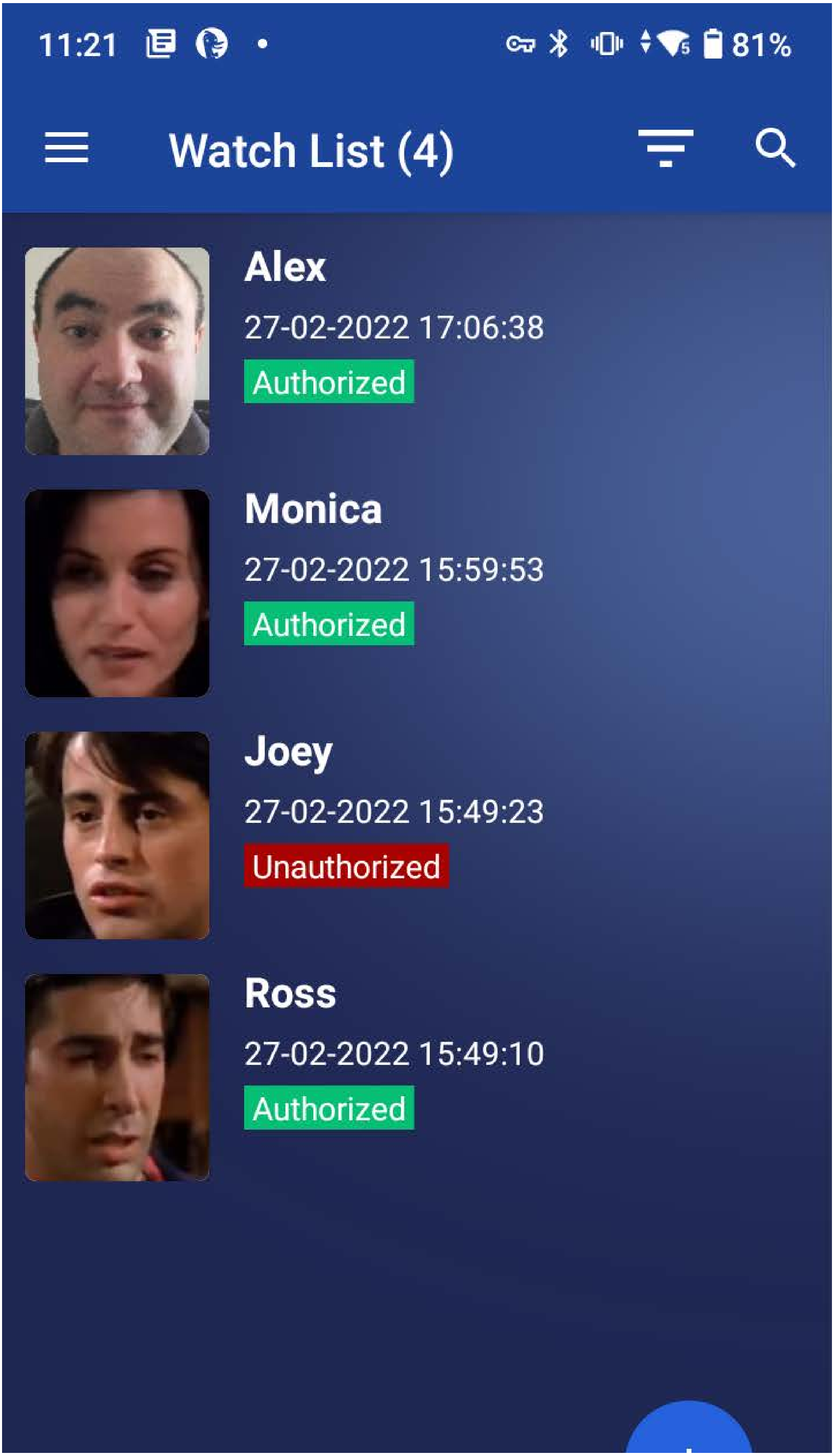
All other actions will be through 3 screens:

1. Alarms (recognitions)
2. Search
3. Watchlist

These screens will allow to add/edit/delete & search for a POI or detections in the remote server according to the uploaded image.

Watch list management

[illegible] by image or name in the system.



11:21 81%

Watch List (4)

Alex

27-02-2022 17:06:38

Authorized

Monica

27-02-2022 15:59:53

Authorized

Joey

27-02-2022 15:49:23

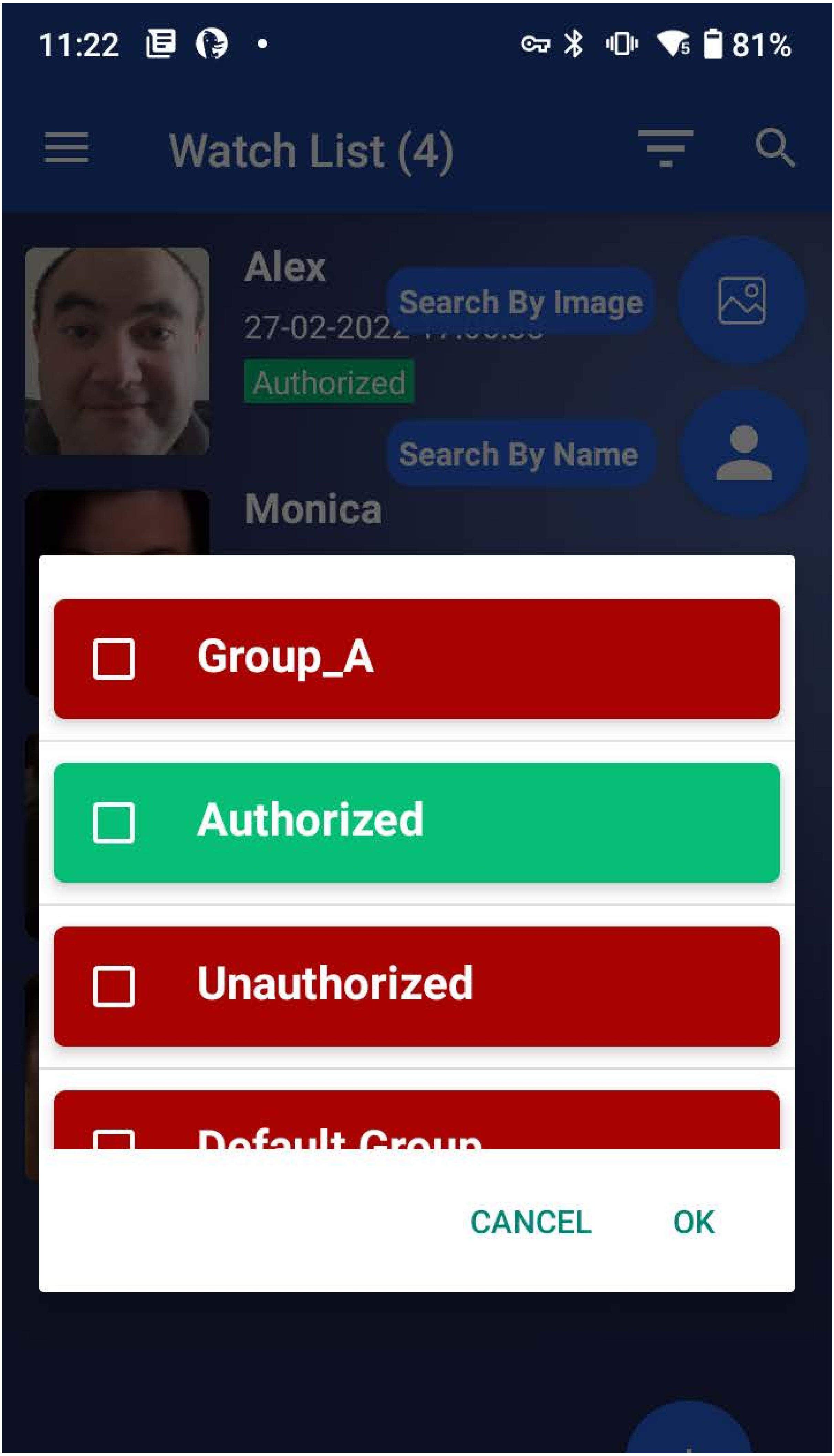
Unauthorized

Ross

27-02-2022 15:49:10

Authorized

And also to filter the watchlist by subject group.



□ Group_A

□ Authorized

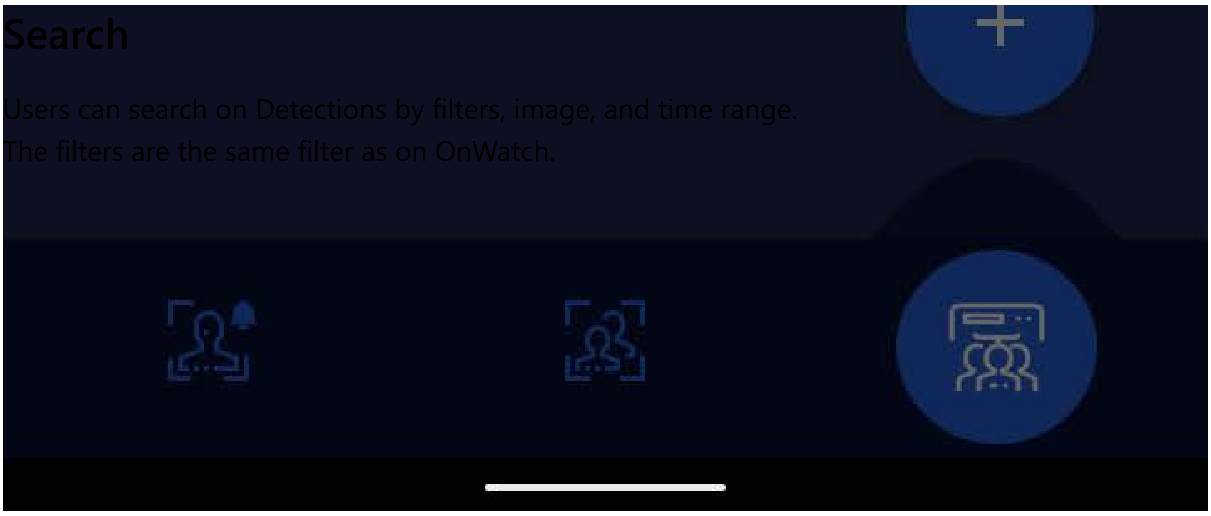
□ Unauthorized

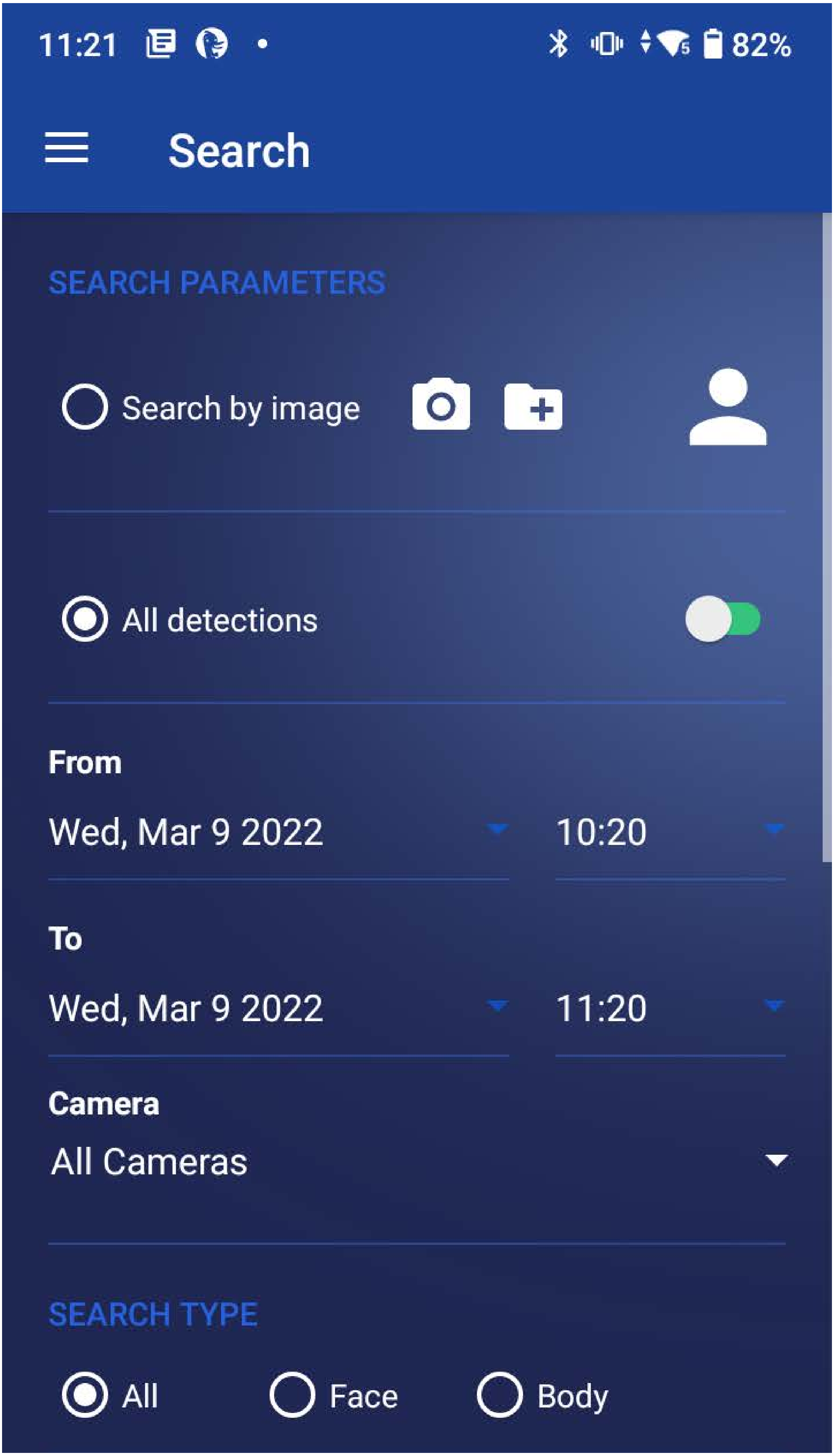
□ Default Group

Search

Users can search on Detections by filters, image, and time range.

The filters are the same filter as on OnWatch.





11:21 82%

Search

SEARCH PARAMETERS

○ Search by image

● All detections

From

Wed, Mar 9 2022 10:20

To

Wed, Mar 9 2022 11:20

Camera

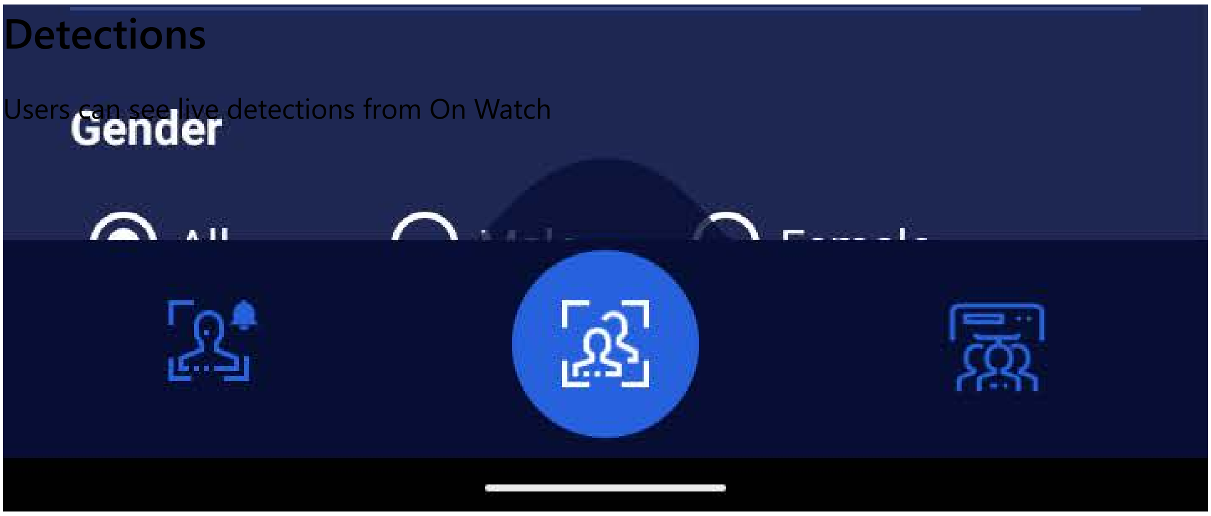
All Cameras

SEARCH TYPE

● All ○ Face ○ Body

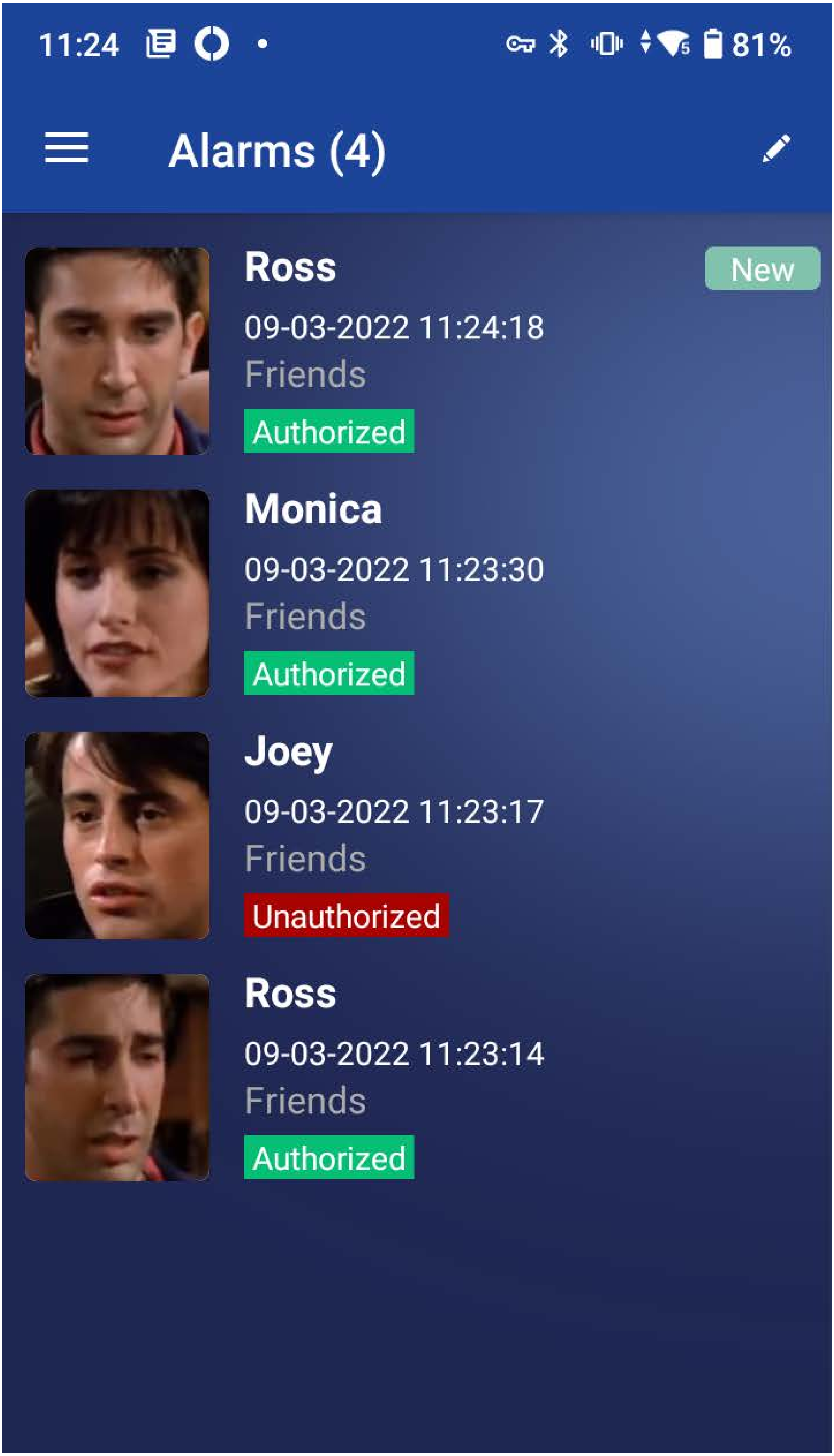
Detections

Users can see live detections from On Watch



Gender

● All ○ Male ○ Female



11:24 81%

Alarms (4)

Ross New
09-03-2022 11:24:18
Friends
Authorized

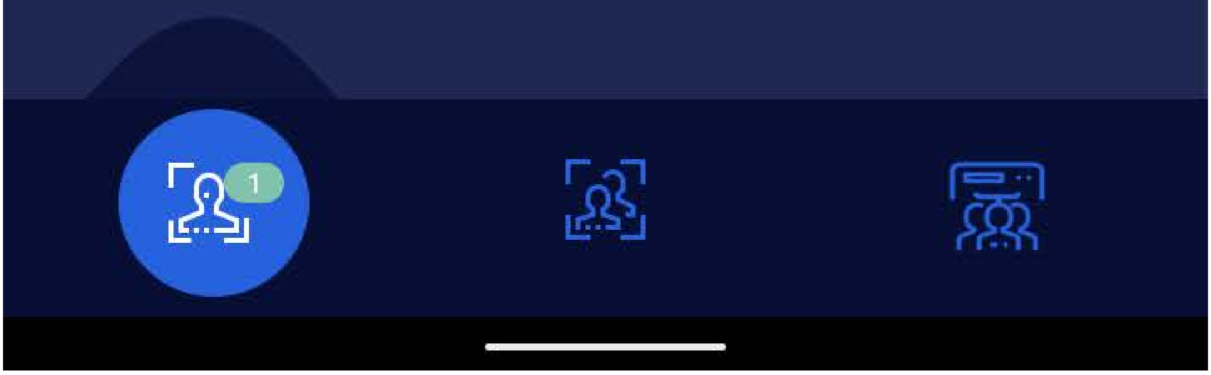
Monica
09-03-2022 11:23:30
Friends
Authorized

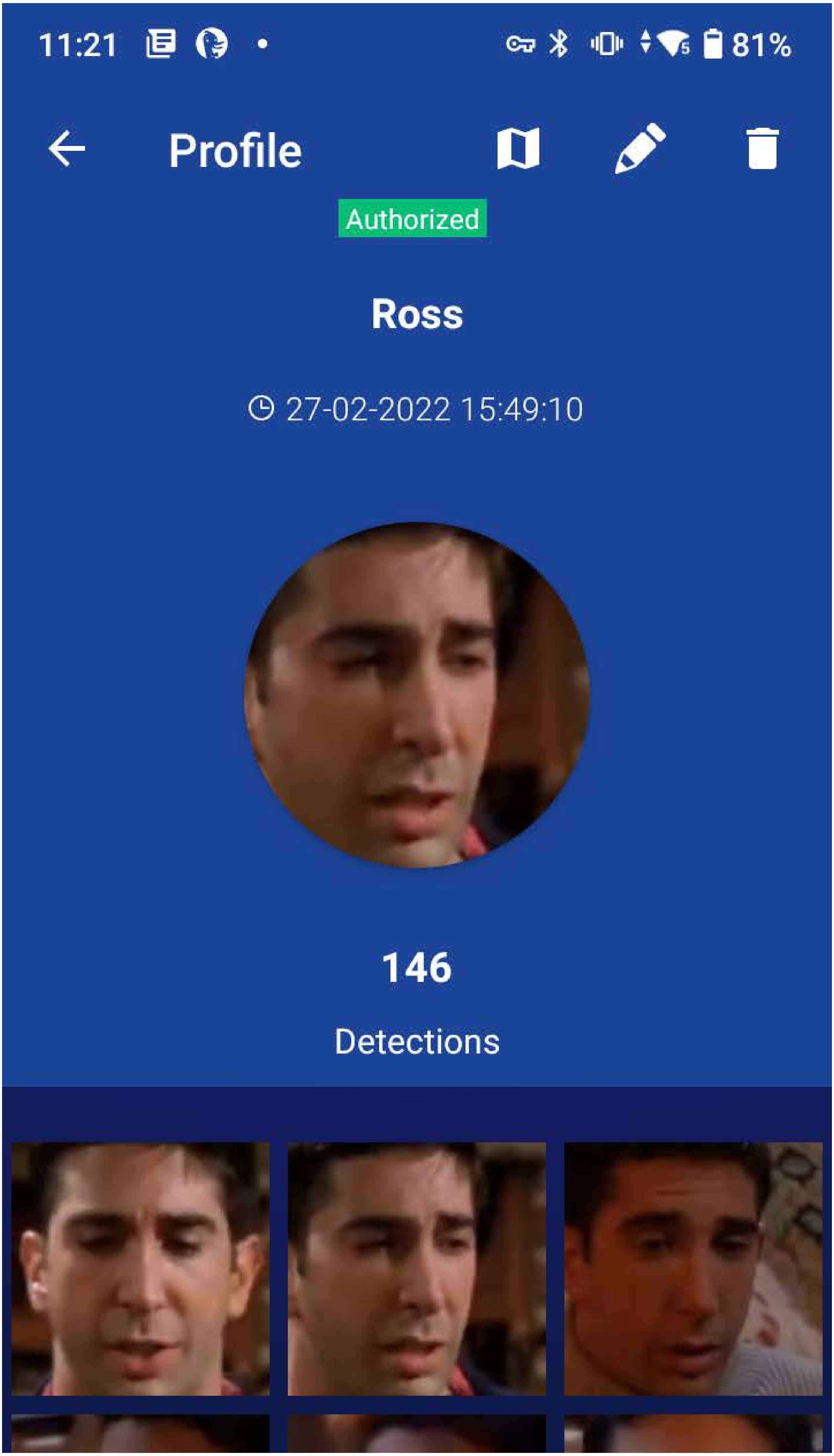
Joey
09-03-2022 11:23:17
Friends
Unauthorized

Ross
09-03-2022 11:23:14
Friends
Authorized

Subject profile

Users can edit the subject profile, and also see the subject timeline and play detection tracks.





Profile

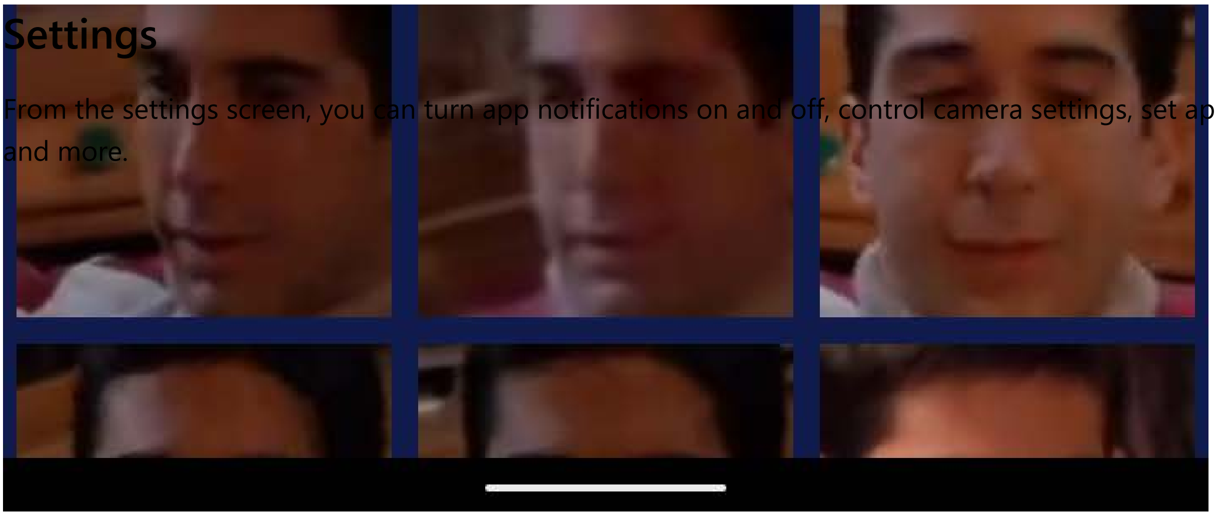
Authorized

Ross

27-02-2022 15:49:10

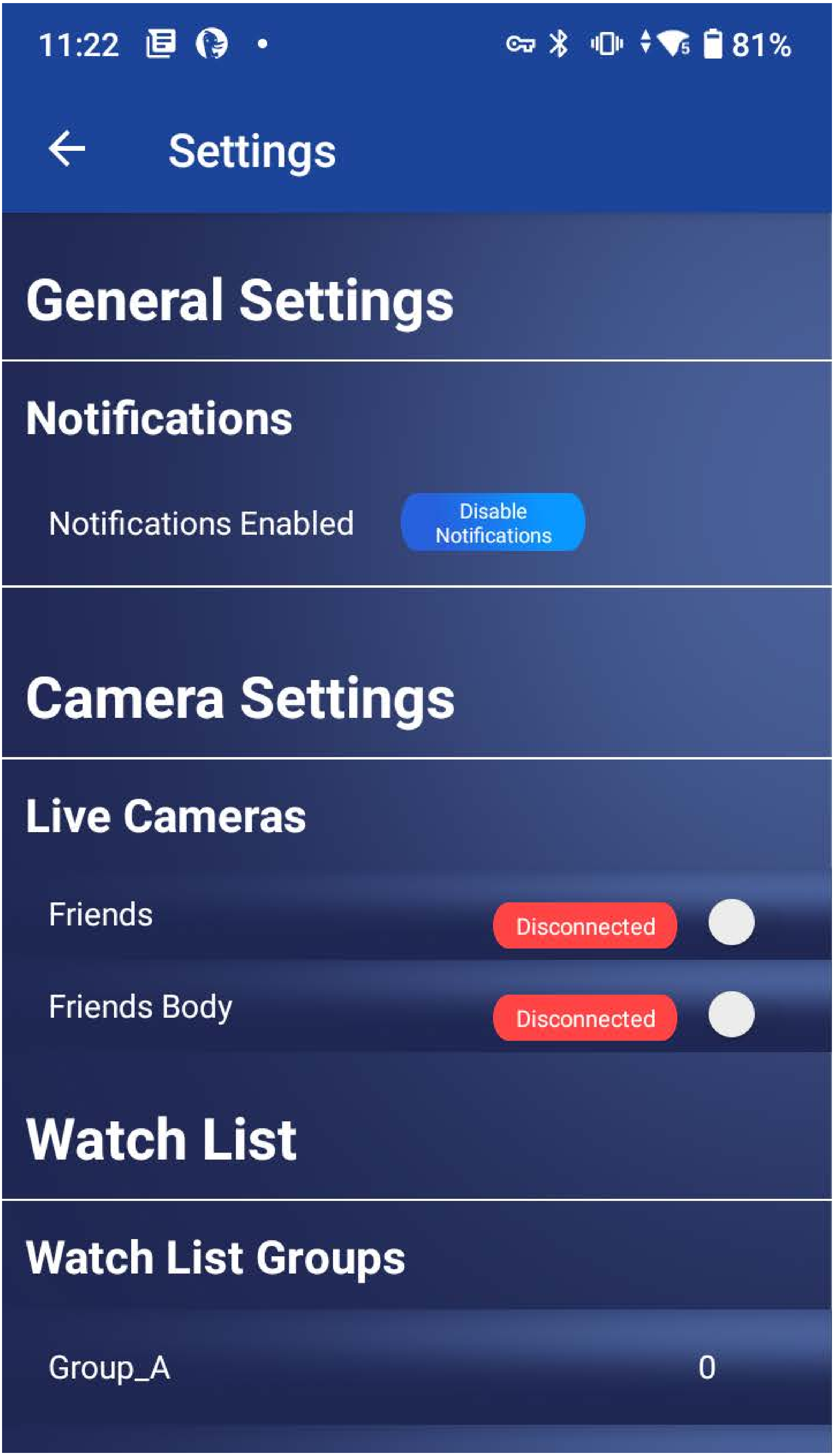
146

Detections



Settings

From the settings screen, you can turn app notifications on and off, control camera settings, set app storage warning limit, and more.



