User Manual

MOBOTIX Cloud

Version 3.02

Table of Contents

Notices

General Notices

- This Manual is for reference only.
- All designs / procedures shown are subject to change without prior written notice.
- All trademarks and registered trademarks mentioned are the properties of their respective owners.
- Please visit our website www.mobotix.com or contact your local service engineer for further information.

Precautions for Use

- Device operability is subject to network capabilities of the install location. Please contact your local sales representative for information on network requirements.
- Handle the device with care. Do not apply shock or drop the device. Failure to adhere may cause the device to malfunction.
- This device is designed to be used indoors.
- Do not directly disconnect device from the power when running. Power down by pressing the power button on the front of the device.
- Do not use the device in hot or humid environments for an extended period of time. Failure to adhere causes component degradation and shortened life span of the device.
- Do not expose the device to a direct heat source.
- Ensure that all data is wiped from the device before disposal.

Legal Notes

Legal aspects of video and sound recording:

You must comply with all data protection regulations for video and sound monitoring when using MOBOTIXAG products. Depending on national laws and the installation location of the MOBOTIX Cloud, the recording of video and sound data may be subject to special documentation, or it may be prohibited. All users of MOBOTIX products are therefore required to familiarize themselves with all applicable regulations and to comply with these laws. MOBOTIXAG is not liable for any illegal use of its products.

Declaration of Conformity

The products of MOBOTIX AG are certified according to the applicable regulations of the EC and other countries. You can find the declarations of conformity for the products of MOBOTIX under **www.mobotix.com > Support > Download Center > Marketing & Documentation > Certificates & Declarations of Conformity**

Disclaimer

MOBOTIX AG does not assume any responsibility for damages, which are the result of improper use or failure to comply to the manuals or the applicable rules and regulations. Our General Terms and Conditions apply. You can download the current version of the General Terms and Conditions from our website www.mobotix.com by clicking on the **General Terms and Conditions General Terms and Conditions** link at the bottom of every page.

RoHS Declaration

The products of MOBOTIX AG are in full compliance with European Unions Restrictions of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment (RoHS Directive 2011/65/EC) as far as they are subject to these regulations (for the RoHS Declaration of MOBOTIX, please see **www.mobotix.com > Support > Download Center > Marketing & Documentation > Certificates & Declarations of Conformity**).

Disposal

Electrical and electronic products contain many valuable materials. For this reason, we recommend that you dispose of MOBOTIX products at the end of their service life in accordance with all legal requirements and regulations (or deposit these products at a municipal collection center). MOBOTIX products must not be disposed of in household waste! If the product contains a battery, please dis-pose of the battery separately (the corresponding product manuals contain specific directions if the product contains a battery).

Information for Users on Collection and Disposal of Old Equipment and used Batteries within the European Union

These symbols on the product's packaging or accompanying documents indicate that used electrical and electronic products and batteries should not be dis-posed together with household waste. For more information about collection and recycling of old products and batteries, please contact your dealer, point of sale or local municipality. In accordance with national legislation, penalties may be applicable for incorrect disposal of this waste.

Information for Disposal in Countries Outside the European Union

When discarding these items please contact your dealer or local authorities for further information regarding the correct method of disposal.

Delivered Parts, Connectors, and Dimensions

MOBOTIX Cloud Bridge – Scope of Delivery

Scope of Delivery MOBOTIX Cloud Bridge

Item	Count	Description
1.1	1	MOBOTIX CLOUD Bridge
1.2	1	Power cord
1.3	3	External power supply
1.4	1	Important Safety Instructions
1.5	1	MOBOTIX CLOUD Attach ID

MOBOTIX Cloud Bridge – Connectors (Front)

Mobotix Cloud Bridge Connectors (Rear)

MOBOTIX Cloud Bridge – Dimensions

Glossary

Important Terms

MOBOTIX Bridge — A cloud-managed, on-premise appliance that connects cameras to the cloud data center in the Mobotix Cloud VMS. It acts as a bridge between the Mobotix Cloud and the on-site cameras. The bridge buffers the video in case the internet connection goes down, and performs the encryption, data deduplication, bandwidth management, motion analysis, and compression of the video. Mobotix Bridges have a version for wireless cameras as well.

MOBOTIX Camera Tunnel — A secure (https / TLS) connection from the Mobotix Cloud VMS web browser GUI to the individual camera web GUI which allows remote camera configurations e.g. setting resolution, bit rate and on- camera analytics/AI configuration.

MOBOTIX Cloud — The server that Mobotix Bridges and CMVRs communicate with. The infrastructure has been specifically designed for video and is directly managed by Mobotix personnel to provide maximum security, performance, and availability.

MOBOTIX Cloud Managed Video Recorder (CMVR) — CMVRs have all the functions of the Mobotix Bridge and provide on-premise storage in addition to the cloud storage available from the Mobotix Cloud. CMVRs implement the Mobotix Cloud-Premises Flex Storage that allows the customer to select the amount of videos sent to the cloud and the amount stored on premises.

MOBOTIX Cloud-Premise Flex Storage — Storage plan that lets customers choose the percentage of video stored in the cloud and the percentage stored on premise. Video can be stored entirely on premise, entirely in the cloud, or any combination based on the available bandwidth, customer security requirements, the number of cameras, and the application. You can easily and dynamically adjust where videos are stored.

MOBOTIX Cloud VMS Analytics —Suite of analytics offered on the Mobotix Cloud VMS platform. These analytics include People Counting, Line Crossing, Intrusion Detection, Loitering, and Camera Tampering.

MOBOTIX Complete Privacy Encryption — Technology implemented in the Mobotix Cloud VMS and the Mobotix Video API Platform that encrypts and keeps video private and secure. Data is encrypted at rest and during transmission.

MOBOTIX First Responder Real-Time Video Access — Setting that allows Mobotix Cloud VMS administrators to designate first responders and determine the groups of cameras they can access during an emergency. Administrators can also specify personnel authorized to activate emergency video feed.

MOBOTIX Intelligent Bandwidth Management — Technology that adjusts video transmission and bandwidth dynamically, prioritizes transmissions, and verifies internet connection functional

MOBOTIX Video API Platform — Cloud service provided by Mobotix for recording, managing, and accessing video from cameras and video sources of all kinds. This service includes the Mobotix Bridge or an Mobotix CMVR, the VMS cloud recording system, redundancy, and the big data framework, analytics, and alerts. The entire platform is accessible via the API.

Key Images – Images extracted from the video recording based on the amount of motion and activity. Key images can improve navigation.

On-Premise – Either the hardware or the storage of video at the customer's location.

Power over Ethernet (PoE) – Camera is powered from the Ethernet port (in supported devices) through the Ethernet cable, and therefore does not need to be plugged into a dedicated power source.

PTZ –Pan-tilt-zoom (PTZ) cameras can be added to the Mobotix Cloud VMS; their pan, tilt, and zoom controls can be manipulated directly from the Live View.

Trusted Device – A mobile device or a browser on a computer associated with an Mobotix user that has previously been securely accessed using Two Factor Authentication.

Two Factor Authentication (2FA) – An extra layer of security that only allows access to an Mobotix Cloud Account and cameras from a trusted device.

Overview

The Mobotix Cloud Video Management System (VMS) is an AI-powered, cloud-based service that replaces traditional digital video recorders (DVRs) and network video recorders (NVRs). The system communicates with a secure, redundant cloud architecture that provides a web-browser-based interface and comprehensive mobile applications for both iOS and Android. The Mobotix VMS is an open platform that supports any camera and has a publicly available API that can be accessed through our Video API Platform.
The Mobotix Cloud VMS is used for traditional surveillance applications such as securing buildings, properties, apartment complexes, factories, critical infrastructure, police stations, retail stores, and restaurant chains. Using smart data captured by your VMS enables you to gain visibility across your business, react swiftly to opportunities, and improve overall processes and performance. Additionally, it is useful for business optimization. Video surveillance of employees can improve reliability, efficiency, and customer service.

Audience

This guide is intended for end users of the Mobotix Cloud VMS. If you are a Reseller looking for more information on Reseller-specific functionalities, contact your Mobotix AG representative. You can also find more information on the Product Features section of our website.

Editions

Mobotix Cloud VMS is available in the following editions:

- **Standard** – Designed for small businesses and franchisees with a limited number of sites and users. The Standard Edition is for businesses that value remote access to surveillance video and cloud storage at a reasonable cost.
- **Professional** – Designed for mid-sized (10–25 sites) and rapidly growing business operations. The Professional Edition includes features to better manage large quantities of sites, users, and cameras.
- **Enterprise** – Ideal for large, distributed, and multinational businesses. The Enterprise Edition supports an unlimited number of users and provides a sophisticated access management solution and advanced operational reporting to meet audit and regulatory requirements.

Note: If a feature covered in this user guide is limited to a certain edition, it is always mentioned in the content. **Tip**: Identify your current edition by clicking the drop-down arrow next to your username from anywhere in the VMS. For more information on editions and how to upgrade, please contact your Reseller.

System Requirements

As the Mobotix Cloud VMS is cloud-based, you only need a web browser and internet access. Mobotix Cloud VMS supports the latest versions of the following browsers:

- Chrome
- Safari
- Edge
- Firefox
- Opera

The Mobotix Cloud mobile app is available on both the Google Play Store (for Android) and App Store (for iOS).

Bandwidth Considerations

Important: The Mobotix Cloud VMS is a cloud-based solution designed specifically for customers with internet connectivity. Operating the Mobotix Cloud VMS requires an active internet connection.

In general, higher bandwidth improves system performance. Upload speed is the key element affecting bandwidth usage of The Mobotix Cloud VMS but download speed affects performance as well. For more information about bandwidth optimization, see the application notes section of our website.
If bandwidth is a problem, potential alternatives are lower-resolution cameras or cloud-managed video recorders (CMVR) with higher resolution.

VMS Overview

Basic operation of the Mobotix Cloud VMS is simple: Cameras communicate with a bridge or CMVR device on your local network. That device communicates through the internet connection with the cloud, where the video, settings, and other data are stored. You can access that information from anywhere with an internet connection, either through a web browser or our mobile app.
Digital and analog cameras communicate with an Mobotix Bridge or CMVR located at the customer site. This communication can occur either over the network digitally by Ethernet, wirelessly, or through an analog coaxial cable connection.
The Bridge or CMVR records the video and audio initially to the local storage on the device. This step is necessary for buffering the video and backing up the latest files in case the internet connection fails. There are a range of options for Bridges and CMVRs, that can be configured for customer needs, depending on the camera subscriptions and device types.
Once the data is recorded to local storage, the Bridge or CMVR processes the video and analyzes it for motion. If motion is detected, the video is tagged with object and motion information. Then the video is encrypted and transferred to the Mobotix Cloud for longer-term storage. When using a CMVR, video can also be stored locally as well as sent to the cloud. A CMVR provides complete flexibility for audio and video storage. Different retention periods can be set for on-premise (local) and cloud storage for each camera based on user needs. It is possible to transmit low-resolution video to the cloud and keep high-resolution video locally.
Access both the live and recorded video by connecting to the Mobotix Cloud VMS using a web browser or the mobile application. Modify all configurations and settings through this cloud connection. If a video has not been transmitted to the cloud, or a live video feed is requested, the Mobotix Cloud quickly requests the necessary data or feed from the bridge or CMVR. This is considered “on-demand” viewing. There are also a few other ways to view video streams. If the web browser determines that the bridge is located on the same LAN as the browser, video streams directly from the bridge. A monitor connected directly to the bridge can be used as a video display for live video stream.

Security

Security is crucial in a cloud-based environment. All data is encrypted from the moment it reaches the Bridge or CMVR and is only accessible through the Mobotix Cloud VMS. Stored Bridge and CMVR data is encrypted, so if a device is stolen, its data cannot be accessed. The Mobotix Bridges and CMVRs utilize outbound communication with the Mobotix Cloud. This means that the devices do not have any open ports, nor do they require any port forwarding on firewalls, making them inherently safer and more secure.
The Mobotix Cloud, although referred to as a single data center, is a series of data centers distributed throughout the world. These data centers communicate with each other and maintain connections to Mobotix Bridges and CMVRs. Data is protected through a redundant architecture where three copies of customer video are stored, making loss of any video highly unlikely.

AI Video Analytics

The VMS offers smart video analytics features to improve security and transform a video surveillance system into a tool for business optimization. Powerful artificial intelligence combined with cloud-based video retention automatically detect security risks and send alerts, freeing business owners and operators to focus on other aspects of their business.

License Plate Recognition (LPR)

Mobotix LPR is an AI-powered license plate recognition technology that works with any surveillance camera in all kinds of challenging conditions – increasing business security and efficiency while lowering costs. Mobotix LPR is an affordable, cloud-managed solution for accurate detection and recognition of license plates. Leveraging Mobotix's powerful artificial intelligence (AI), the system does not require on-site hardware or maintenance. Innovative new features and improvements are instantly delivered to customers via the cloud. Mobotix LPR turns an existing ONVIF security camera into a highly accurate license plate reader.

Hardware

Hardware for the Mobotix Cloud VMS consists of three main components: a Bridge or CMVR, a switch, and cameras. Choosing the correct hardware is very important for your VMS to perform optimally.

Bridges and CMVRs

Mobotix Bridges and CMVRs are critical components for Mobotix Cloud VMS operation. They connect the cameras (and other input devices) to the Mobotix Cloud. Without these devices, no data reaches the cloud, and no data or video can be seen by the user. This guide does not cover all functions performed by the bridges and CMVRs. It is important to understand that the Bridge or CMVR receives all video and audio from cameras. IP cameras are configured and controlled by the ONVIF camera protocol.

Bridge and CMVR Security and Maintenance

Bridges and CMVRs only communicate with the Mobotix Cloud; because of this, they only require outbound ports to be open in firewall configurations. This keeps the data on the Bridge or CMVR secure.
The Mobotix Bridges and CMVRs are remotely managed and maintained by Mobotix AG. You do not need to perform any software, firmware, or security updates. All maintenance occurs automatically by the Mobotix Cloud VMS. This creates a more secure and reliable environment.

Storage

On Bridges, storage is intended only as a buffer to store the video for a short time in case bandwidth is not immediately available to transmit it to the cloud. CMVRs are designed for longer-term on-premise storage, depending on the model; however, the videos stored on the CMVR are still managed, controlled, and viewed from the Mobotix Cloud VMS. Even if using a CMVR, to view video, the encrypted data is sent through the cloud to the Mobotix Cloud VMS, allowing the video to be seen anywhere with an internet connection. This provides a consistent user experience regardless of the hardware type, as long as minimum upload bandwidth is available.

Bridge and CMVR Failure

Bridges and CMVRs have similar components to servers and are therefore susceptible to hardware failures, such as problems with the power supply, hard disk, or general electronics. If the Bridge or CMVR fails, video recording will typically stop. With a Bridge, video that has not been transmitted to the Mobotix Cloud may be lost, and the Bridge will need to be replaced. A CMVR might need to be replaced, or it could be repaired (depending on its size). Replacing a Bridge or CMVR is quick and painless because the configuration is stored in the cloud. The Mobotix

Cloud VMS will push all the configuration for the Bridge or CMVR and cameras to the new device. The only work required is to physically replace the Bridge or CMVR. This is made possible by our Bridge Swap feature and Rapid Replacement. See the application notes section of the website for more information.

Note: Overloading a Bridge or CMVR or using a non-PoE switch when power is not directly available for the cameras can cause a system failure. Consult your Reseller to get the proper equipment for your needs and ensure the system is set up correctly.

Cameras

The Mobotix Cloud VMS supports thousands of camera models, not just those sold directly by Mobotix AG. The list of supported cameras is located on the MOBOTIX website in the Support section If you do not see a particular camera listed, please contact support to help with the device.

The Mobotix Cloud VMS uses the ONVIF standard to communicate with digital IP cameras. If a camera is not compatible, it may be able to be configured for temporary use until fully compliant. Contact your Reseller to configure the device for use with the system.

Other Cameras

The Mobotix Cloud VMS supports analog cameras and HD over coax with the use of an additional encoder. Mobotix offers native support for standard definition analog cameras via specific model units. These units come with an adapter to allow up to 16 analog cameras to be connected directly via coaxial cable.

The Mobotix Combo Bridges support both NTSC and PAL. Additionally, the combo bridges have been tested with over 1,000 different analog cameras with 100% success.

Wiring

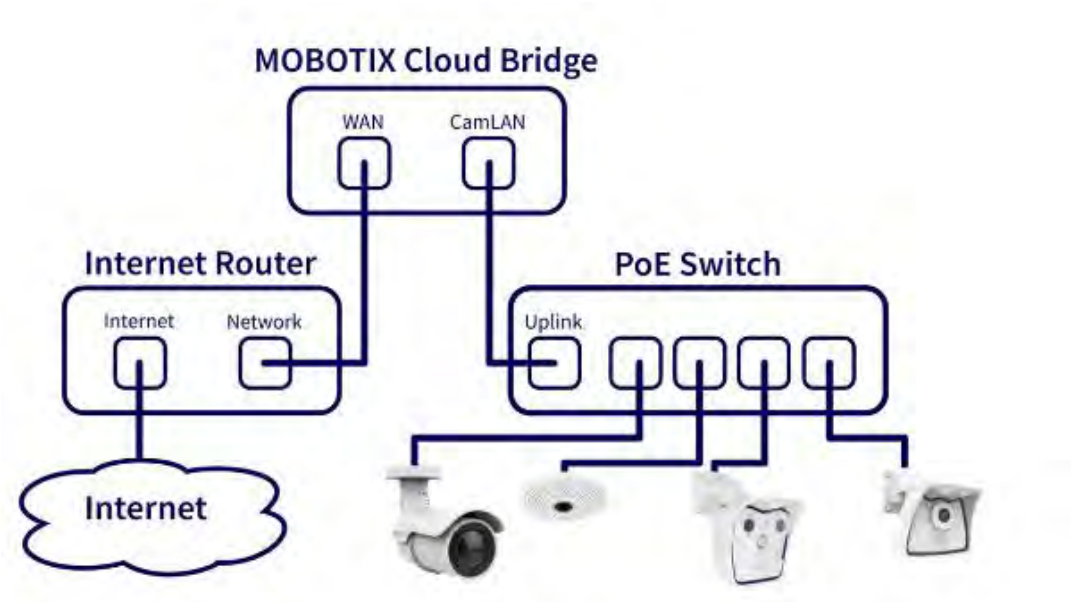


Figure: 1. Wiring Diagram for Mobotix Cloud VMS

For optimal security, it's important to wire your hardware correctly. The cameras should be connected to a switch, and then the switch should be connected to the CamLAN port of the Bridge or CMVR. If you connect the switch to the WAN port, the camera IP addresses can be broadcast to the entire network. Please follow the wiring diagram in Figure: 1. when installing hardware for the Mobotix Cloud VMS.

Note: For information about wiring more complex systems, including hub-and-spoke systems, see the application notes section of our website.

Getting Started

Once the hardware for the Mobotix Cloud VMS has been installed and your account has been set up, you'll receive an email asking you to set a password for your VMS account. Follow the instructions in the email to finish setting up your Mobotix account.
The activation email expires in 24hrs, so be sure to set up your password before then. If you do not activate in time contact your Reseller so they can send you a new link.

Logging In and Out

1. Go to the web-based user interface for the Mobotix Cloud VMS: https://c013.mobotixcloud.com/login.html
2. Enter your email address and password to log in to your account.

Note: If you do not know your login credentials, check your email account. When your account was created by Mobotix AG or a Reseller, you should have received an email with a link to set your password. If you did not receive this email, please contact your Reseller.

Resetting a Forgotten Password

If you have forgotten your password, you will need to reset it by taking the following steps:

1. Click the **Reset your Password** next to "Forgotten Password" on the login page.
2. Enter your email address in the corresponding field on the newly opened page.
3. Click Reset your password.
4. Check your email for a password reset email. If you have not received the email after a few minutes, check your Spam folder or email quarantine.
5. Click the Reset Password button in the email.
6. Enter a new password, confirm it, then click Change Password to complete the process.

Using the Dashboard

The Dashboard gives you an overview of the bridges and cameras in your VMS and their status. You can also track the health of your bridges, see cameras that are shared with you, and much more.

Important: To add a Bridge select the ••• icon on the Bridge/ Cameras header and select **Add Bridge** from the drop-down menu. To add cameras to an account, scroll to the bottom of the dashboard to the **Available Cameras** section.
Note: The Dashboard has several panels. You might not have access to all of them depending on your account, and they will not appear in your VMS. Contact your reseller for additional access options.

Summary

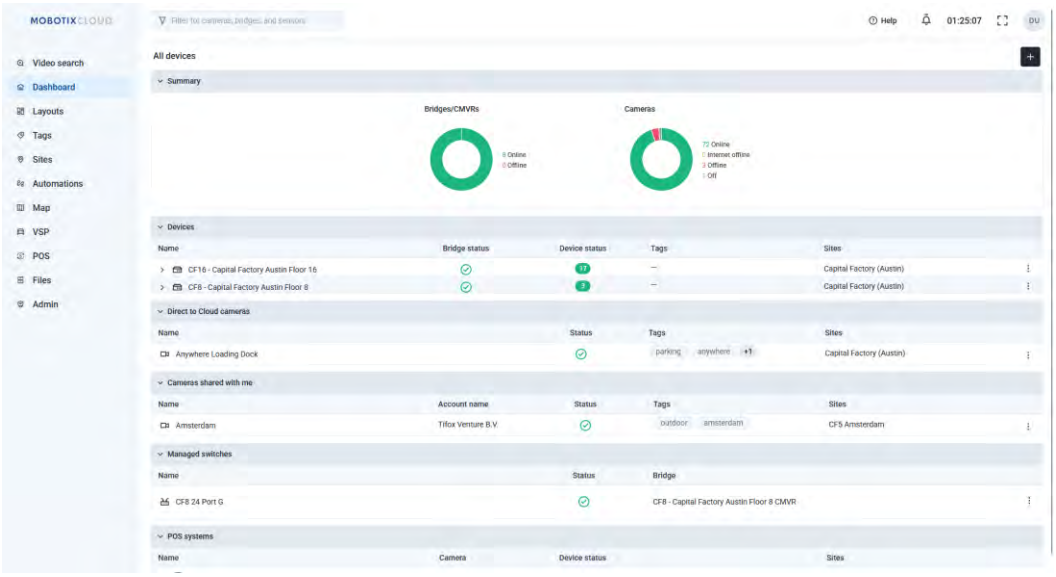


Figure: 2. Viewing the Dashboard Summary

The pie charts in the Dashboard Summary panel display the overall status of the devices in your VMS. There is a chart for Bridges/CMVRs, cameras, and shared cameras. Each chart shows the percentages of each status: **Devices Online**, **Devices Offline**, and **Internet Offline**. See Figure: 2. . Click the down arrow in the top-right corner to hide the charts.
The Dashboard consist of the following sections:

Devices

The devices section consists of all the connected devices to the cloud including bridges, Cameras connected via bridges, Sensors, Switches, etc.
It contains of Name, Bridge Status, Device Status, Tags, Sites for every Device connected to the Cloud.

You can add new Devices by clicking the plus icon + in the top right corner. You can see more about add devices in Camera Actions and Adding Bridges/CMVRs to the VMS sections.

Direct to Cloud Cameras

This section consists of list of All the cameras which are directly connected to the Cloud without using a bridge.

You can add Camera Direct to VMS by clicking on the plus icon + in the top right corner and then click on Add Camera Direct. See more about Adding Camera Direct to the VMS

Adding Bridges/CMVRs to the VMS

End users should not have to add bridges or CMVRs to a VMS account. This section is for Resellers or administrators Before adding bridges/CMVRs, complete the following steps:

- Install all necessary hardware and connect everything to your network.
- Set up your login information and grant access to other users.

Bridge/CMVR Actions

Attaching Bridges/CMVRs to the Account

Note: A bridge or CMVR must be attached to your Mobotix AG account before you can add cameras, record video, or perform any functions.
To attach a bridge or CMVR:

1. Select Dashboard from the left pane.
2. Click the plus icon + in the top-right corner of the Summary section. See Figure: 3.

Figure: 3. Attaching a Bridge

1. Enter the **AttachID** and name the bridge.

   Note: The **AttachID** is listed on an insert that arrived with the bridge. If you have a "+" model bridge, you can also find the **AttachID** using the LCD display.
   Tip: The **AttachID** can be typed with or without the dashes.
   Note: Naming the bridge is for your convenience. We recommend using a bridge name that refers to its site and follows a standard naming convention.

2. Click **Add Bridge** to complete the process.

Finding your AttachID

Your **AttachID** insert should be taped to the unit and have a QR code. If you cannot find your **AttachID** insert and are not using a "+" model bridge, contact support to recover the AttachID. Alternatively, attach a monitor and keyboard to your Bridge.

1. Plug in the monitor using the HDMI port. Refer to the bridge data sheet for more information.
2. Plug in a keyboard to the USB port.
3. Log in to the bridge.

Note: The login credentials are typically the username "admin", and the last 5 or 6 digits of the bridge's serial number as the password. Try the digits in reversed order if they do not work initially.
Result: After logging in, the AttachID is available on the bridge's user interface.

Configuring Bridge Settings

Once a bridge is attached to the VMS, you can configure its settings. Click the three-dot icon ⋮ next to the bridge's name and click on **Settings** on the Dashboard to open the Bridge Settings window. See Figure: 4.

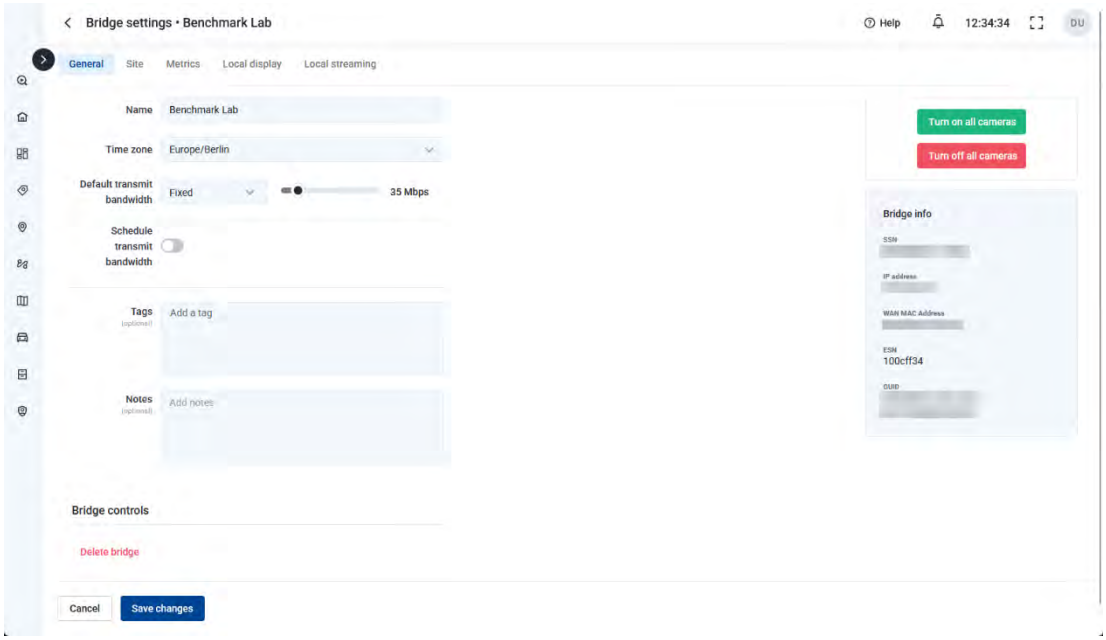


Figure: 4. Accessing Bridge Settings

You can adjust the settings as follows:
Bridge Name: Set the name for the bridge that is displayed in the dashboard.
Time Zone: Set this to the time zone where the bridge is located. Changing the time zone here will also change the time zone for cameras attached to this bridge.
Video Standard: Used for Analog inputs: NTSC or PAL.
Default Transmit Bandwidth: This is the rate that the bridge will transmit Full Video Recording (not preview) to the cloud. This is the Background Transmit mode found in Camera Settings on the Resolution tab under Full Video Recording. By default, the bridge will use up to 30% of the available throughput bandwidth measured to the cloud. It is important to set this to a value high enough to transmit all video prior to purging. We recommend all video to be transmitted (synchronized) to the cloud within two days. Check bridge metrics for a 7-day graph of bandwidth and disk space used and adjust as needed.
The drop-down menu for Default Transmit Bandwidth has four choices:

- **% of Available**: Set the percentage of available bandwidth to use as the transmit bandwidth.
- **Fixed**: Set a fixed rate for the transmit bandwidth in mbps (megabits per second). This is the rate that the bridge will transmit full video to the cloud.
- **Minimum bw Mode**: This mode overrides any preview transmit settings of cameras and puts the bridge into 'on demand' only mode. Bandwidth will only be used when a user views layouts, views historic video, or when an image is transmitted as a result of an alert.
- **Maximum bw Mode**: The bridge will use the maximum amount it possibly can to transmit video to the cloud. Use this option if the bridge is about to purge to allow it to catch up, or if you want to make sure that all video is synchronized daily. Monitor the bridge metrics to ensure all video is synchronized to the cloud.

Slider for % of available or fixed transmit rate - the slider can be adjusted by clicking on it and dragging left and right with the mouse. For more granular control, after clicking the left and right arrow keys on the keyboard can be used to make adjustments.

Scheduled Transmit Bandwidth: video can be transmitted to the cloud on a schedule to minimize bandwidth use during business hours. The schedule and transmission can be set. Outside of this schedule, the default transmit bandwidth setting will be used. For example, if the default transmit bandwidth is 2 mbps, the bridge will use up to 2 mbps of bandwidth except during a scheduled transmit time, if a schedule is set.
The Scheduled Transmit Bandwidth drop-down has four choices:

- **None**: Only the default transmit bandwidth is used.
- **Work Hours**: The work hours entered in Account Settings on the Days tab is used for the scheduled transmit.
- **Non-work Hours**: The opposite of the works hours set in Account Settings on the Days tab is used for the scheduled transmit.
- **Custom**: Custom hours are set using a slider. The time set on the left is the start time of the schedule. The time set on the right is the stop time of the schedule. Custom time is daily

Based on the default transmit settings, the slider for scheduled transmit rate will show fixed rate in mbps (megabits per second) or % of the available upload bandwidth. The choice on which to use for both sliders is made under default transmit settings. The scheduled transmit rate only appears if a schedule is selected.
Bridge Information: Displays the SSN, IP address, ESN, GUID, and other information about the bridge.
Delete Bridge: Press this to delete a bridge. You may delete a bridge only when no cameras are connected to it.
Turn off Cameras: Press this to turn off all cameras connected to the bridge. This does not turn off power, but turns off recording. No video is recorded when cameras are turned off.
Turn on Cameras: Press this to turn on all cameras that are off. This is not power. Cameras that are off do not record. This will turn cameras on and record video based on each camera's settings.

Bridge Settings: Site

Sites serve as a grouping method for your cameras and devices, allowing you quick-looks at cameras at that site, as well as dynamic filtering around site and viewing your cameras on the map.
The site (including address) is mandatory, and any cameras added to the bridge/CMVR will automatically inherit the bridge/CMVR site. The additional fields (coordinates, floor, notes) are optional, but can be useful in the map and dynamic filtering.
Use the selections in the **Bridge Settings > Site** window to add details about the bridge's site. See Figure: 5. .

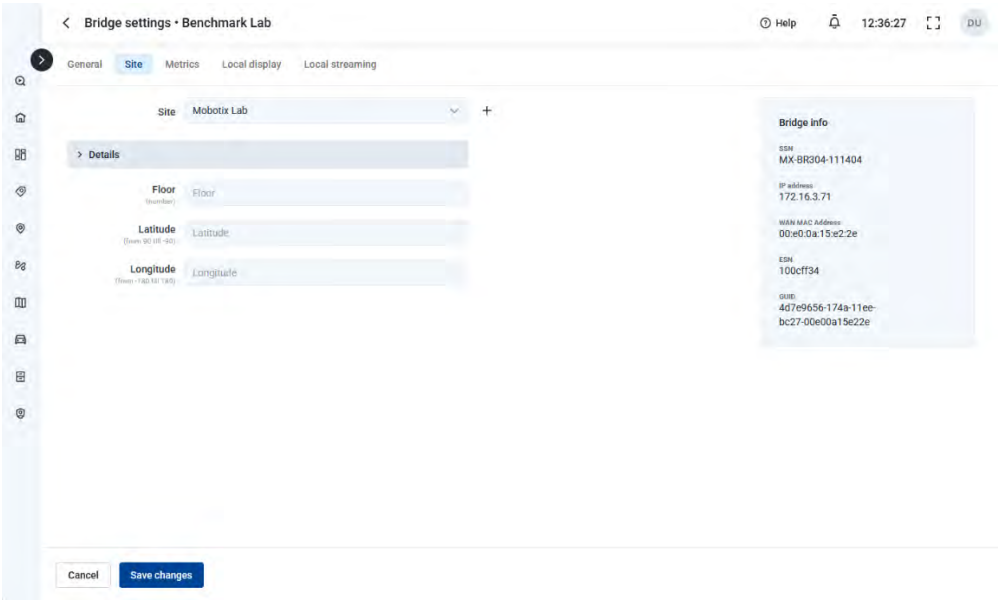


Figure: 5. Bridge Settings: Site

Site Name: Select a saved site to add this bridge/CMVR to that site. If this is the first device at a new site, click the yellow plus sign to create a new site.
Street Address: These fields will be automatically populated with the information saved to the site that was selected.
Site Type: You can choose to select one of the predefined site types from the list here. This will let you use the dynamic filter search box to show devices of only that type.
Latitude/Longitude: A way to precisely place your bridge on the map in the VMS. You can enter the coordinates to these fields to have your bridges/CMVRs displayed at their exact site in a building, or useful when the camera isn't located at a specific street address.
Floor: Enter the floor number for the camera to be able to use dynamic filtering to only show cameras on certain floors.
Notes: Enter any information you might find useful.

Bridge Settings: Metrics

Use the selections in the **Bridge Settings: Metrics** window to view bridge metrics. See Figure: 6. .

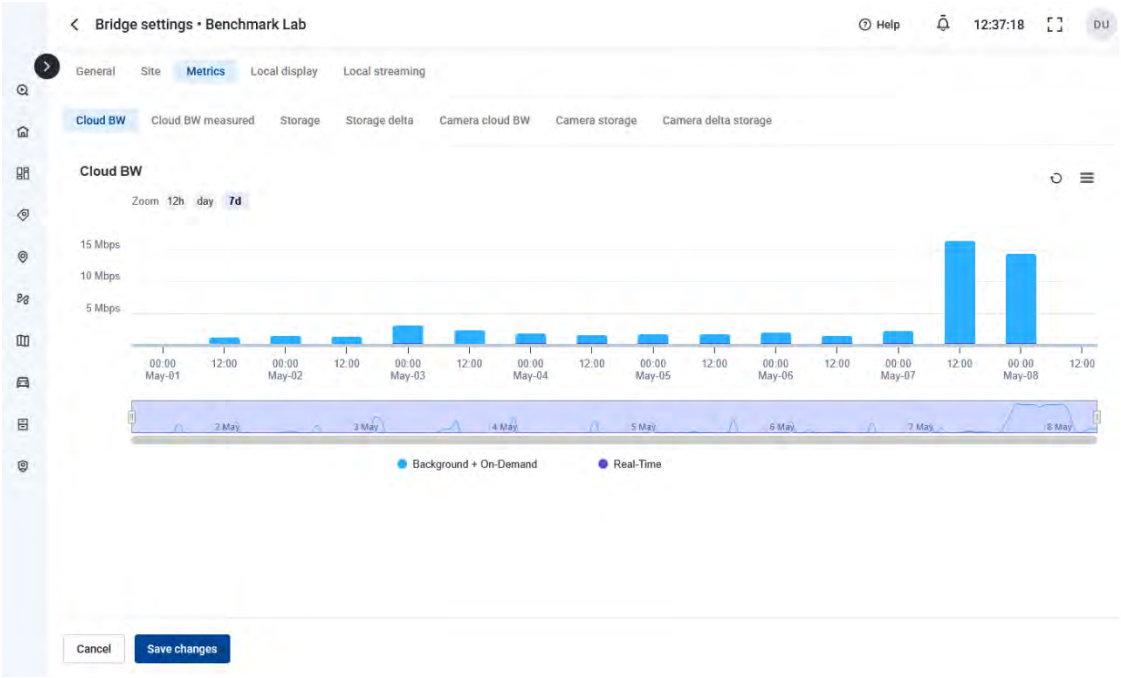


Figure: 6. Bridge Settings: Metrics

Cloud BW: The bandwidth used during live viewing and uploading video to the cloud.
Background + On-Demand: The synchronization of video to the cloud as well as the viewing of video that is not yet in the cloud. Real-Time is the preview video that is being transmitted directly to the cloud. Either can be viewed one at a time by clicking directly on the name.
Cloud BW Measured: The bandwidth as measured while sending data from the bridge to the cloud.
Note: This bandwidth might not match the results of a speed test.
Storage: The space Available and In Use, which is video temporarily buffered prior to synchronizing with the cloud. If video does not get transmitted to the cloud before the Available space is filled, then the oldest day's video will be purged to make room for current video.
Delta Storage: The difference between the video buffered locally and the space freed by synchronizing to the cloud or by purging. Positive represents In Use storage and negative represents successful synchronization to the cloud. Any video that is purged prior to the retention period will show negative in purple. Click on the arrow to the right of “Purge” to view a list of cameras that have purged. Each camera's data is displayed as a different shade of purple. Individual cameras may be enabled and disabled on the graph by clicking the camera name from the list. Press and hold “shift” while clicking on a single camera to view only that camera on the graph. When there are more than 18 cameras listed, the results are paginated. Click the up and down arrows at the bottom of the camera list to navigate the pages.
Cam Cloud BW: The amount of bandwidth used to live view and synchronize video from the bridge to the cloud per camera, displayed as separate colors. Each camera's data may be enabled and disabled on the graph by clicking the camera name from the list on the left. Press and hold “shift” while clicking on a single camera to view only that camera on the graph. When there are more than 18 cameras listed, the results are paginated. Click the up and down arrows at the bottom of the camera list to navigate the pages.
Cam Storage: The amount of video stored per camera locally displayed as separate colors. Each camera's data may be enabled and disabled on the graph by clicking the camera name from the list on the left. Press and hold “shift” while clicking on a single camera to view only that camera on the graph. When there are more than 18 cameras listed, the results are paginated. Click the up and down arrows at the bottom of the camera list to navigate the pages.
Delta Cam Storage: The amount of video stored locally and the space freed by synchronizing to the cloud. Each camera's data may be enabled and disabled on the graph by clicking the camera name from the list on the left. Press and hold “shift” while clicking on a single camera to view only that camera on the graph. When there are more than 18 cameras listed, the results are paginated. Click the up and down arrows at the bottom of the camera list to navigate the pages.

Local Display

Viewing of preview and live video using an external monitor and/or web browser may be enabled. At least one layout must be added for Local Display to work. By default, '(All Cameras)' will be used.
Go to **Bridge Settings > Local Display** to adjust the local display settings on the bridge. See Figure: 7. .