11:22 81%

Settings

General Settings

Notifications

Notifications Enabled

Camera Settings

Live Cameras

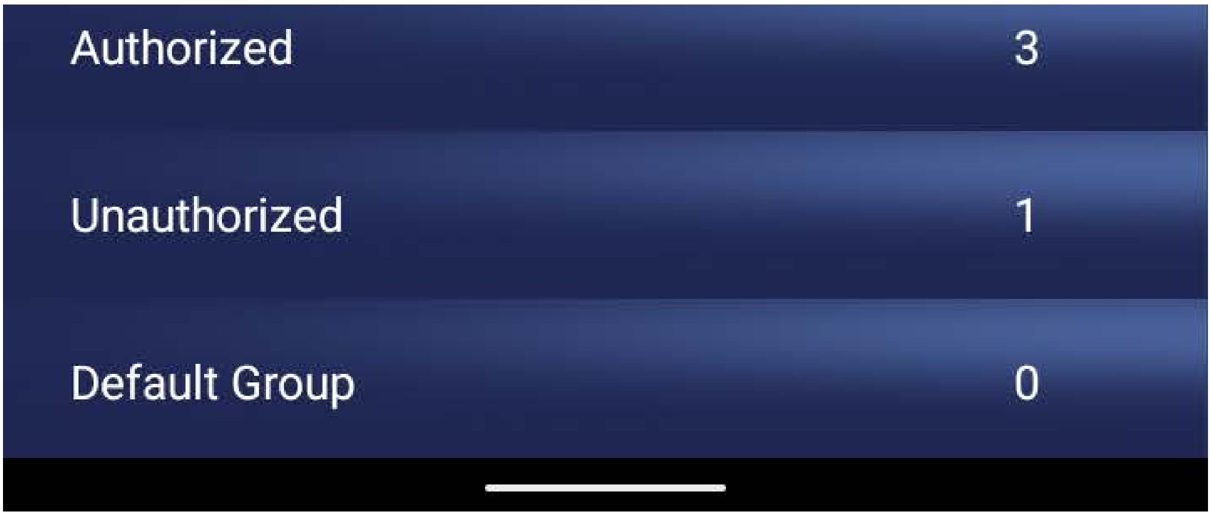
Friends Disconnected ○

Friends Body Disconnected ○

Watch List

Watch List Groups

Group_A 0



Authorized	3
Unauthorized	1
Default Group	0

Maintenance

Bug Fixes, Known Limitations & Change Log

Here you can find the following

- Fixed bugs
- Open Issues
- Known Limitations

For each main release and its maintenance packs

- For 2.6.x Fixes & Change Log
- For 2.5.x Fixes & Change Log

2.6.x Change Log

Fixes and Improvements

2.6.0-X

Fix Change Log	ID	Description
User group with multiple subject groups	14348	setting a user group with more than one subject group causes an empty mass import list
Search backward toggle	14325	Although the user runs mass import with enabled search backward feature it stays disable
Subject group popup	14318	Not all subject groups are displayed on the "Subjects groups" popup on the Mass Import issues page
Description text UI	14317	The subject description is cut on the Mass Import issues page
Camera pipe selection	14312	Users can select the AI camera's pipe for a CCTV camera (Camera stuck on reconnecting)
Audit log missing information	14308	The Audit log page is written with no useful information when a forensic case subject group is changed by the user
Login page	14306	Connect with SSO button is shown when LDAP is Enabled
Camera Video preview	14299	Camera Video Preview fails to stream video when the camera is created via API
Send events to VMS issue	14276	Detections&Recognitions are not sent to VMS
AI camera options	14275	Watch video button is accidentally displayed on AI Camera Tracks Manu
Roles table fix	14273	Super Operator is displayed as "Superator" in the user role info table
Logout issue	14270	Logout not working
Edit Subject	14186	User is not able to edit a subject description
Super operator permissions	14155	Super Operator can create Subject Groups via API (shouldn't be able to)
Email Alert	14143	The system failed to send alert email for a subject with no image
Mass import subject image	14142	Link to an invalid image is shown on the Mass Import Issues page
Subject image in a search result	14138	Link to an invalid image is shown on the search results
HQ subject sync	14126	Subjects with no images can not be synced with HQ
Edit subject images	14122	User is not able to delete the image from the subject if the image was assigned to a subject from a track
Add track image to the subject	14129	The subject image is saved, but UI keeps presenting a placeholder image

Fix Change Log	ID	Description
Export camera list	14111	Export Camera list to CSV fails to retrieve all cameras in the system
Custom system logo	14110	Main logo does not display on an email alert
Subject group selection on the inquiry page	14091	When the user navigates to subject group lists the subject groups are unselected
View inquiry case	14347	The inquiry "view case" option Shows an empty list
Conditional Authorization	14137	Conditional Authorization not working by the time profile
Camera grid pagination	10572	The camera table only shows the last 3000 cameras, adding more cameras will remove the first cameras from the table
Cameras status	5851	Cameras remain in "connecting" state after we reset the camera from the camera webpage
Cameras filters	5159	Get cameras with filters doesn't work when the route gets "streamTypes" and "filters" together

2.6.2-X

Fix Change Log	ID	Description
Resolve poor quality Mass Import issue	14360	Resolve poor quality Mass import issue fails on mass import report
Confirm leaving the camera page	14292	Stop request to confirm leaving when returning back to Devices without making any change
V1 to V2 migration	15294	Default group subjects imported to the OnPatrol group
Subject Group limit exceeding	14841	Missing System Message
Filter Mass imports grid	14829	The incorrect time selected when a user tries to filter the Mass import page by date/time
Resolve mass import issues in bulk	14818	If the user resolves mass import issues by bulk and some issues cannot be resolved because of the deleted subject, then images of the existing subjects will be deleted
On Patrol subject Group limit exceeding	14775	Missing System Message
Resolve issue notification	14756	Mass import resolve issues, do not show notification of the previously deleted subject
Replace reference image	14571	Additional images of the subject are deleted
Forensic short video loop	14358	Inquiry analyzing short video goes in an infinite loop and produces infinite detections
Search detections results	14271	The last detection image is cut on the search result page
Liveness error	5315	Streams running on Jetsons provide 0.0 liveness scores

2.6.3-X

Fix Change Log	ID	Description
Send unknown detection to VMS	16027	Unknown detections from the restricted camera don't show on VMS
Export cameras foramt	15044	Export Camera CSV has misaligned rows & headers

2.6.4-X

Fix Change Log	ID	Description
Watch video playback	5846	Watch Video playback is sometimes not available
Deprecated watch list	16391	Deprecated watchlist with open-vino install
Backup storage	15676	The storage became overloaded after running delta backups for several days
Association search	16301	The association search is not available sometimes
OnWatch text fix	16253	Settings Menu refers to BT Remote instead of OnPatrol
AD/LDAP Login Fails	16018	Added conditions to improve connection logic
Mass import stuck and failed	16120	Mass Import Fails After being stuck on "Processing 0%

2.6.5-X

Fix Change Log	ID	Description
Mass import quality issue	205	Duplicate items with a score 80 are shown with poor results
User is notlogged out	16935	When the user's role is changed by another user the original user is not logged out
Camera Timezone	16873	Disabled camera timezone as this is not required. It is derived from the map or the long / lat coordinates
Audit log	16732	Audit log format was updated for site detection
Unable to add new subject	147	This can occur when existing subjects were deleted and a new subject was added within a short period of time after the delete

2.6.6-X

Fix Change Log	ID	Description
Search by track	184	In specific circumstances, a search by track wouldn't return any results
ffmpeg configurations	95	Allow new pipeline to support ffmpeg options such as TCP/UDP
Livness activation	94	Enabling liveness setting did not work
Search by Image	93	Search by image sometimes caused an SQL error
Audit log is shown to end user	76	End user is shown an internal system job audit log for deleted devices
OnPatrol Remote no video playback for alerts	74	When receiving alerts video playback not working, although it will work when searching
Camera additional settings are overwritten in API	66	When changing mask classified in UI the additional setting would be overwritten
Inquiry alerts not deep linking to search by track or locate detection	65	When clicking on an alert generated form inquiry some functions would not deep link
"Realtime route" and "Historical route" hidden in case context	64	When using case track "Realtime route" and "Historical route" are not hidden
Watchlist subject count is not correct	63	In some circumstances, the watchlist count when deleting is not displayed correctly
Licensing errors	61, 60, 53, 55, 52, 51	Licensing errors not shown in the correct context for multiple locations in the application including mass upload and camera details
Liveness o[ption not disabled for body/person camera	56	Livness was now disabled in the correct context
Audit log improvement	49	Search by association with dwell time not written to audit log properly formatted
Search by image with association	47	Error occurred in some circumstances
Incorrect authorization status	45	Incorrect authorization status for conditionally authorized subject in some circumstances
Extra large watchlist on GPU	32	When updating user details without updating the image the subject will not be matched any longer
Automatic camera load balancing	28	Some cameras would loose the automatic status when updating the camera details
Super Operator Acknowledgment	38	Operator role and up are able to acknowledge alerts
Email settings text correction	30	A test message will be sent to the mentioned email address if the connection was established correctly

Fix Change Log	ID	Description
Audit log	22	Source IP not shown and not ordered on download
Inquiry configuration issue	21	When editing some inquiry advanced configurations it would throw an error
Allow specific pipe to be chosen from inquiry	27	Allow specific pipe to be chosen from inquiry
Error creating a time profile	24	Error creating a time profile
Bulk camera action results	18	Not all cameras were included in all filter

2.5.x Change Log

Fixes and Improvements

2.5.0-1

Fix Change Log	ID	Description
Inquiry camera status not patched	12202	When showing a camera within the context of inquiry cases its shows the connection status, if the status is changed whilst viewing it doesn't get patched until refresh
MKV File upload	12697	The user interface was blocking MKV files
Realtime/Historic route failed	12554	When initiating Realtime route and historic rout outside of view sources it failed
Deletion of case Job failed over 10K files	12631	Inquiry cases can't be deleted over 10K files which is an edge case. (We targeted 5K files) Already in Known issues
Crops are not deleted from S3, although relevant tracks were deleted together with deleted case by cron job	12651	Zombie content expands the DB for no reason
DB Zombi camera group (case) even though the case doesn't exist and the deletion job scheduled	12657	Zombie content expands the DB for no reason
Camera group (case) is not deleted if only images are within the case	4856	Zombie content expands the DB for no reason
After the case deletion, the relevant tracks and recognitions were not marked as isDeleted =true, although case files and cameras were marked as isDeleted = true	12730	Zombie content expands the DB for no reason
Case with auto delete true with overdue TTL is not deleted after the relevant cron job execution	12672	Case not deleted automatically
Aggregated view result	12564	UI showing images in different sizes when results dont fill the page
Long subject group names	11317	Support for extra long subject group names without breaks

2.5.0-2

Fix Change Log	ID	Description
System crash	13437	The system crashes, if user click on unselect all cameras checkbox on Search page
More than 10 subject groups not being displayed	13434, 13429, 13436	User is able to see only 10 subject groups on the Watch List and search page and on the Edit Case page
Alternative camera TH not being set	13469	If alternative camera TH feature enabled, then TH value does not sent to the server and user is not able to save the camera changes.
Padding misaligned	13468	Values are misaligned to set padding
FFMPEG custom calibration	13462	FFMPEG custom calibration field configured to be available
Duplicate email notifications	13113	When a subject is is multiple groups duplicate emails would be sent
Unselected camera data stays on live view	13447	Although cameras are not selected, their detections, recognitions and alerts displayed on the panel in some cases
Email alert Null displayed in text	13421	When product name isnt defined Null was displayed
Single Alert stretched in some cases	13439	In alerts view a single alert sometimes stretched across expanded view
Cluster installation issue	3459	Services permission were fixed to allow cluster installation
User cannot edit a camera	12933	If the description field is null (camera could be created via API without description)
V1.24.0 - V2 migration added	3471	V1.24.0 - V2 migration added
AVI support	12695	Support for a custom malformed AVI was added

2.5.1-0

Fix Change Log	ID	Description
Camera API Fix	13741	API calls fails and parameters are not in the right format
User cannot see all search result	13429	User is not able to see more than 10 subjects on Subjects pane on Search page
Licensing API Fix	13739	Unnecessary parameters removed from API
Disable camera liveness issue	13596	User is not able to disable a face camera liveness feature
Route access with API keys issue	13536	Can't reach /storage route with API keys
Viewer on inquiry page error	13442	Viewer get authorization error from Inquiries page
Email notification content	13421	"Null" displayed on alert email notification instead of product name
Expired Token	13333	Token expiration does not logout user from UI
Search backward	13231	Search backwards fails if there is 0 cameras/forensics in the system
Missing information on the Audit log	13154	User full name is missing sometimes
Search specific dates UI	13080	Text cuts on Search specific Dates
Cant get Locate detection	13001	Locate detection feature does not work for inquirie's video file track
Previous Dates filter	12958	The "Previous Dates" filter radio button is unselected when user changes the filter value
Specific Dates filter	12956	Tracks are not filtered appropriately by "specific dates" filter
User cannot see all subject groups	12777	Only 10 subject groups are displayed on the Assign/Move popup, although there are more subject groups
Mask Detection filter	12725	Mask Detection is active even when toggled "Off"
inquiry drag & drop limit	12718	Drag & Drop folder in Inquiry only uploads 100 files max
Subject map route trace	12709	Cameras, which taken part in subject route are not displayed on the Live Cameras map
Inquiry AVI preview	12696	Added video preview for AVI formats is not supported massage
Detections count text	12615	Live view (cases) showing detections from X source instead of cases
Cameras grid filter	12590	Cameras filter grid state is not being kept after editing camera
Search fields sync	12507	Search fields Drop Down not synced properly

Fix Change Log	ID	Description
Sort watchlist UI	12326	close drop down after (click) sort on the watchlist page
Save camera	12258	User is not able to save camera with threshold 0
Camera status change	12202	The camera status does not change on the file management page
Unknown icon UI	11340	Unknown alert icon displayed outside the alert notification
System crash when adding camera	11160	"Add Camera" when having more then 1000 "Camera groups"
Jeston Max streams	5047	Max streams on jetson aren't limited

2.5.1-2

Fix Change Log	ID	Description
Map zoom	14291	Maps Zoom settings not persistent
Delete subjects tracks	14295	Deleted subjects were not removed from Alerts
Bulk delete	14294	PostgreSQL DB got crashed due to bulk delete subjects messages from the subjects service

2.5.1-3

Fix Change Log	ID	Description
Streams & tracks datetime	14355	Unaligned source_datetime between tracks & streams tables affect watch video

Known Issues

Known Issues	Details
Inquiry cases deletion	Occasionally inquiry cases cannot be deleted on the first attempt
Camera calibration tool	When opening the calibration tool without any changes it causes an error on closing
Alternative threshold	When disabling an alternative threshold the change does not take effect

2.5.0-x Limitations

Known Limitations	Details
Delete case fails	If a case has more than 10K files delete case fails
Body attribute Grey Top is not available	When searching by body attribute color grey/top search fails to detect grey tops
HQ subject groups in site	HQ subject groups are shown in the bulk actions menu although they cannot be controlled on the site
Live preview (VIsion AI Appliance)	Live Preview icon should not be enabled for Jetson channels
Bulk jobs in watchlist	When two people do bulk jobs both user's actions will happen, which may negate the other users request
Padding for camera calibration via image selection only	No manual numeric padding adjustment
Mass upload of a single image not available	A single image in mass upload not will not work

Advanced System Setup

Large Watchlist Support via GPU

To enable Oosto Large Watchlist support which can be over 50K on a small server or over 300K on a large server the system is able to utilize GPU-based watchlist vector matching.

Face/Body features in our system are vectors that can be compared against each other very efficiently by utilizing this new technology.

On request, the track vectors will be queued and then fetched in bulks to utilise the ability to verify batched queries in high efficiency.

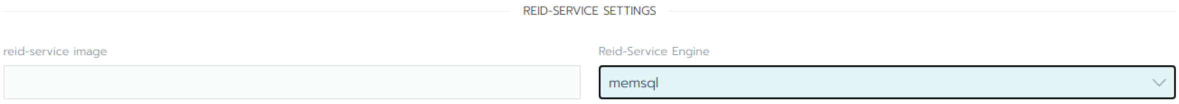
In order to support higher tracks/detections throughput the below configuration needs to be utlilized

How to configure?

In order to be able to support a large watchlist via GPU need to configure it by connecting to the Rancher do the following -

Manually configure the following

- Log in to the rancher
- Upgrade the App layer
- Edit the Reid Service Engine section to "faiss" (default is "memsql")



REID-SERVICE SETTINGS

reid-service image

Reid-Service Engine: memsql

Environment variables that can be adjusted:

reid-service:
This parameter allows the control of the number of GPUS that the Large Watchlist Service is utilizing

GPUS_TO_DETECT

```
GPUS_TO_DETECT=0
```

stream-scheduler-service:

LOAD_BALANCER_EXCLUDED_PIPE_ADDRESSES

```
LOAD_BALANCER_EXCLUDED_PIPE_ADDRESSES = ["pipeng.tls.ai:50051,pipeng.tls.ai:50052"]
```

No GPU Server

Ossto is able to utilise a technology called OpenVino to support Non GPU based servers.
The configuration should be discussed and optimized wth your Oosto technical contact as each deployment will have

different needs according to capacity demands.

OpenVINO utilized Intel Chips to provide AI processing.

We recommend this configuration is used for systems focused around Edge-based processing such as the Oosto Appliance, Honeywell S70 and the OOSTO OnPoint.

The central server is able to handle a few channels of Inquiry, watchlist management or RTSP steams if required.

Configuration of OpenVino Support

In order to be able to support Non-GPU based processing the following should be configured by connecting to the Rancher and editing the Environment variables section.

Just need to add those new variables:

Text

```
PIPENG_pipe_defs__OV: "1"
PIPENG_pipe_defs__TRT: "0"
NVIDIA_VISIBLE_DEVICES: "void"
```

- PIPENG_pipe_defs__OV - telling the system to work with non-GPU (openvino) mode (0 - off, 1 - on).
- PIPENG_pipe_defs__TRT - telling the system to work with GPU mode (0 - off, 1 - on).
- NVIDIA_VISIBLE_DEVICES - void means ignoring the GPUs on the host instead of using the GPU amount.

[2.0.1] OnPatrol Edge

Welcome to OnPatrol Edge

Welcome,

OnPatrol Edge provides a tactical solution for mobile forces in the field with live, real-time, mobile facial recognition. An alert on your mobile phone notifies you as soon as a person of interest is recognized. This does not require mobile reception or internet access!

OnPatrol Edge works with any one of the following: a Wi-Fi or USB camera, or your mobile phone's internal camera.

You can sync subjects from the OnWatch server to the OnPatrol Edge app to get subjects right from the central system.

When a subject (in a watch list group) is detected crossing the field of view (FOV) of the camera, the configured alert is triggered (sound alarm, visual popup and/or vibration). Color-coded watch list groups allow for easy differentiation between different types of subjects.

You can then view the location of the subject on a map, and if the subject were previously spotted, their detections would be presented on the subject profile.

At any stage, you can add (or delete) a detected subject to (or from) a watch list, and record information on their profile.

Accurately identifying a subject reduces the probability of misidentification. Combined with the use of appropriate watch list groups, this offers increased protection to both civilians and law enforcement bodies.

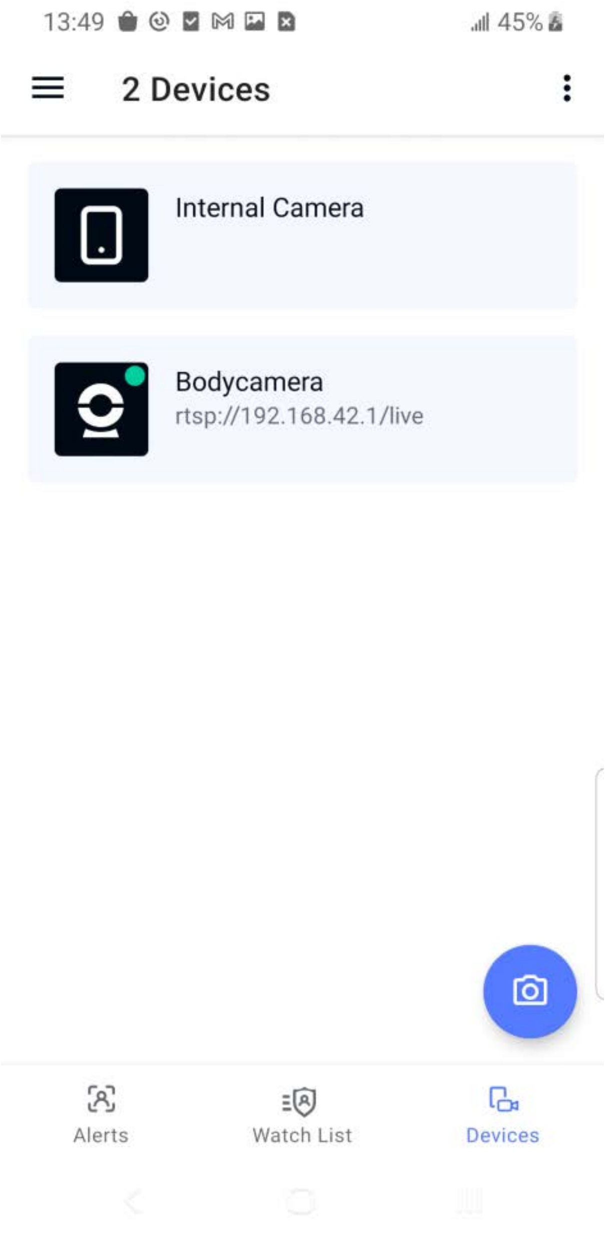
Manage Devices

For live operations, you can use the internal camera, or add USB, wireless, or Wi-Fi cameras. You can tap to select which camera to use, and switch between live and background modes.

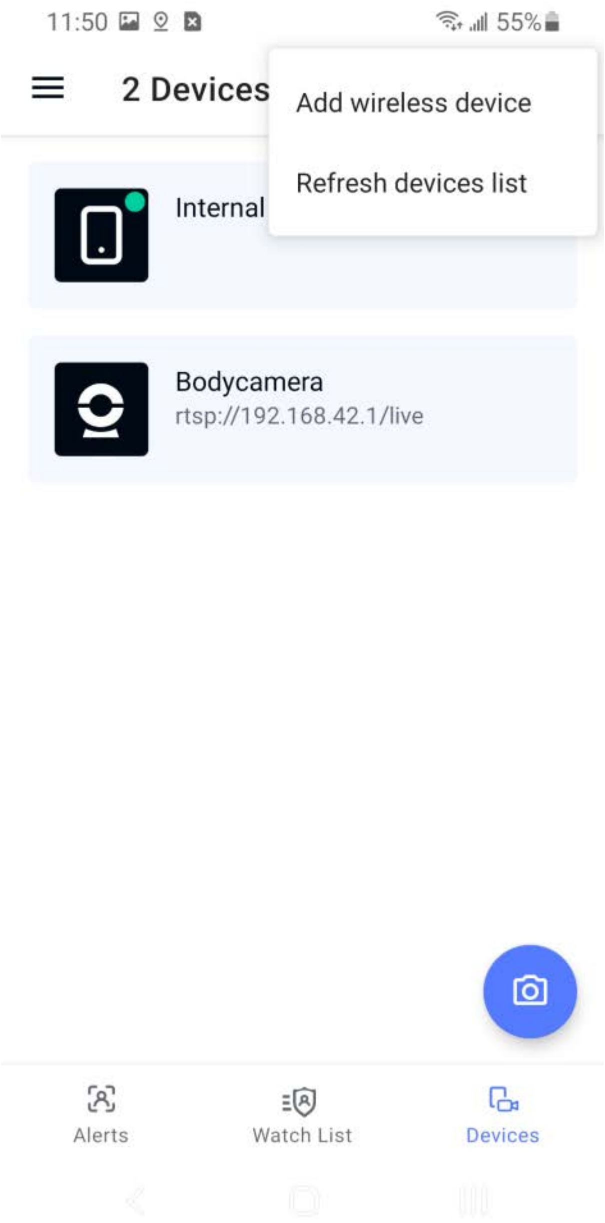
Add Wi-FI or wireless camera

> 📘 **Wireless Camera Limit**
>
> You can add up to 50 wireless cameras.

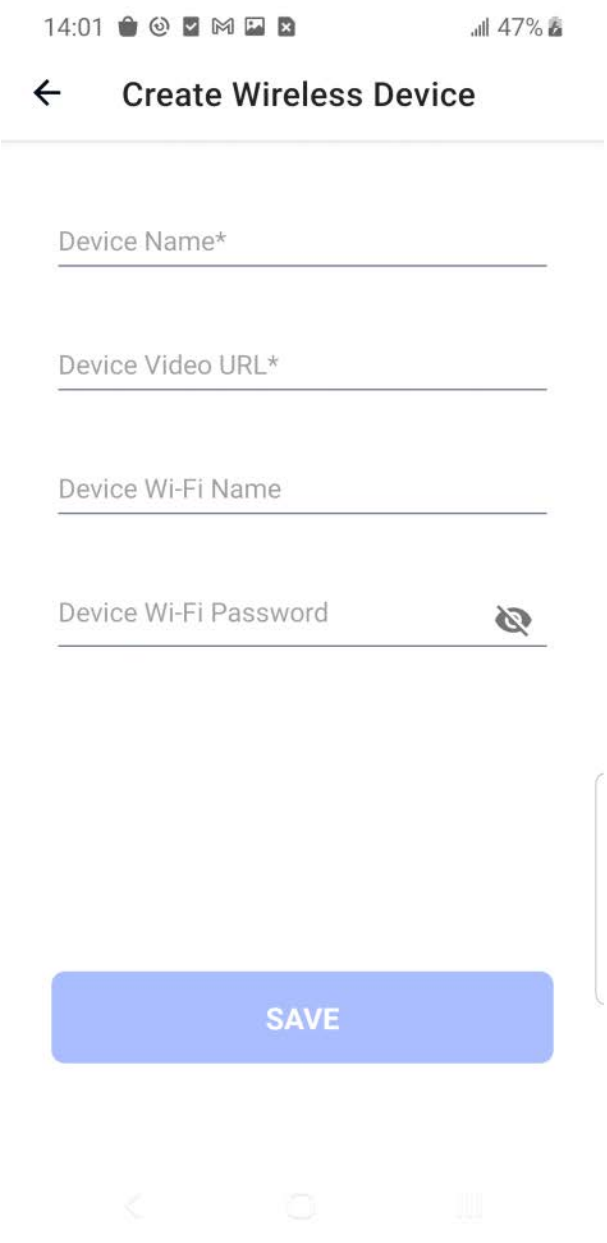
1. Tap **Devices** on the bottom of the screen. The Devices screen is displayed.



2. Tap the vertical ellipsis in the upper right-hand corner of the Devices screen and tap **Add wireless device**.



3. Enter the necessary details on the Create Wireless Device screen. Device Name and Device Video URL are required, other details are optional.


14:01 47%

Create Wireless Device

Device Name*

Device Video URL*

Device Wi-Fi Name

Device Wi-Fi Password

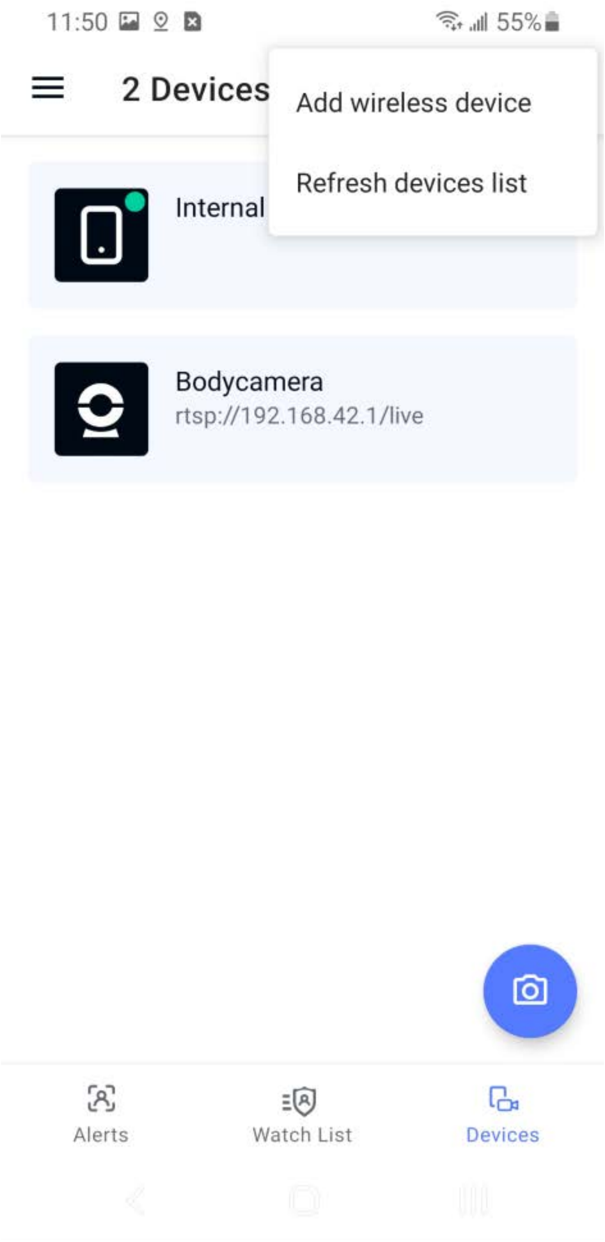
SAVE

4. Tap **SAVE**. The new wireless camera is added to your list.

> 📘 **Using a Wireless Camera**
>
> Ensure that when using a wireless camera, your telephone or tablet is connected to the same wireless network as the camera.