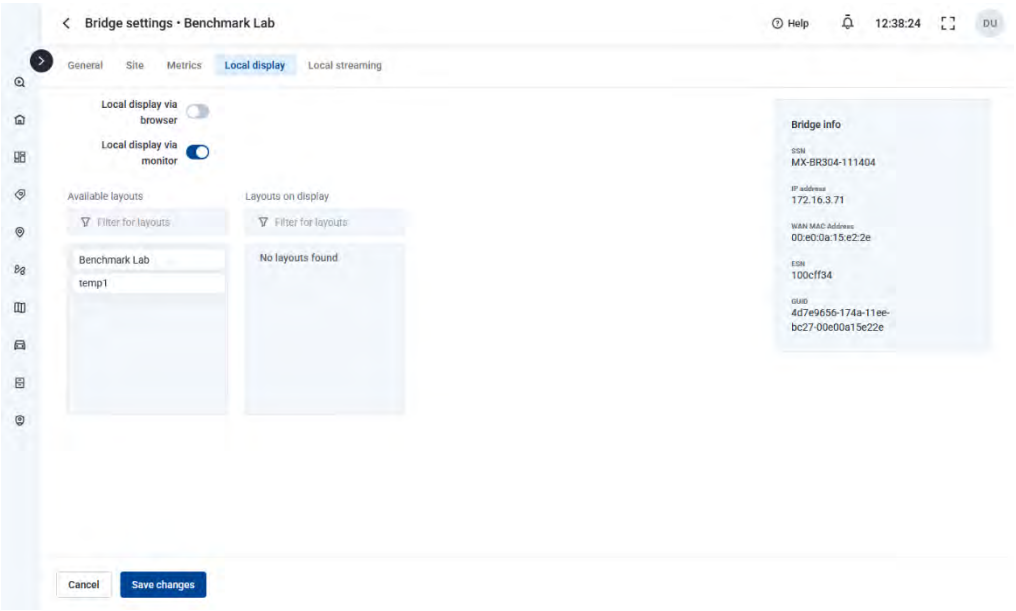


Figure: 7. Bridge Settings: Local Display

Local Display via Browser: Check this box to enable direct login to the bridge via web browser on LAN (Local Area Network). A valid username and password are required for Local Display via Browser.
Local Display via Monitor: Check this box to enable video output on the bridge's external video connector which depends on the bridge model. (HDMI/VGA/DVI/DDP). If the bridge has multiple output connectors, only one is active at a time. **Layouts Available**: Only layouts that contain cameras attached to this bridge can be used for local display. Select one or more layouts by clicking, then drag and drop to the right. Search may be used to narrow down the list. Layouts on the right will be available to view on the local display.
Add All >>: Adds all available layouts to the local display.
<< Remove All: Removes all layouts from the local display.
Cancel: Discards any changes and closes Bridge Settings.
Save Changes: Saves the changes and closes Bridge Settings.
Notes: Local Display keeps each layout's settings for **Show Camera Title Bars** just as they are shown in the Mobotix AG Cloud. If enabled, the name of the camera will be displayed in the black bar above each camera. The '(All Cameras)' layout does not include camera names.
Local Display Keys (via USB keyboard to bridge): The help file is available on the monitor by pressing 'h' using a keyboard.

- Start/Stop audio: S
- Enter full-screen: Space
- Exit full-screen: Space or Esc
- Hide highlight: Esc
- Next/previous layout: Pageup/PageDown
- Select camera: ← ↑ → ↓
- Exit to command: Q
- Help File: H

Local Streaming

Enable QL Stream (RTSP): Check this box to enable QL Stream (Real Time Streaming Protocol) from Bridge network connections. This setting allows for cameras on the bridge to be streamed in full resolution, and quality over the local network.

Important: This setting can only be enabled/disabled by an account with access to edit Bridge Settings. This feature cannot be set from a Reseller account.
Enable QL Stream Auth: Enable the checkbox which enables authentication to access the QL Stream when QL Stream is requested. With QL Stream Auth enabled, an additional Username and Password is needed to access the RTSP stream, or to use it in another application. If QL Stream Auth is disabled, the camera stream is available to anyone with access to the streaming URL to watch or use in another application.
Media Shortcut Enabled: Media Shortcut is powered by QL Stream and provides enhanced local viewing of video content when accessing the VMS from the same local network as the bridge. This provides access to video playback, full video live view, and layout preview video without requiring data transmission via the Cloud. This feature is accessible only from the local network to which the bridge or CMVR is connected via the WAN. Use of Media Shortcut allows for improved load times, increased viewing quality, and reduced latency.
Media Shortcut Override: The Media Shortcut Override is used when applying Media Shortcut across mapped virtual local area networks (VLANs). The Override's default is the detected network assigned by the network DHCP services.

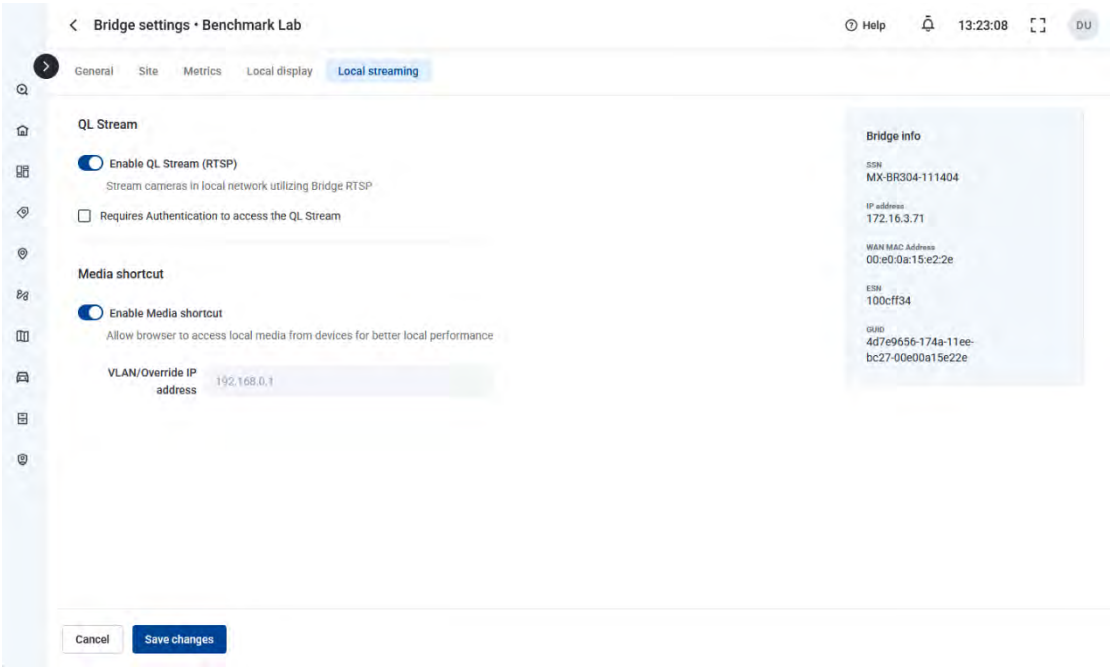


Figure: 8. Bridge Settings: Local Streaming.

Deleting Bridges

To delete a bridge from your VMS, click the Delete bridge button in the Bridge controls in General settings.
Important: This deletes all saved videos from the cameras attached to the bridge. To make sure that users do not delete bridges by accident, all cameras attached to a bridge must be deleted before a bridge can be deleted.

Camera Actions

Before adding cameras, complete the following steps:

- Install all necessary hardware and connect everything to your network.
- Set up your login information and grant access to other users.

For more information, see the Getting Started and Other Viewing Options.

Adding Cameras to the VMS

Once a bridge has been added to an account it will begin to scan the network for compatible cameras through both the WAN and CamLAN ports of the bridge. When cameras are found, they appear in the **Available Cameras** section.

Note: The process may take up to five minutes. If a camera still does not show in the VMS, or if it appears as “Unknown Camera,” reboot the camera.

Important: Mobotix AG recommends connecting cameras only to the CamLAN port. In more complex network environments, it may be necessary to have cameras on the WAN, but take into consideration that this can expose camera IP addresses.

Important: A camera will not show as available unless it is on the same IP scheme as the bridge. Additionally, it must have ONVIF configured, or the bridge will be unable to find the device.

Note: It is possible to add RTSP cameras to the VMS. See Adding RTSP Cameras to the VMS for instructions. To add an available camera:

1. Click the plus icon in the top right corner and click on Add Cameras.
2. Click on the plus icon to the right of the camera name. See Figure: 9. .

   Note: This will open a dialog box where you can adjust the camera’s initial settings. See Figure: 10.

Figure: 9. Adding a Camera to the VMS

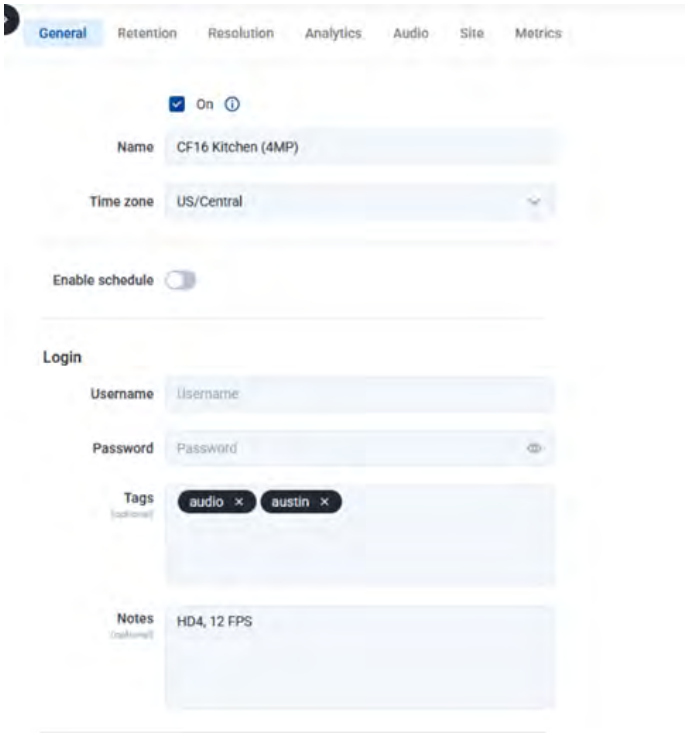


Figure: 10. Viewing Initial Camera Settings

3. Review the settings and make adjustments as necessary. The available initial camera settings are:

   - **Camera Name**: Assign a name to the camera. This name is shown in the Dashboard, Alerts, and Layout displays. Best practice is to use a naming convention descriptive enough to identify the camera and can be applied to cameras added to the VMS later.
   - **Cloud Retention**: Choose how long the camera's data will be stored in the cloud. This value affects billing.
   - **Scene**: Choose the scene of the camera. This is optional but can be used for dynamic filtering.
   - **Tags**: Select from previously used tags or create new ones for the camera. These tags are used to create groupings of cameras. Like Layouts, use tags to view preview feeds of all cameras with that tag.
   - **Username and Password**: Assign a username and password to access the camera. For most cameras this is the same username and password that access the web interface. For AXIS cameras this is the username and password for ONVIF access. These values are not always required, such as if the camera logs in by default. Analog cameras do not need the login fields. If the **Account → Camera Settings** login field was used, the information does not need to be duplicated here. This is typically used when there are a lot of cameras that share the same login credentials.

Note: There are certain password limitations. Most special characters can be used for camera passwords, but there are a few exceptions. You might need to update the camera's password if the Mobotix Cloud VMS cannot properly log in to the device. Password characters that cannot be used on the VMS are: &, “,<, @, and /.

If the connected cameras do not appear in the **Available Cameras** list after five minutes, try power cycling them. Some cameras only broadcast an ONVIF signal upon initial startup. Ensure that ONVIF is properly configured before attempting to attach them to the bridge.

Deleting Cameras

Click the three dot icon ⋮ next to the camera on the Dashboard and click on Settings. Then click on Delete Camera under Camera Controls to delete the camera from your VMS. You must confirm this action in the next prompt to permanently remove the camera from the VMS.
Important: All video is lost and cannot be retrieved after a camera is deleted. Save any video you want to keep before deleting a camera from the VMS.

Setting the Camera Web Password

It is strongly recommended that you change the default passwords on your cameras using their web interface. Most cameras use the same password for ONVIF and their web interface so you will need to update the ONVIF username and password in Camera Settings with the correct password when you change the web password.

Setting a Camera's Static IP Address

Before you begin: Make sure the IP addresses you use do not conflict with each other or any other devices on the network.

Note: You must set the static address for the camera using the camera's web interface. If using CamLAN, addresses 10.143.0.2–99 are available to use as static addresses. CamLAN begins serving DHCP addresses at 10.143.0.1.

Adding RTSP Cameras to the VMS

The Mobotix Cloud VMS can connect to almost any IP camera via ONVIF, but in certain cases, it is necessary to connect the camera using Real Time Streaming Protocol (RTSP). This can be either single or dual stream.

Note: The processing power required to connect single-stream RTSP streams is almost four times higher than ONVIF, because the Bridge/CMVR has to transcode the stream for high-resolution (H264) and preview (MJPEG) viewing.

Important: To add a camera through RTSP requires a static IP for the camera and the RTSP URLs from the manufacturer. Although the RTSP protocol is standardized, the actual URLs for each device vary. Most brands include this information with the camera's documentation; however the installer may need to contact the manufacturer.

To add an RTSP camera to the Mobotix Cloud VMS:

1. Log in to the VMS as an administrator.
2. Under the Admin section, go to **Admin** -> **Account Settings**. Navigate to the camera settings tab. Enable the toggle for RTPS Cameras. See Figure: 11. .

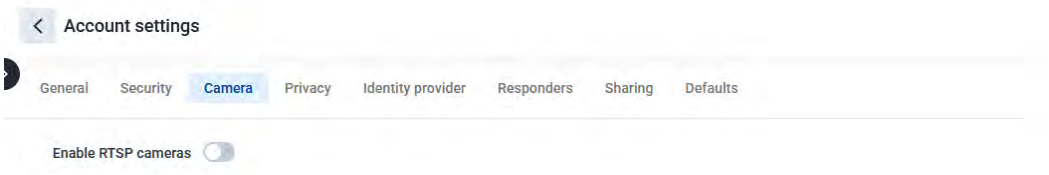


Figure: 11. Locating Account Settings

3. Click the plus button + to the right of the screen on the **Dashboard** and click on Add Camera button. See Figure: 12. .

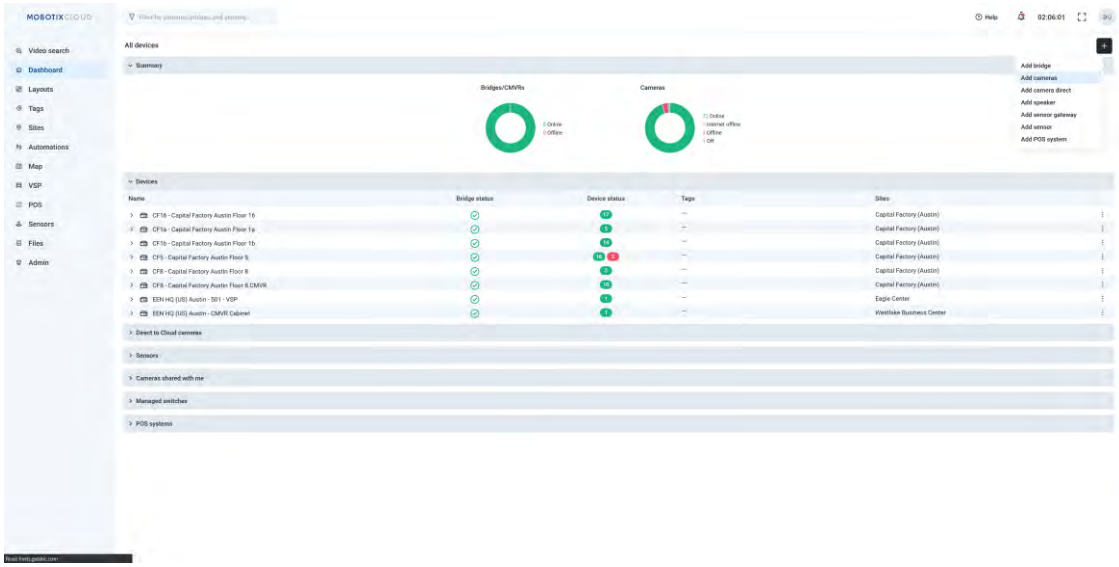


Figure: 12. Available RTSP Cameras

4. Click the ⋮ in the upper right corner of the **Add Cameras** pane. Then click on **Add RTSP Camera** button. It opens the configuration box to setup RTPS camera. See Figure: 13. .

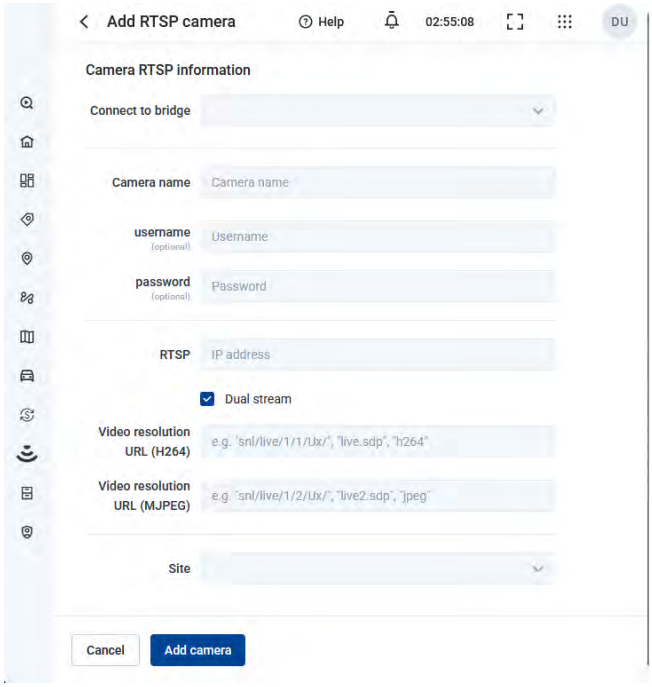


Figure: 13. Adding an RTSP Camera

5. Under **Login**, enter the user name and password of the RTSP camera.
6. Enter the IP address and the RTSP URL of the camera. Check the **Dual Stream** box if the camera is dual stream. For single-stream cameras, leave the box unchecked.

   Important: One single-stream RTSP camera uses the same amount of Bridge resources as four dual-stream cameras. Be sure that the Bridge is not overloaded.
7. Click Add Camera.
8. Confirm that the RTSP camera appears in the VMS.

   Note: It can take up to an hour for a single-stream RTSP camera to appear in the VMS.
9. If the RTSP camera does not appear in the VMS after several minutes, you can try restarting the Bridge manually via the **On/Off** button or remotely by doing the following:

a) On the Dashboard, click the icon ⋮ next to the Bridge name to open the Bridge settings. See Figure: 14. .

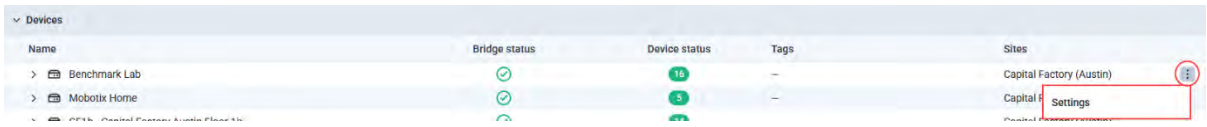


Figure: 14. Opening the Bridge Settings

b) The Bridge Settings dialog box opens. Click the “r” key on the keyboard to access the Restart button on the Bridge. See Figure: 15. .

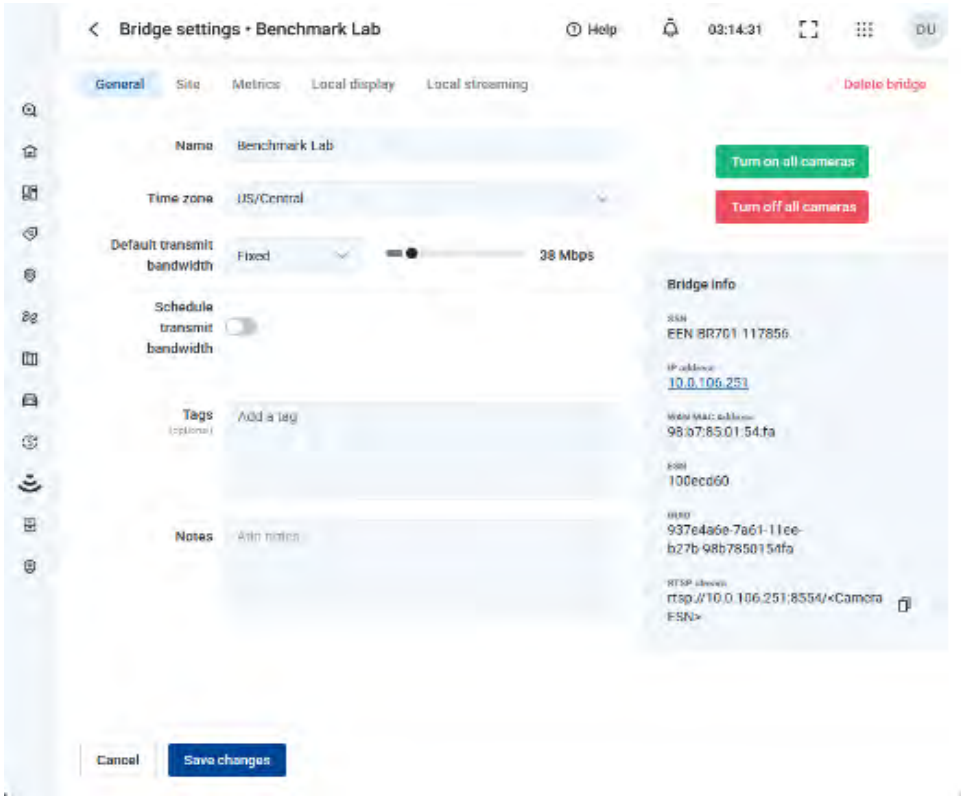


Figure: 15. Accessing the Restart Button in Bridge Settings

c) Click **Restart** to restart the Bridge

Note: Contact your reseller or see
Getting Help to contact support for more information.

Camera Direct Actions

Adding Camera Direct to the VMS

With the Mobotix VMS Camera Direct, you can easily integrate your cameras with the Mobotix Cloud VMS without the need for a Bridge or CMVR. Connect your camera to the internet and add it to the Mobotix Cloud VMS using its MAC address. Once added, your cameras are immediately ready for viewing within the Cloud VMS.

Prerequisites

In order to set up your Mobotix Camera Direct, you need the following:

- An Mobotix Cloud VMS account.
- A camera model that is supported by Camera Direct.

  Note: Make sure the camera is using factory default settings and running the latest firmware for its model.
- The MAC address of the Camera Direct camera.

Procedure

Before you begin: Be sure the camera is powered on and is connected to the internet.

1. Go to the Mobotix Cloud VMS and log in with your credentials.
2. Go to the **Dashboard**.
3. Click the plus icon + and choose **Add Camera Direct** from the drop-down menu.
4. In the **Add Camera Direct** dialog, name the camera and enter its MAC address. See Figure: 16. .

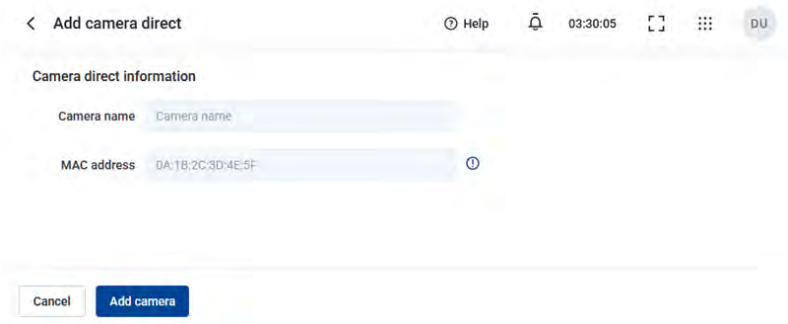


Figure: 16. Adding Camera Direct

5. Click **Add Camera** to save your settings.

Result: The Camera Direct Camera is added to your Mobotix Cloud VMS account.

Note: The camera is initially listed as offline on the dashboard, but after a maximum of two minutes a green check mark appears, indicating its online status as seen in Figure: 17. .

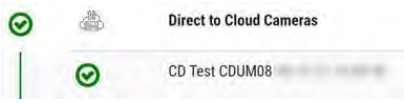


Figure: 17. Verifying Camera Direct Installation

Adding Camera Direct to Cloud using the Mobotix Cloud Application

Before you begin, make sure the camera is powered on and connected to the internet.
To connect a Camera Direct camera, do the following.

1. Open the Mobotix Cloud Mobile Application and log in with your credentials.
2. Go to More > Dashboard.
3. Click the **+** icon and choose **Add Direct to Cloud** from the drop-down list. See Figure: 18. .

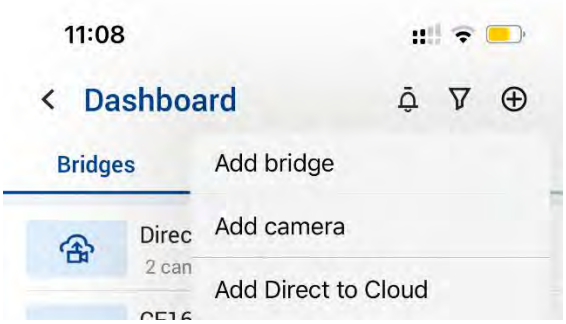


Figure: 18. Adding Camera Direct to Cloud using the Mobotix Cloud Application

4. In the Add Direct to Cloud dialog box, name the camera and enter its MAC address. See Figure: 19. .

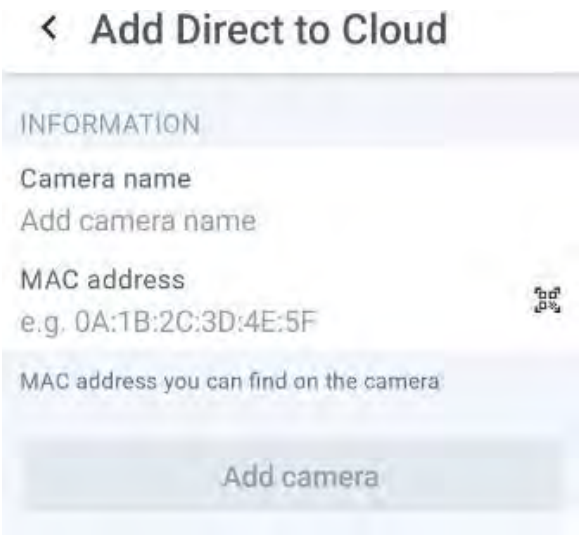


Figure: 19. Entering the Camera Name and MAC Address

5. The camera is now added to the VMS. You can view live and recorded videos.

Deleting Camera Direct cameras

See Deleting Cameras.

My Profile and Account Settings

Use the information in this section to set up your profile and account settings.

Initial View

When you first log into the VMS, the Layouts window opens. If your reseller has configured a Layout, you will see the cameras on that layout. If not, the window shows All Cameras available on your VMS subscription. See Figure: 20. .

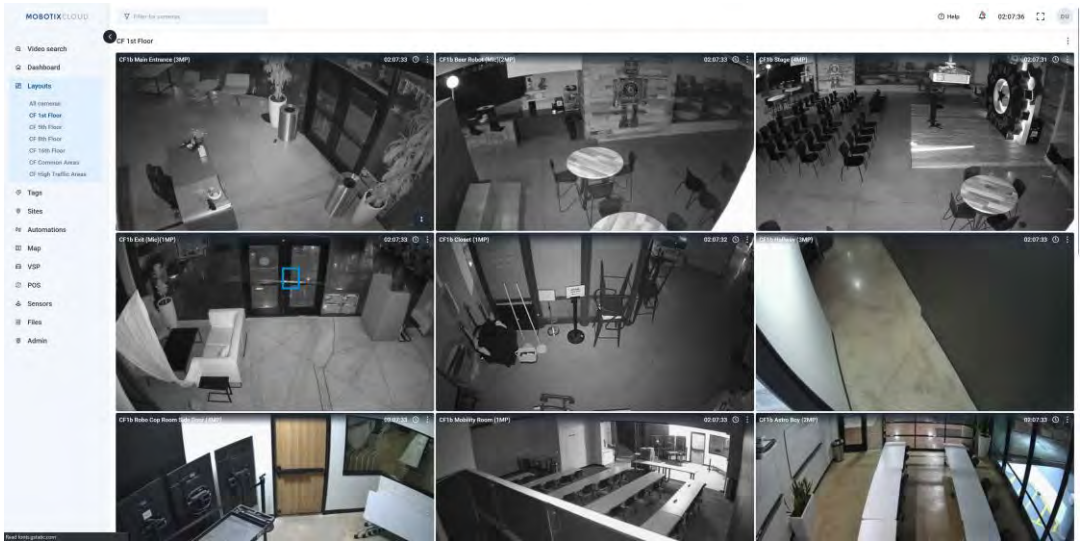


Figure: 20. Initial View (All Cameras)

- Click on this icon if you want to see a full screen view of the interface.
- 01:42:07 You can see the current time.
- Help Click on this button if you need help in configuration.
- Here you can find all the notifications.

My Profile

To access **My Profile**, click on your name on the left side menu and click **My Profile** from the drop-down menu on the top right-hand side of the window. See Figure: 21. .

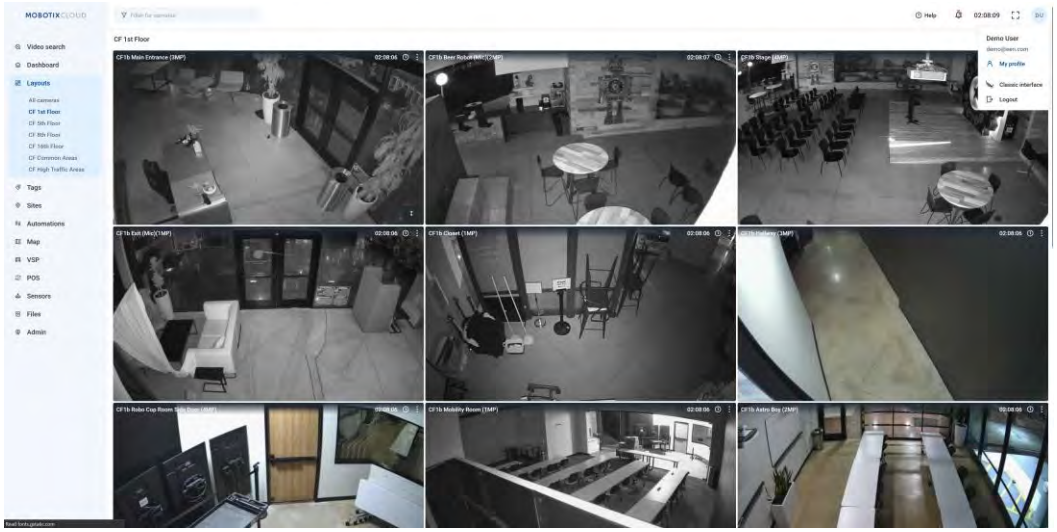


Figure: 21. My Profile

General

The **My Profile: General** menu contains the following options:

- **First name**: your first name.
- **Last name**: your last name
- **Login (Email)**: your email address. Changing this address will send an email to the new address with a Security Code that must be verified. Once verified, this will be the new email used to login to your account.
- **Alternate Email**: A different email address other than the Login can be used in order to receive email alerts. If an email address is entered, all alert emails will be sent this address and not to the Login address. This alternate email is not used to login.
- **Support Pin**: Provide this number to an Mobotix AG Support representative to authenticate your access to the account as an authorized user when requesting remote support. The support pin is automatically generated per user, but it can be changed to any 6-digit number
- **Language**: choose the language for your account.

See Figure: 22. for an example of a **My Profile: General** page.

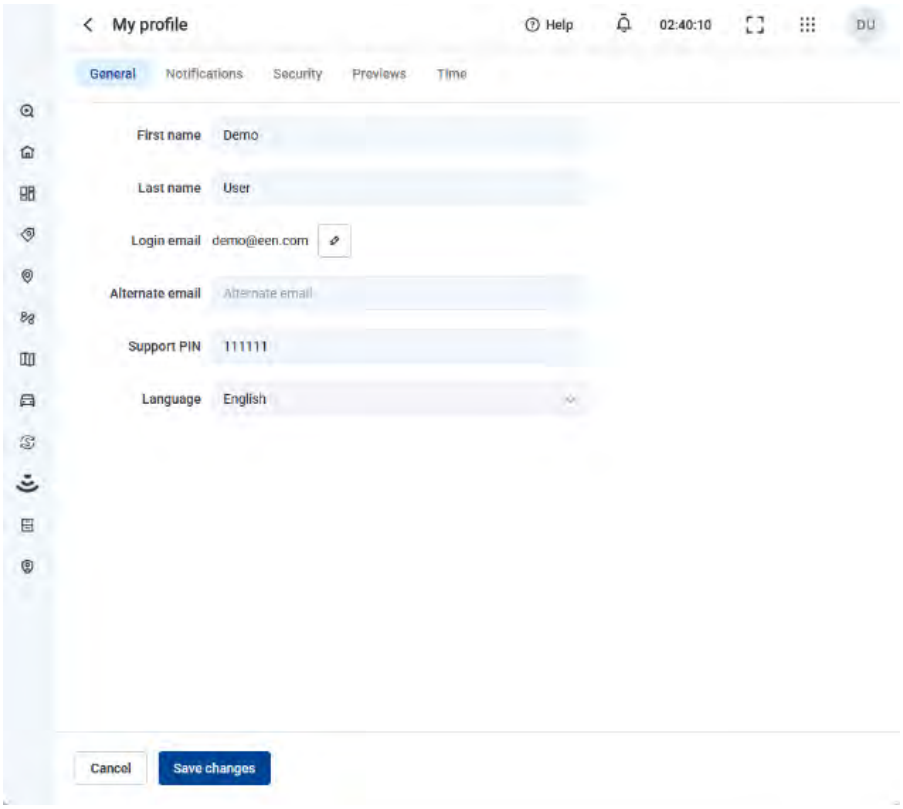


Figure: 22. My Profile: General

Notifications

The **My Profile: Notifications** menu contains the following options:

- **Email Notifications**: Notifications are sent via email.
- **Push Notifications**: Notifications are sent to a mobile phone that is using the Mobotix AG Viewer application. Note: notifications are not sent via SMS.

See Figure: 23. for an example of a **My Profile: Notifications** page.

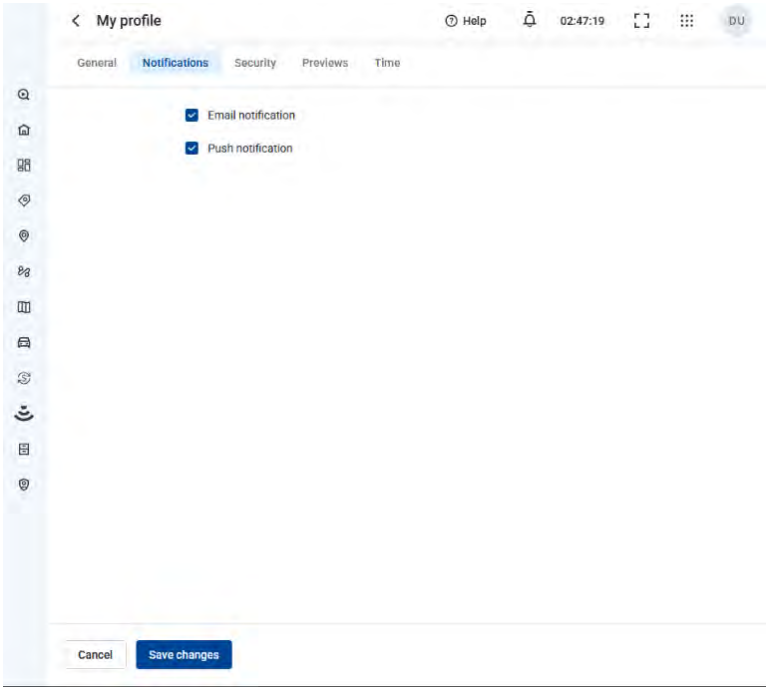


Figure: 23. My Profile: Notifications

Security

The **My Profile: Security** menu contains the following options:

- **Reset Password**: Reset your password by entering the previously known password and the new password.
- **Two-factor authentication:** After enabling this, any changes to your profile will require two-factor authorization. We highly recommend the use of this.
- **Secondary SMS verification**: A phone number may be entered that can be used for two factor authentication. Adding or changing this number will send a Security Code via SMS that must be verified. Once verified, this will be the SMS number for your account.

See Figure: 24. for an example of a **My Profile: Security** page.

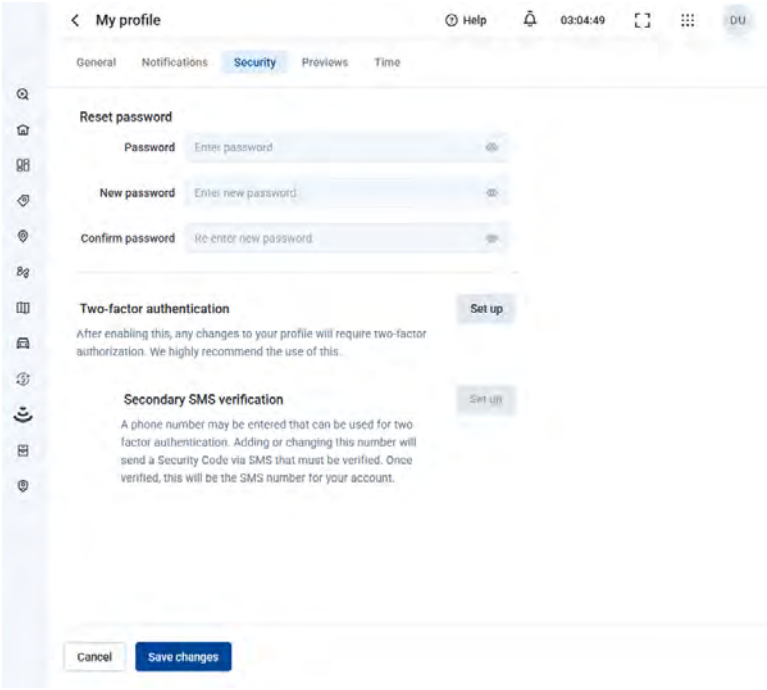


Figure: 24. My Profile: Security.

Previews

Preview videos are shown in Layouts and when clicking the green check mark on the Dashboard. The following options affect how the preview videos are displayed, and what can be overlaid on them within the VMS.
The **My Profile: Previews** menu contains the following options:

- **Show Motion Boxes**: Check this box to have a light-blue motion box around the detected motion in the preview video. The motion boxes indicate changing pixels, but do not represent object sizes.

  Note: This option is not recommended for low bandwidth environments.
- **Show Analytics**: Check this box to show analytic counts overlaid on the preview video.

See Figure: 25. for an example of a **My Profile: Previews** page.