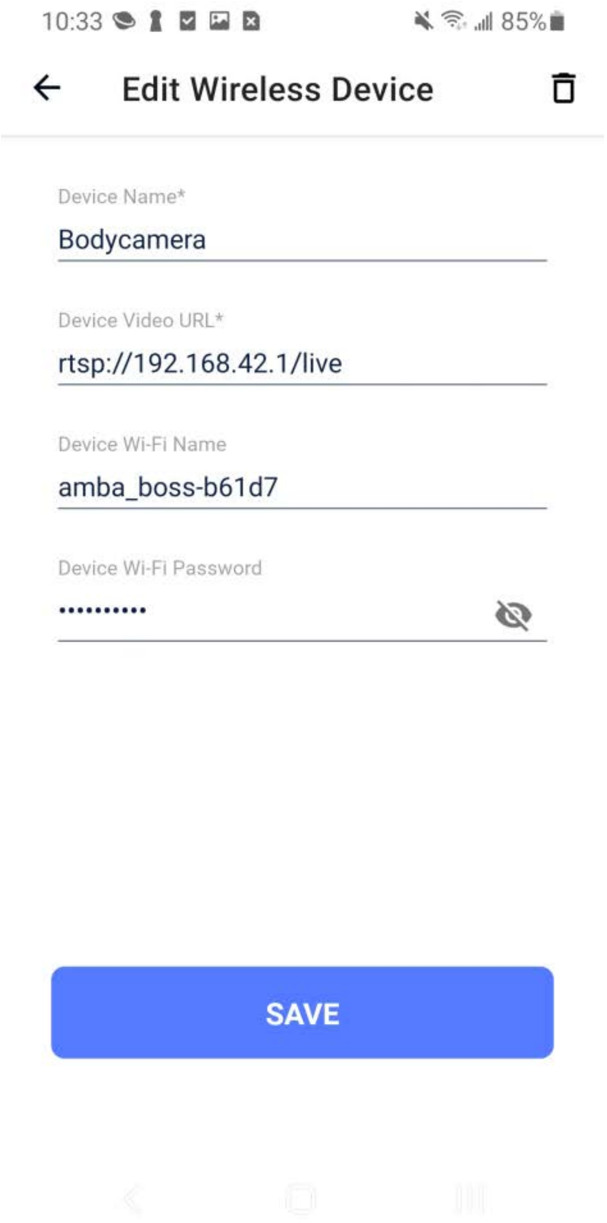
Add a USB camera

1. Physically connect your USB camera to your telephone or tablet.
2. Navigate to the **Devices** screen,
3. If your USB camera is not listed on the screen, refresh the devices list from the vertical ellipsis at the upper righthand corner.



Delete or edit wireless camera

To edit or delete a Wi-Fi camera, tap the camera line on the Devices screen. The Edit Wireless Device screen is displayed.


10:33 85%

Edit Wireless Device

Device Name*

Bodycamera

Device Video URL*

rtsp://192.168.42.1/live

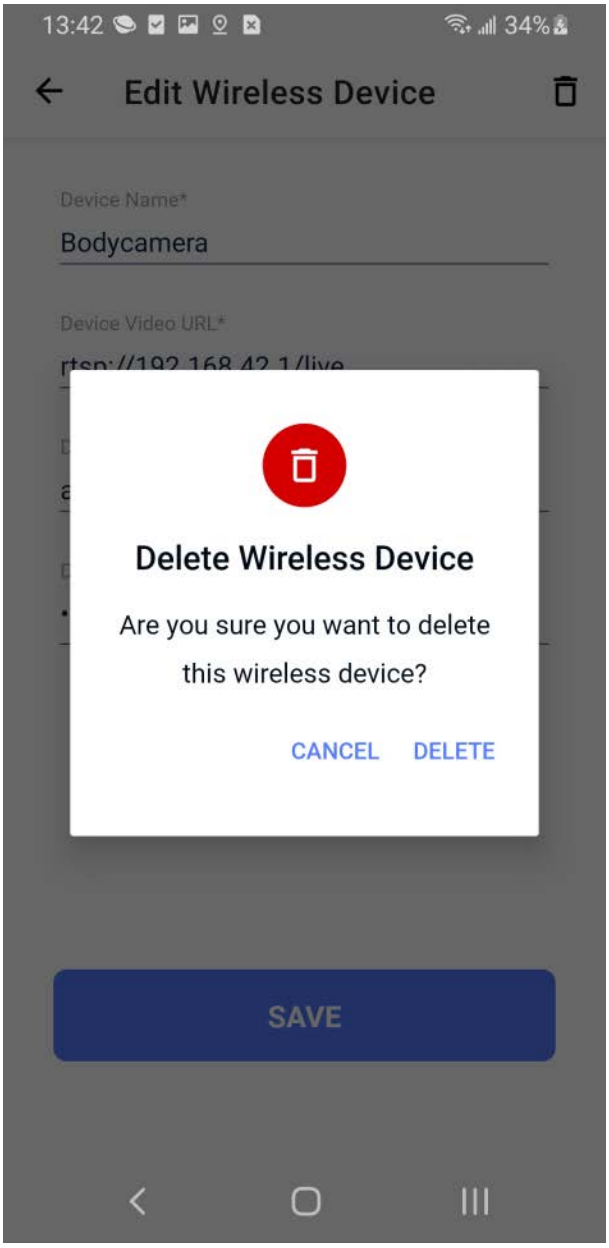
Device Wi-Fi Name

amba_boss-b61d7

Device Wi-Fi Password

••••••••••

To delete the camera, tap the bin in the upper righthand corner of the Edit Wireless Device screen. Tap **DELETE** on the popup that is displayed. to confirm the deletion.



13:42 34%

Edit Wireless Device

Device Name*

Bodycamera

Device Video URL*

rtsp://192.168.42.1/live

Delete Wireless Device

Are you sure you want to delete this wireless device?

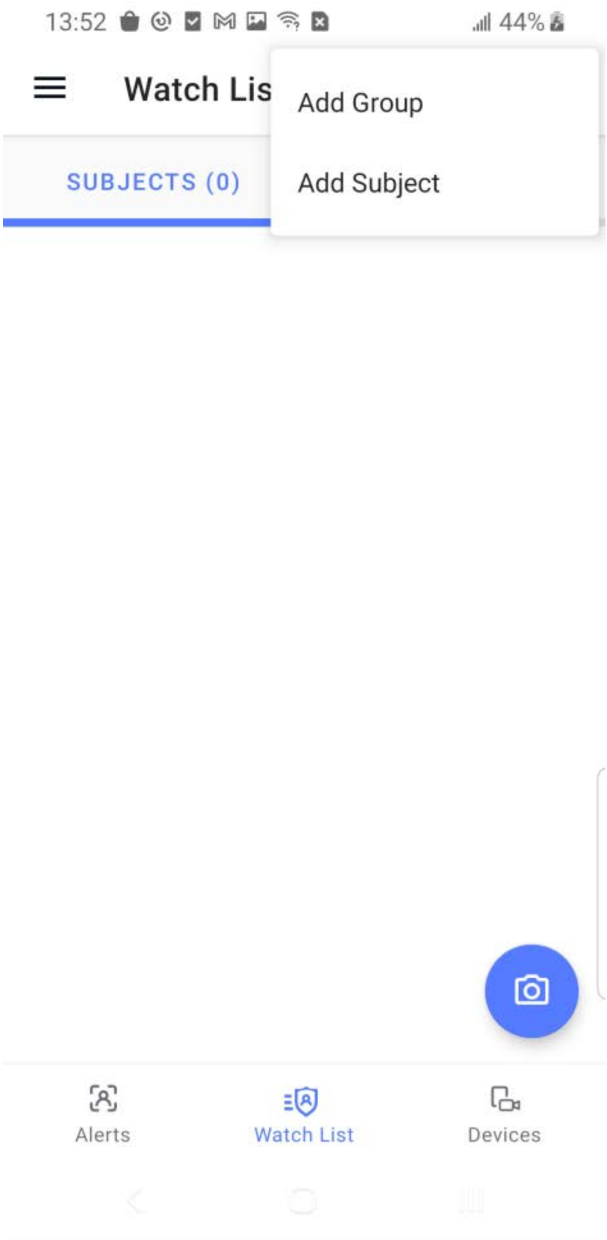
Subject Groups

Subject groups are used to classify subjects. Every subject is added to a subject group. You can create subject groups, for example, WANTED, MISSING PERSONS, and POI for different types of subjects. Alert settings - sound, vibration, and popup - are defined individually for each subject group.
There is a default subject group to which any subject can be added. A subject can be moved from one subject group to another.

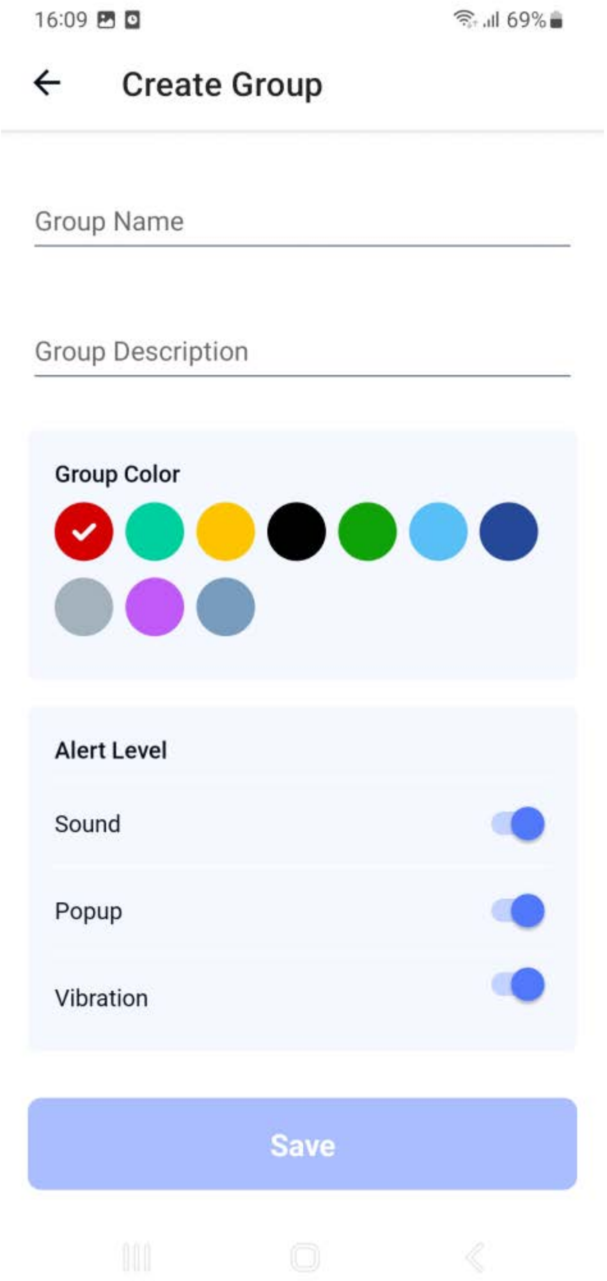
> **Number of Subject Groups is Limited**
>
> You can create up to 20 groups.

Add new subject group

1. Tap **Watch List** at the bottom of the screen.
2. Tap the vertical ellipsis at the upper right-hand corner of the Watch List screen, and tap **Add Group**.



The **Create Group** screen is displayed.



16:09 69%

Create Group

Group Name

Group Description

Group Color

Alert Level

Sound ●

Popup ●

Vibration ●

Save

3. Enter a name for the group in **Group Name**.
4. Tap a color dot to select a **Group Color**.
5. Tap the controls to select the combination of a sound **Sound**, visual **Popup**, or **Vibration** used in the alert for this group.

> 🚧 **Sound**
>
> If the telephone or tablet is in silent mode/muted, no alarm sounds.

> 📘 **Group Alert Level - Sound, popup and vibration settings**
>
> The Alert Level selection per group overrides the **Group Default Alert** selection defined in the **Settings** menu (reached from the main menu).

6. Select a **Threshold** value between **0.35** and **1**.

Threshold

The greater the threshold value, the more certain the match between the subject in the camera's field of view (FOV) and the reference image. If you set this value too high, there may not be sufficient matches, and if you set this value too low, there may be too many false matches.

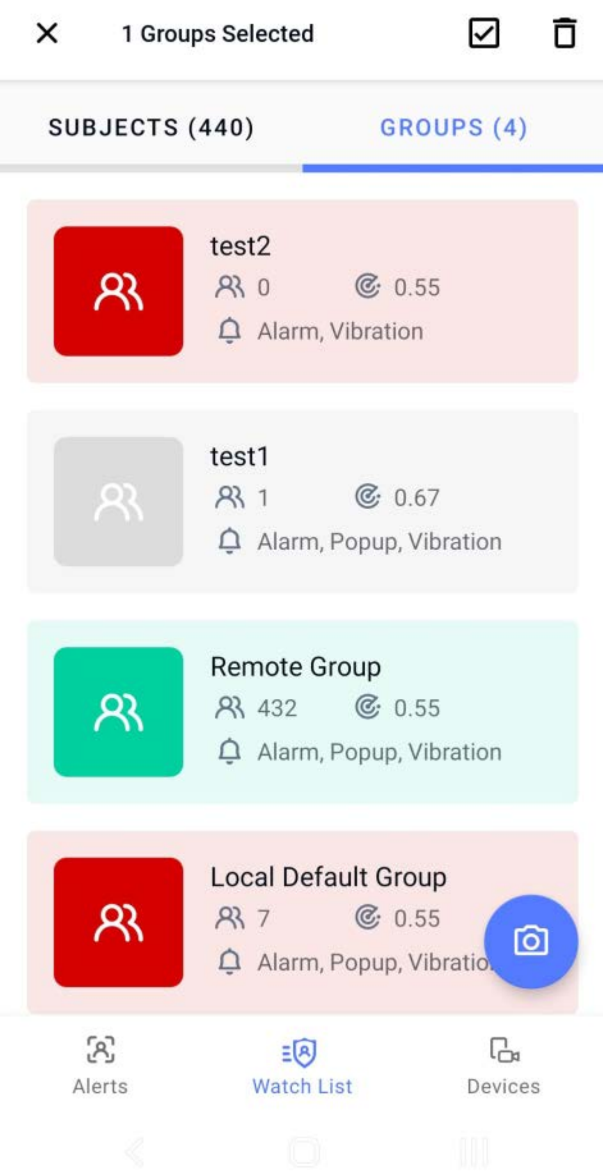
7. Tap **SAVE**.

Delete subject group

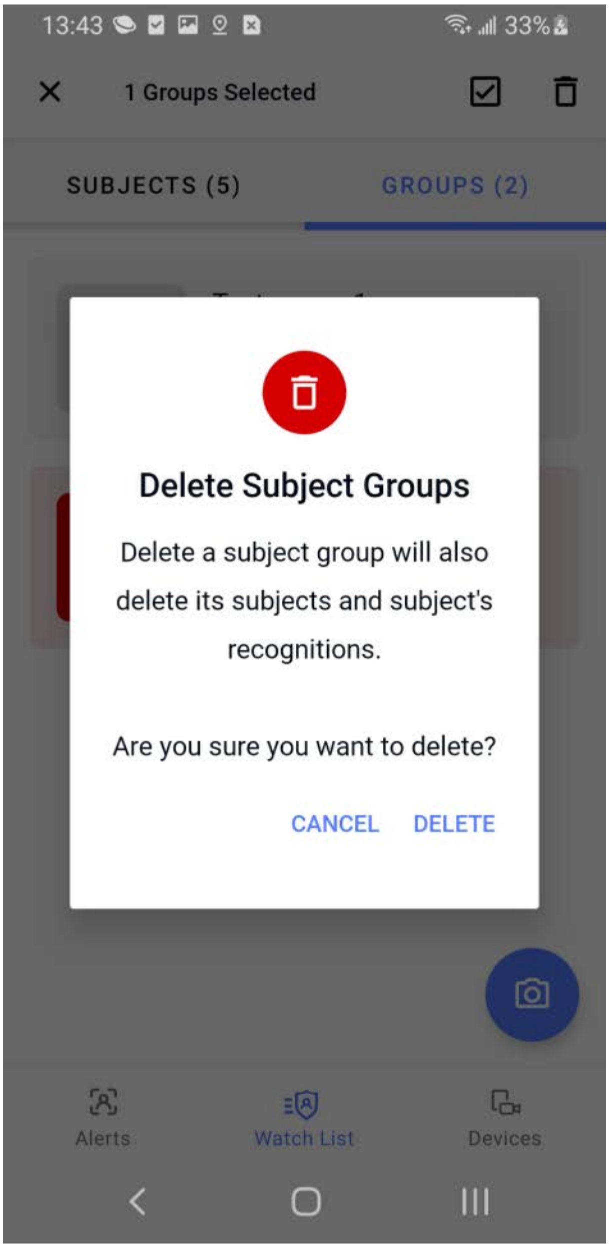
Subject Group Deletion

Note that deleting a group deletes all subjects in the group along with their detections and recognitions.

1. To delete a subject group, long press the group to select it. You can long press more than one subject group to delete more than one subject group at a time.



2. Tap the bin that is displayed in the upper righthand corner.
   You are asked to confirm the deletion.



Delete Subject Groups

Delete a subject group will also delete its subjects and subject's recognitions.

Are you sure you want to delete?

CANCEL DELETE

3. To confirm the deletion, tap **DELETE** on the popup.

> 📘 **Default group**
>
> Neither the Local Default Group nor the Remote Group can be deleted.

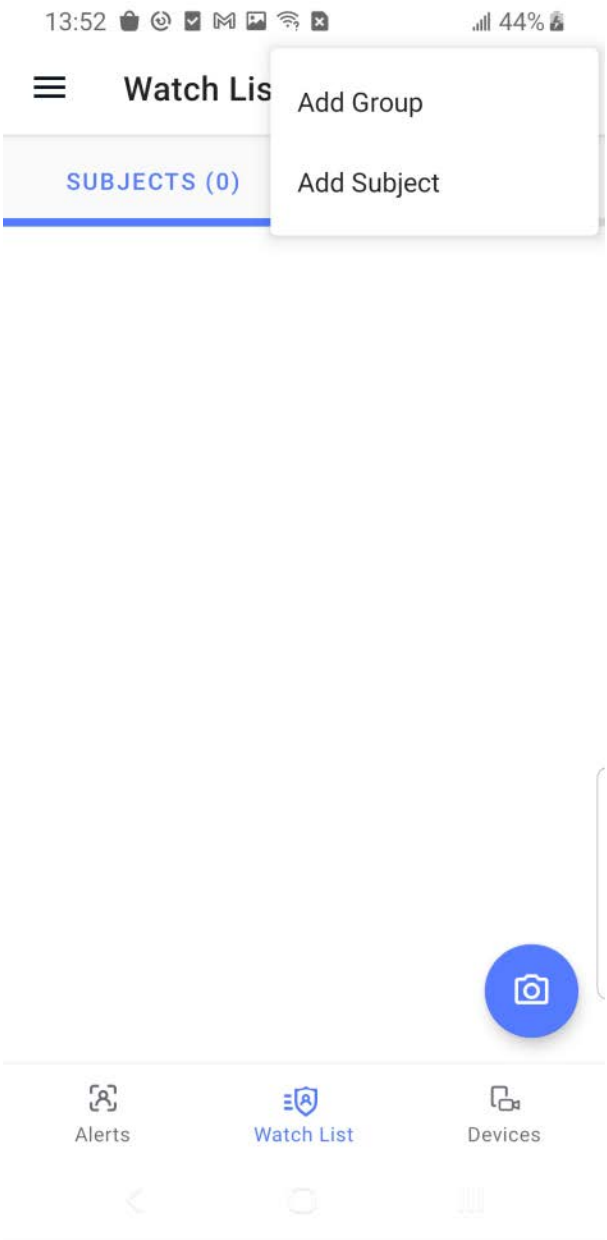
You can also delete a subject group with a quick tap on the group and then from the vertical ellipsis in the subject group profile page displayed.

Subjects

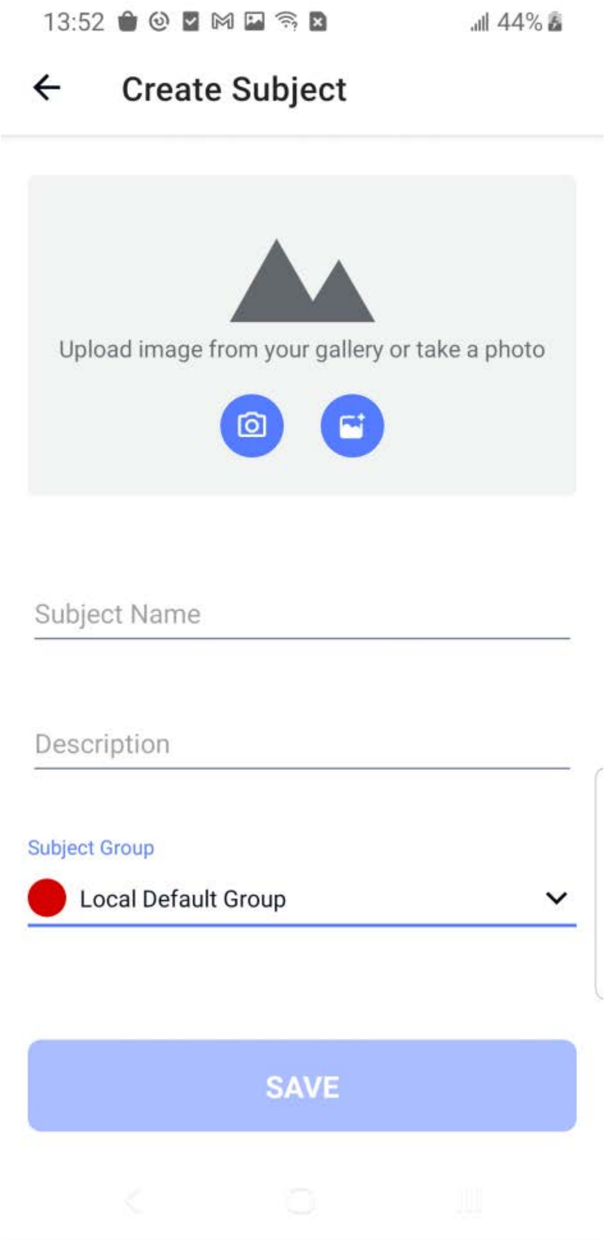
Subjects are created from detections, file photographs, and OnWatch sync. Subjects are assigned to subject groups, and can later be moved from one subject group to another.

Create a new subject

1. Navigate to the Watch List screen.
2. Tap the vertical ellipsis on the right and tap **Add Subject**.

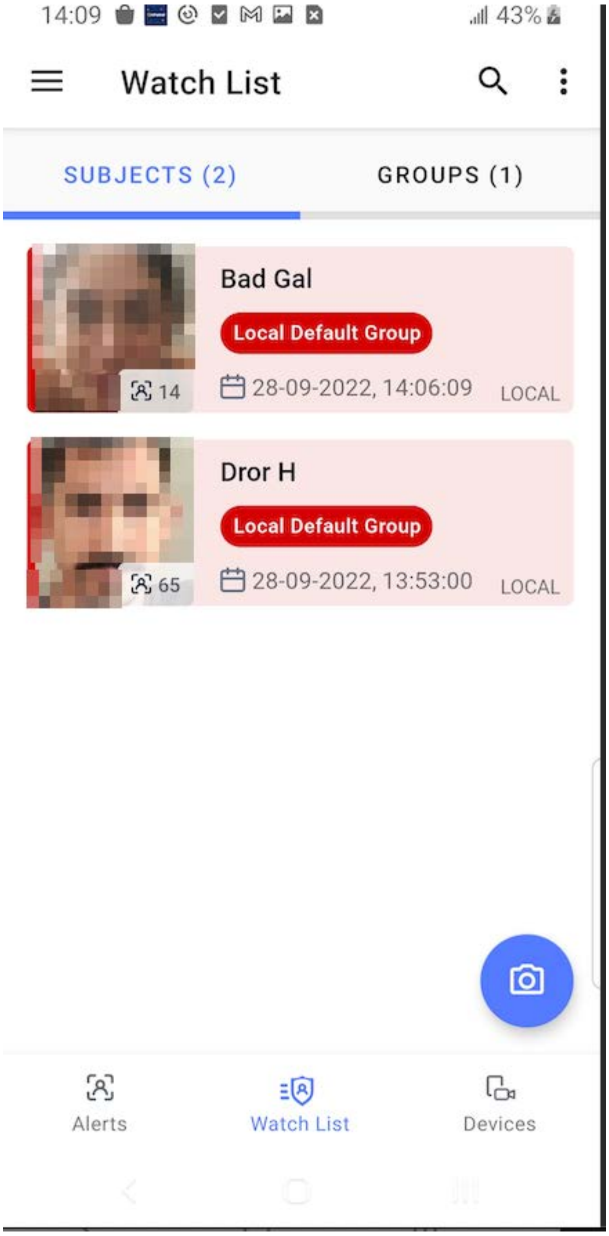


The Create Subject screen is displayed.



3. Enter the relevant information:
   _Image - You can tap the camera icon to take a photograph, or tap the photo icon to upload an image from your device gallery.
   _Subject Name
   _Description - optional
   _Subject Group - tap to view list of options, then tap to select option.
   Tap **SAVE** when done.

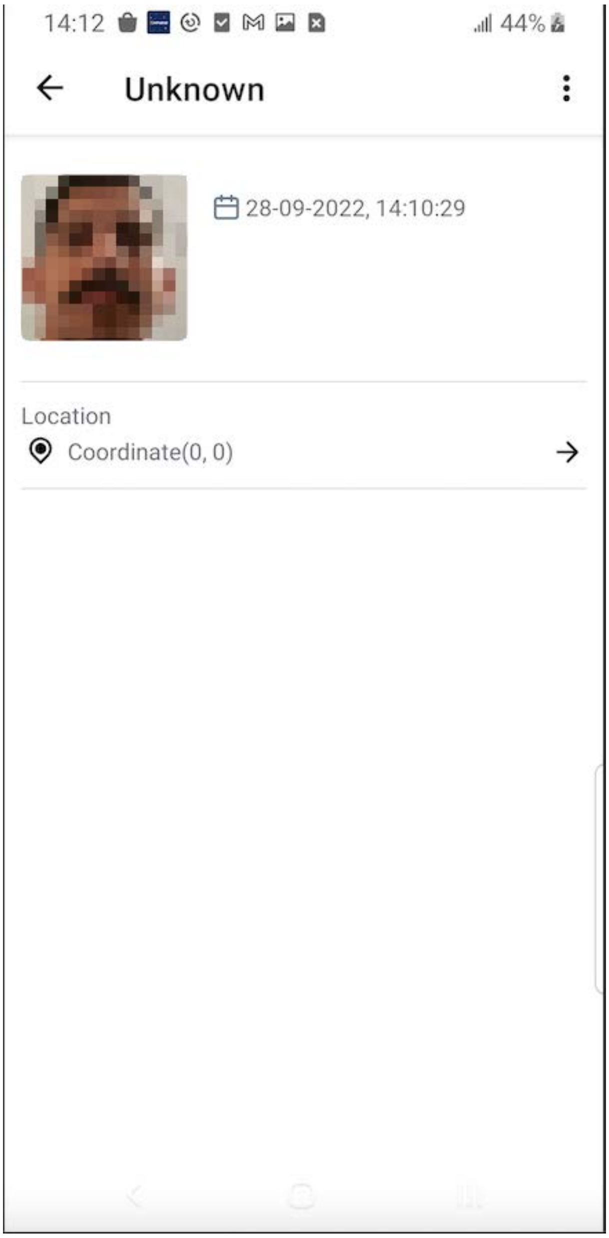
The new subject is displayed in the list of subjects in the Watch List.



You can find subjects in the subject group they belong to or individually in the watch list.

Add a new subject from the list of detections

A subject can be added from the list of detections.
Navigate to the detection's screen by tapping a detection in the search results.
Tap the vertical ellipsis in the upper righthand corner, and then tap **Add subject**.

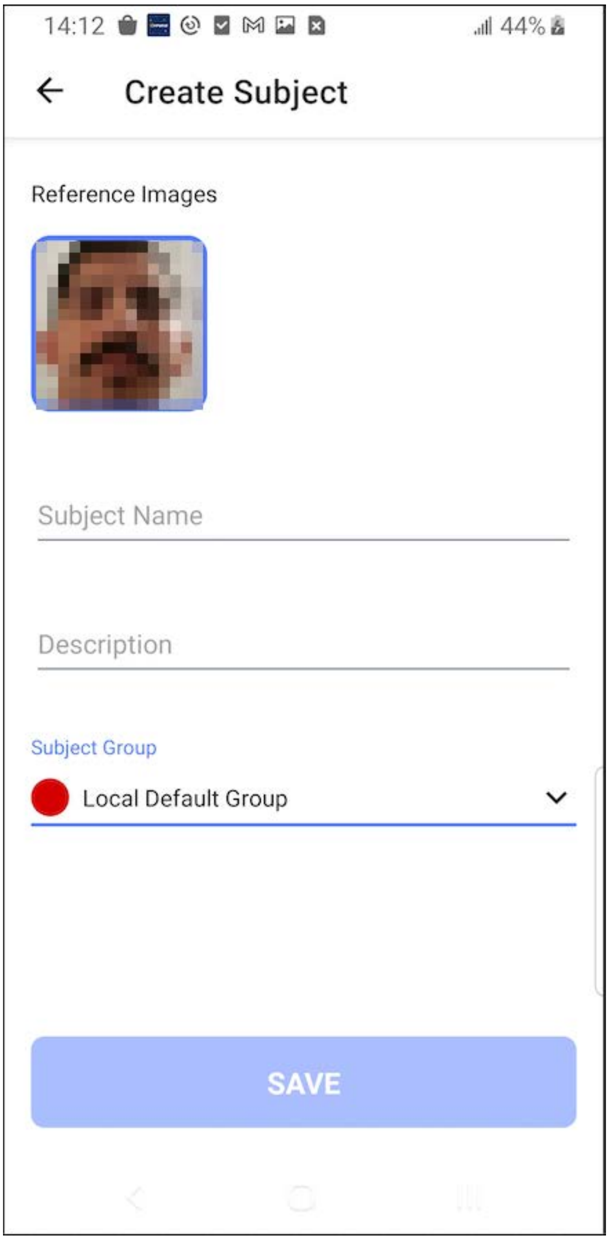


28-09-2022, 14:10:29

Location

Coordinate(0, 0)

The Add new subject screen is displayed with the detection's image.