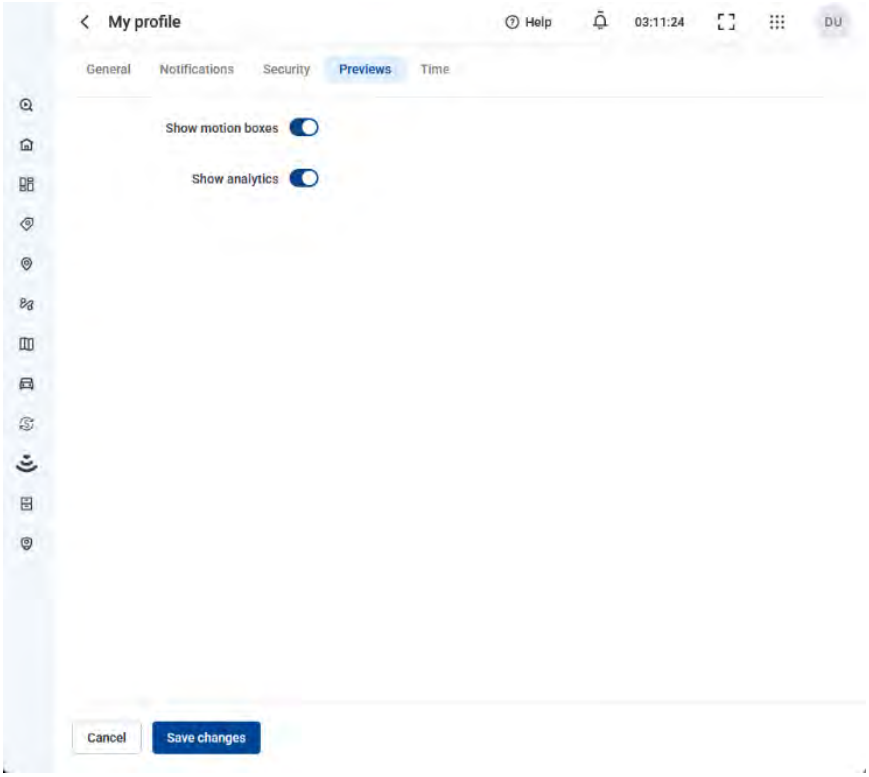


Figure: 25. My Profile: Previews

Time

The **My Profile: Time** menu contains the following options:

- **Time Zone**: Select your Time Zone.
- **24 Hour Clock**: Select between 12- and 24-hour mode for the display of time.
- **Millisecond Display**: Select to display milliseconds in preview video.

See Figure: 26. for an example of a **My Profile: Time** page.

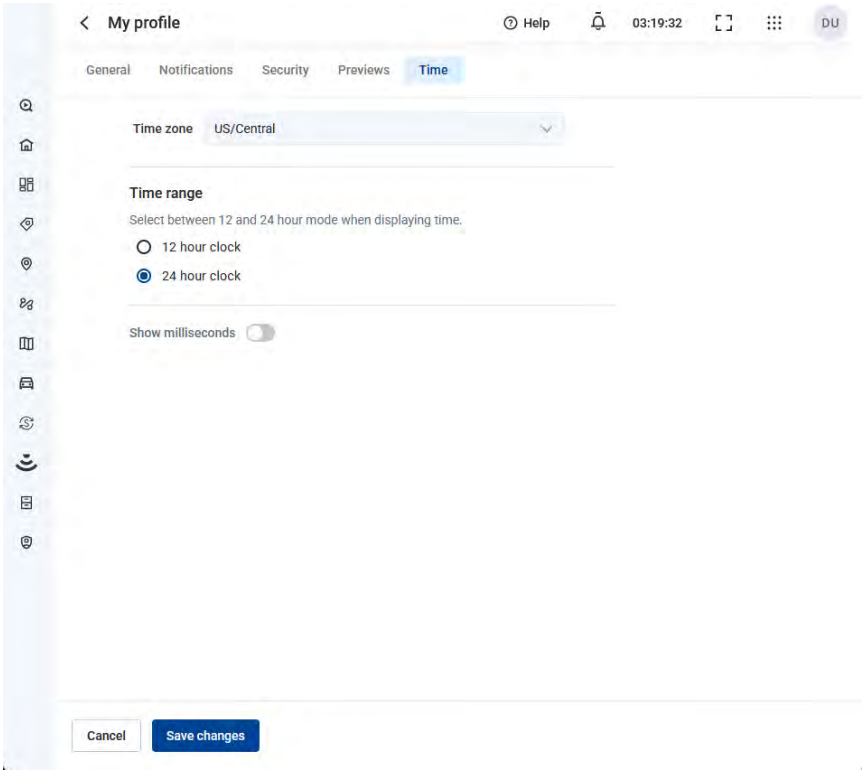


Figure: 26. My Profile: Time

Account Settings

This section contains information for changing the various account settings on your VMS.
To access Account Settings, click on **Admin** on the left side menu and click **Account Settings**.
See Figure: 27. .

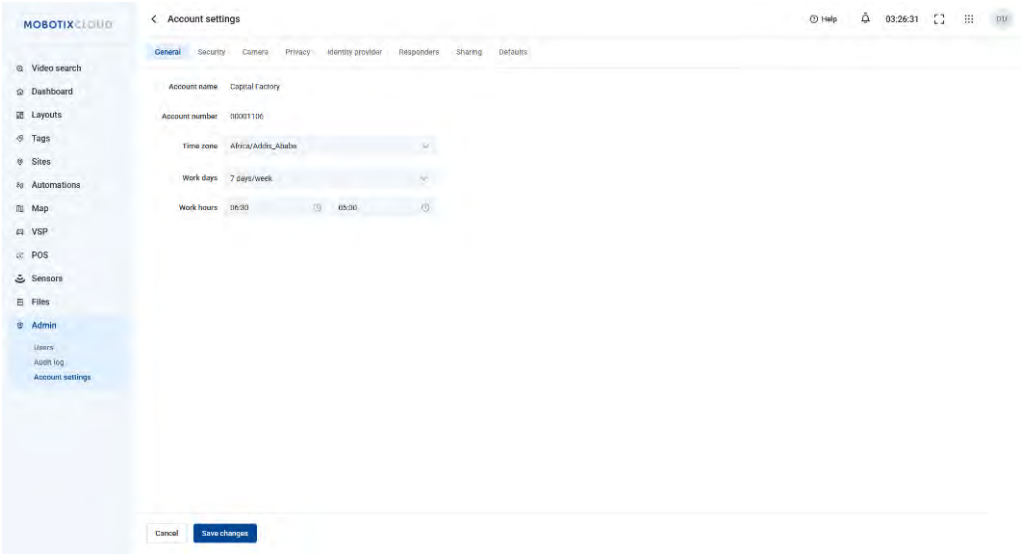


Figure: 27. Account Settings

General

The **Account Settings: General** menu contains the following options:

- **Account Name**: Displays the VMS account name. This field is not editable.
- **Account Number**: Displays the VMS account number. This field is not editable.
- **Time Zone**: Set this to the time zone where the account is located.
- **Work Days**: Select which days of the week to be included as work days.
- **Work Hours**: Select the time period which will be your working hours.

See Figure: 28. for an example of the **Account Settings: General** page.

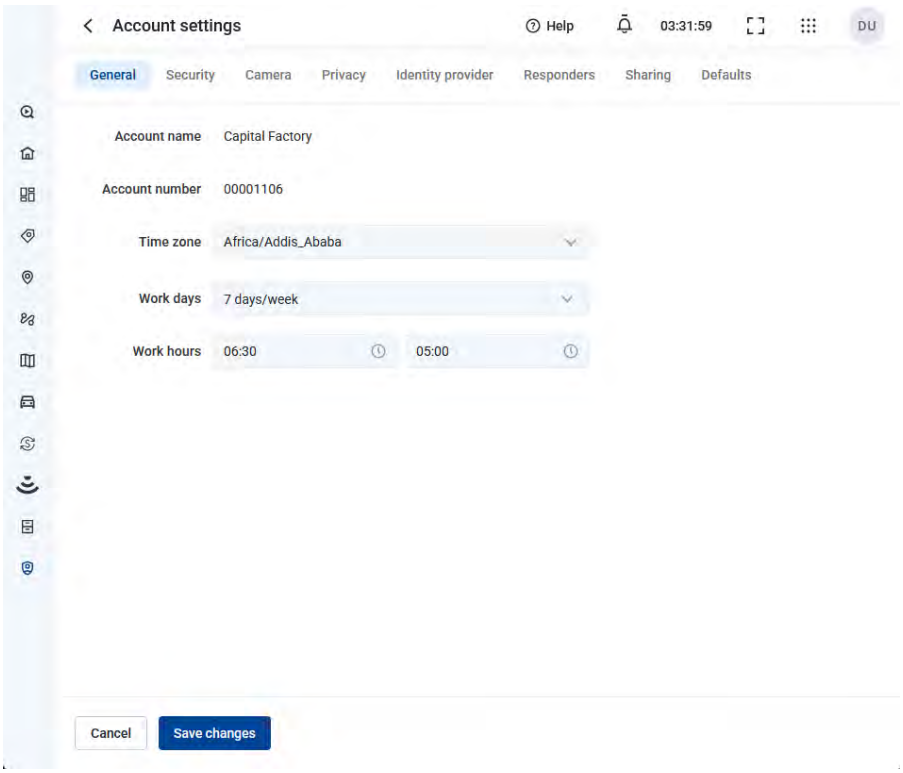


Figure: 28. Account Settings: General

Security

The **Account Settings: Security** window contains the following options:

- **Web Timeout**: The time after user is automatically logged out.
- **Inactive Session Timeout**: The period of inactivity after users will be automatically logged out.
- **Note**: Mouse clicks and keyboard presses count as activity.
- **Max Login Attempts**: Maximum number of consecutive failed login attempts within a 24-hour period that a user is allowed before being forced to do a password reset.
- **Two Factor Authentication**: If enabled, sets all users on the account to Two Factor Authentication. Two factor authentication uses email and/or SMS messages with a mobile phone. For more information, see Setting up Two-Factor Authentication (2FA).
- **Password Minimum Length:** At password reset, the user will be required to create a password with the minimum length of the set value. The minimum length allowed in the VMS is 10 characters
- **Password Maximum Length:** At password reset, the user will be required to create a password with the maximum length of the set value. The maximum length allowed in the VMS is 64 characters
- **Numeric character required:** At password reset, the user will be required to create a password with at least one numeric character if this box is checked.
- **Special character required:** At password reset, the user will be required to create a password with at least one special character if this box is checked.
- **Username cannot be part of the password:** At password reset, the user will be required to create a password that does not contain a username of the given user if this box is checked

- **Password Expiration:** The user will be required to create a new password in the given number of days.
- **Password Reuse Restriction:**
  - Number of days: At password reset, the user will be required to create a password that was not previously used for the selected number of days.
  - Number of previous passwords: At password reset, the user will be required to create a password that was not previously used for the selected number of previous passwords of the given user.

See Figure: 29. for an example of the **Account Settings: Security** page.

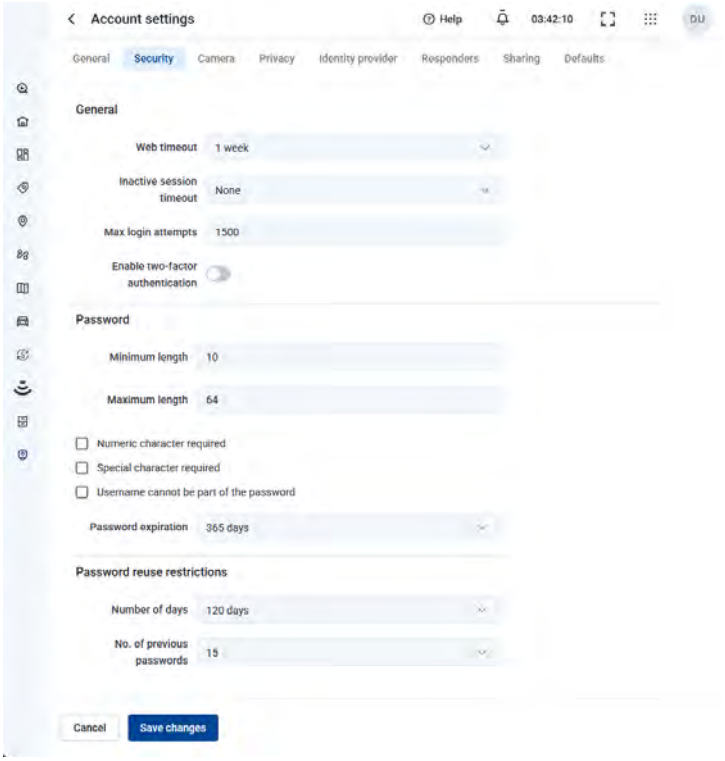


Figure: 29. Account Settings: Security

Camera

The **Account** Settings**: Camera** window contains the following options.

- **Enable RTSP Cameras**: Check this box to enable cameras that do not support the ONVIF protocol to appear as cameras you can add on the Dashboard. You can add them to the system if you know the 2 RTSP resource URLs. You can add RTSP cameras two ways. You can specify an IP address or click the indicator on the Dashboard. Both methods of adding an RTSP camera are enabled by this check box. You must manually configure the cameras to output the proper RTSP streams using the camera's web interface.
- **Standard Camera Logins**: Properly configured cameras will have usernames and passwords so that individuals on the local network cannot access them. Each camera in your system may have a different username or password or you may use the same username and password on all the cameras. If you have the same username and password on all your cameras, you can enter it here. This way you will not have to enter it for each camera.

See Figure: 30. for an example of the **Account Settings: Camera** window.

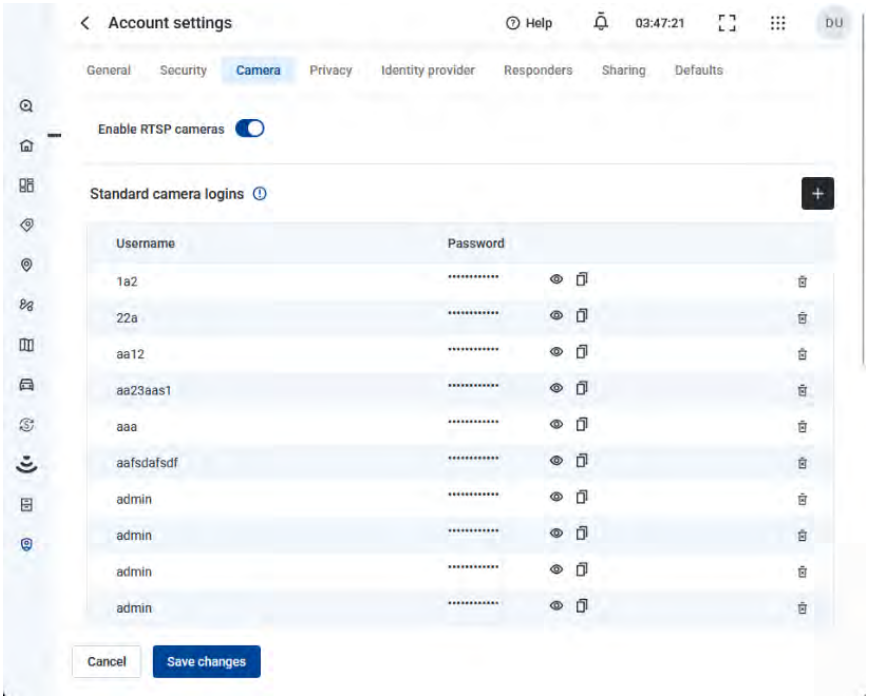


Figure: 30. Account Settings: Camera

Privacy

The **Account Settings: Privacy** window contains the following options:

- **Video Privacy**: when you check this box, your dealer or installer will be unable to see any video. **Note**: Enabling video privacy can interfere with the ability to troubleshoot or service your cameras.

See Figure: 31. for an example of the **Account Settings: Privacy** page.

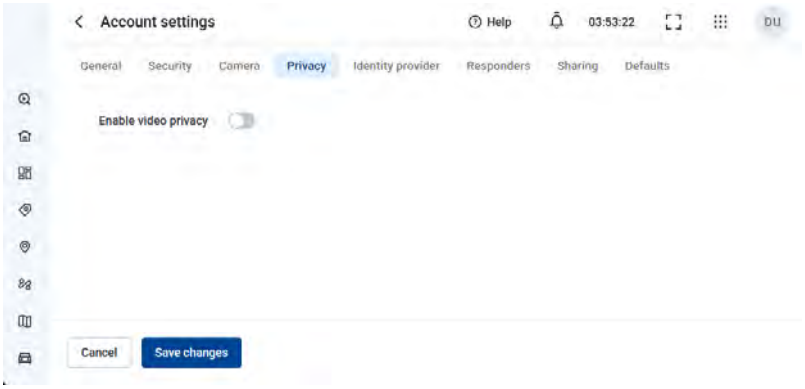


Figure: 31. Account Settings: Privacy

Identity Provider

Identity Provider Integration via Single Sign-on (SSO)
Use the choices in this section to select and configure the Identity Provider (IDP) you want to enable.
The **Account Settings: Identity Provider** contains the following options:

- **None**: Select if you do not want to configure SSO. This is the default selection.
- **Microsoft**: Select this option if you want to configure Microsoft authentication.
- **Okta**: Select this option if you want to configure Okta authentication.
- **Google**: Select this option if you want to configure Microsoft authentication.
- **Custom SSO**: Select this option if you want to configure Custom IDP authentication

See Figure: 32. for an example of the **Account Settings: Identity Provider** page

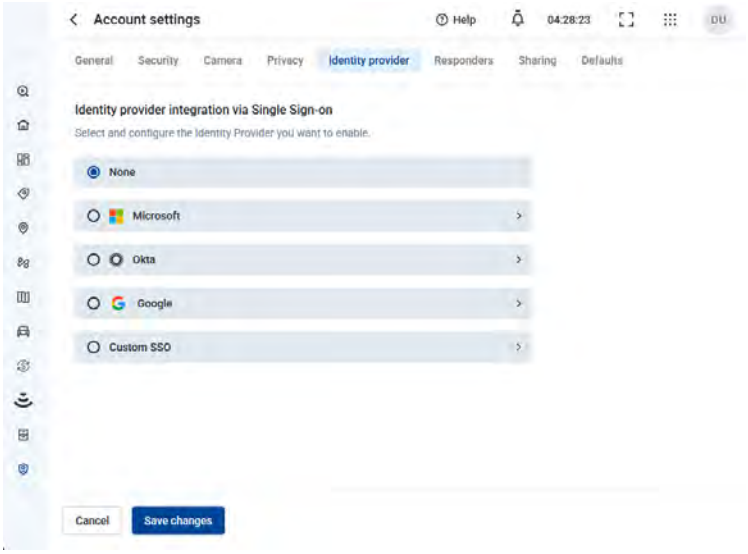


Figure: 32. Account Settings: Identity Provider.

Responders

The **Account Settings: Responders** window contains the following options:

- **Manage Cameras** - Select cameras to share with responders
- **Add Responder** - Select the plus icon in the right corner to add responders. Add their email address, first name (optional), last name, (optional), and organization (optional).
- **Edit Responder** - Select the three dots icon next to a responder in the First Responders List to edit their information. Edit their email address, first name (optional), last name, (optional), and organization (optional).
- **Delete Responder** - Select the three dots icon next to a responder in the First Responders List and choose Delete Responder to remove a responder from the list.

The **Responders** setting is used to designate **First Responders** who can receive immediate, real-time access to a list of designated **Responder Cameras** when an authorized user activates the First Responder Access feature. After a First Responder is set up and active, it is possible to **Activate Responder Share** when a user is signed into the account. This can be found under the username in the top right corner of the web interface. Click on your username to see **Activate Responder Share** below **My Profile** and just above *Log Out*. Once activated, a notification will be sent, and First Responder camera video is shared instantly. When First Responder is activated, the selection under the username changes to **Deactivate Responder Share** which stop sharing video with First Responders if selected.
See Figure: 33. for an example of the **Account Settings: Responders** page.

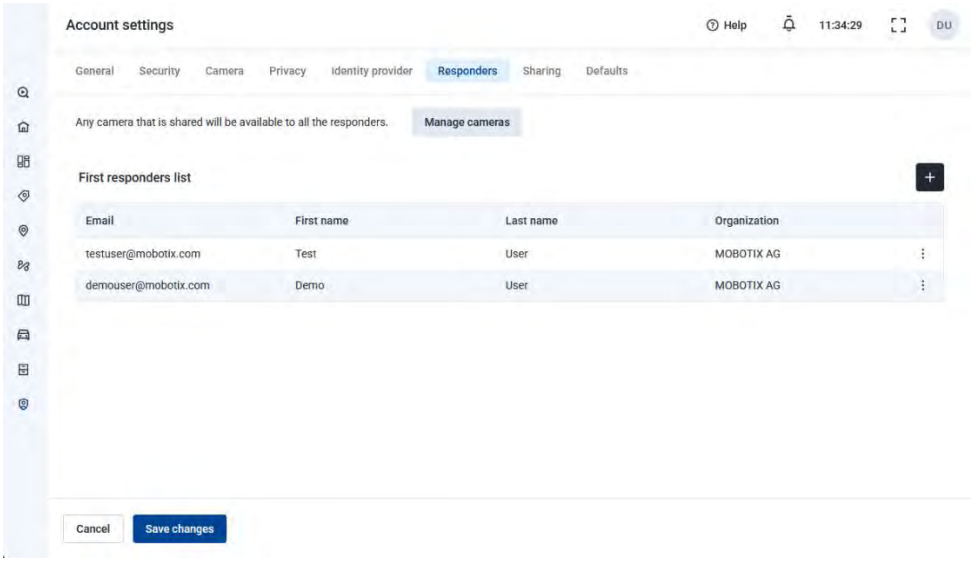


Figure: 33. Account Settings: Responders

Sharing

Click on + icon to add cameras for sharing between different accounts.
The **Account Settings: Sharing** window contains the following options:

- **Available Cameras**: Displays the available cameras on the VMS. Select from the Available Cameras and drag them to the Cameras to Share list. A scroll bar is available to find specific cameras quickly.
- **Cameras to Share**: Displays cameras that are available when Sharing is active.
- **Add All**: Adds all available cameras to the Cameras to Share list, or if using search, the visible cameras.
- **Remove All**: Removes all cameras from the Cameras to Share list or if using search, the visible cameras.
- **Permissions**: Allows selecting among Edit Motion/Analytics, PTZ Live, Edit PTZ Stations, and 2-Way Audio permissions for the Cameras to Share.
- **Edit Motion/Analytics**: Grants permission to edit motion settings including adding and deleting Regions of Interest and also grants permission to edit existing analytics.

  Note: Adding or deleting analytics is not allowed.
- **PTZ Live**: Grants permission to control a PTZ camera in live view and to recall PTZ Stations.
- **Edit PTZ Stations**: Grants permission to control a PTZ camera and to edit PTZ Stations.
- **2-Way Audio**: Grants permission to activate the 2-Way Audio functionality on supported devices. This allows the user to broadcast their voice over a speaker associated with a camera, using the microphone in their device.
- **Share Email Addresses**: Allows entering an email address for a user on the shared cameras account.
- **Shared Cameras**: Displays the list of shared cameras.
- **Account**: Displays the email and account names that share the cameras.
- **Cameras**: Displays the list of cameras that have been shared with the given account.

Note: Cameras can be shared between different accounts through email addresses. When sharing to a user that already has an Mobotix AG VMS account, the camera is shared into the account and not just to the single user. If sharing to a user without an account, an account will automatically be created for the user and the cameras shared to the new account. The cameras will appear in the dashboard as Cameras Shared with Me. Cameras can be shared with multiple accounts via email addresses.

- Shared cameras allow live viewing, historic viewing and downloading of video.
- **Permissions**: Contains the list of permissions shared for the selected cameras and the selected account.
- **Actions**: Click the ⋮ icon to either Edit Cameras or Delete the Share.

Note: It is not possible to share a camera with a reseller user.

See Figure: 34. for an example of a **Account Settings: Sharing** page.

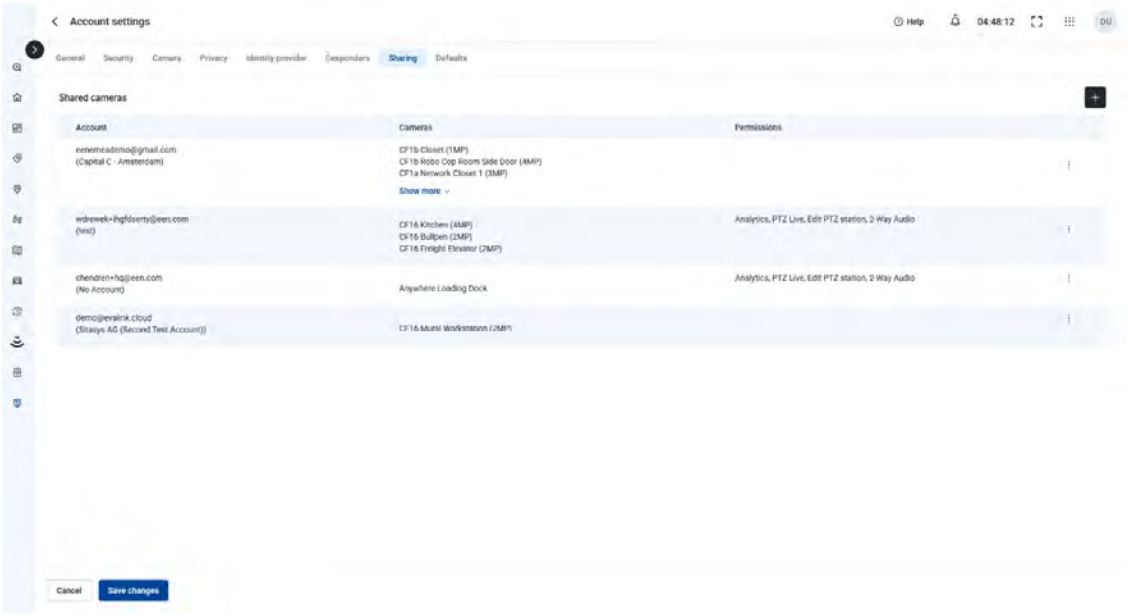


Figure: 34. Account Settings: Sharing

Defaults

The **Account Settings: Defaults** window contains the following options:
Camera Defaults: Use the selections in this section to set the camera defaults.

- **Cloud Retention**: Set the default Cloud Retention for cameras on the VMS. The options are 1, 2, 5, 7, 12, 28, 30, 31, 60, 90, 180, 365, 730, 1095, and 1825 days.
- **On Premise Retention**: Use the slider to set the default range for On Premise Retention. Choices are between 0 and 365 days.
- **Default Preview Resolution**: Set the Default Preview Resolution. Choices are Std or Clf.
- **Default Full Video Resolution**: Set the Default Full Video Resolution. The choices are Std, High, 1080P, 3MP, 4MP, 5MP, and 10MP.

User Defaults: Use the selections in this section to set the camera defaults.

- **Enable Roles for Users:** Check this box to enable roles for users by default.

See Figure: 35. for an example of the **Account Settings: Default** page.

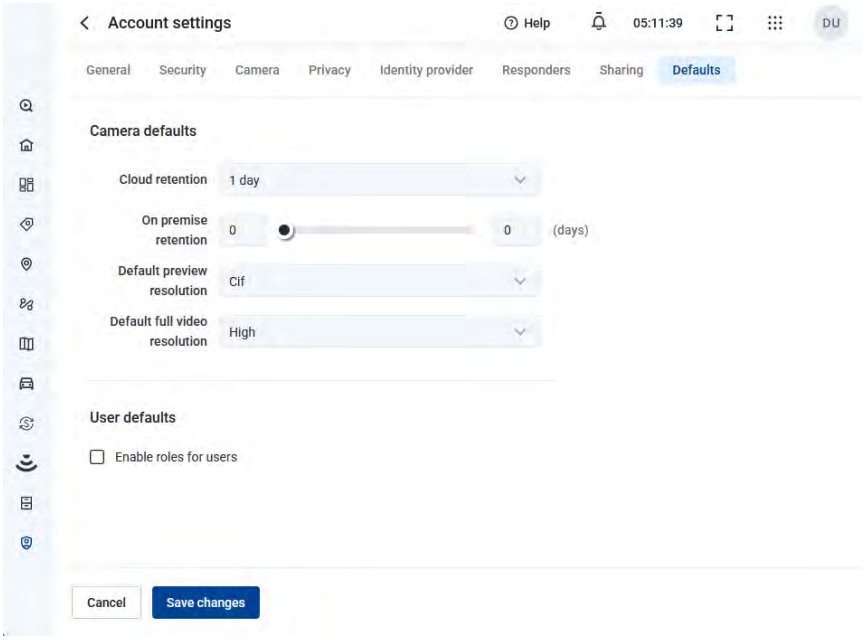


Figure: 35. Account Settings: Defaults

Setting up Two-Factor Authentication (2FA)

Two-factor Authentication must be initially enabled by your Reseller. If you want to utilize this extra layer of security for your VMS, please contact your Reseller to set it up. After your Reseller has enabled 2FA, you will have the following options:

1. Enable 2FA for yourself (each user in your VMS will also have this option).
2. As an admin, enable 2FA for all users.

Enabling Two-Factor Authentication for a Single User

1. Click your profile name and select **My Profile**. Then navigate to **Security** section and click on the **Set Up** button. See Figure: 36.

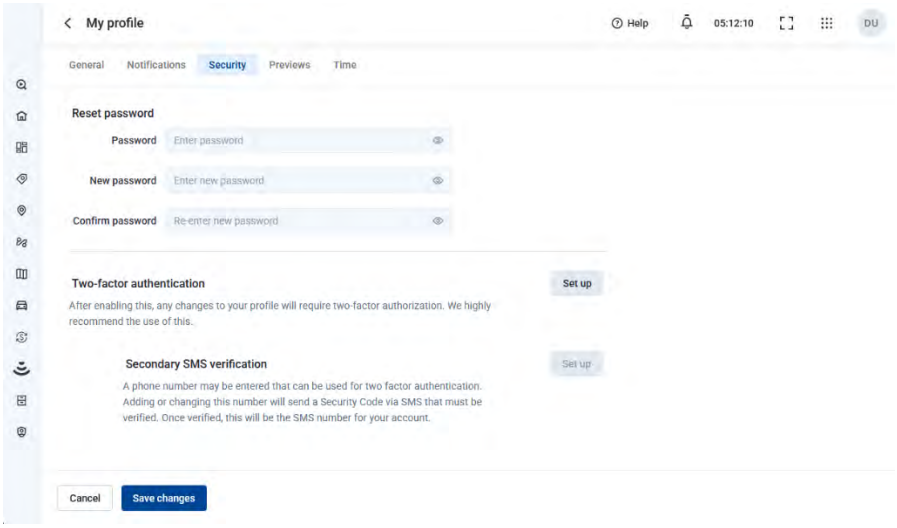


Figure: 36. Two-Factor Authentication: My Profile

2. Enter the password. See Figure: 37. .

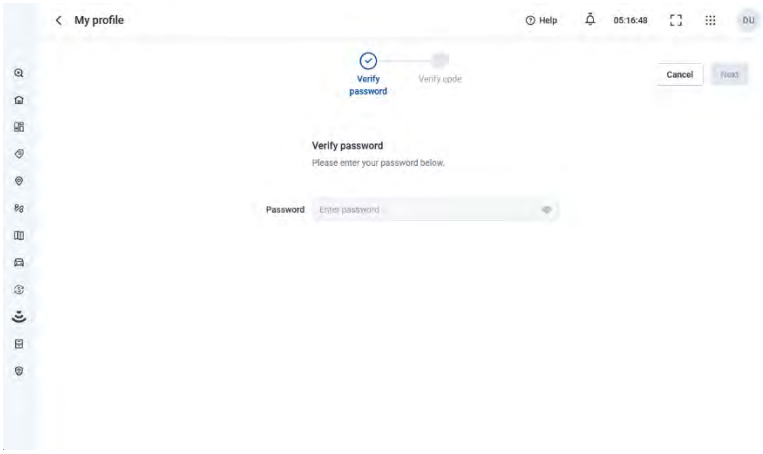


Figure: 37. Enable 2FA for Yourself

3. Enter your security code when prompted, then click the button to **Send Security Code**.

   Note: A code will be sent to your email address.

4. Enter the security code in the field shown and click **Verify Code**. See Figure: 38. .

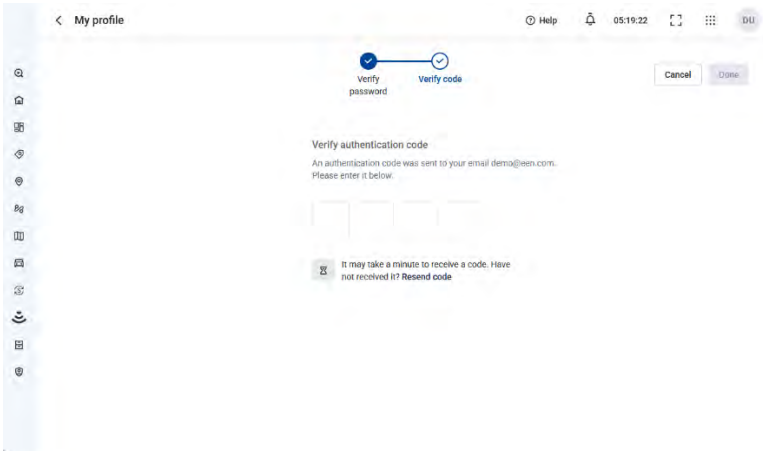


Figure: 38. 2FA Security Code

Result: Two-Factor Authentication is now enabled for your account. You will need to enter a security code sent to your email address whenever you log in to the Mobotix Cloud VMS

Enabling Two-Factor Authentication for All Users

To enable two-factor authentication (2FA) for all users, do the following:
Note: This option is only available for admin users.

1. Click your Admin in the left navigation bar and select **Account Settings**. See Figure: 39. .

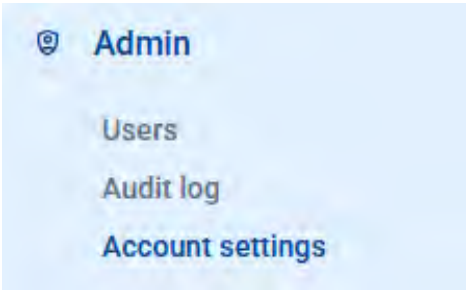


Figure: 39. Two-Factor Authentication Account Settings

2. Click the **Security** tab, toggle the **Enable Two Factor Authentication for All Users** button, then click **Save Changes**. See Figure: 40. .

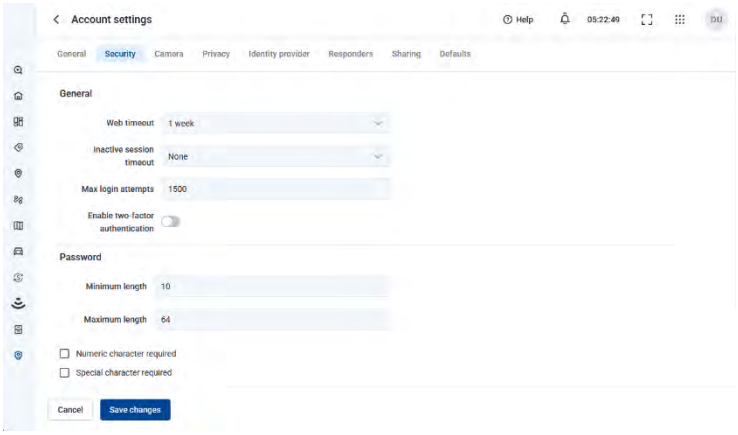


Figure: 40. Enable 2FA for All Users

Results: The next time your users log in, they will be prompted to send a security code to their email address for two- factor authentication. See Figure: 41. .

Figure: 41. Two-Factor Authentication Login Verification

Verifying using SMS (Text)

After two-factor authentication has been set up, you can add a phone as a trusted device to verify your login by SMS (text).

1. Click your profile name and select My Profile.
2. Now enter your phone number (with country code) in the appropriate field as shown in Figure: 41. .

Note: After you click Save Changes you will be prompted to enter your password and will receive a text message with a security code.

1. Enter the security code and click **Verify Code.**

Result: The next time you log in from a new device, you can choose to verify through SMS.

Camera Settings

Configuring Cameras

You can configure common settings across all added cameras. Such settings include retention, resolution, bandwidth, bit rate, motion settings and alerts. Specific options will change based on the camera.

General

- **Turn On Camera** - If the box is checked the camera records during the specified hours. If the box is not checked the camera recording remains off all the time (nothing is recorded, however the actual power state of the camera is not affected by this setting).

  Note: Turning the camera off does not change billing. You will still pay for the camera as long as it is connected to your account.

- **Name -** Assign a name to the camera. This name is shown in the Dashboard, Alerts, and Layout displays. It is recommended to use a naming convention that is descriptive enough to identify the camera and can be applied to all future cameras added to the VMS.
- **Enable Schedule** - When this setting is on, you are able to set the camera mode and working schedule for each camera.
- **Camera Mode** - Choose **Turn On** to turn the camera on at a set time. Choose **Turn Off** to turn the camera off at a set time.
- **Schedule** - Choose whether you want the camera turned on or off as set in the previous field during **Working Hours**, or **Custom Hours** This setting dictates the times that the camera is on (if Turn On Camera is selected). Choose Working Hours for the camera to only operate during the work hours specified in Account Settings. Likewise, Non-Work Hours keeps the camera off during the specified working hours and on outside of them. Alternatively, set specific days and times by choosing Custom Hours and using the fields to set on and off times.
- **Time Zone -** Set this to the time zone where the camera is located.
- **Login -** The username and password used to access the camera. For most cameras this is the same Username/Password as used to access the web interface. For AXIS cameras this is the username and password for ONVIF access. These values aren't always required. For instance:
  - If the login is the camera's default, they don't need to be entered
  - Analog cameras do not need the login fields
  - If you use the login field located in Account Settings – Camera, the information does not need to be duplicated here (you would typically use the camera login field under Account Settings – Camera when there are a lot of cameras that share the same login credentials)
- **Tags -** Select from previously used tags, or create new ones for the camera. These tags are used to create groupings of cameras. Similar to Layouts, you can use tags to view the preview feeds of all cameras with that tag.
- **Notes** - This field is optional. Add any notes about the camera settings here.
- **Delete Camera** - Click to delete the camera from the VMS

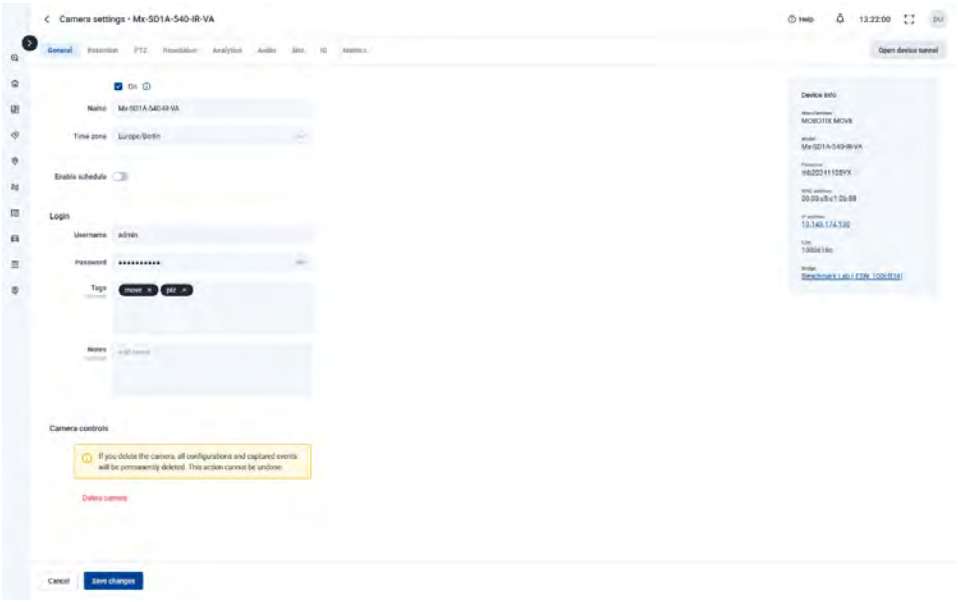


Figure: 42. Camera Settings

Retention

Cloud Retention: Sets the number of days that recorded video will be kept in the cloud. Note that changing this value may affect billing. See Figure: 43.