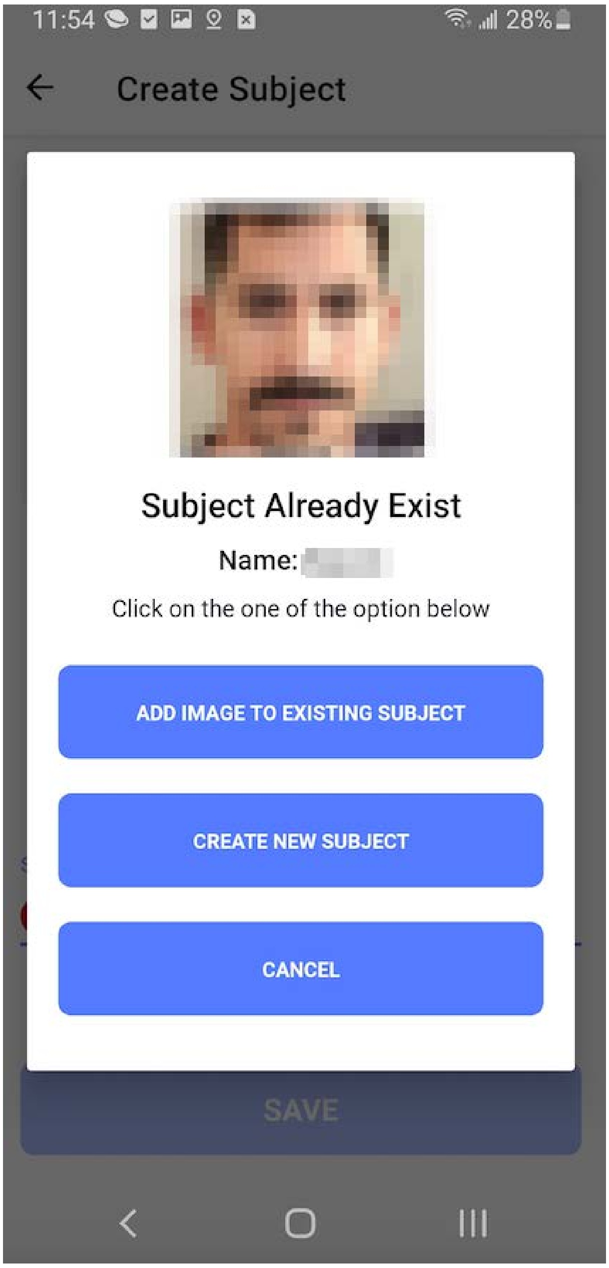


Subject Group
● Local Default Group

Fill in the subject name, and a description. Select a subject group. Tap **Save**.

Subject Already Exists

If you try to add a subject that already exists in the app, a popup is displayed stating that this subject already exists, with 3 options -
_Add image to the existing subject - the app presents the most similar subject and provides the option to add this image to its profile.
_Create a new subject - you can continue creating a new subject.
*Cancel


Create Subject

Subject Already Exist

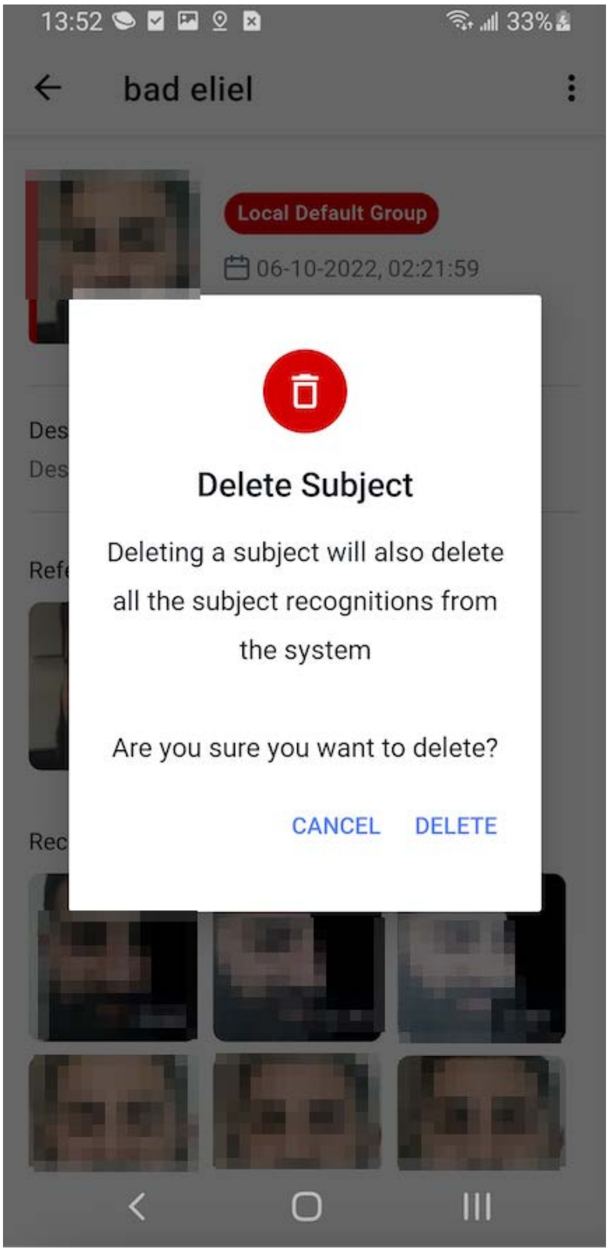
Name:

Click on the one of the option below

Delete subject

> ### 📘 Deleting a subject
>
> Deleting a subject deletes all the subject's detections from the system.

To delete a subject, long tap the subject and then tap the bin in the upper righthand corner.
You can also delete a subject with a quick tap on the subject and then from the vertical ellipsis inside the subject profile view. To continue, click **DELETE** on the popup.



Delete Subject

Deleting a subject will also delete all the subject recognitions from the system

Are you sure you want to delete?

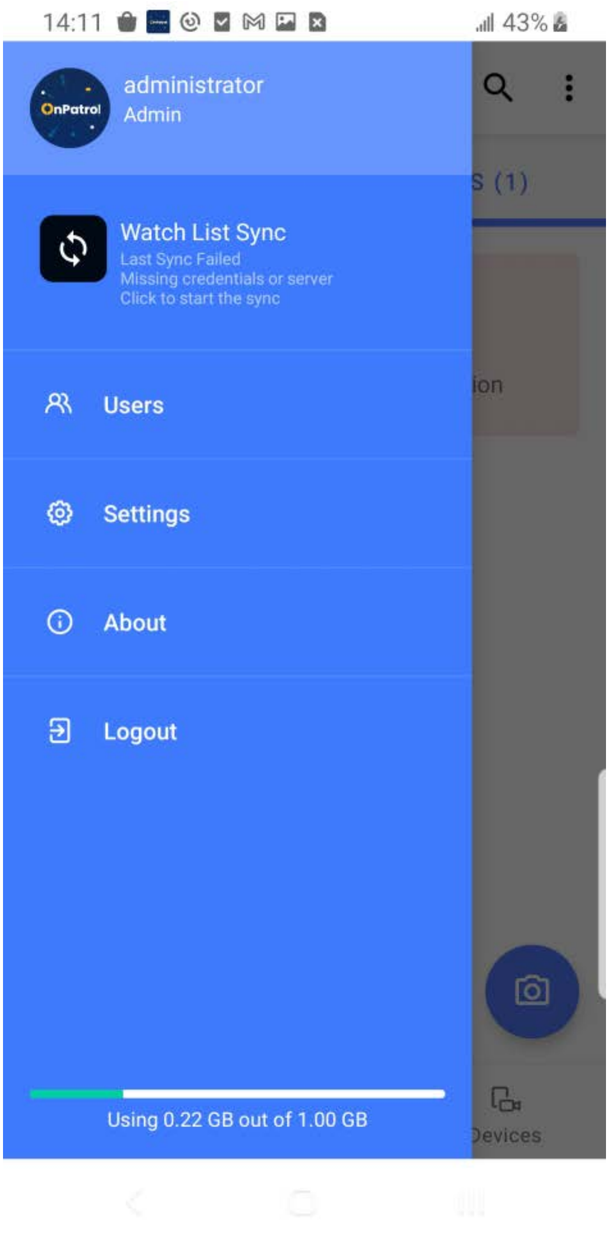
Sync subjects

You can sync subjects from the OnWatch server to the OnPatrol Edge app to obtain those subjects directly from the central system.
The sync is to a pre-defined group called Remote Group. The Remote Group is hidden and appears only after the setup sync to the OnWatch system.

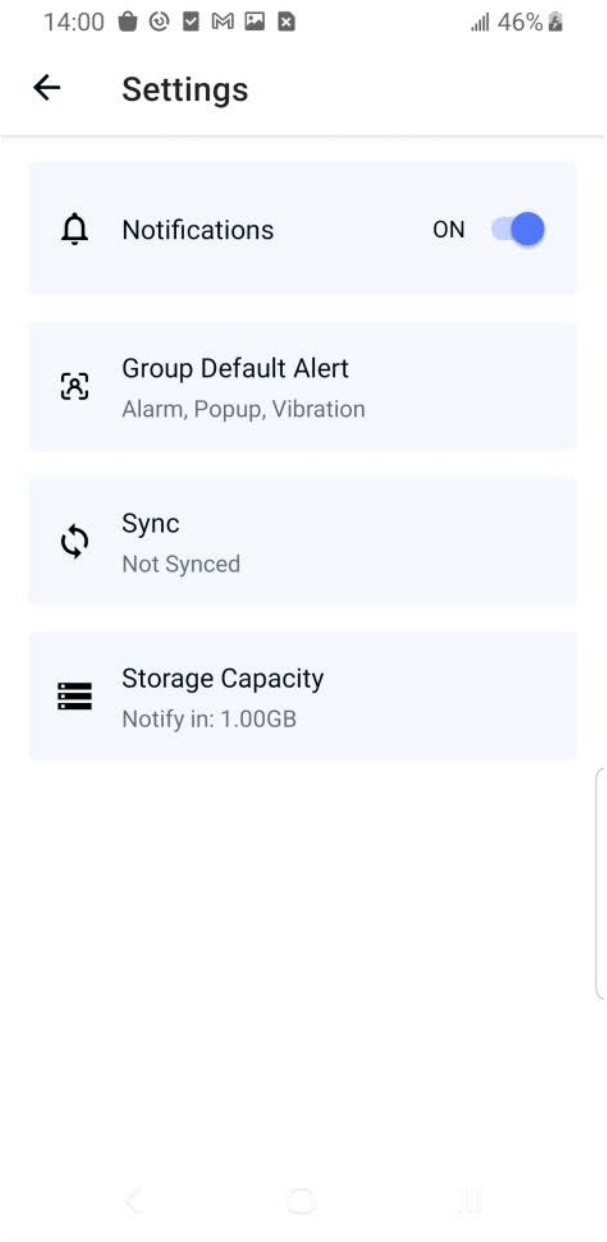
> 📘 **OnWatch Version**
>
> The sync subjects feature is supported by OnWatch version 2.6 and above

Setup Sync subjects

1. Tap the hamburger icon to display the main page



2. Tap **Settings** to display the Settings menu.


14:00 46%

Settings

Notifications ON

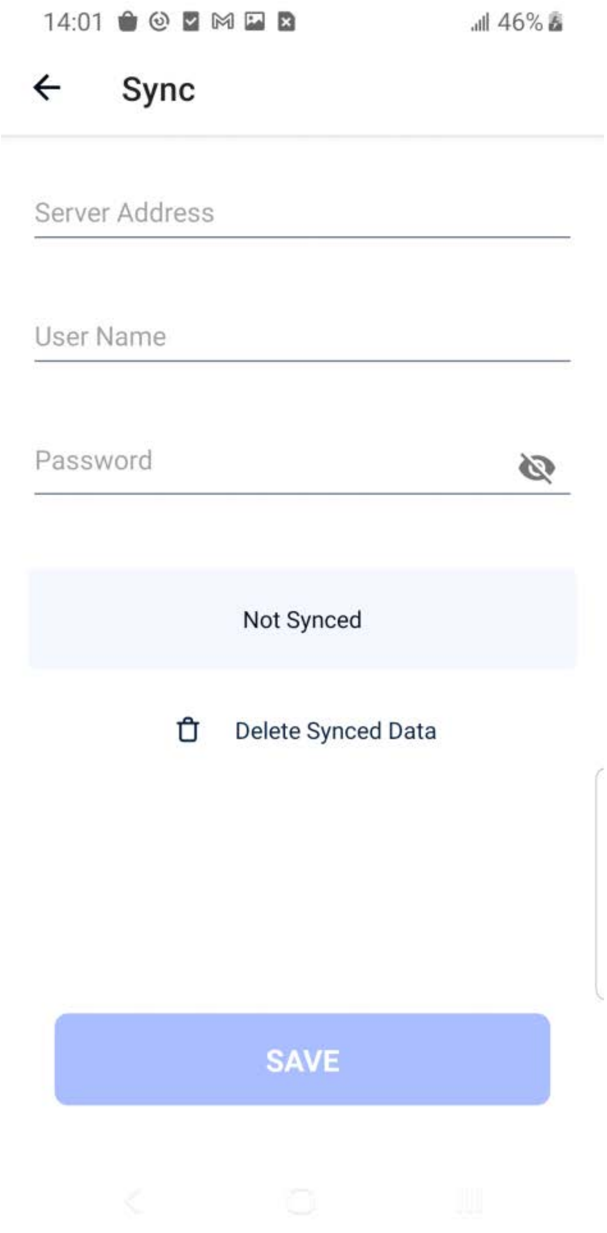
Group Default Alert
Alarm, Popup, Vibration

Sync
Not Synced

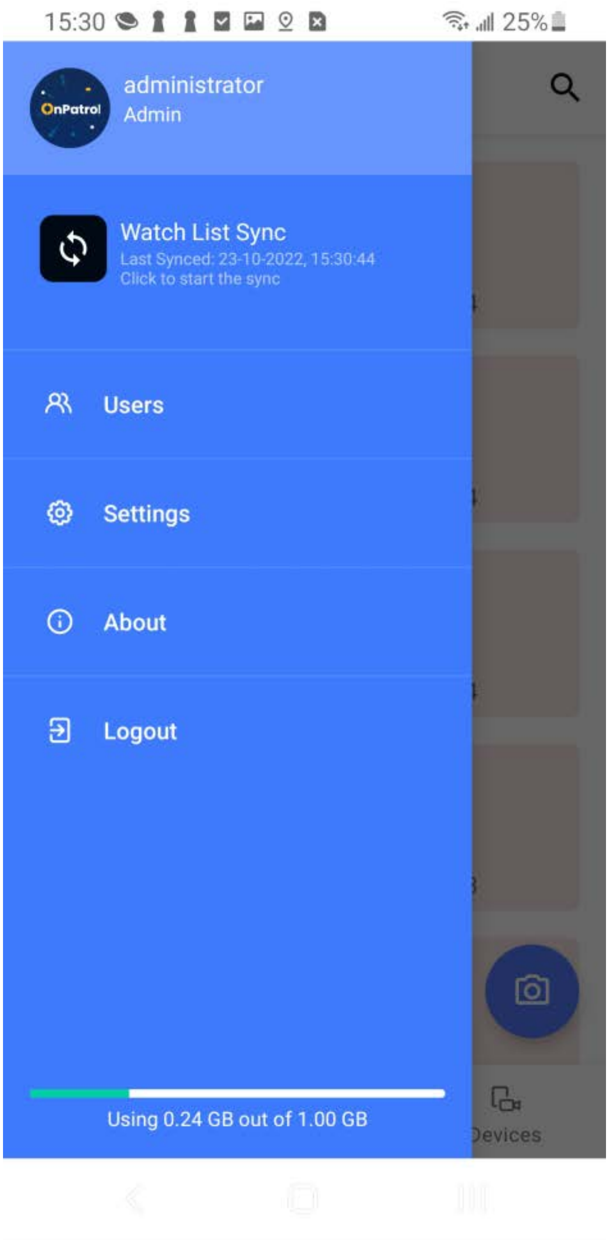
Storage Capacity
Notify in: 1.00GB

3. Tap Sync to display the **Sync** screen.

4. Enter the server credentials and tap **Save**.

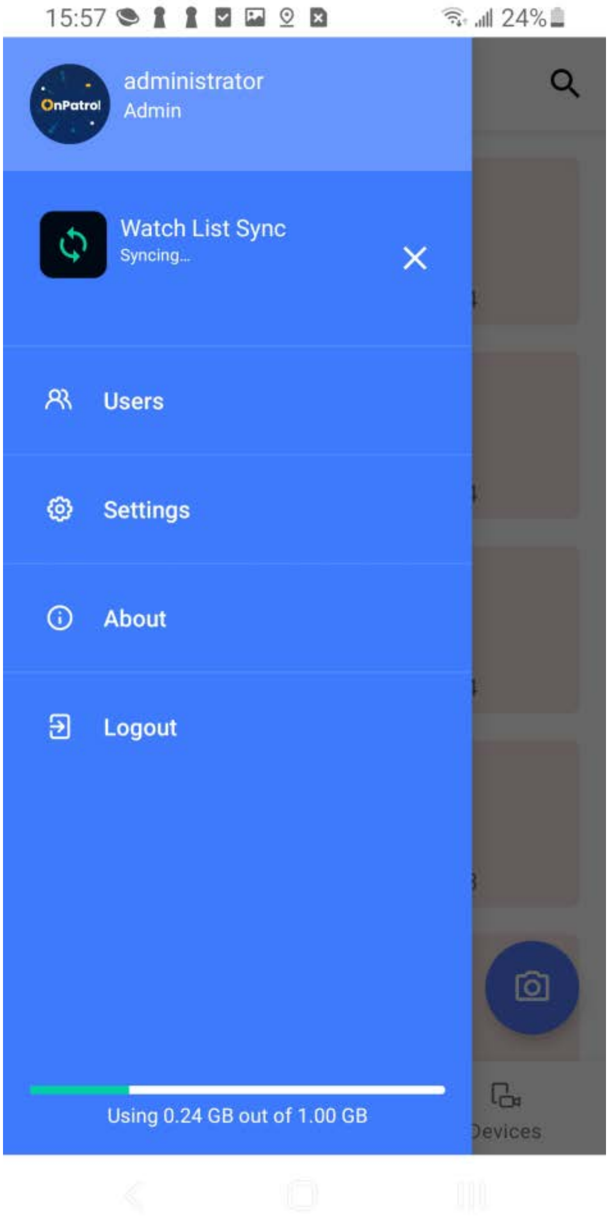


5. Tap the hamburger icon to display the main menu.

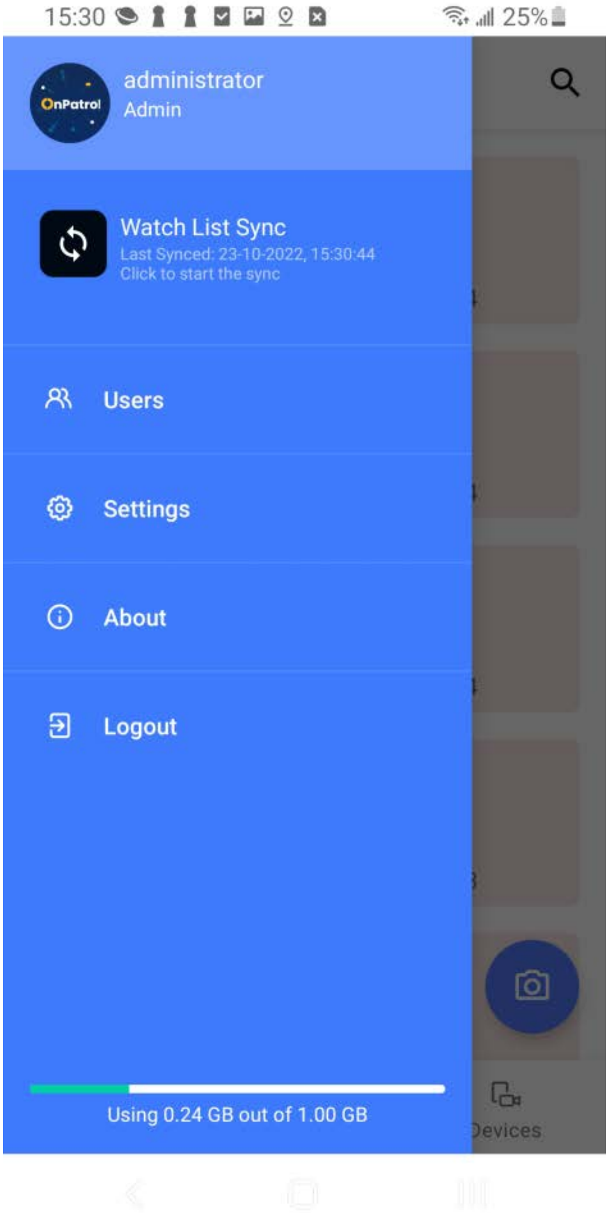


6. Tap **Watch List Sync**.

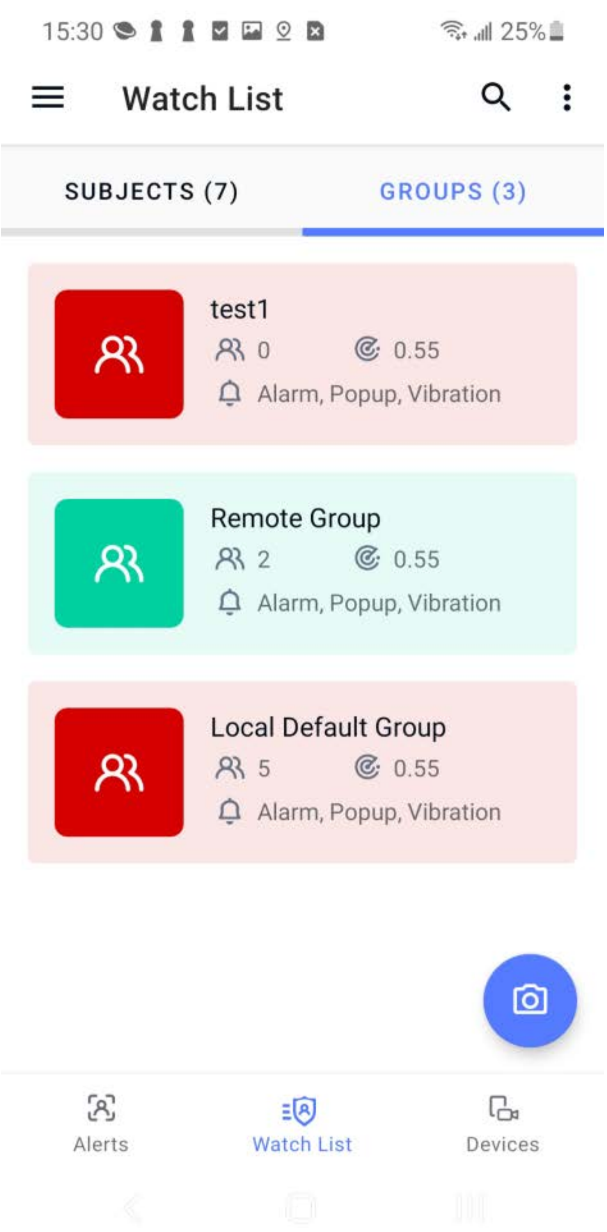
7. The sync icon turns green during syncing. Wait until the sync is finished.



When the sync is finished, the sync details are displayed in the Watch list sync row of the menu.



If this is the first sync, the Remote Group subject group is added to the Watch List.

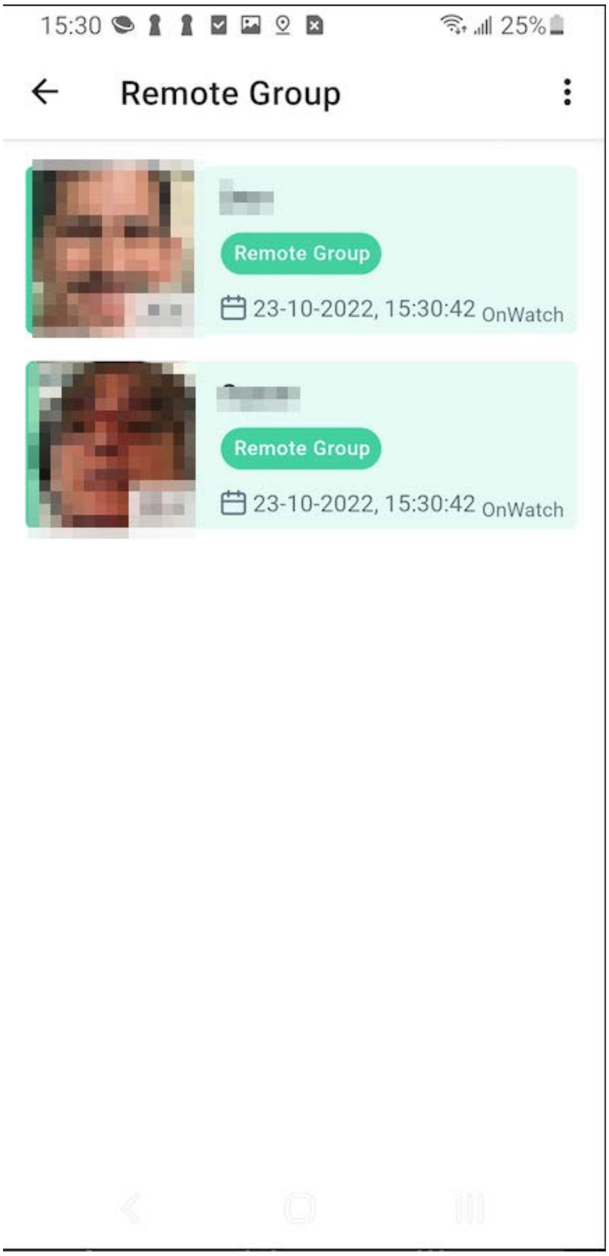


test1
0 0.55
Alarm, Popup, Vibration

Remote Group
2 0.55
Alarm, Popup, Vibration

Local Default Group
5 0.55
Alarm, Popup, Vibration

The group contains the subjects that synced from the server.



15:30 25%

Remote Group

[redacted]

Remote Group

23-10-2022, 15:30:42 OnWatch

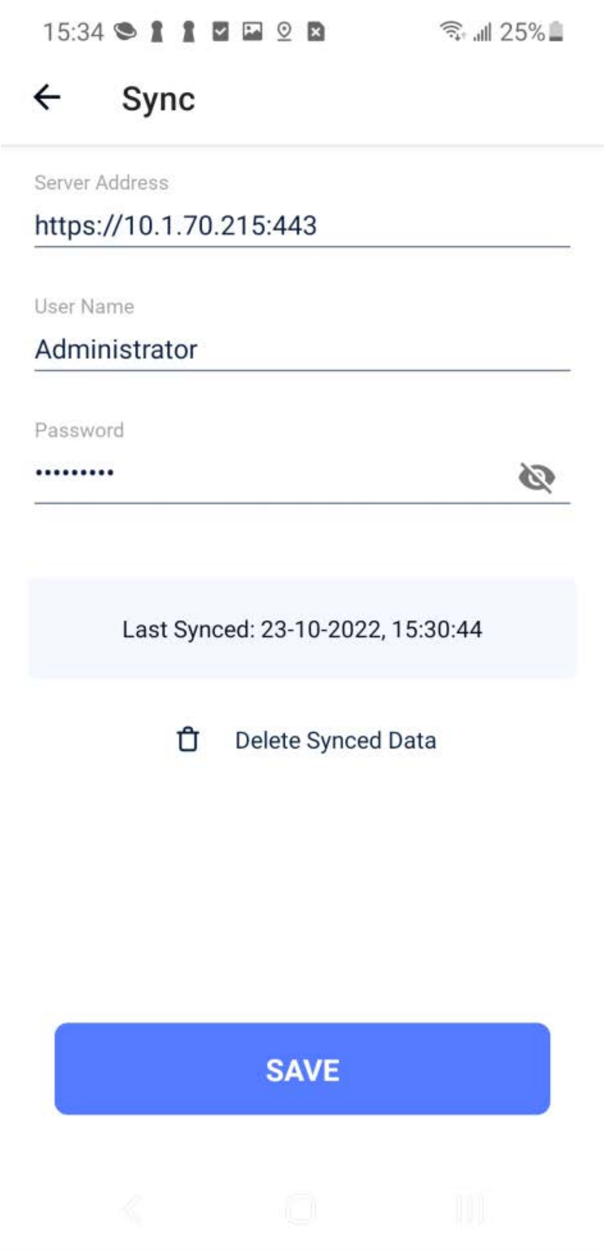
[redacted]

Remote Group

23-10-2022, 15:30:42 OnWatch

Delete synced data

You can delete all the synced data (subjects that were synced).
Tap the hamburger icon. then Settings and then Sync to reach the Sync screen. Tap **Delete Synced Data**.



Sync

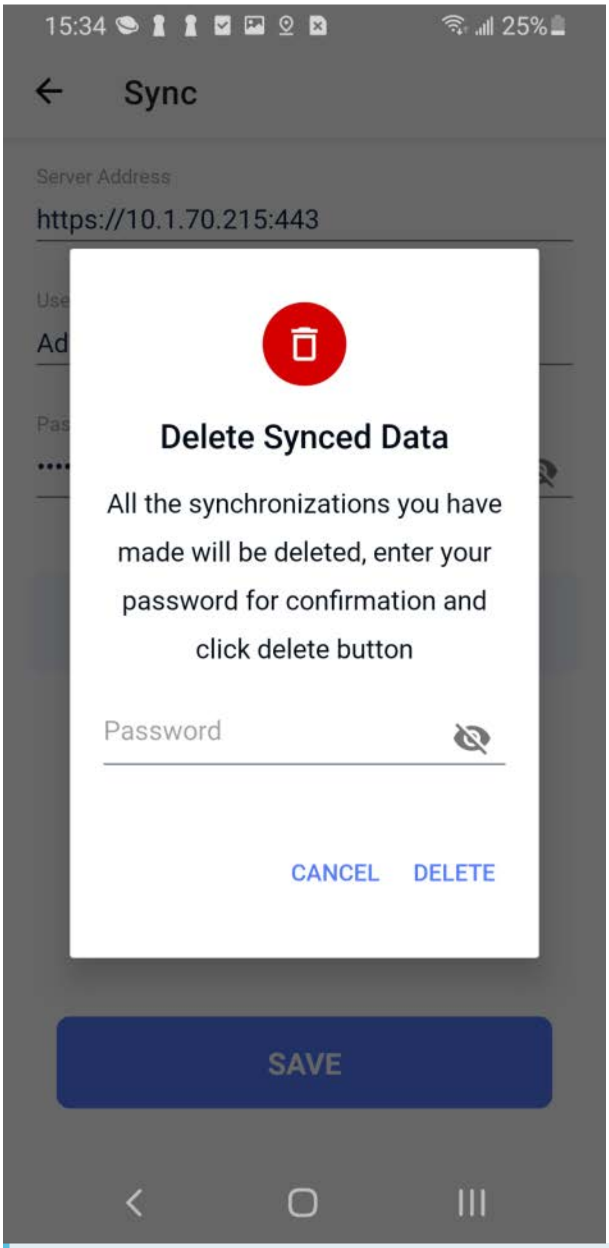
Server Address: https://10.1.70.215:443

User Name: Administrator

Password: ••••••••••

Last Synced: 23-10-2022, 15:30:44

Enter your password to confirm the deletion.



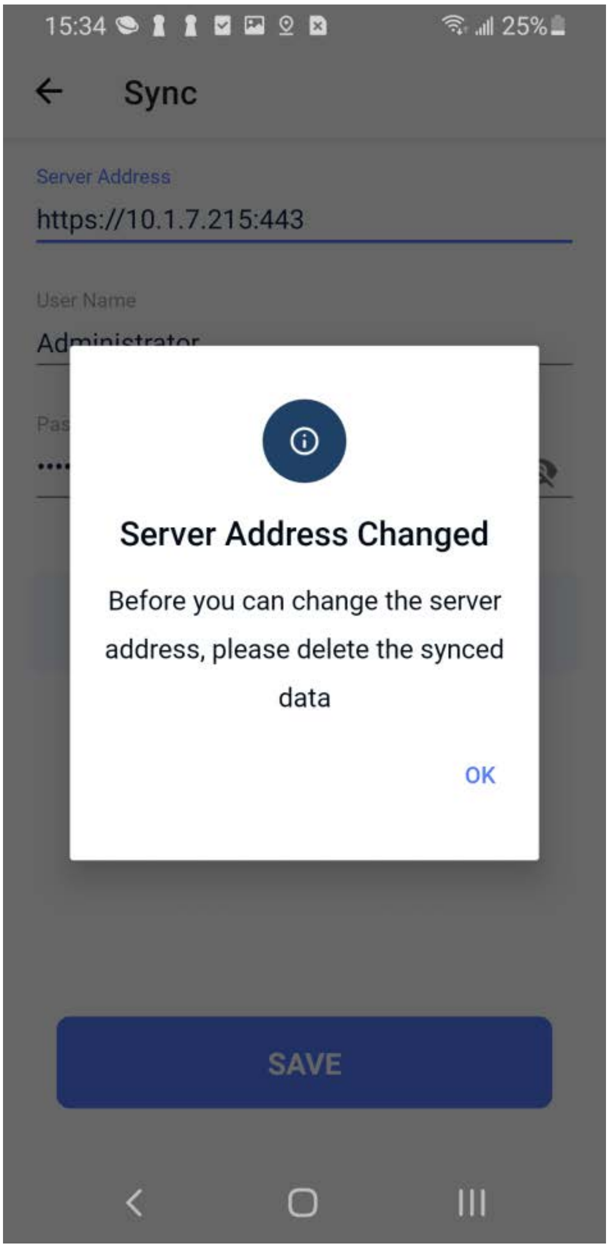
https://10.1.70.215:443

Delete Synced Data

All the synchronizations you have made will be deleted, enter your password for confirmation and click delete button

Changing the Central Server

If for any reason you need to change the central server, the synced data must be deleted before editing server credentials.



15:34

Sync

Server Address

https://10.1.7.215:443

User Name

Administrator

Server Address Changed

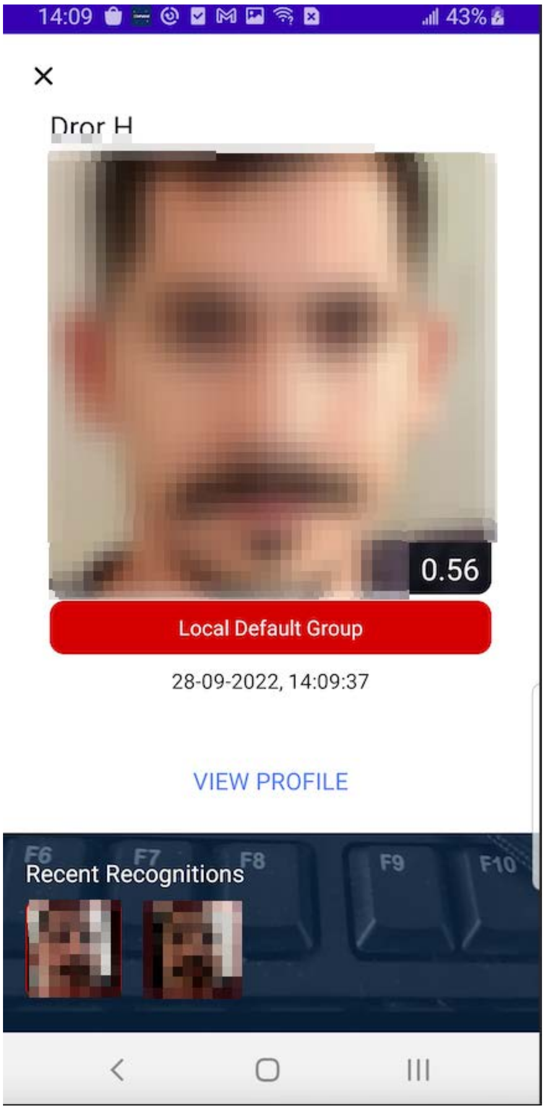
Before you can change the server address, please delete the synced data

Notifications

There are several types of notifications on the app.

In Live mode, there are in-app notifications of recognitions, depending on subject group alert settings.

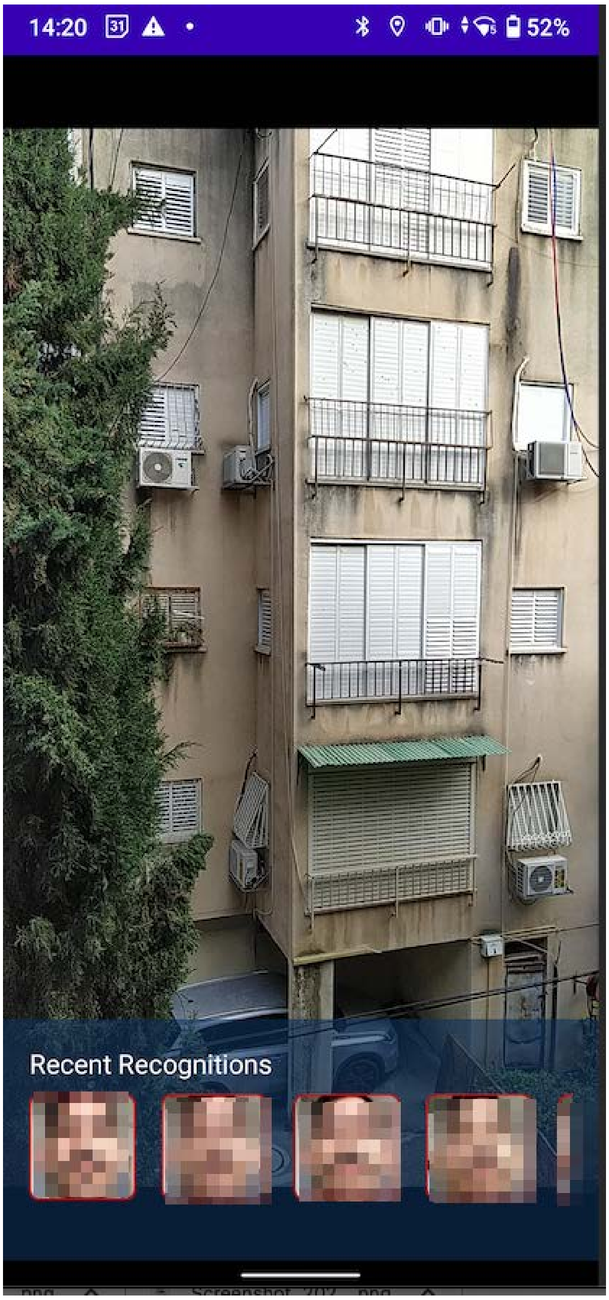
*Popup -- Detection notifications can be displayed as a popup on the screen with a link to the subject profile. Option for sound and/or vibration.



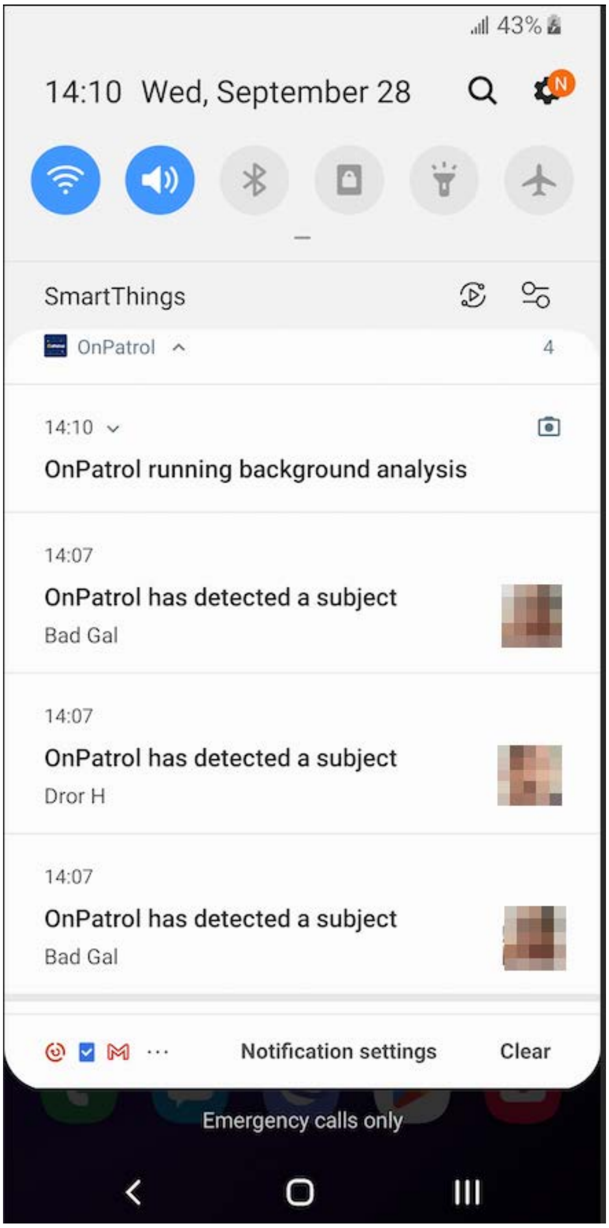
Popup Notification

*No popup -- sound and/or vibration only

- Recognitions are always displayed in the recent recognition panel at the bottom of the screen.



In Background mode, you can use the telephone or tablet while the app is operating in the background and analyzing the selected input stream. Notifications are displayed only in the telephone/tablet notification drawer.



43%

14:10 Wed, September 28

SmartThings

OnPatrol 4

14:10

OnPatrol running background analysis

14:07

OnPatrol has detected a subject

Bad Gal

14:07

OnPatrol has detected a subject

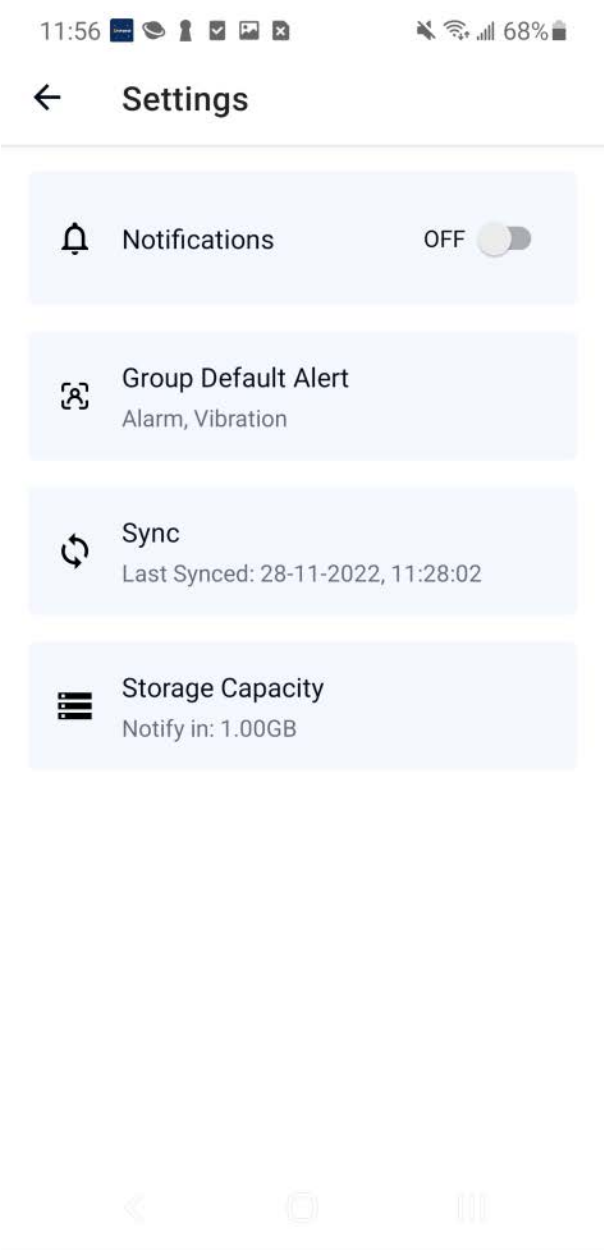
Dror H

14:07

OnPatrol has detected a subject

Bad Gal

There is an option to turn off all background mode notifications from the Main menu> Settings page.



11:56 68%

Settings

Notifications OFF

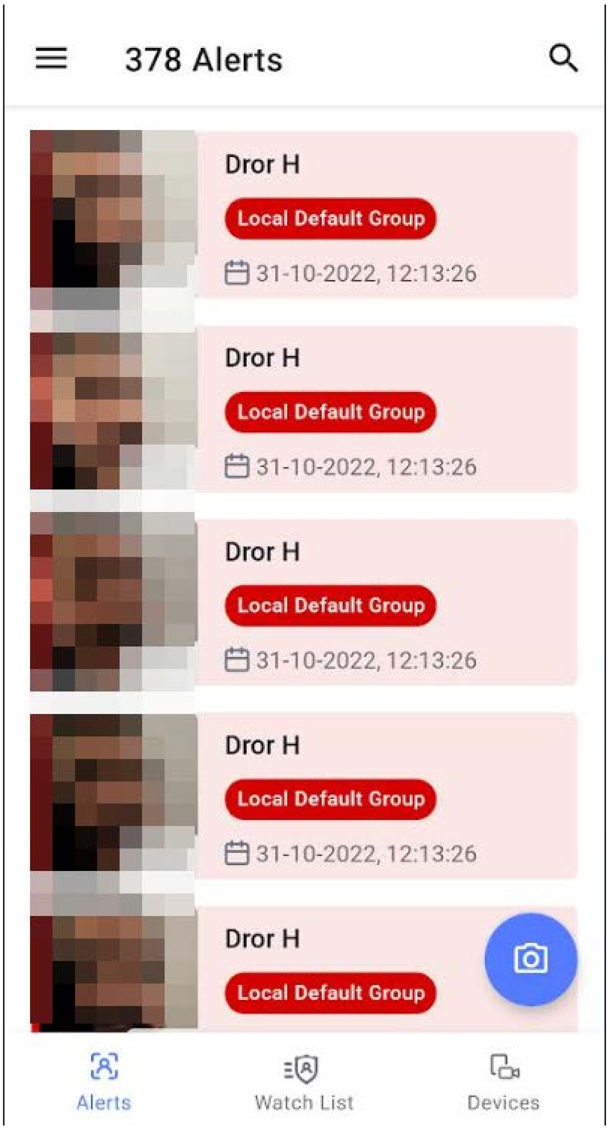
Group Default Alert
Alarm, Vibration

Sync
Last Synced: 28-11-2022, 11:28:02

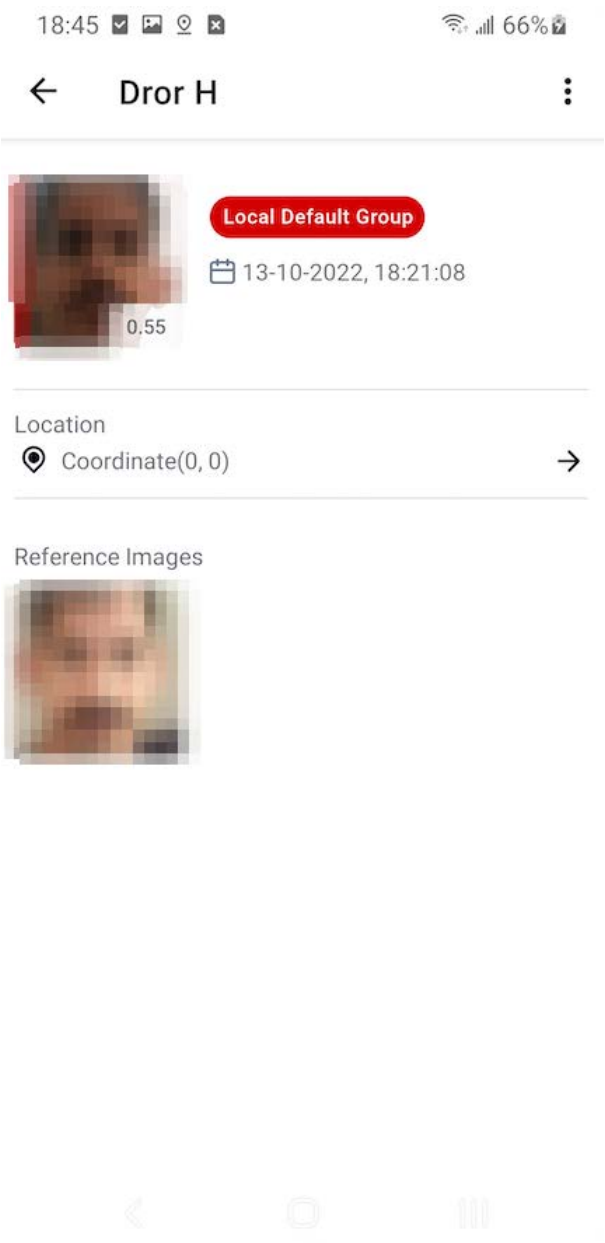
Storage Capacity
Notify in: 1.00GB

Alerts

Alerts are detections that were recognized - sometimes referred to as recognitions.
Alerts are displayed on the Alerts screen. Tap **Alerts** on the bottom of the screen to display this screen.



You can tap an alert from the least to reach the alert's profile screen.



Dror H

Local Default Group

13-10-2022, 18:21:08

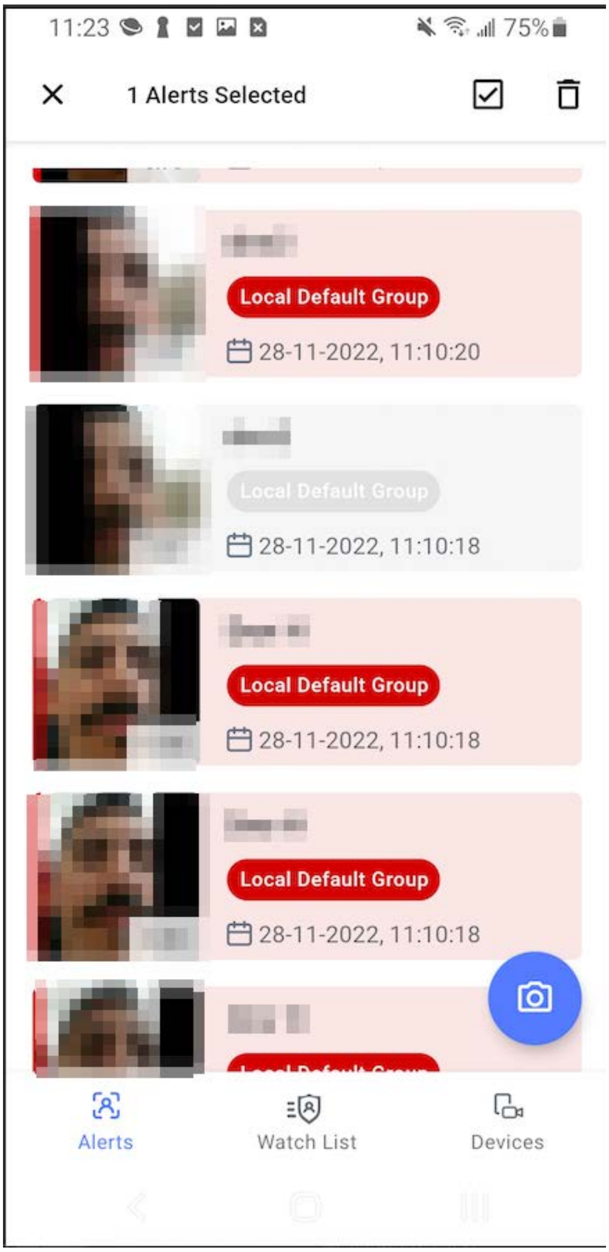
0.55

Location

Coordinate(0, 0)

Reference Images

On the alert screen, you can see the subject details, reference images, location, and time.
You can delete an alert by entering the alert screen with a short tap, or bulk delete with a long tap to each of the alerts to be deleted and then a tap to the bin in the upper righthand corner.

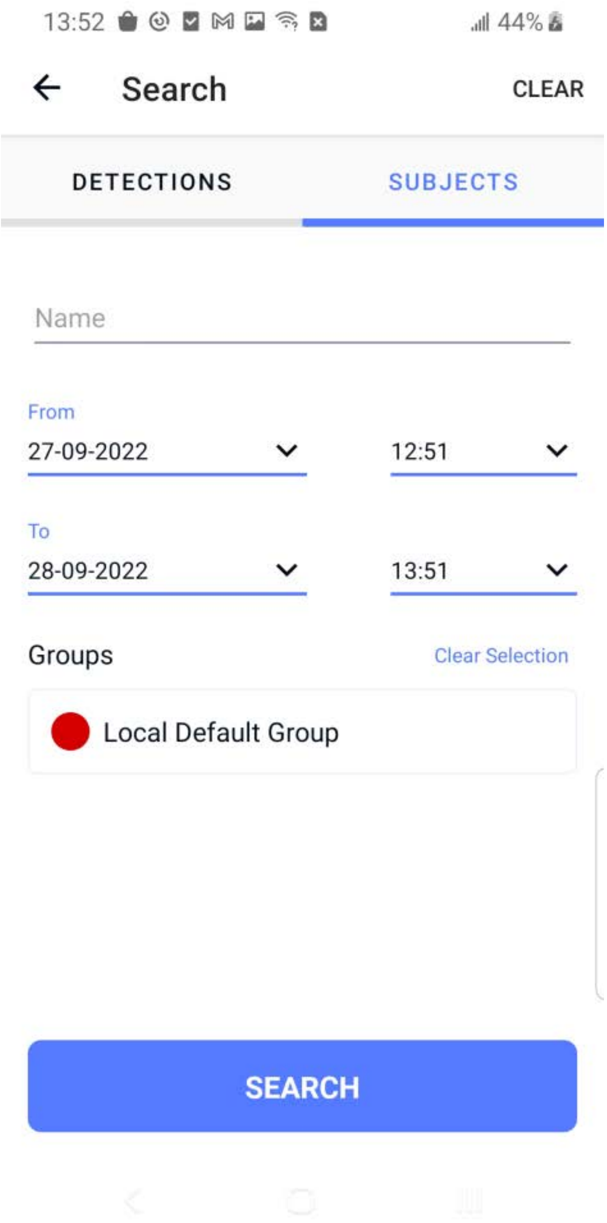


Search

You can search within the application for
_Subjects
_Detections
*Alerts

Search for subjects

Search for a specific subject within the app by selecting the search for Subjects tab by navigating as follows: Watch list>Search icon>Subjects.
The search can be by subject name, creation date, or group.
You can enter a subject name, select a range for creation date and time, select any or all groups.
Tap **Search** when ready.


13:52 44%

Search

CLEAR

DETECTIONS

SUBJECTS

Name

From

27-09-2022

12:51

To

28-09-2022

13:51

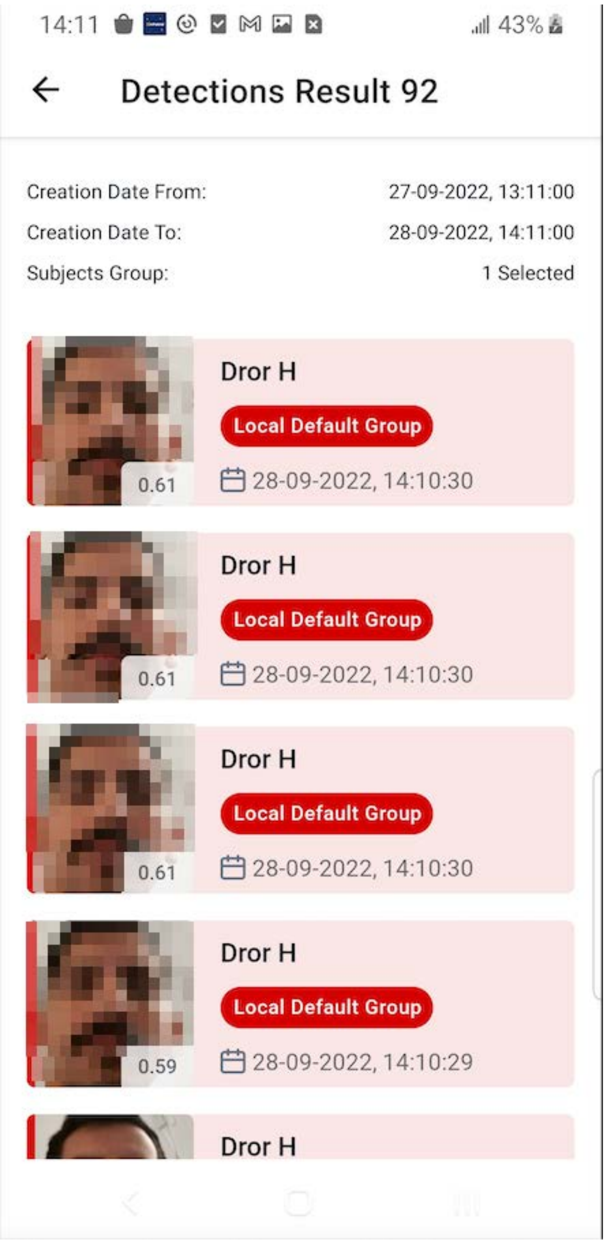
Groups

Clear Selection

● Local Default Group

SEARCH

The results of the search are displayed in the search parameters panel.



14:11 43%

Detections Result 92

Creation Date From: 27-09-2022, 13:11:00

Creation Date To: 28-09-2022, 14:11:00

Subjects Group: 1 Selected

Dror H
Local Default Group
0.61
28-09-2022, 14:10:30

Dror H
Local Default Group
0.61
28-09-2022, 14:10:30

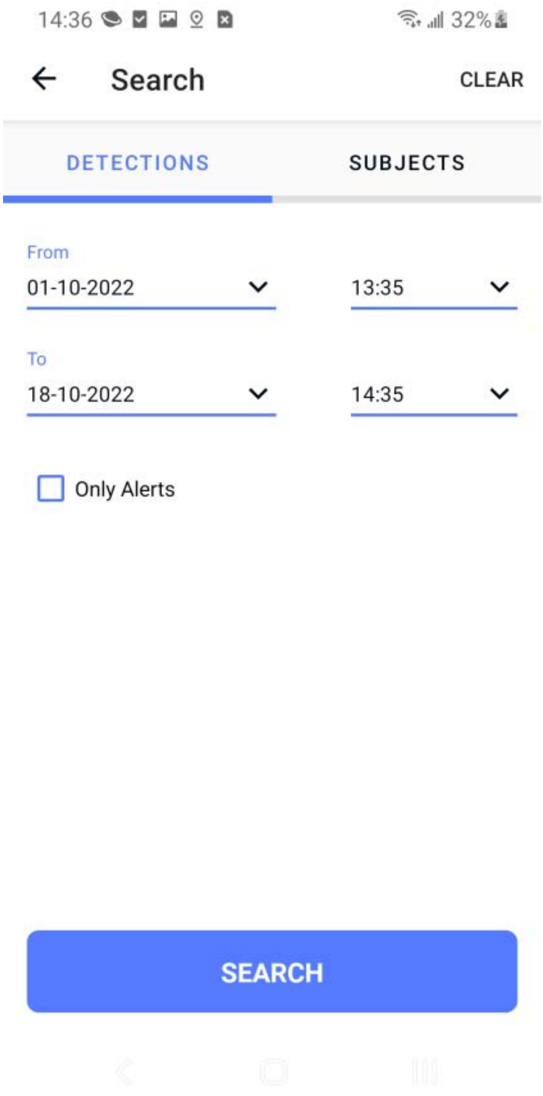
Dror H
Local Default Group
0.61
28-09-2022, 14:10:30

Dror H
Local Default Group
0.59
28-09-2022, 14:10:29

Dror H

Search for detections

Search for detections from the search for Detections tab. Navigate as follows Watch list>search icon>Detections. The detection search allows you to search for detections in a time range.



From
01-10-2022 13:35

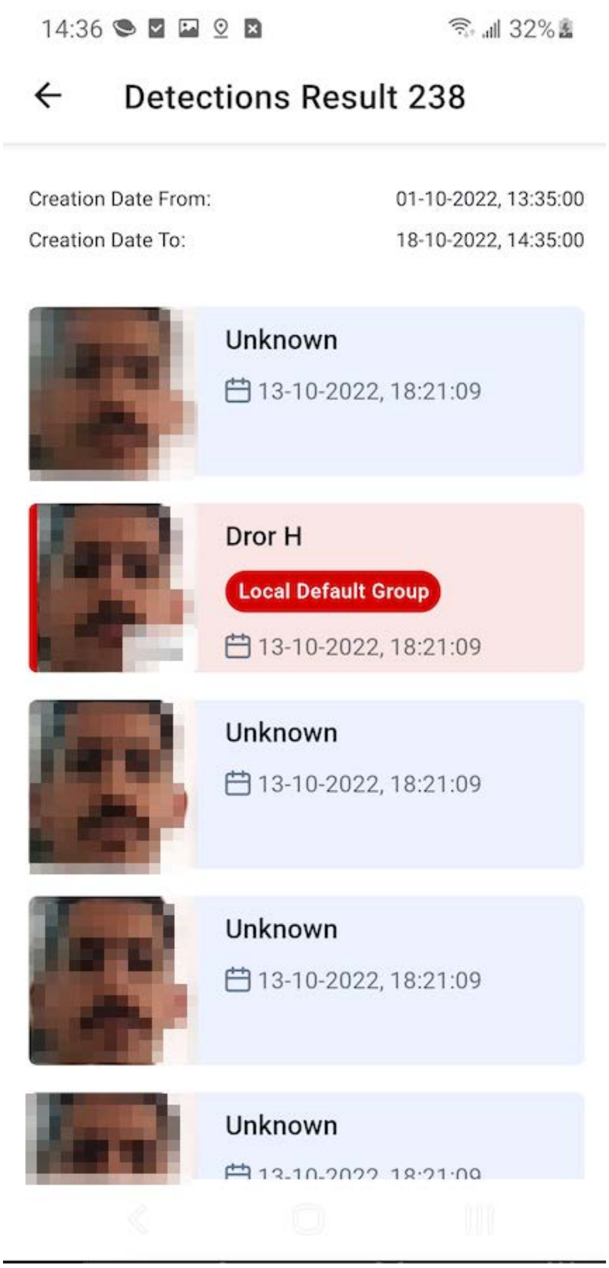
To
18-10-2022 14:35

□ Only Alerts

need pic

Select a detection creation date time range for the search and tap **Search**.
There is an option to search for alerts only, i.e. detections that were recognized. See Searching for alerts below.