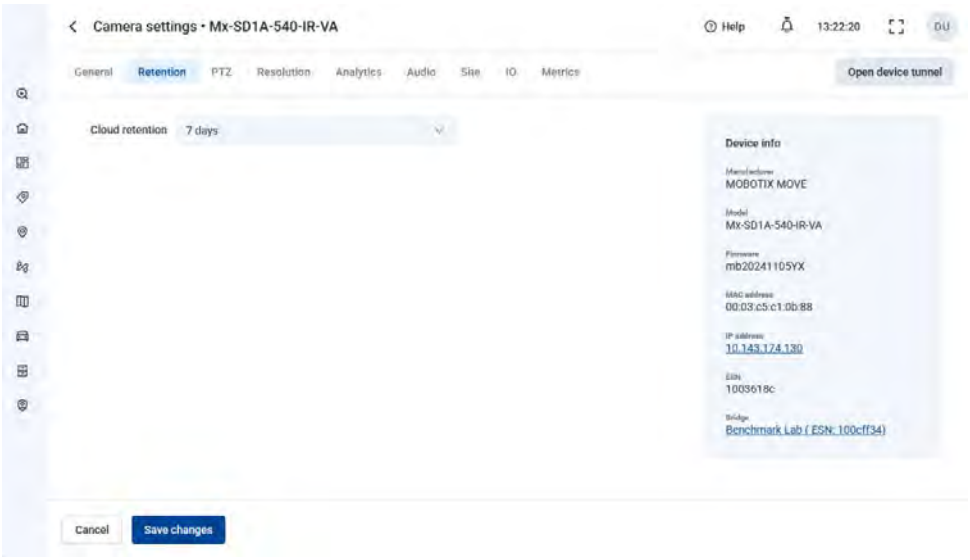


Figure: 43. Camera Retention Settings

Resolution

The MOBOTIX CLOUD 304+ VMS utilizes two streams of video. The first is Preview Video and the second is Full Video. Normally, preview video is recorded continuously, and full video is recorded only on motion (events). See Figure: 44.

Preview Video

- **Resolution**: Sets the resolution of the preview video that will be recorded. We recommend CIF resolution.
- **Note** The resolution set here will override the settings in the camera's browser-based user interface. This is intended behavior!
- **Quality**: Controls the amount of compression on the preview video. Low Quality will use the least bandwidth.

- **Update Rate**: Sets the frames per second for the preview video. We recommend 1 frame per second.
- **Transmit Mode**: Controls when the preview video is sent to the cloud data center:
  - **Always**: The preview video is immediately sent to the cloud (recommended setting).
  - **Event**: The preview video is sent to the cloud when motion or other events occur.
  - **Background**: The preview video is only sent when bandwidth is available on the schedule for the bridge.
  - **On Demand**: The preview video is only sent to the cloud when someone is watching it.

Max Bandwidth: Set the maximum bandwidth for the bridge to use when sending the preview video to the cloud. The bridge will not exceed this bandwidth for transmission. A low value will cause the previews to appear slowly when viewing them in a layout.
Note You should not set the total of your preview video maximum bandwidths to more than 50 % of your total available bandwidth.

Full Video Recording

- **Resolution**: Resolution that will be used for H.264 recording with full frame rate.
- **Quality**: Controls the compression rate on the H.264 recording. Recommend values are Low or Medium.
- **Bit Rate**: Controls the compression rate of the video recording. The setting depends greatly on the camera. We recommend leaving this at its default value.
- **Transmit Mode**: Controls when the full video is sent to the cloud data center:
  - **Background**: The video is only sent when bandwidth is available on the schedule for the bridge (recommended setting).
  - **On Demand**: The video is only sent to the cloud when someone is watching it or requesting it.
- **Record When**: Specifies when full video is to be recorded. Normally, the bridge only records video if it detects motion, but you can also select to do full recording all the time. Keep in mind that the preview video is always recorded.
  - **Always**: Requires at least double the amount of upload bandwidth.
  - **EVENT**: This setting makes the most efficient use of bandwidth and helps to quicker find interesting video clips (recommended setting).

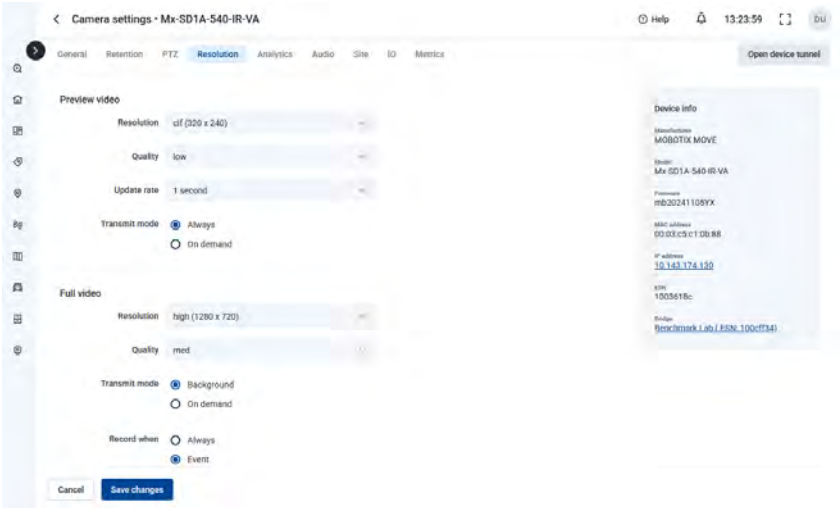


Figure: 44. Camera Resolution Settings

Audio

Audio Enabled: Enables audio recording if the camera has audio capabilities.
Copy Audio Used if the microphone is an external microphone or is in close proximity to a camera that does not have audio capabilities. Check the camera(s) in the drop-down list that you want to copy the audio from. Only cameras attached to the same bridge show up on the list

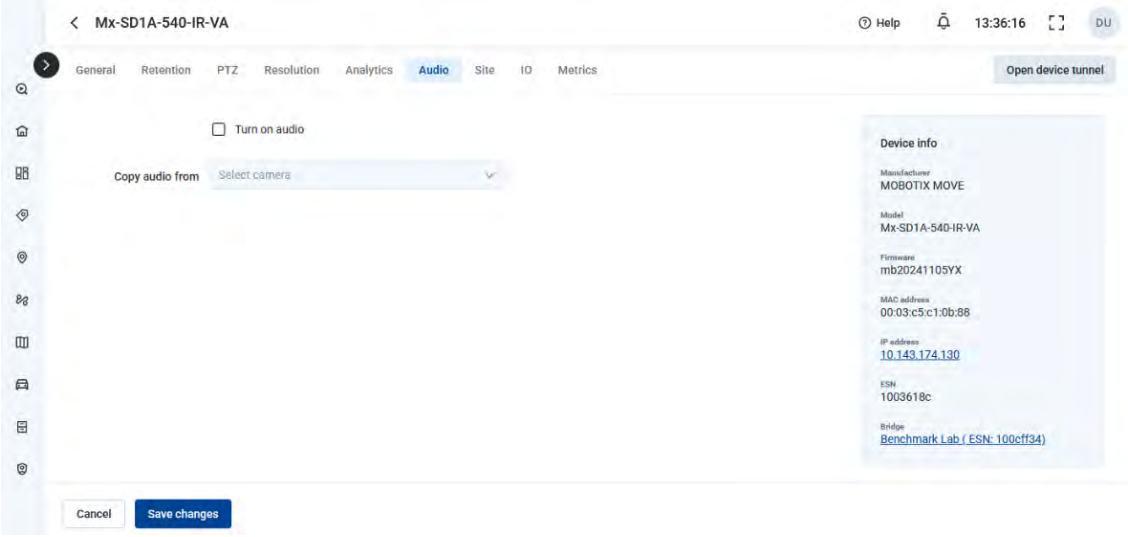


Figure: 45. Camera Audio Settings

Site

Sites serve as a grouping method for your cameras and devices, allowing you quick-looks at cameras at that site, as well as Dynamic Filtering around sites and viewing your cameras on the map.
The site (including address) is mandatory and will be automatically inherited from the bridge for newly added cameras. The additional fields (coordinates, azimuth, range, floor, notes) are optional, but if you intend to use the map feature, these will help with the exact positioning of your cameras.

Site Setting Fields

- **Site** - Select a saved site to add this camera to that site. If this is the first device at a new site, click the yellow plus sign to create a new site.
- **Street Address** - These fields will be automatically populated with the information saved to the site that was selected.
- **Floor** - Enter the floor number for the camera to be able to use dynamic filtering to only show cameras on certain floors.
- **Latitude/Longitude** - A way to precisely place your camera on the map in the VMS. You can enter the coordinates to these fields to have your cameras displayed at their exact site in a building, or useful when the camera isn't located at a specific street address.
- **Azimuth/Range** - These values will show the field of view on the map, which is a very convenient way to see areas of coverage (or areas lacking coverage). Azimuth defines the direction the camera is facing and is in degrees. North is defined as 0.0; so East is 90, South is 180, and West is 270. Enter the value (down to the tenth of a degree) to have the specific direction represented.

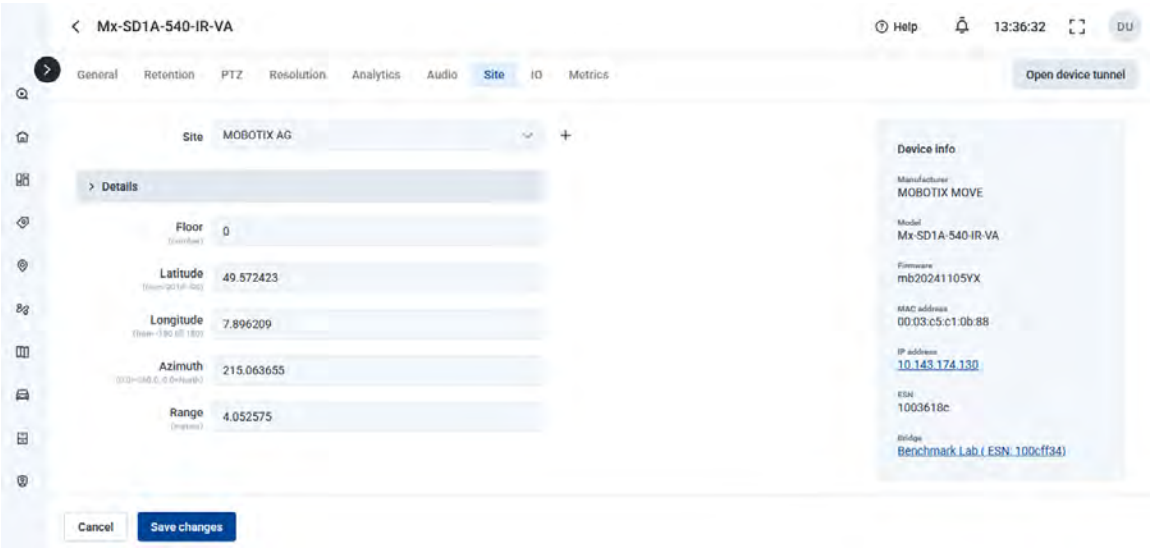


Figure: 46. Camera Site Settings

IO(Input/Output)

- **Input** - Select an Input from the list of configured inputs.
- **Turn on Input** - Toggle to turn on the selected input.
- **Name** - Enter a name for the selected input.
- **Default Status** - Select Open or Closed for the selected input.
- **Video Recording** - Toggle to turn the video recording for the selected input on or off.
- **Icon on Screen** - Toggle to make an icon for the selected input appear on the screen or not.
- **Output** - Select an Input from the list of configured outputs.
- **Turn on Output** - Toggle to turn on the selected output.
- **Name** - Enter a name for the selected output.
- **Default Status** - Select Open or Closed for the selected output.
- **Video Recording** - Toggle to turn the video recording for the selected output on or off.
- **Icon on Screen** - Toggle to make an icon for the selected output appear on the screen or not.

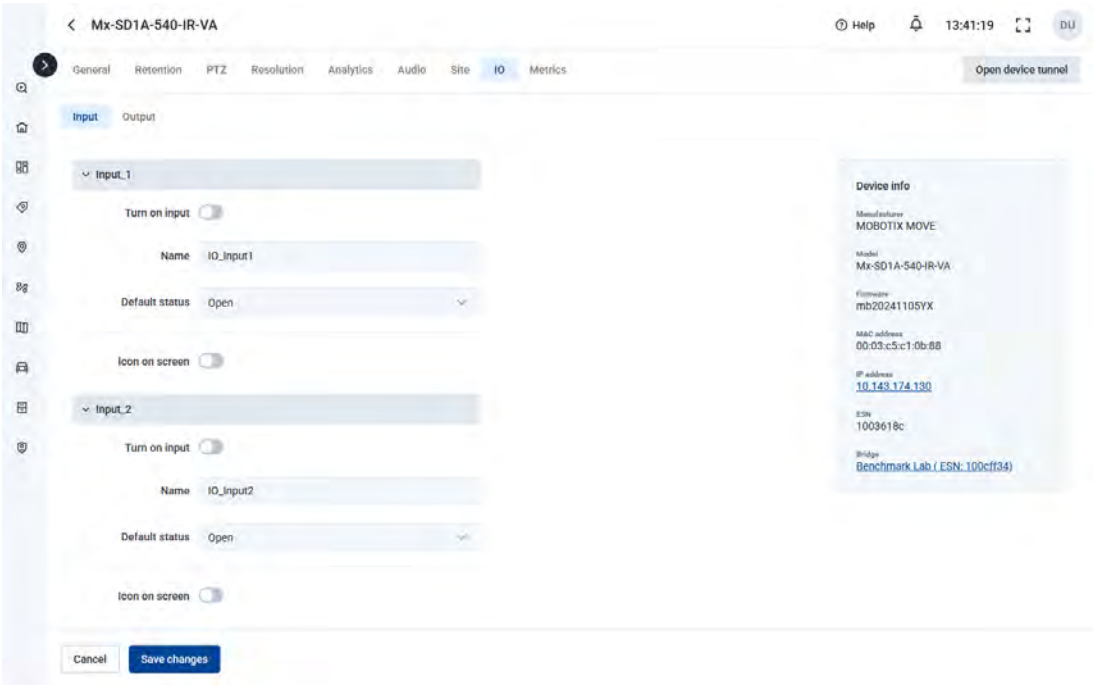


Figure: 47. Camera Settings IO(Input/Output)

Metrics

Bandwidth: A graph of how much data has been transmitted to the cloud data center for this camera.
Packet Loss: A graph of packet loss between the camera and the bridge. If this graph shows red, it means that your network may have problems. Check the cabling and resolve the packet loss problem between the camera and the bridge for reliable operation.

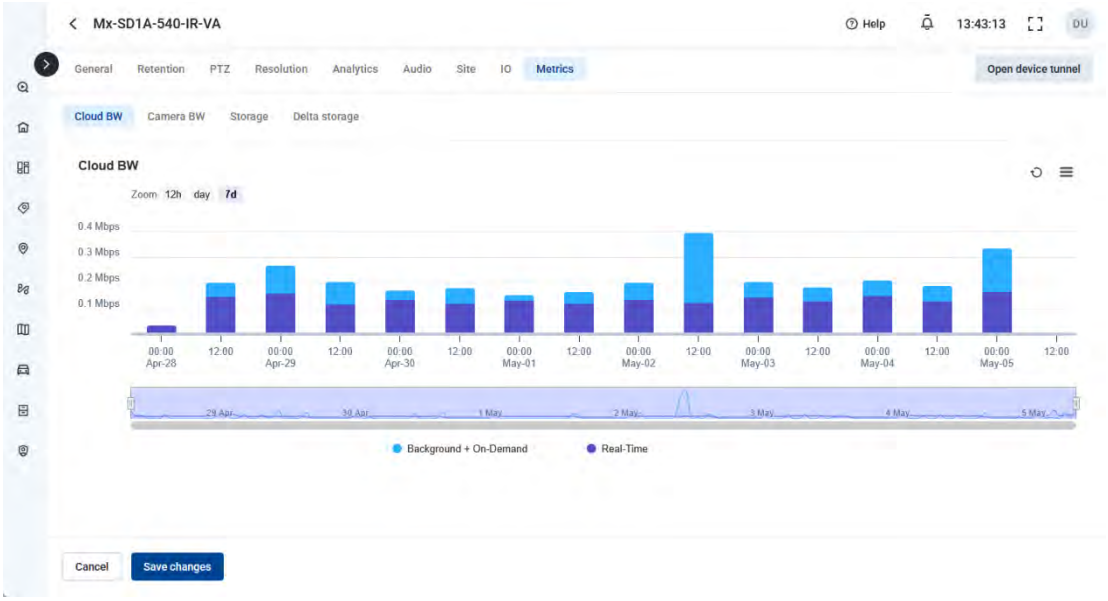


Figure: 48. Camera Metrics

Live View and History Browser

This chapter provides information on viewing live video and creating clips with the History Browser in the Mobotix Network Cloud VMS.

Live View

Live videos can be accessed from any preview video pane (in **Layouts**, **Tags**, **Locations**, etc.), or through the Dashboard. See Figure: 49. .

- **Preview Video Panes** – Click the video pane to open live, full-resolution video for that camera.
- **Dashboard** – Click the status check mark next to the camera to access the preview video, then click the preview video to open live, full-resolution video.

Figure: 49. Live Video Pane

Live Video Controls

Review the live video controls below.

-  Click the three dots icon in the camera frame and choose one of the following:
- **History Browser** - Select to open the History Browser.
- **Settings**: Opens the Camera settings.
- **Snapshot**: Select to save the current video frame to the downloads folder on your computer.
-  Click the arrow icon to open the camera's live view in another window.
-  Click the clock icon to open the History Browser.
-  Click to stop the live camera view.
-  Click to take a snapshot of the live camera view.
-  Click to connect to a call if the camera has a microphone.
-  Click to Zoom in on the camera view.
-  Click to Zoom out on the camera view.
-  Open the Preset points of the camera view.

- Click the split-screen icon to open a split-screen view of the Live View and History Browser. See Figure: 50. to view the split screen view of live and history browser.