Results-


14:36 32%

Detections Result 238

Creation Date From: 01-10-2022, 13:35:00

Creation Date To: 18-10-2022, 14:35:00

Unknown
13-10-2022, 18:21:09

Dror H
Local Default Group
13-10-2022, 18:21:09

Unknown
13-10-2022, 18:21:09

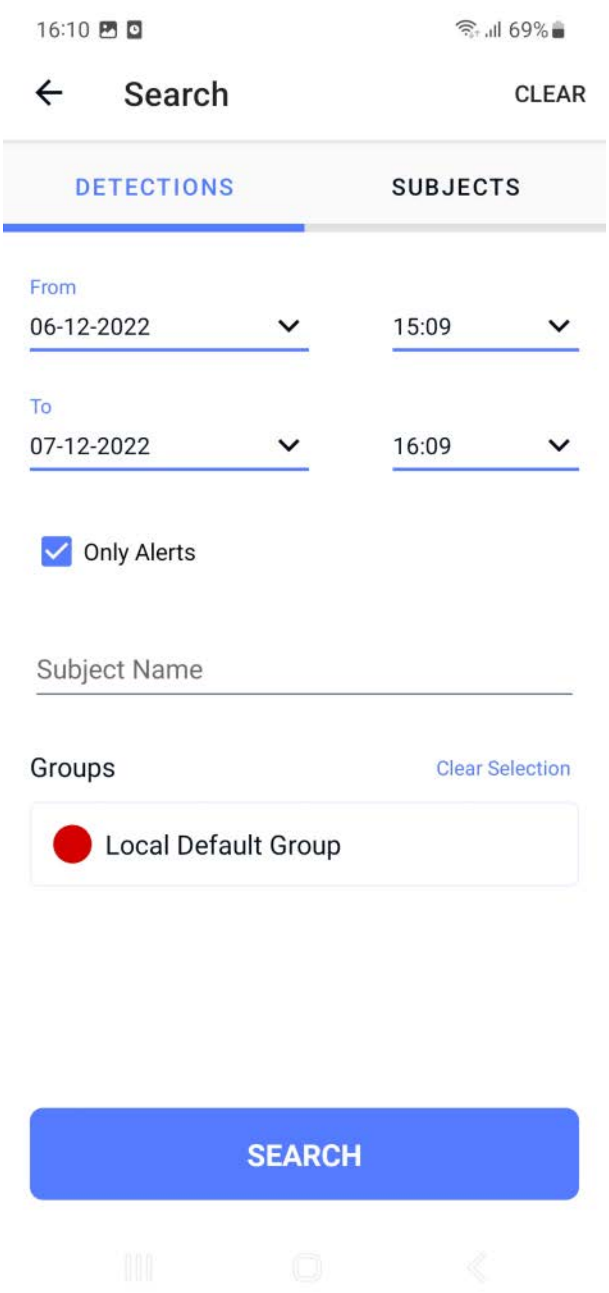
Unknown
13-10-2022, 18:21:09

Unknown
13-10-2022, 18:21:09

Searching for alerts

You can search for alerts only, i.e. recognized detections, by marking the Only Alerts option on the search detections screen.

After you mark Only Alerts, you then have the additional options to search by subject group or groups, and/or subject name, besides by time range.



From
06-12-2022 15:09

To
07-12-2022 16:09

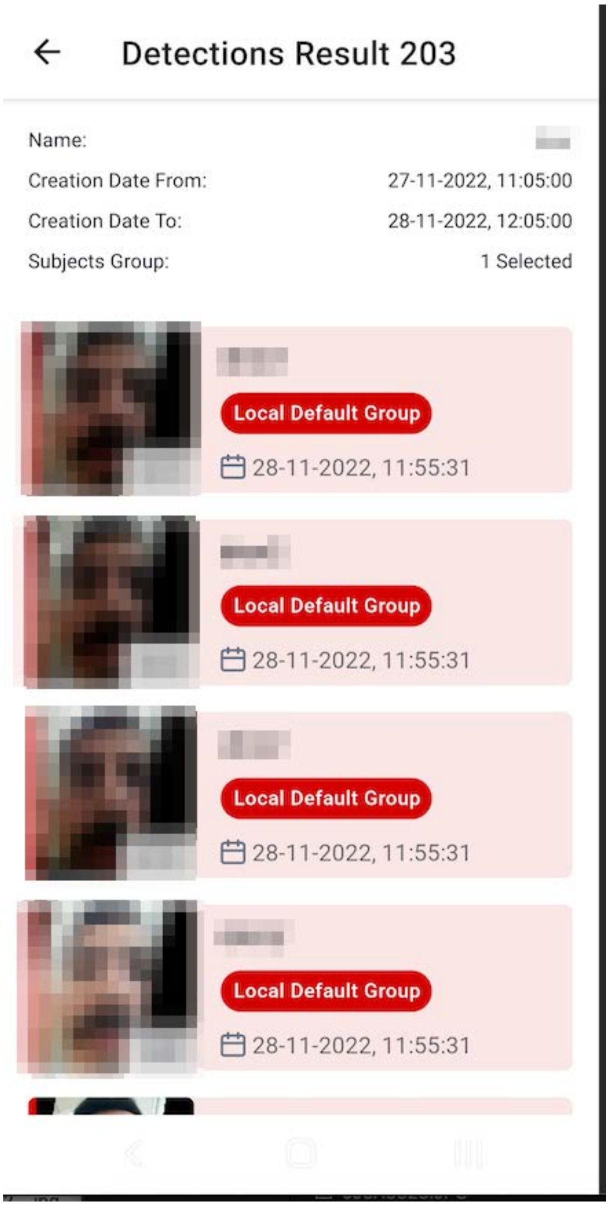
☑ Only Alerts

Subject Name

Groups Clear Selection

● Local Default Group

Results -



Detections Result 203

Name:

Creation Date From: 27-11-2022, 11:05:00

Creation Date To: 28-11-2022, 12:05:00

Subjects Group: 1 Selected

Local Default Group
28-11-2022, 11:55:31

Local Default Group
28-11-2022, 11:55:31

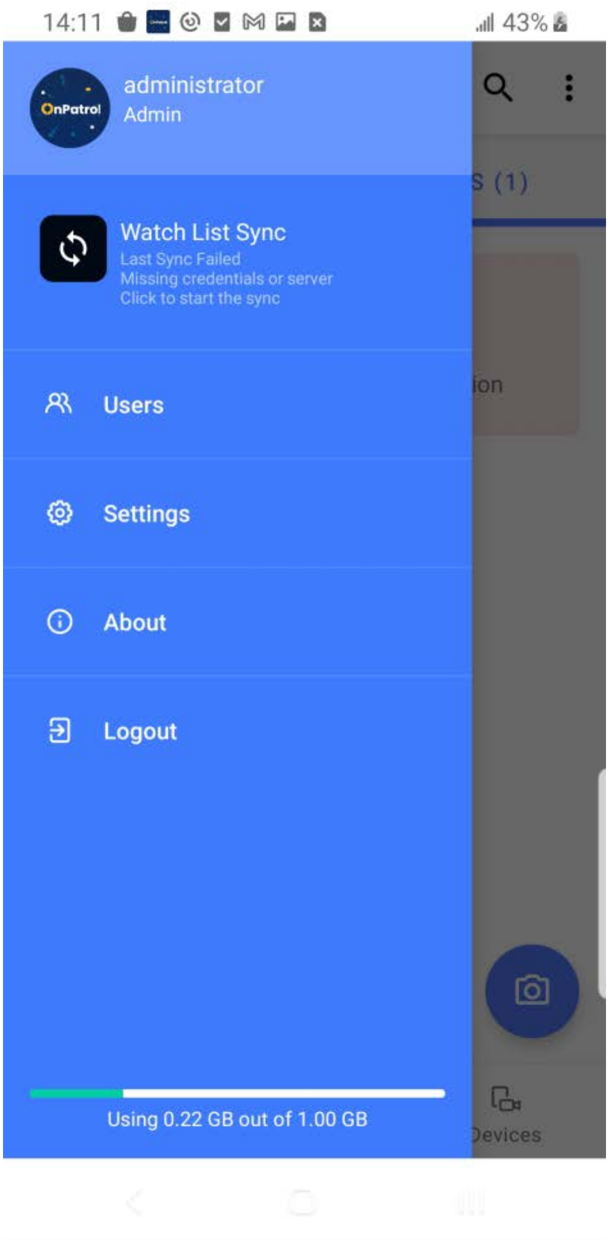
Local Default Group
28-11-2022, 11:55:31

Local Default Group
28-11-2022, 11:55:31

Settings and About

From the settings screen, you can turn app notifications on and off, change default subject group settings, set up sync with OnWatch, set app storage warning limit, and more.

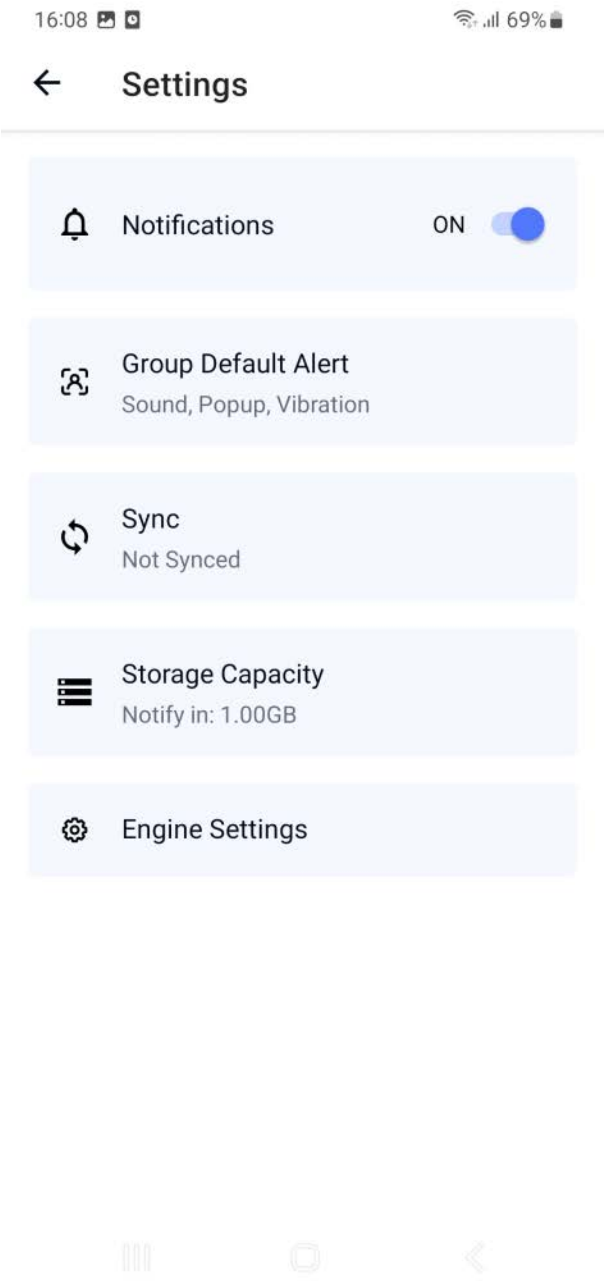
Reach the Settings screen from the main menu.



Watch List Sync
Last Sync Failed
Missing credentials or server
Click to start the sync

Notifications

You can turn app notifications on and off using the blue toggle.



16:08 69%

Settings

Notifications ON

Group Default Alert
Sound, Popup, Vibration

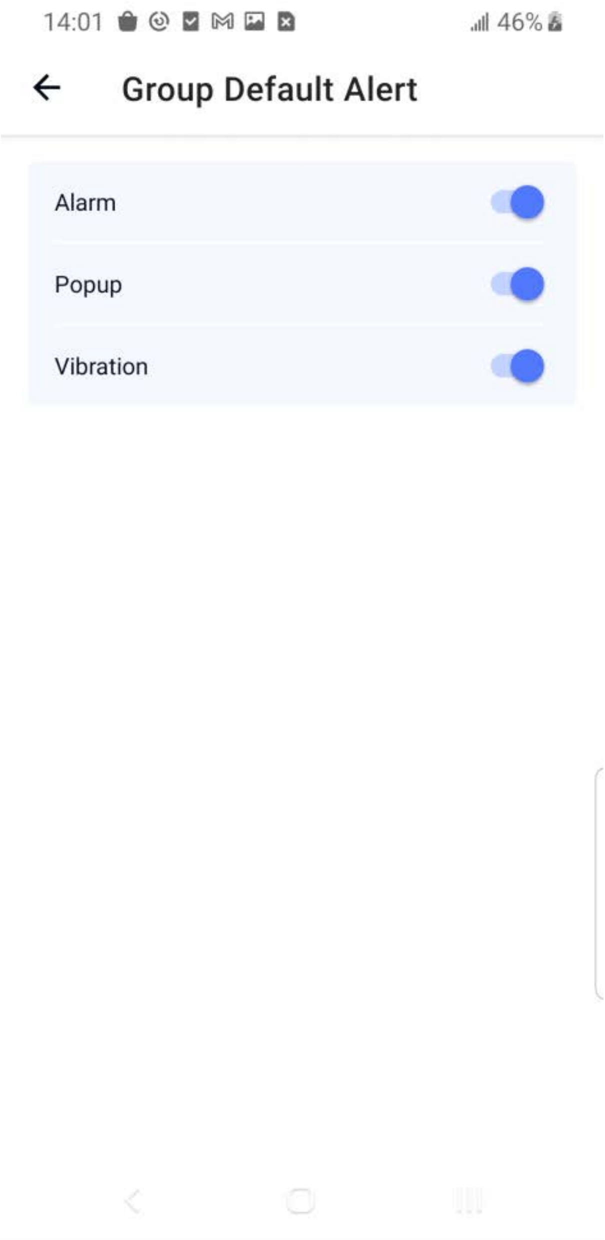
Sync
Not Synced

Storage Capacity
Notify in: 1.00GB

Engine Settings

Subject Group Default Alerts

You can change the default alerts for subject groups.



Group Default Alert

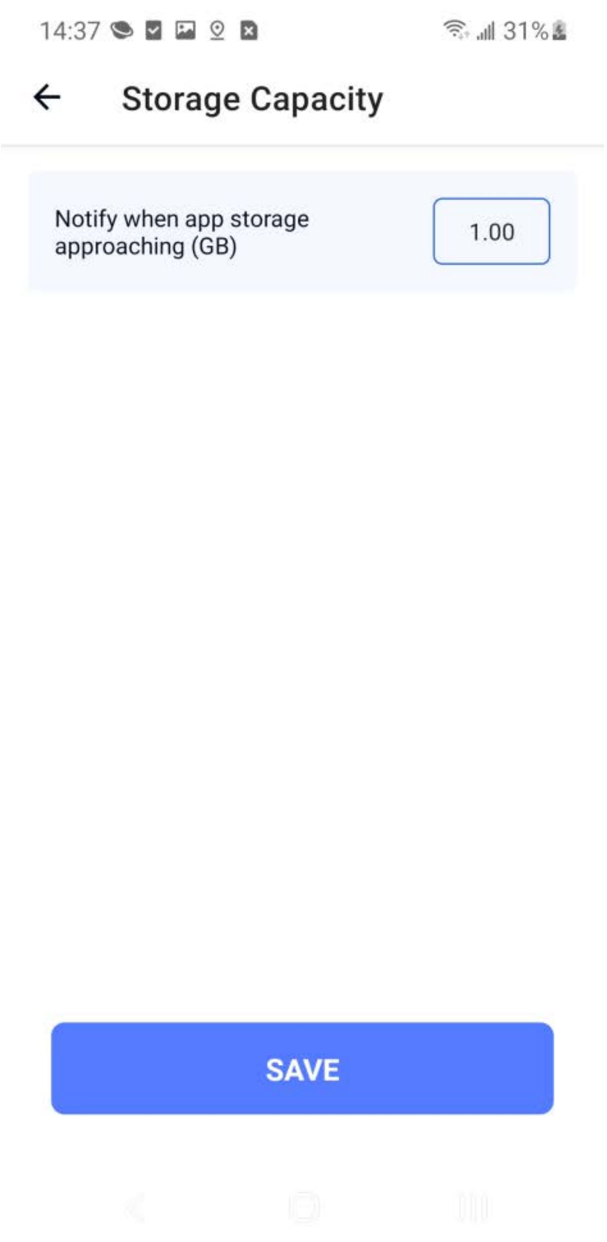
Alarm: on

Popup: on

Vibration: on

Storage Capacity

You can specify when you will receive notifications regarding app storage approaching a certain amount (in GB).



Storage Capacity

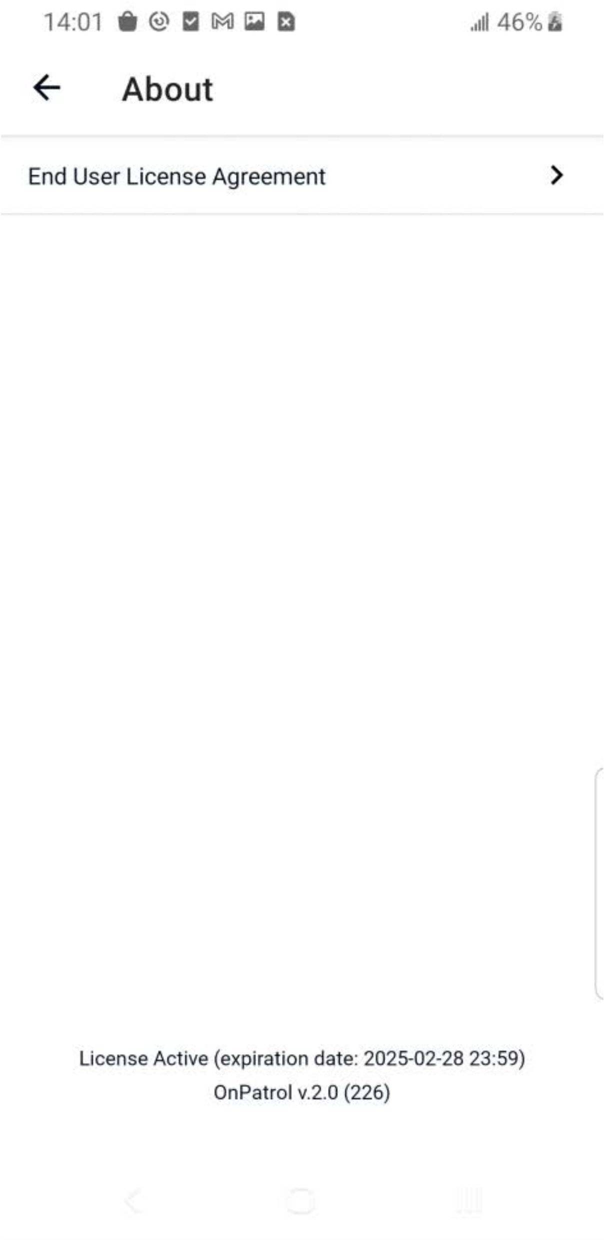
Notify when app storage approaching (GB) 1.00

📘 Storage limit

This is the OnPatrol recommended storage limit.
Nevertheless, after reaching this limit, you can still use the app until the phone storage is full.

About

On the about screen you can see the EULA and license information.

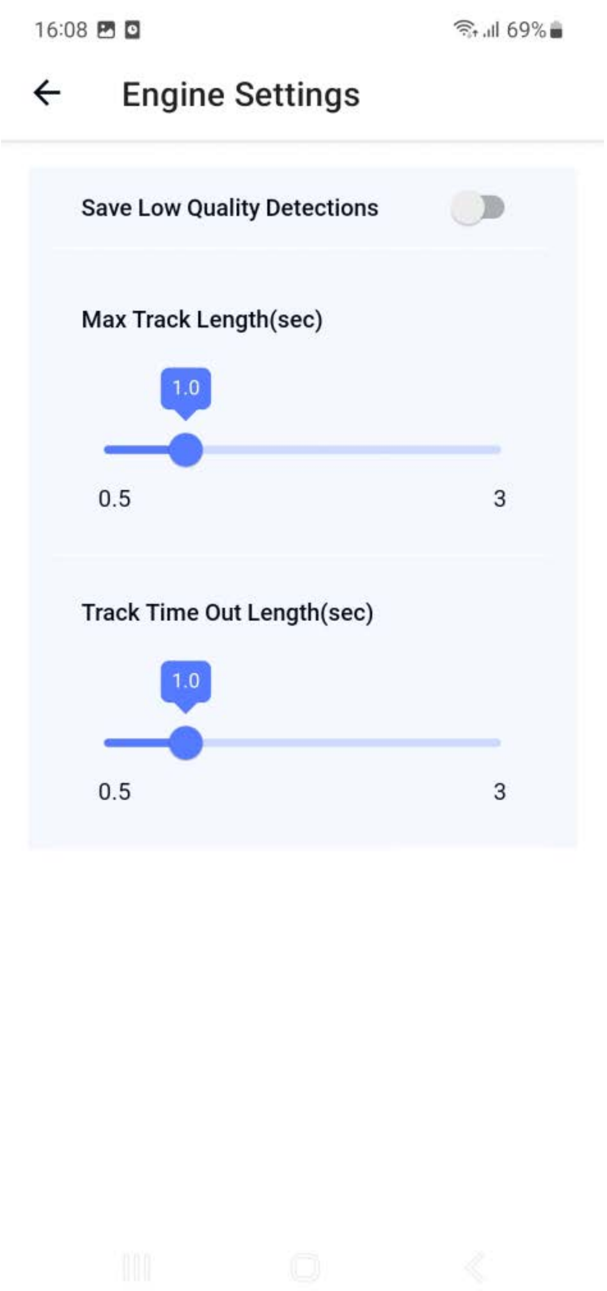

14:01 46%

About

End User License Agreement

License Active (expiration date: 2025-02-28 23:59)
OnPatrol v.2.0 (226)

Engine Settings



16:08 69%

Engine Settings

Save Low Quality Detections

Max Track Length(sec)

1.0

0.5 3

Track Time Out Length(sec)

1.0

0.5 3

On the engine settings, there are 3 options to control the App Engine -

Save Low-Quality Detections

User can choose if the App *Save Low-Quality Detections* by using the toggle.
As a result, every face detection will be saved by the app, this can lead to even blurry faces being saved.

Max Track Length

User can select *Max Track Length* in seconds.
For example, if this value is set for 3 seconds after a person's face is detected in 3 continuous seconds, the system will send the track to analyze and begin a new one.

Track Time Out Lenght

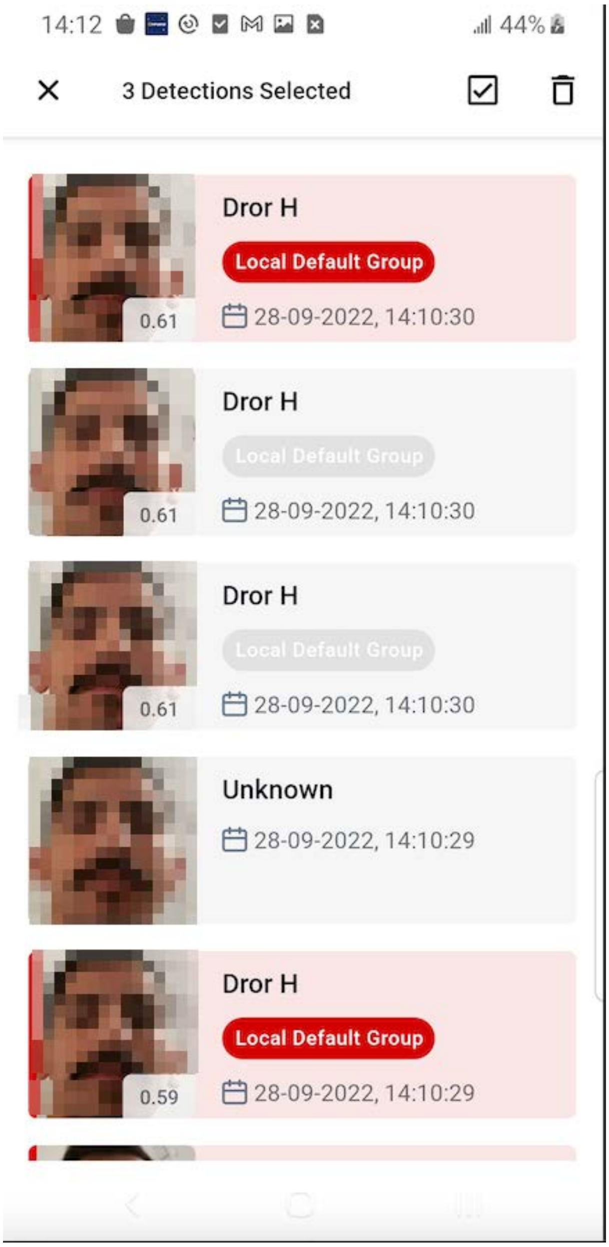
User can select *Track Time Out Lenght* in seconds.
This value defines how many seconds a person does not appear in the FOV before his track is created.

Detections

Understanding detections

Detections are saved when a person crosses a camera's field of view.

Detections of people not included in a subject group are saved on the telephone or tablet and can be accessed using the search function.



14:12 44%

3 Detections Selected

Dror H
Local Default Group
28-09-2022, 14:10:30
0.61

Dror H
Local Default Group
28-09-2022, 14:10:30
0.61

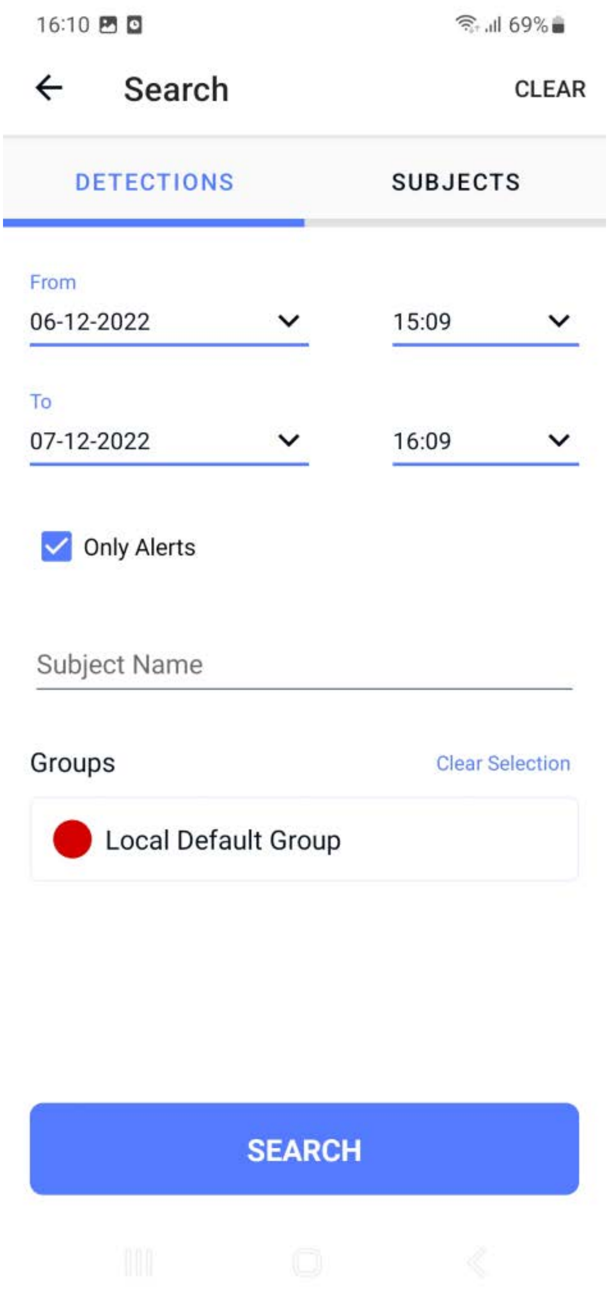
Dror H
Local Default Group
28-09-2022, 14:10:30
0.61

Unknown
28-09-2022, 14:10:29

Dror H
Local Default Group
28-09-2022, 14:10:29
0.59

Working with detections

Navigate to the search screen Alerts>search icon>Detections and choose a time period for the detection search. You can also search for Alerts only. See the Search page.



From
06-12-2022
15:09

To
07-12-2022
16:09

☑ Only Alerts

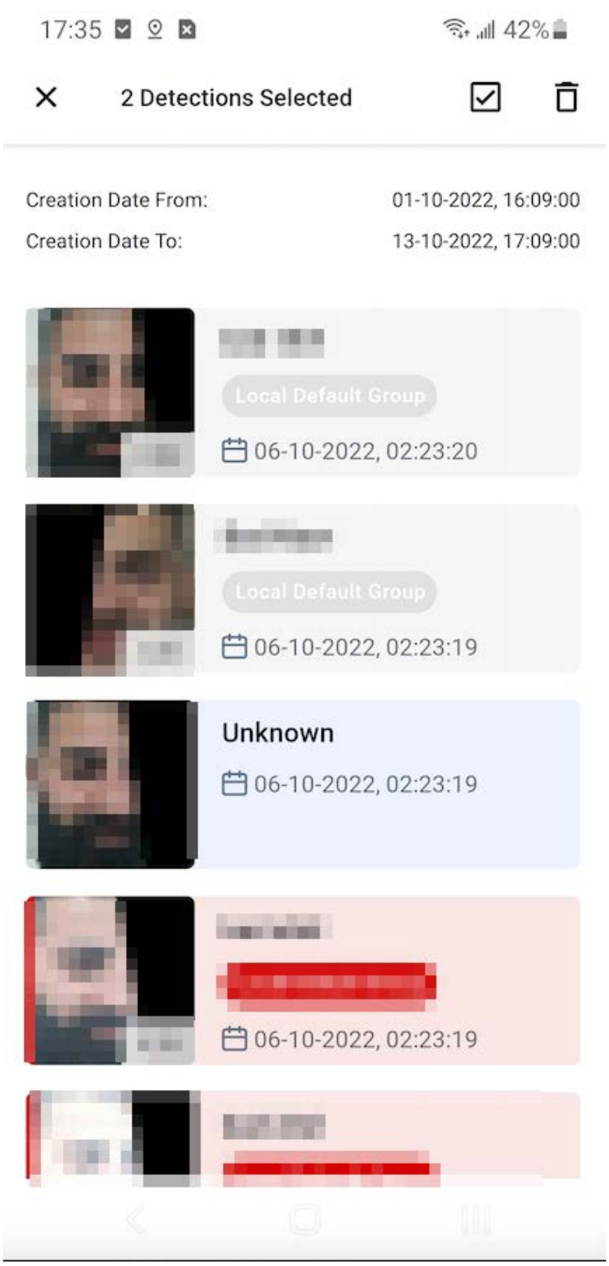
Subject Name

Groups
Clear Selection

● Local Default Group

Delete Detection

You can delete a detection from the detection screen with a long press on the detection and tapping the bin that is displayed in the upper righthand corner.



17:35 42%

2 Detections Selected

Creation Date From: 01-10-2022, 16:09:00

Creation Date To: 13-10-2022, 17:09:00

[redacted]

Local Default Group

06-10-2022, 02:23:20

[redacted]

Local Default Group

06-10-2022, 02:23:19

Unknown

06-10-2022, 02:23:19

[redacted]

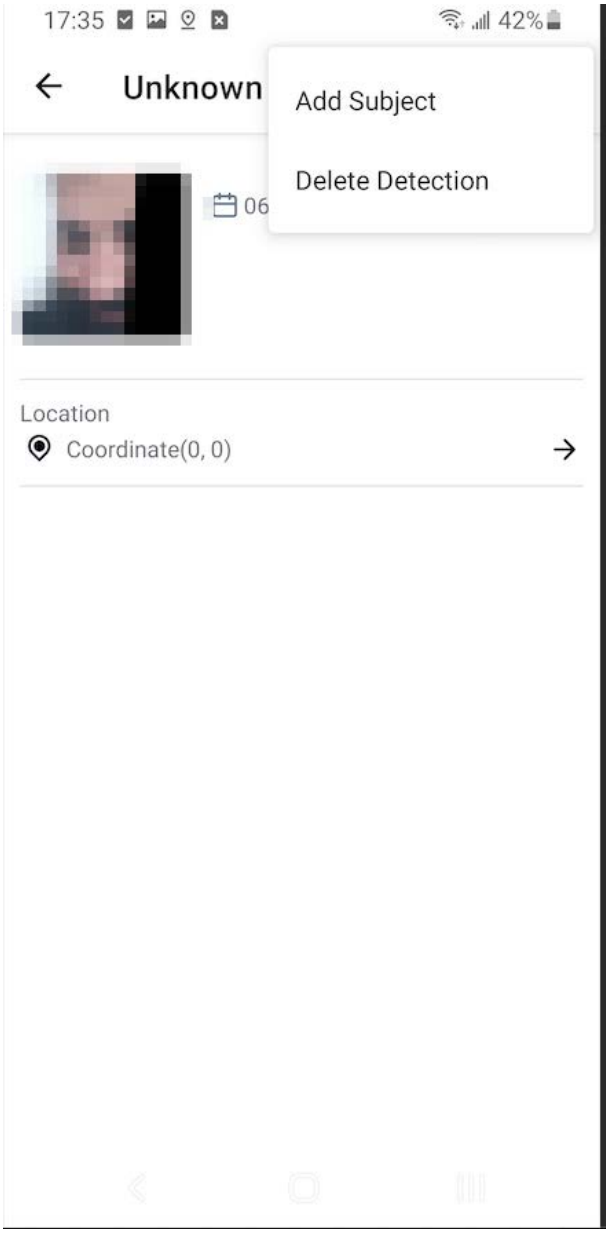
[redacted]

06-10-2022, 02:23:19

[redacted]

[redacted]

or by entering a specific detection and deleting from the vertical ellipsis.



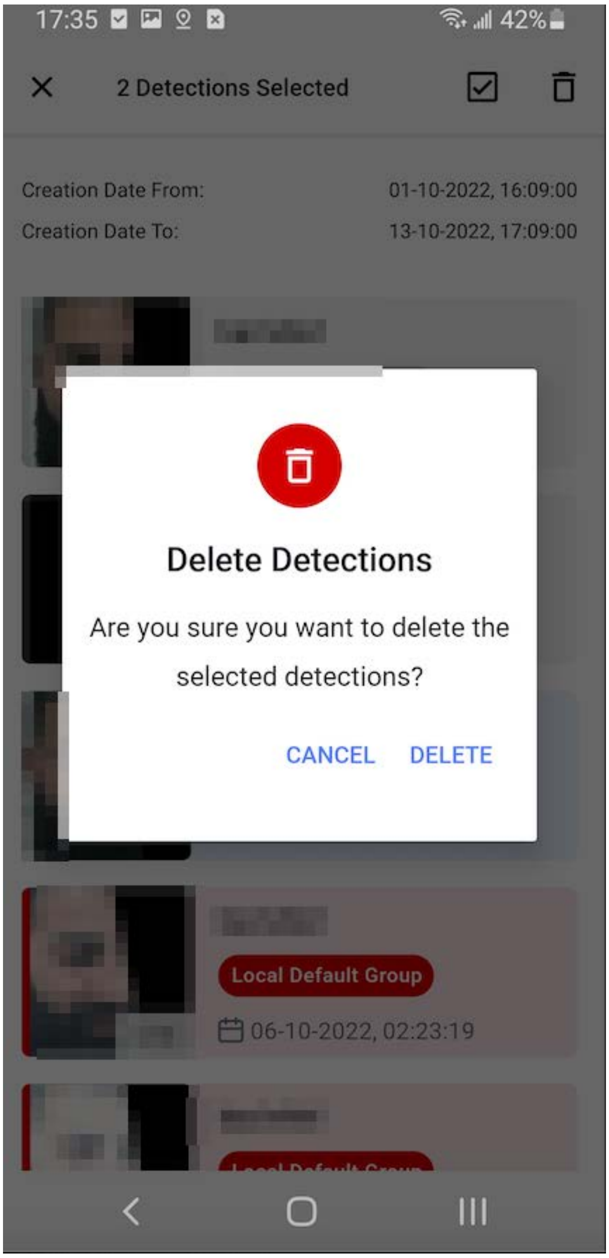
Unknown

06

Location

Coordinate(0, 0)

Tap Delete on the popup to confirm the deletion.



2 Detections Selected

Creation Date From: 01-10-2022, 16:09:00

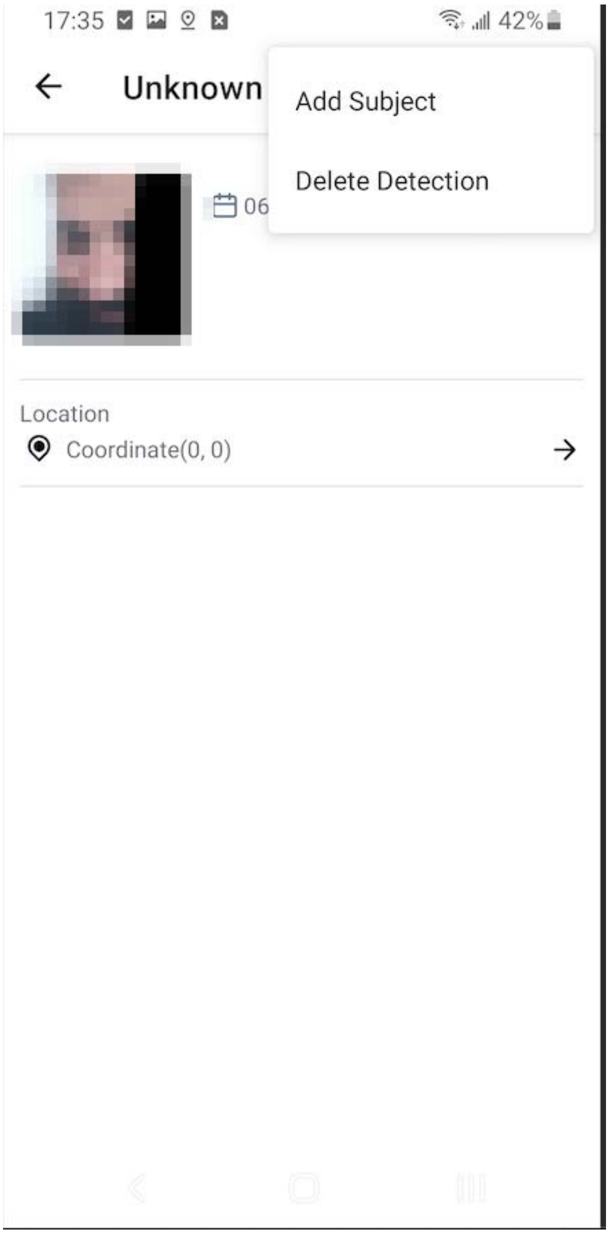
Creation Date To: 13-10-2022, 17:09:00

Delete Detections

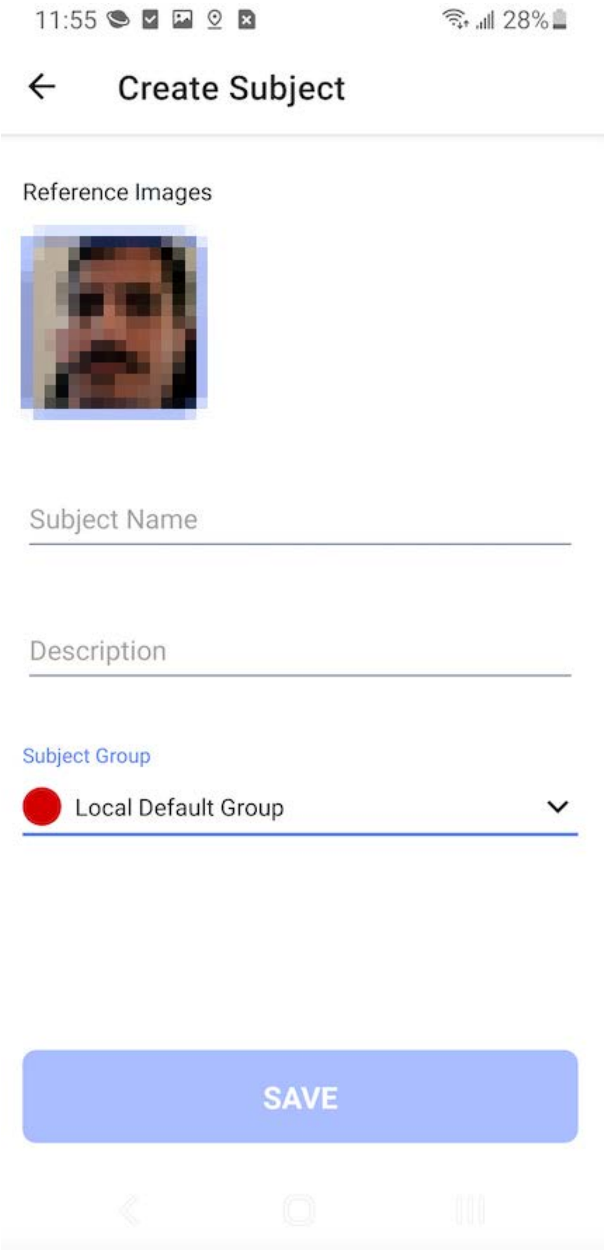
Are you sure you want to delete the selected detections?

Add a new subject from the list of detections

You can add a new subject from the list of detection by tapping a specific detection and selecting Add Subject from the vertical ellipsis menu.



The Create subject screen is displayed with the detection image.



Using Devices

Start using your cameras to detect people and recognize people of interest (those in a watch list group).

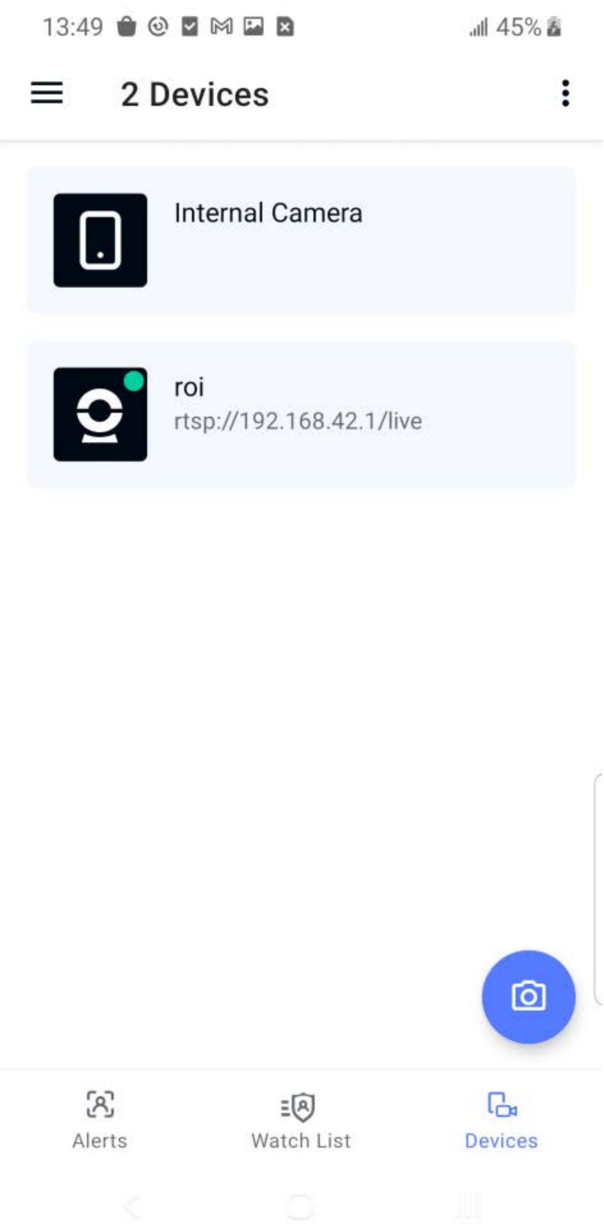
Camera Modes

Cameras can operate in Live or Background mode.
Navigate to Devices. (Tap **Devices** at the bottom of the screen.)
The green dot on one of the cameras reflects that this camera is selected.

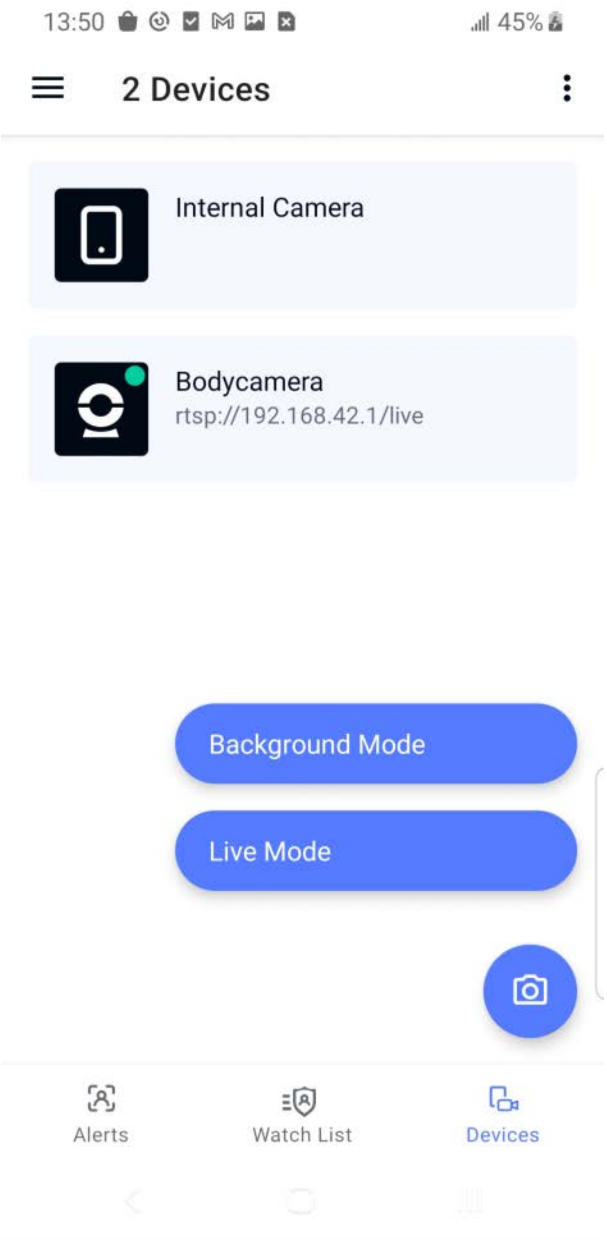
> ### One camera at a time
>
> Only one camera can be operating at a time..

Default device

The internal camera is the default device.



Tap the blue camera icon on the bottom of the screen, to select between the two options -
_Background Mode
_Live Mode



Live Mode

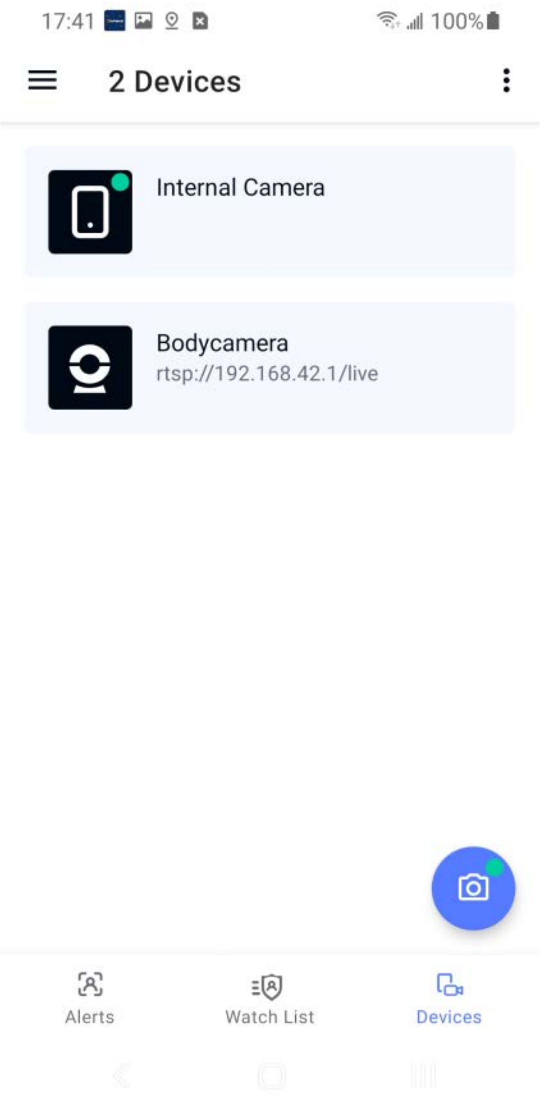
Live mode opens the selected camera's FOV, and the app starts to analyze the video stream and search for faces. When a person from a subject group is detected, a notification appears on the screen in the Recent Recognition panel, across the bottom of the screen. (The use of sound, vibration, popup for the notification depends on the subject group alert settings).

Background mode

In background mode, you can use the phone while the app analyzes the selected camera in the background.
You can continue using the OnPatrol app or minimize the app to work in the background and use the telephone. When in background mode, alerts are displayed in the telephone or tablet notification drawer.

> 🚧 **Access location in the background**
>
> To retrieve location while stream analysis is running in the background, access to the app location should be allowed at all times.

The green dot on the camera icon at the bottom indicates that the camera is working in background mode.

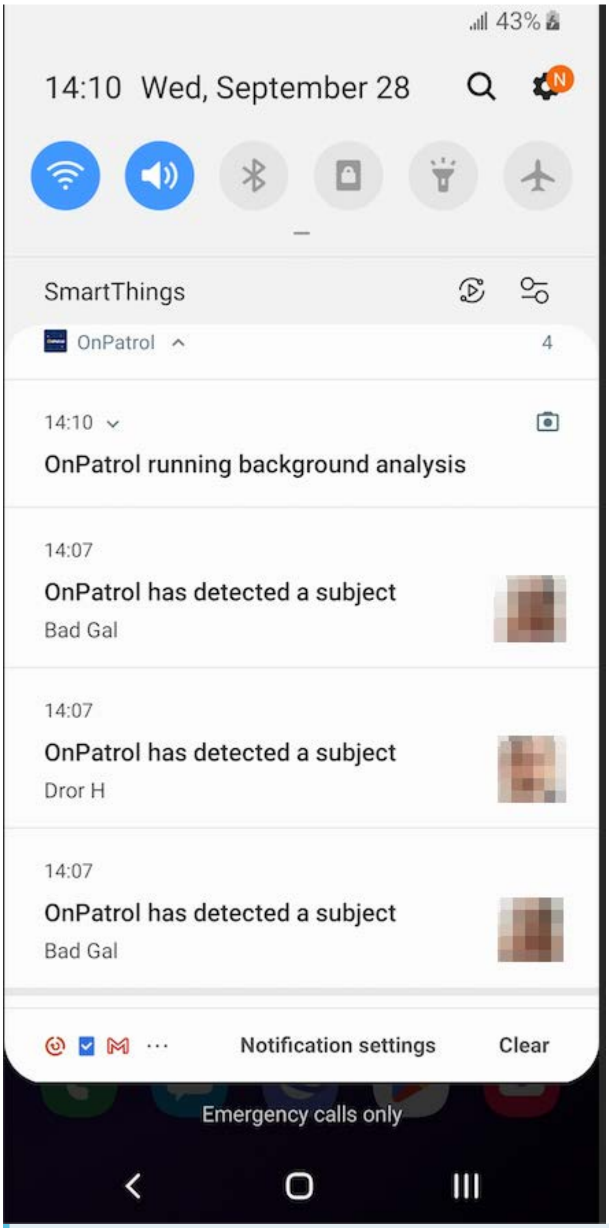

17:41 100%

2 Devices

Internal Camera

Bodycamera
rtsp://192.168.42.1/live

An indication that OnPatrol is working in background mode is displayed in the notification drawer.



14:10 Wed, September 28

SmartThings

OnPatrol 4

14:10

OnPatrol running background analysis

14:07

OnPatrol has detected a subject

Bad Gal

14:07

OnPatrol has detected a subject

Dror H

14:07

OnPatrol has detected a subject

Bad Gal

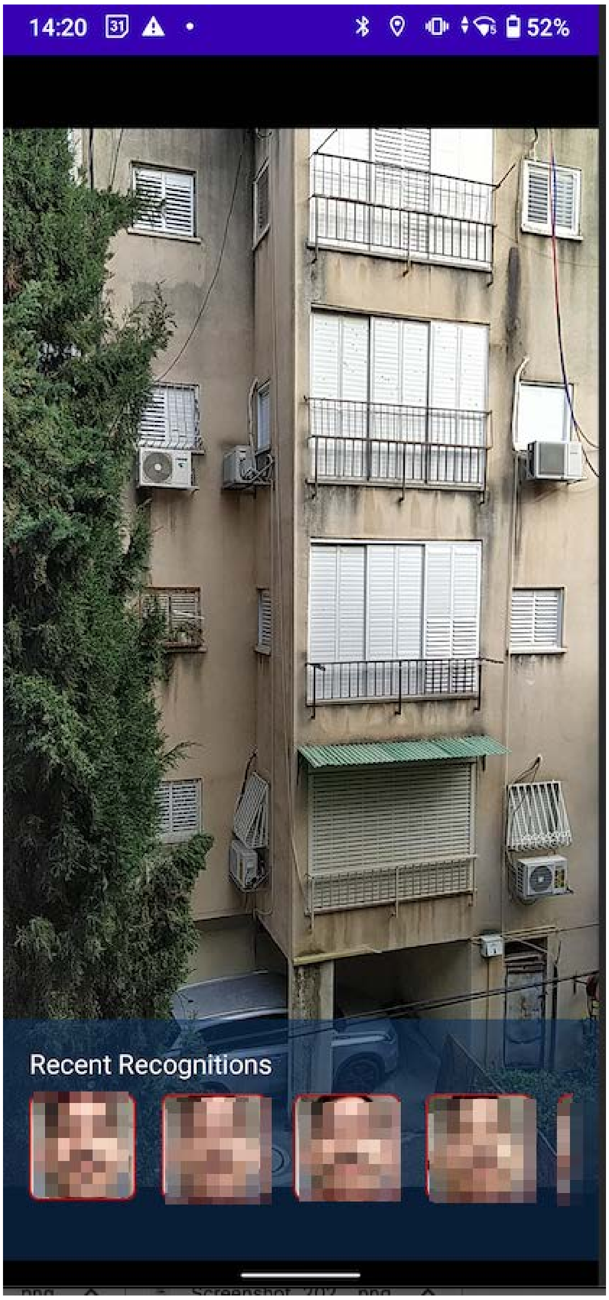
> ### Detections
>
> Detections of people that are not part of any subject group are saved on the OnPatrol device and can be accessed from the search function.

Portrait or Landscape View

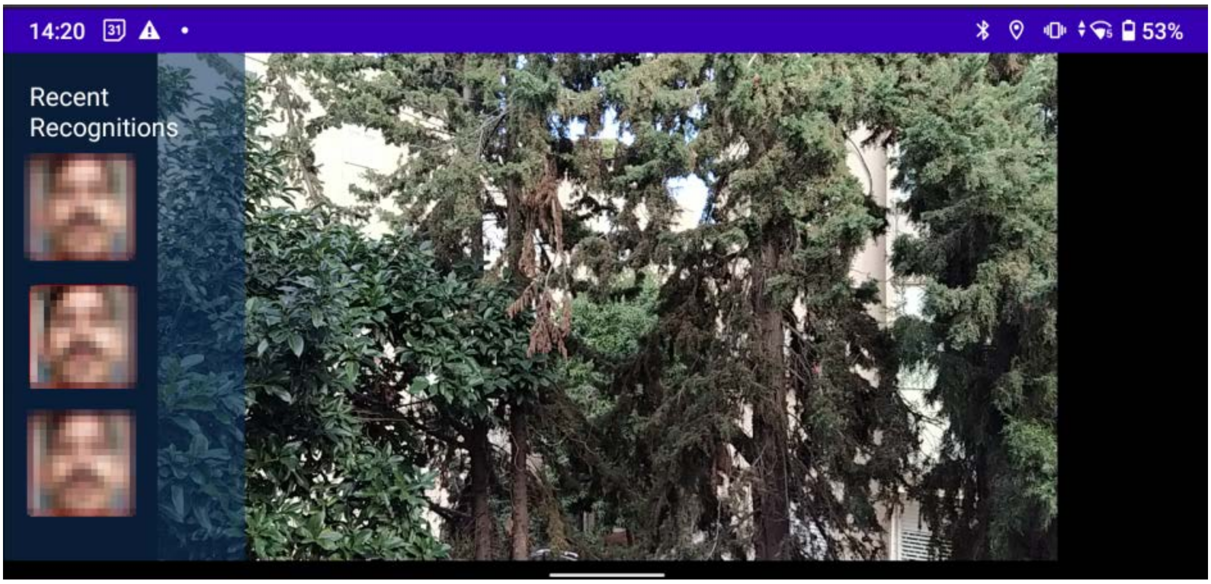
You can use the camera in portrait or landscape view.

> ### Moving between portrait and landscape view
>
> This setting is made on the telephone or tablet navigation bar or autorotate settings.

Portrait View

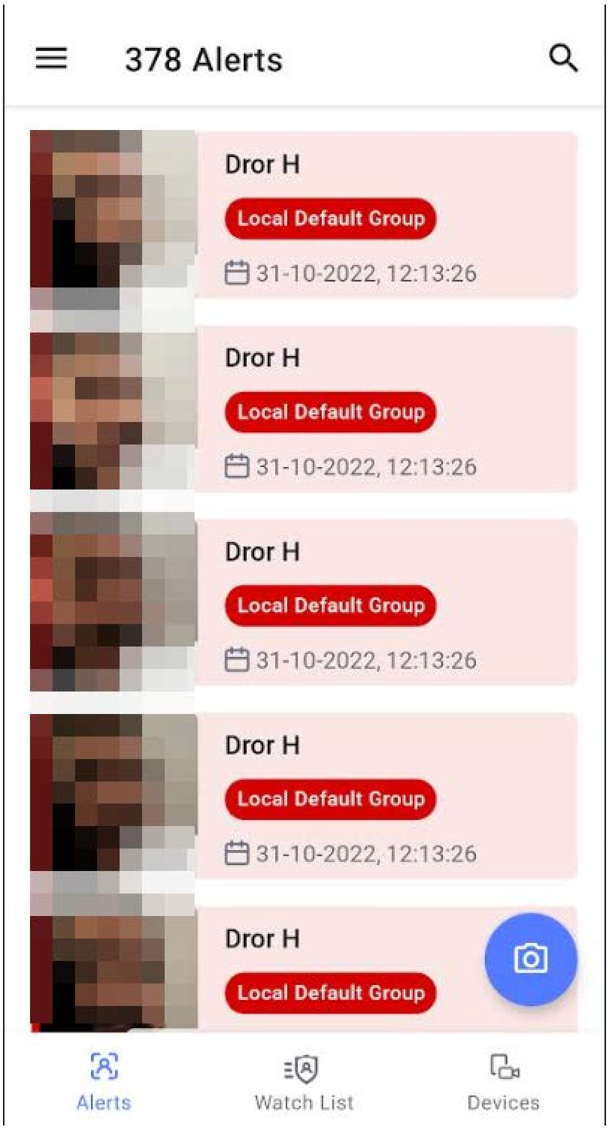


Landscape View



Alerts

Alerts are detections that were recognized - sometimes referred to as recognitions.
Alerts are displayed on the Alerts screen. Tap **Alerts** on the bottom of the screen to display this screen.



378 Alerts

Dror H
Local Default Group
31-10-2022, 12:13:26

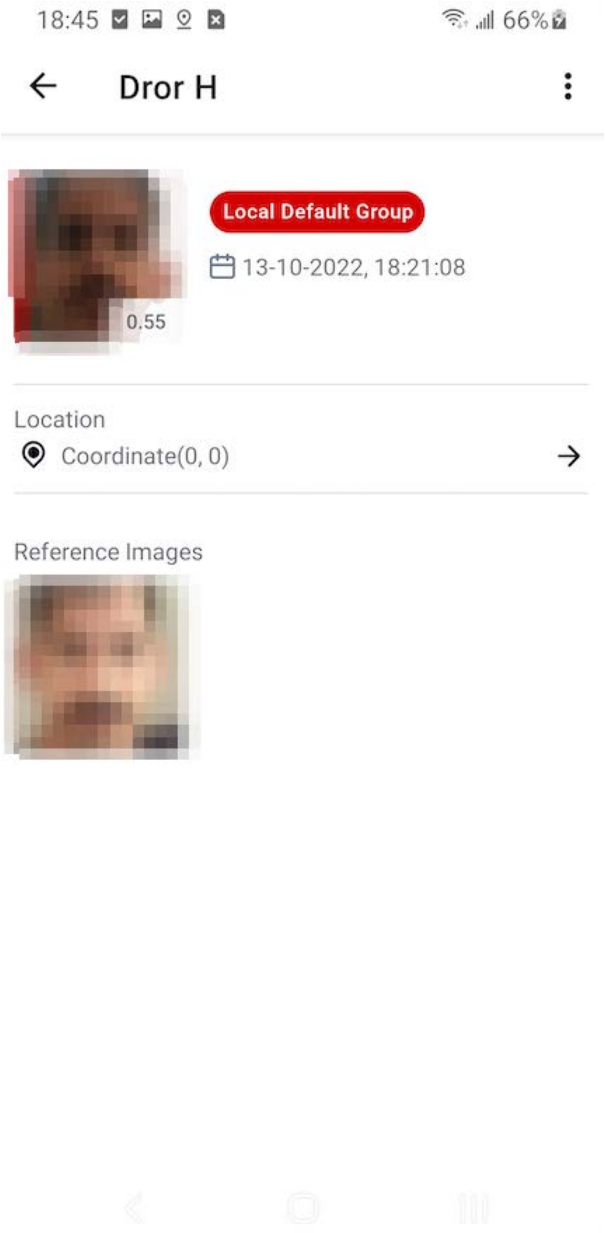
Dror H
Local Default Group
31-10-2022, 12:13:26

Dror H
Local Default Group
31-10-2022, 12:13:26

Dror H
Local Default Group
31-10-2022, 12:13:26

Dror H
Local Default Group

You can tap an alert from the least to reach the alert's profile screen.



Dror H

Local Default Group

13-10-2022, 18:21:08

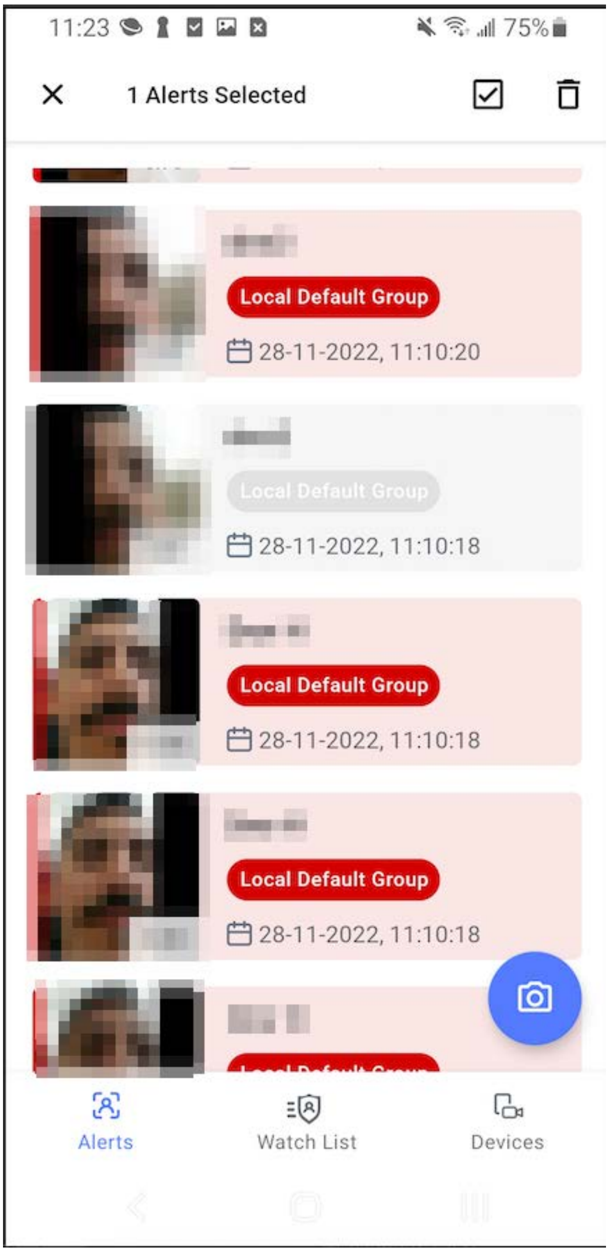
0.55

Location

Coordinate(0, 0)

Reference Images

On the alert screen, you can see the subject details, reference images, location, and time.
You can delete an alert by entering the alert screen with a short tap, or bulk delete with a long tap to each of the alerts to be deleted and then a tap to the bin in the upper righthand corner.

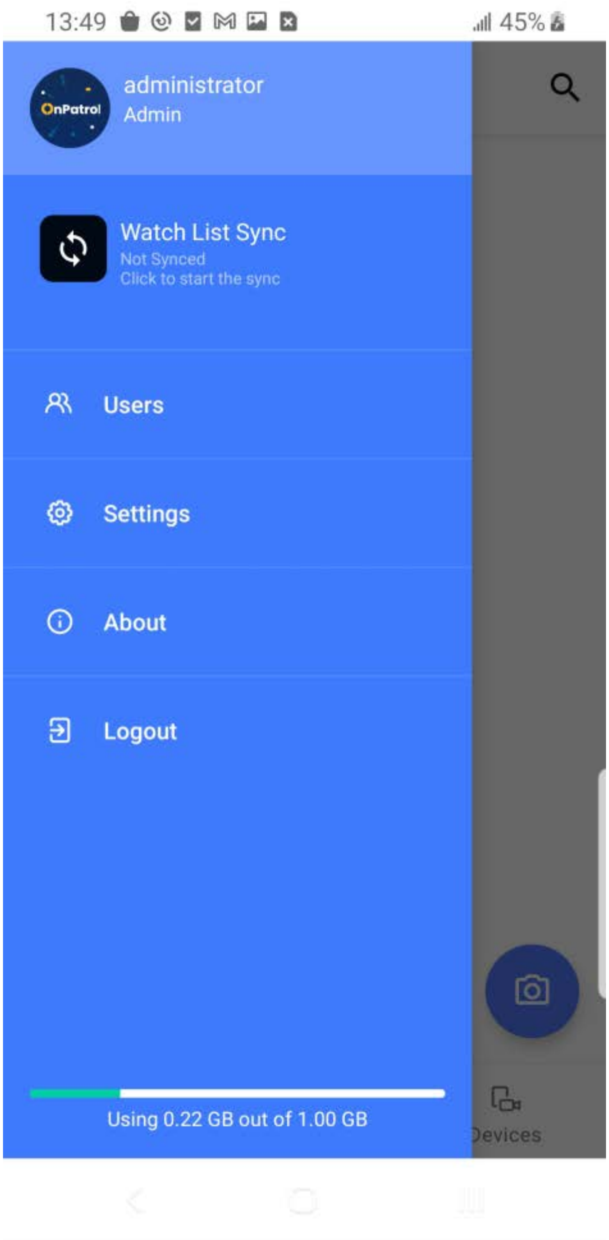


Administrator - Manage Users

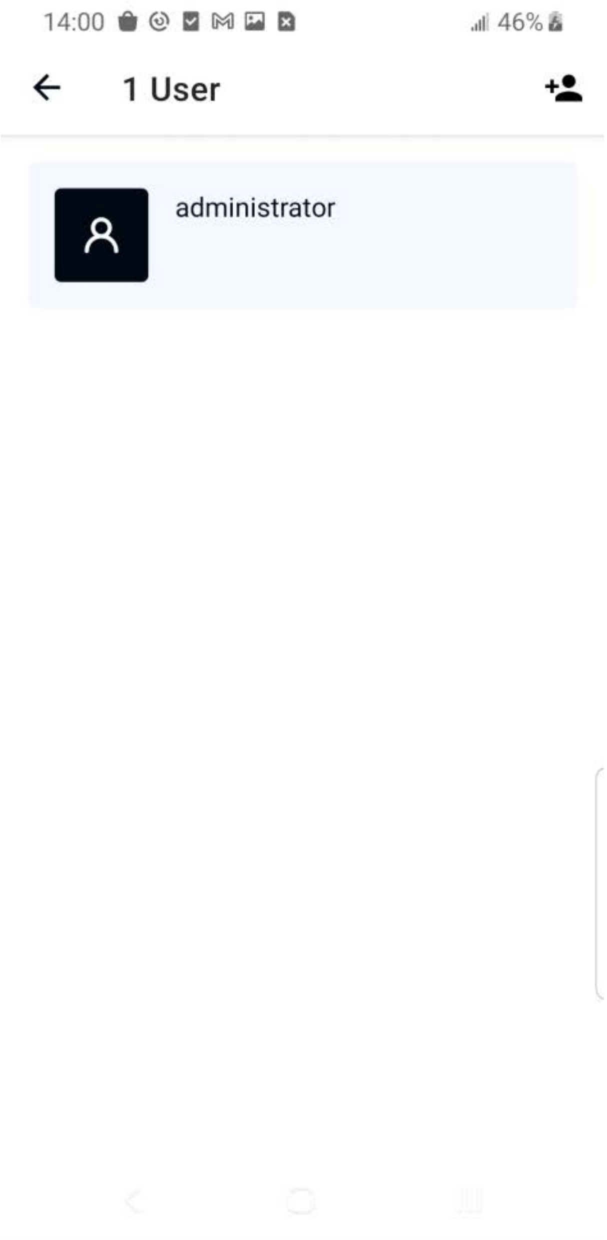
A new user has all user functionality except for the ability to add users. All users on the phone share the same OnPatrol data. Only administrators can manage users.

Add a user

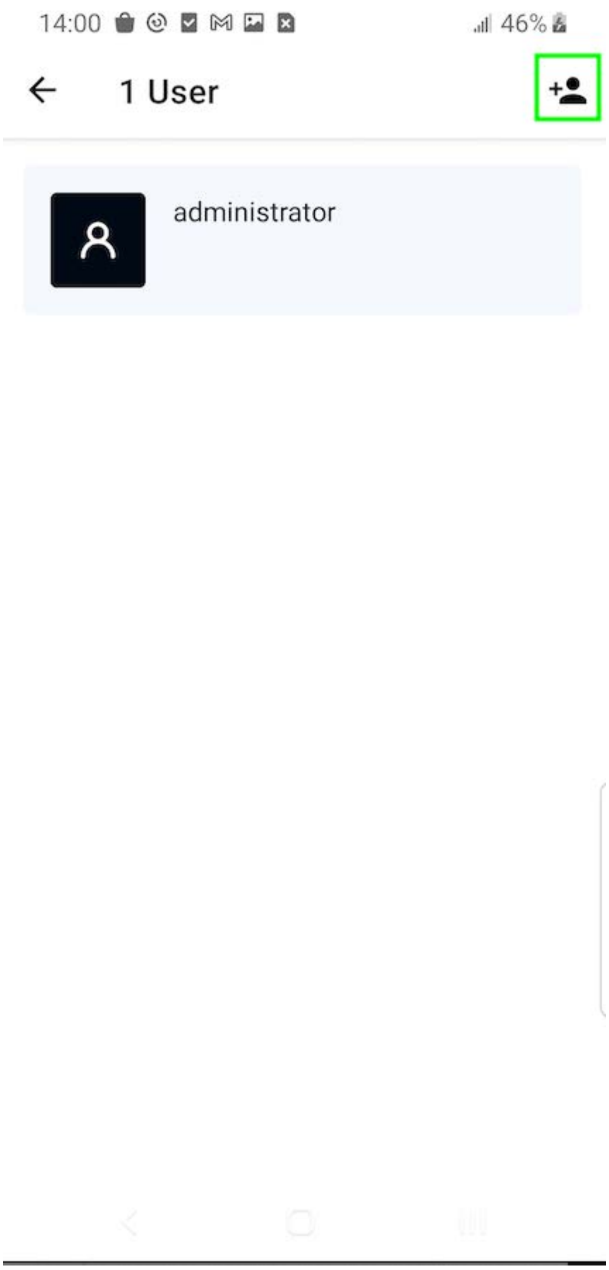
1. Tap the hamburger menu icon from any of the main screens



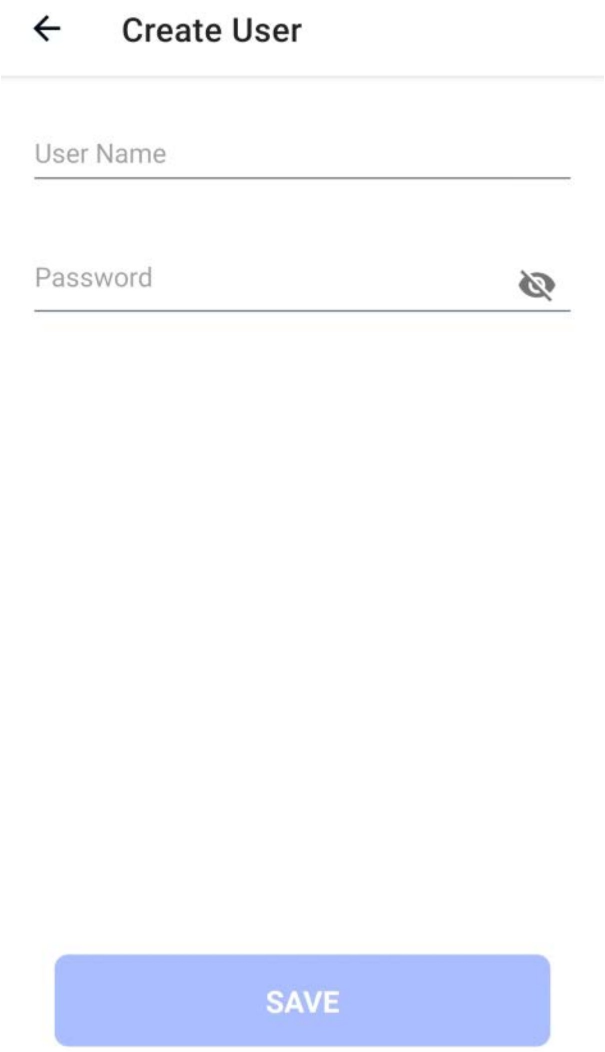
2. Tap **Users**. The users are displayed.



3. Tap +.



4. The **Create User** screen is displayed.



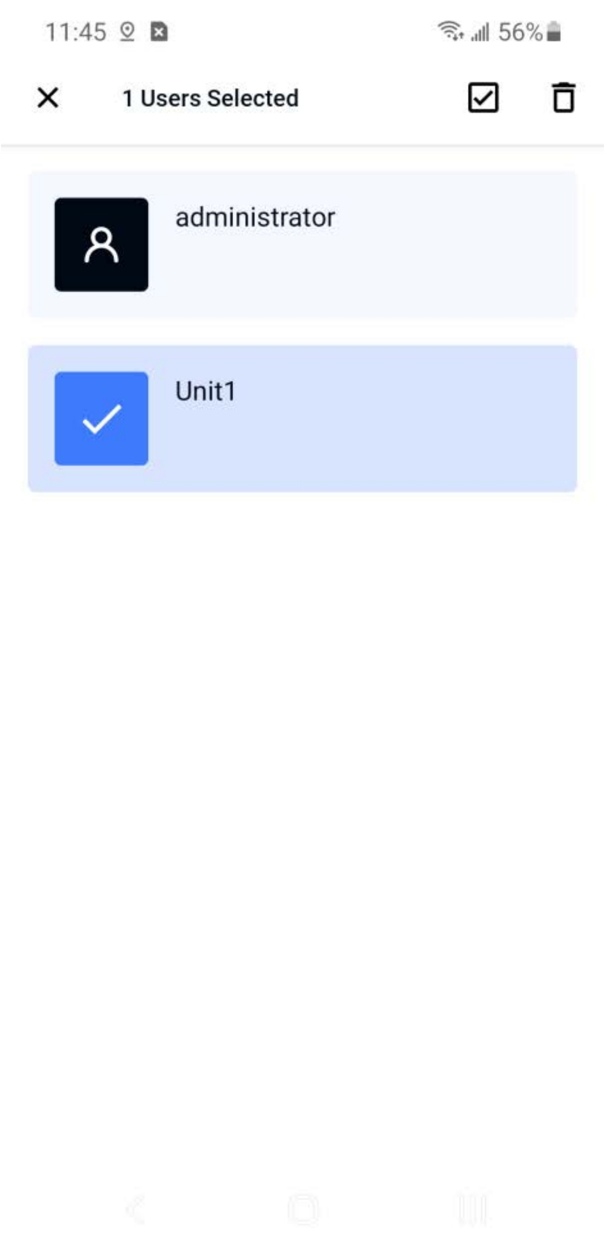
Enter the **User Name** and **Password**.

> 📘 User Name and Password Requirements
>
> ## User name - min 4 chars, only English letters
>
> ## Password - minimum 8 chars, maximum 30 chars.
>
> No special characters, must include at least one English letter and one number.

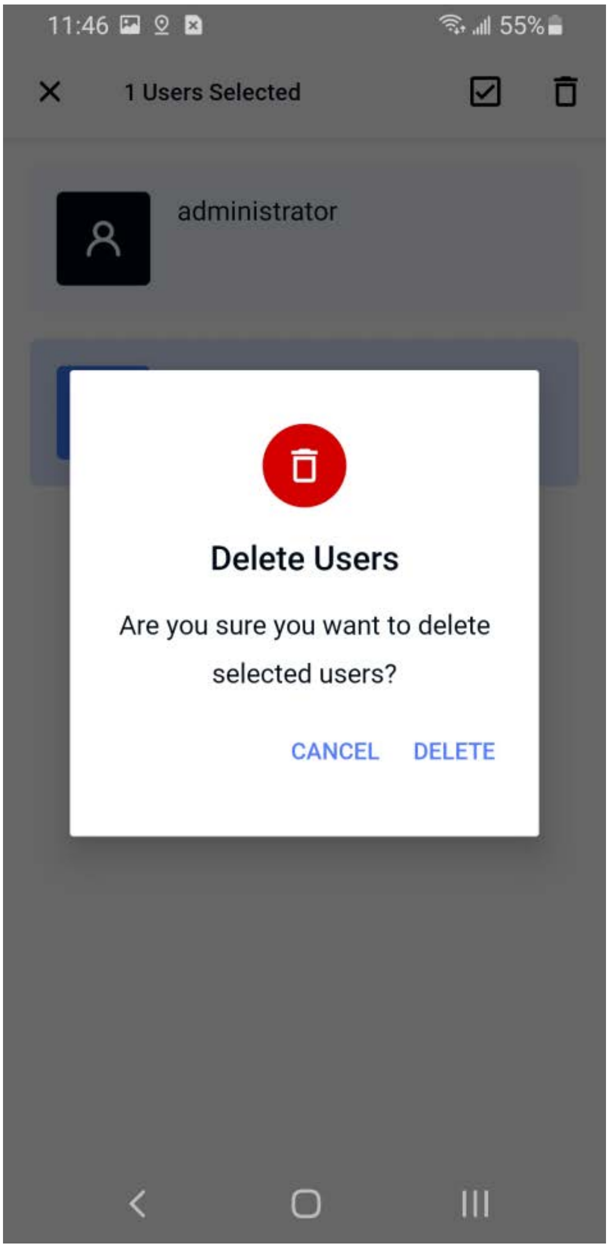
5. Tap **Save**.

Delete a user

1. Tap the hamburger menu icon.
2. Tap **Users**.
3. Select the user for deletion with a long tap.



4. Tap the bin at the end of the top row. The confirmation message is displayed.



Delete Users

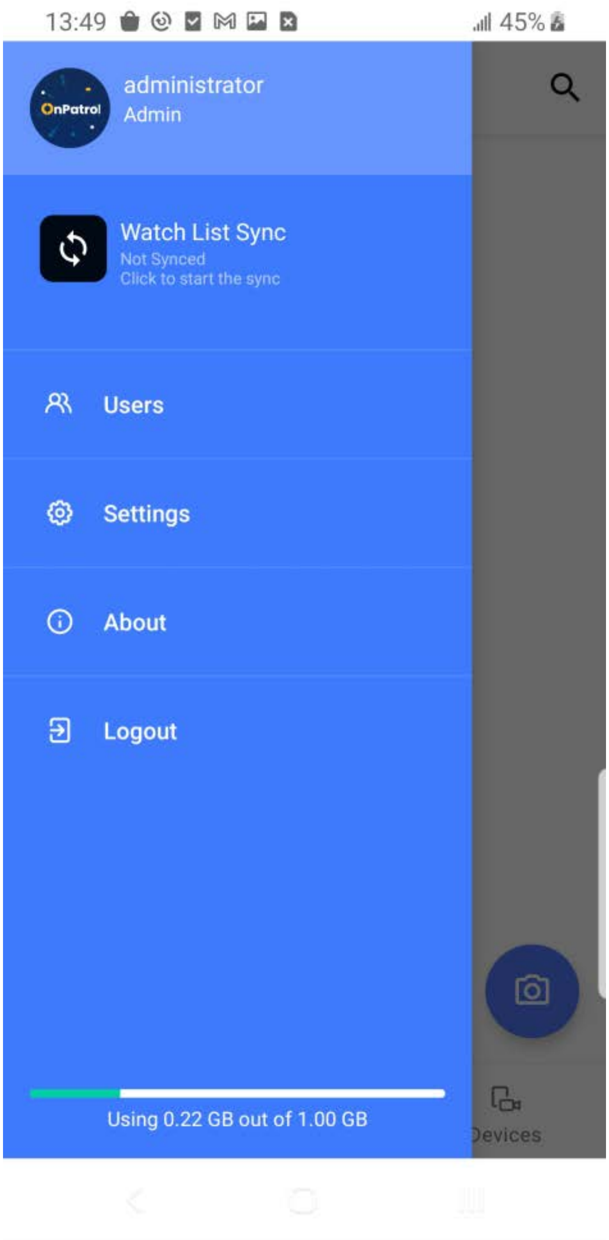
Are you sure you want to delete selected users?

6. Tap **Delete**.

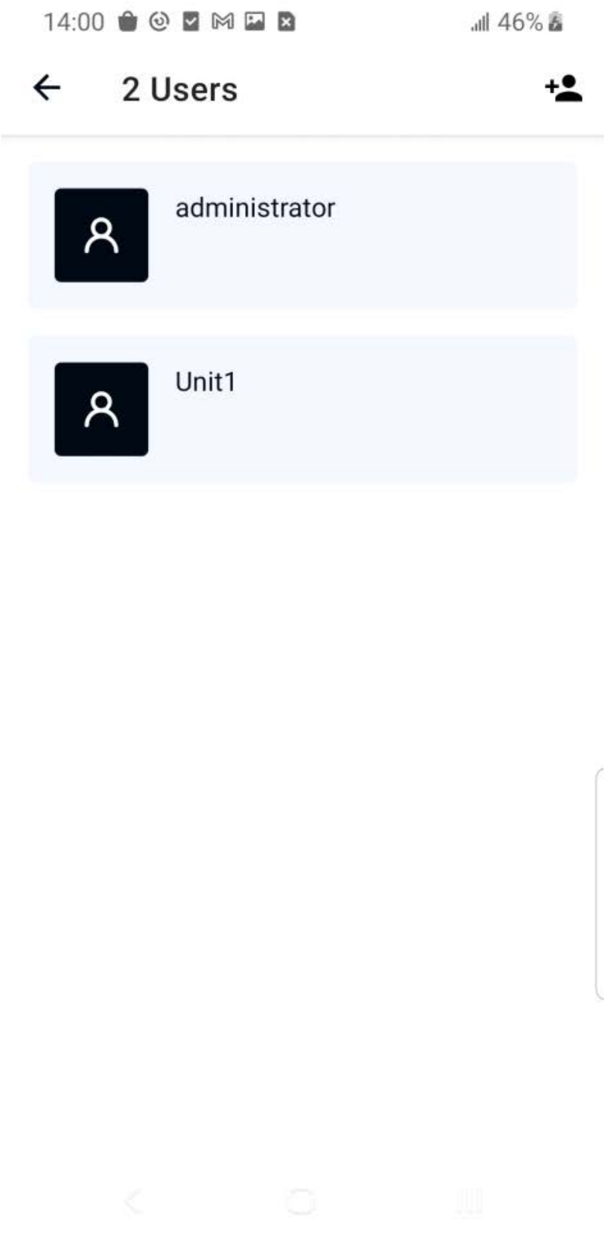
Administrator - Change User Name and Password

After the first login to the app, the app prompts you to change the default administrator password.

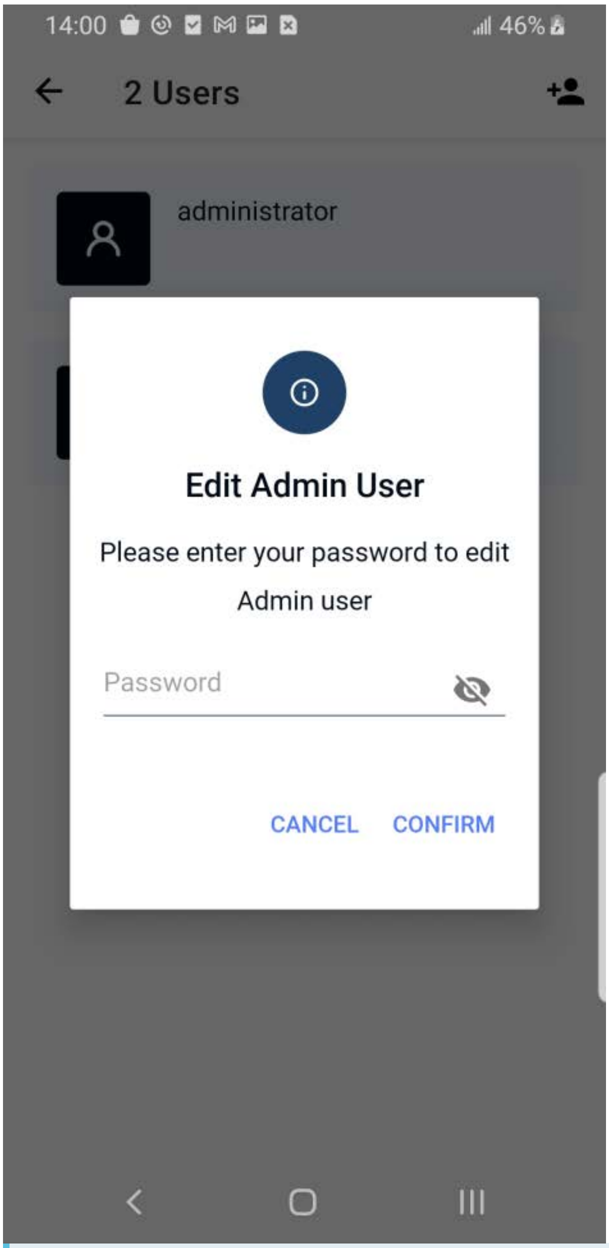
An admin can edit any user and password at any time by navigating to the Users screen from the hamburger menu.



Tap the user to be edited



To edit administrator credentials, you must enter the current administrator password



Edit Admin User

Please enter your password to edit Admin user

📘 User Name and Password Requirements

User name - minimum 4 characters, only English letters

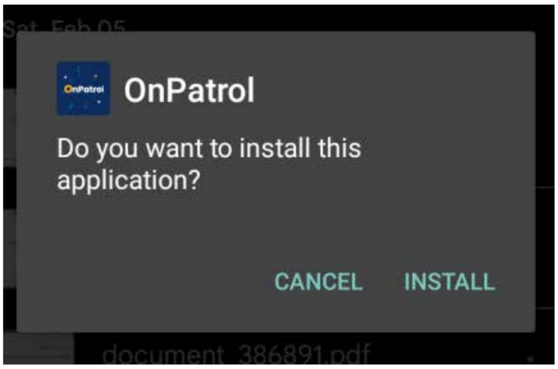
Password - minimum 8 characters, maximum 30 characters. No special characters. There must be at least one English character and one number.

OnPatrol Edge Installation

Step 1: Download & Install OnPatrol Edge

To install the OnPatrol application on a mobile device:

1. Click here to open and download the OnPatrol file.
2. Once the application is downloaded, a screen is displayed. Tap **Install**. If the installation process fails, turn off Google Play Protect.
3. After the installation is complete, open the application by tapping **Open**.



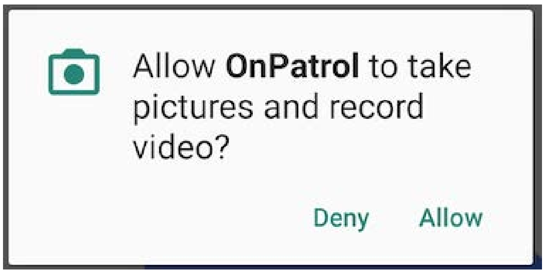
OnPatrol

Do you want to install this application?

Step 2: Run OnPatrol Edge the first time

1. Once the app is installed, tap **Open**.
2. Tap **Allow** to allow OnPatrol to take pictures, record videos, device location, and access photos, media, and files on your device.

> **Permissions**
>
> These permissions are needed to use all OnPatrol functionalities.

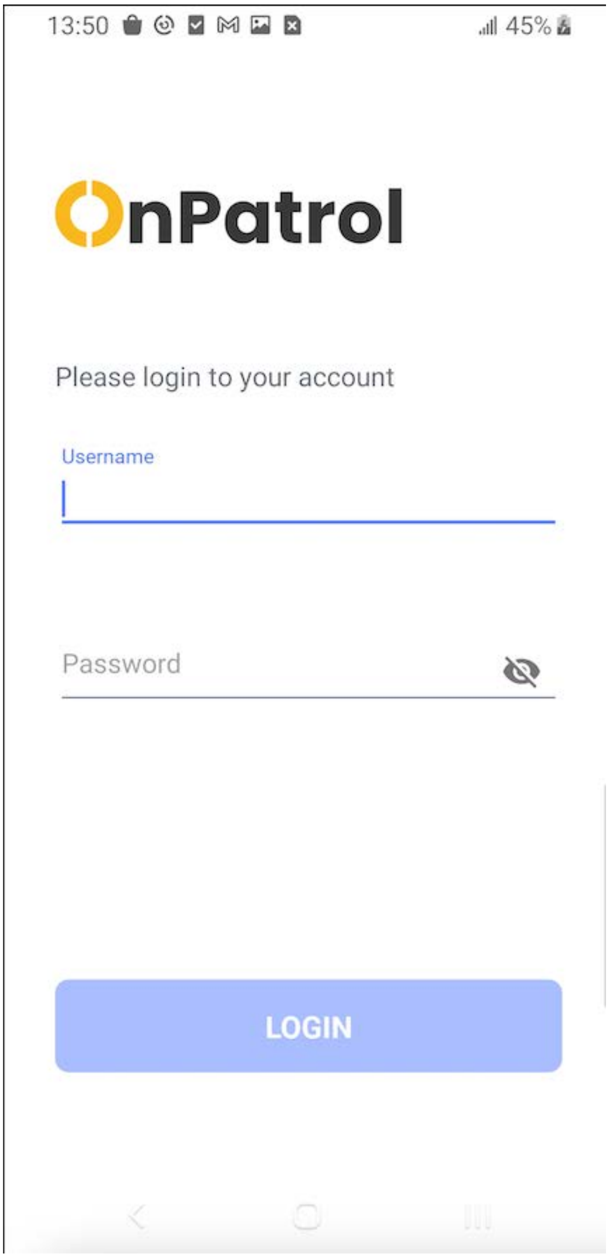


Allow **OnPatrol** to take pictures and record video?

Need to update

3. Enter your activation key and tap **Activate**.

4 . If it's the first sign-in to the app, enter your Administrator **Username** and the default **Password** provided by Oosto or your local integrator for the application.



13:50 45%

OnPatrol

Please login to your account

Username

Password

LOGIN

5. Change default administrator password.

Requirements

Software Requirements:

To use this application, you need an Android mobile device with Android 10 or above.

Hardware Requirments -

The OnPatrol is certified with the flagships phones from the major phones manufacturers, including:

- Samsung Galaxy S20 and above.

- Xiaomi Mi 10 and above.
- OnePlus 9 and above.
- Huawei Mate 40 and above.
- Google Pixel 5 and above.

The OnPatrol App is compatible with major processor manufacturers which have been tested in our labs, such as -

- Qualcomm Snapdragon
- MediaTek Dimensity
- Samsung Exynos
- Hisilicon Kirin
- Google Tensor

> 📘 **For Optimal performance**
>
> The Device should have-
>
> - Android 12
> - 6GB RAM
> - One of these processors or newer -
>   --Qualcomm Snapdragon 888
>   --MediaTek Dimensity 1000
>   --Samsung Exynos 990
>   --Hisilicon Kirin 9000
>   --Google Tensor