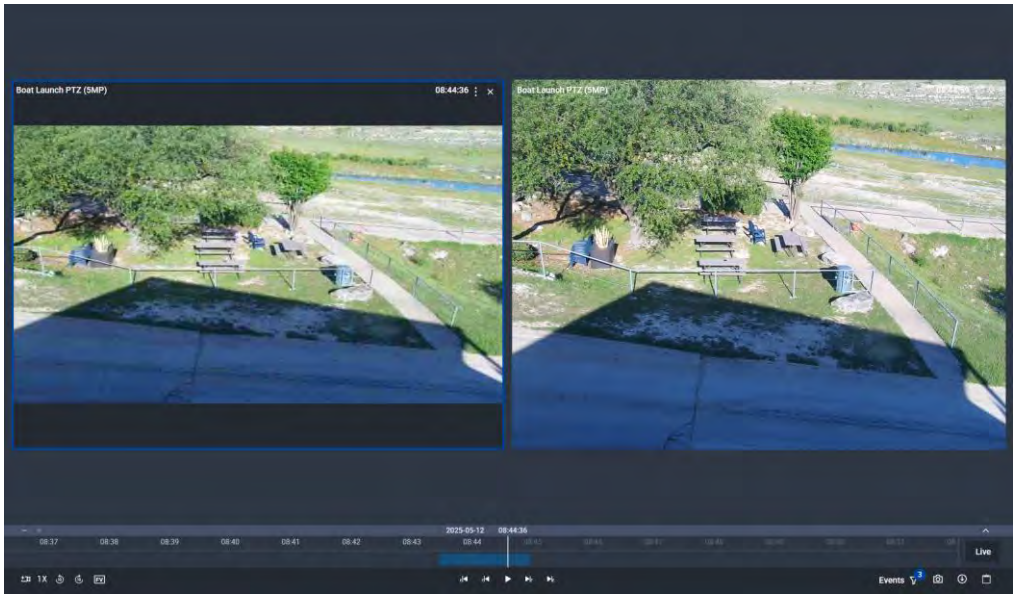


Figure: 50. Live View and History Browser

History Browser

The History Browser allows users to review video recordings.
By default, the live, lower-resolution preview video image shows. The lower part of the screen is a Timeline control with navigation buttons used to view the video history.

Timeline Overview

The Timeline lets you browse through the event history of the camera you have selected. It shows alternating areas of light and dark gray that indicate the time intervals selected in the top-left corner of the Timeline (more on this below). In the center of the timeline, there is a vertical pink bar that indicates the time you are viewing. The specific time is also displayed above the pink bar.
The most important things to note in the Timeline are the colored blocks in the gray space. These indicate events that you might want to pay attention to. You can see the meaning of the different colors in Figure: 51.

Figure: 51. Timeline

The most common thing you see is the light blue color (representing detected motion) with dark blue video around it. This is because whenever the camera detects motion, full resolution video is saved with a three-second buffer around the detected motion.
In the History Browser, the top of the screen shows the current video image. This is normally a Preview video image. The lower part of the screen is a Timeline control with navigation buttons. To access the History Browser, click the blue clock icon in the upper right-hand corner of the preview view or the clock icon in the Dashboard. See Figure: 52. . for more information about saving video.

Figure: 52. History Browser

The History Browser consists of a video pane, which is where the video will be shown, a Timeline that allows you to scrub through the recording history of the camera with important events highlighted, zoom buttons to allow you to access the Gallery view that highlights important events detected by the camera, and tools to save and share video clips.

Cycling Through the Timeline

The Timeline can be clicked and dragged left or right to cycle through the video history. You can also click and drag the date bar below the Timeline to change the day that is being displayed.

- 2025-04-06 You can quickly select a specific date using this button.
- Live Click the Live button to activate Now mode. This moves the cursor to the current time, continually updates the timeline with data, and attempts to keep the cursor at the latest image.

  Note: The **Live** button does not work while the video is playing and is grayed out. Pause the video before clicking the **Live** button.

Playing Video

Once you've found the video clip you want to view, click the **Play** button to begin playing the full resolution video. If the pink bar is not on an area with full resolution video available (dark blue areas on the Timeline), the playback jumps ahead to the next area with full resolution video available. Press Play again to pause the video.
There are several other playback navigation buttons available:

- Go to the previous (or next) frame of the video clip.
- Go to the previous (or next) Event. Events are important parts of motion events as determined by the Mobotix AG VMS. For example, if your camera is watching a door, the system typically marks a Key Image for each person who goes through the door.

  You can also use the Shift key and click on the Timeline to set Start and Stop points.
- 1X Change the playback speed of the video using these buttons. Note that the 8x speed in particular can use high bandwidth, causing playback issues.

-  This area is called the Scrub Bar. While full-resolution video is playing, dragging the Timeline causes things to reload completely. Instead, click and drag the black bar in the Scrub Bar to move through the full definition video.

Saving a Clip

Saving a clip gives you two options: archiving the clip to your Mobotix AG VMS account or downloading the clip to your computer or mobile device.

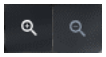
 Use this button to either Archive or Download a video clip. In the window that opens, you can select the time frame for the video to save. If you had created a selection prior to clicking the Save button, the Start and End times are already populated.
There are three options for what type of video to save:

- **Video**: This option saves the full resolution video.
- **Bundle**: This option saves both the full resolution video and the 1 frame per second timelapse preview video.
- **Preview Timelapse**: This option saves the low resolution 1 frame per second preview video.

The video description is populated with the camera name, date, and time but can be configured to fit your needs. You can also add a timestamp and notes.
In the destination select **Archive** or **Download** to save the clip in the manner you need.
Note: Clicking **Export** does not immediately download the clip. The VMS prepares the download, then you will need to navigate to Downloads in the left-side menu to actually save the clip to your device. This can take some time to be prepared, based on the selection length.

Additional Features

The additional features of the history browser are below.

-  Copy a URL to the current timestamp in the video you are viewing. You can share this URL with anyone who has access to the camera in your Mobotix AG VMS. You could also save the URL to access later.
-  Take a screenshot of the current frame in a JPEG format. The image is saved to your **Archive**, where it can be viewed, shared, downloaded, deleted, etc.
-  Zoom in and out of the video you are viewing.
- 

The Events button is used to filter out events recorded by the camera. Such as Loiter Detection, Person Detection, Object Intrusion, Object Line Cross, Motion Detection etc.
-  The forward and backward seek is used to take the video 10sec forward or backward
-  Click to view the full video.

Pan, Tilt, Zoom (PTZ) Camera Controls

PTZ Cameras have a few options not visible for non-PTZ cameras.

-  Click on this icon to turn on the PTZ control of the camera. The cross pointer turns blue when turned on and white when turned off.

-  The joystick is used to control the camera direction and can be moved as desired by the user.
-  This bar is used to control the zoom of the camera at a particular point.

Keyboard Shortcuts

The available keyboard shortcuts are as follows:

- Previous Image: ← or h
- Next Image: → or l
- Previous Key Image: ↑ or j
- Next Key Image: ↓ or k
- Previous Video: Shift + ←
- Next Video: Shift + →
- Zoom Timeline: +/ -
- Play/Pause: Spacebar

Other Viewing Options

There are several third-party applications that you can use to view the Cloud VMS. Please contact Support to learn about our partner integrations.
Go to Bridge/CMVR Actions for additional information.

Layouts

Use layouts to organize your cameras. Layouts are configurable screens that show multiple camera feeds simultaneously. You can choose the display size and position of the camera to preview videos. Layouts are consistent across the web interface and mobile app. You can also control user access to specific layouts.

Creating a New Layout

To create a new layout, do the following:

1. Choose **Layouts** from the navigation menu on the left and select **Add Layout** from the drop-down menu. See Figure: 53. .

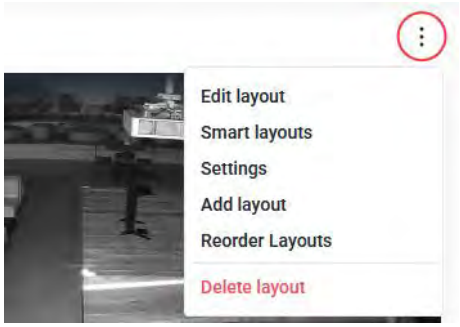


Figure: 53. Creating a New Layout

2. Configure the layout's settings. See Figure: 54. .

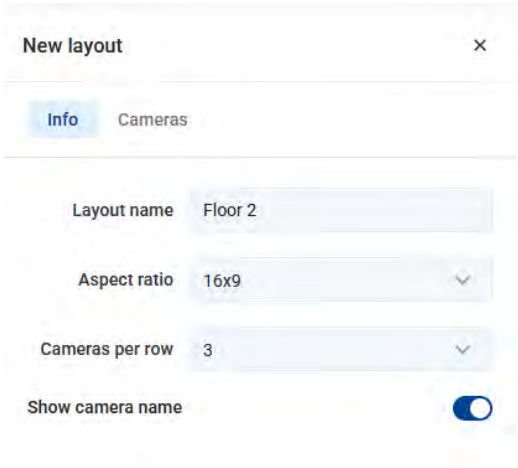


Figure: 54. Configuring Settings in a New Layout

The available layout settings are:

- **Name:** Enter the name of the layout.
- **Camera Aspect Ratio**: Change the aspect ratio of the displayed cameras to either 16 × 9 or 4 × 3.
- **Max Cameras Per Row**: Select the maximum number of cameras that can display on each row.

  Note: The possible number of thumbnails in a row depends on the device used for viewing.
- **Show Camera Title Bars**: Toggle to display or hide the camera name and timestamps on the thumbnails in the layout.
- **Show Camera Pane Borders**: Choose whether a border is displayed around a thumbnail.

3. Switch to the **Add Cameras** tab to select the cameras to add to the layout See Figure: 55. .

   Note: All cameras appear on the list. Search for cameras by typing in the camera name or by camera tags in the **Filter** field. After you select a camera, you can delete the filter and search for further cameras.

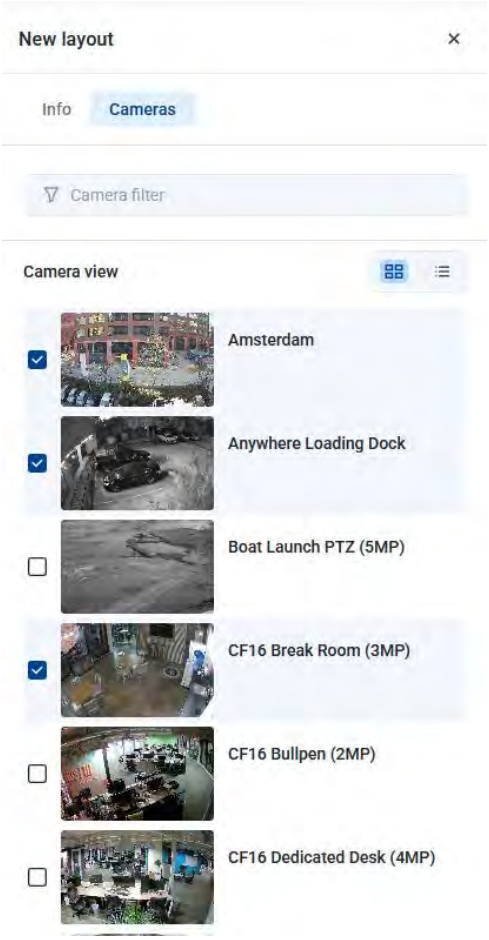


Figure: 55. Viewing a New Layout

Layout Actions

This section contains descriptions of various layout actions. Click on the three dot ⋮ icon to see the available settings.

Editing Layout Settings

On the Layouts screen, click the three dots icon ⋮ on the left side of the screen and select Settings.

- **Aspect Ratio**: Select the aspect ratio for your layout. Selections are 16×9 and 4×3.
- **Cameras per Row**: Choose from 1–6 cameras that you want to appear in a row in your layout.
- **Show Camera Name**: Use the on/off toggle to select if you want to show the camera names on the layout.

Editing a Layout

To edit cameras in a layout, do the following:

- Go to Layouts.
- Navigate to the chosen layout.

- Click the drop-down menu and select Edit.
- Delete a camera by clicking the X icon in the upper left corner of a thumbnail. See Figure: 56. .

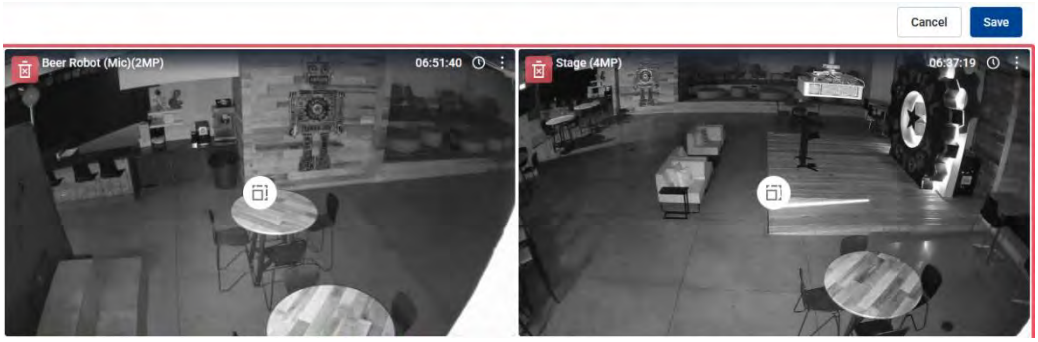


Figure: 56. Deleting a Camera from a Layout

- Click on a thumbnail to change its size and click and drag to move a thumbnail around in the layout. See Figure: 57. .

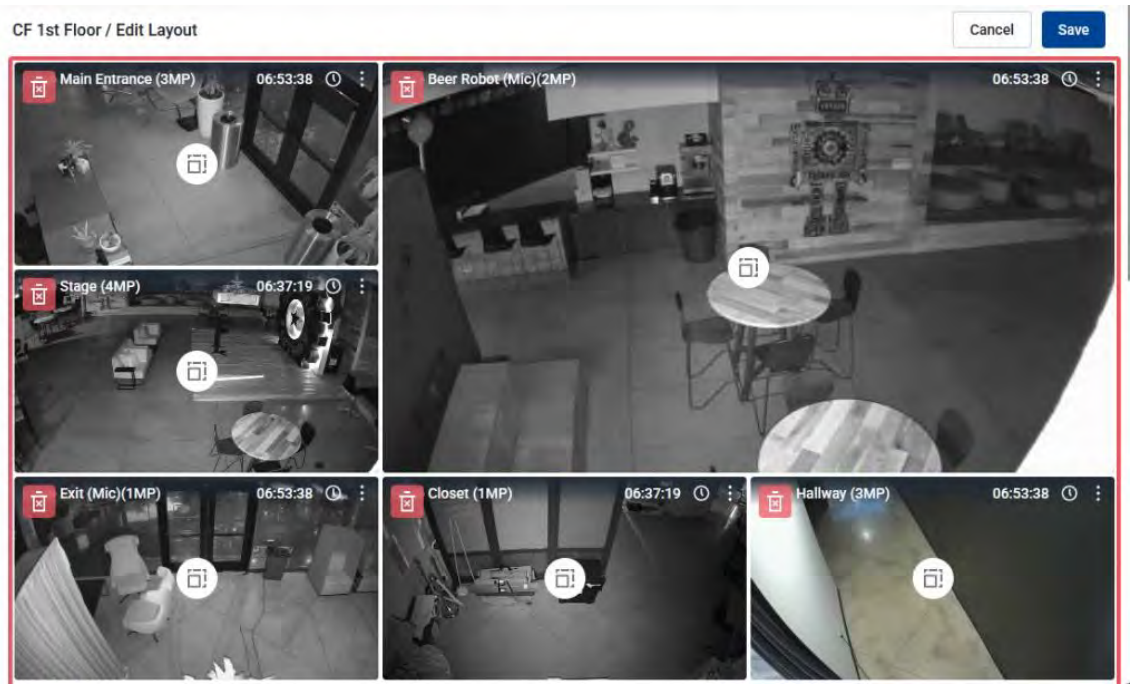


Figure: 57. Moving a Camera Thumbnail within a Layout

Turning On or Off All Cameras in a Layout

On the Layouts screen, click the three dots icon ⋮ on the left side of the screen and select Turn All Cameras On(Off) to turn on(off) all cameras in a Layout.

Deleting a Layout

To delete a layout, do the following:

1. Go to **Layouts**.
2. Navigate to the chosen layout.
3. On the Layout screen, click the three dots icon ⋮ on the right side of the screen and select Delete Layout to delete a Layout..
4. Confirm the action when prompted.

Smart Layouts

This feature is only available in the Enterprise or Professional versions of the Mobotix Network Cloud VMS. Smart layouts introduce AI to the popular Layouts feature. This feature is especially handy during low traffic or off hours, when getting alerted about motion events is a higher priority. Smart layouts are capable of detecting people, vehicles, or both, and automatically highlight the camera thumbnails with new motion events on the layout. It also provides a small preview of the motion event. See Figure: 58. to view the Smart Layouts preview.
Tip: Click the preview to be taken to the History Browser at the time of the event.

Figure: 58. Viewing Smart Layouts Preview

Note: Smart layouts are only recommended for low traffic times. Using it during a busier time might lead to the highlights shifting around too often.

Enabling Smart Layouts

To enable Smart Layouts, do the following:

1. Go to Layouts.
2. Click the drop-down menu and go to Smart Layouts.
3. From the drop-down list, select whether you want to be alerted for people, vehicles, or motion.

Note: This setting applies to all layouts.

Tags

Each camera has a field for adding any number of tags. You can use these tags to get a quick overview of cameras that share the same tags, without needing to organize them onto a layout.

Accessing Tags

To access tags, do the following:

1. Click **Tags** in the left navigation menu to drop down a list of tags.
2. Click one of these tags to open a layout-like page where you can view preview video for all cameras with the same tag.

See Figure: 59. for an example of Tags in the VMS.

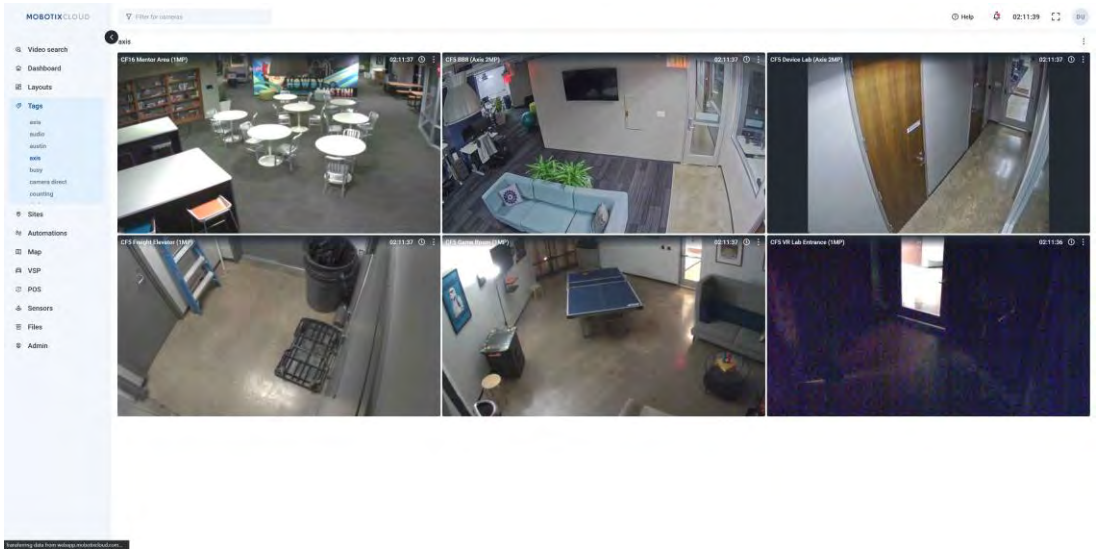


Figure: 59. Setting up Tags

Sites and Floor Plans

Sites and Floor Plans are advanced features of the VMS that are mostly used by Resellers or admins.

Sites

Important: This feature is only available in the Professional and Enterprise Editions.

Sites provide a way to manage and group cameras. Organizing cameras by location is helpful for accounts with a larger number of cameras dispersed across several locations.

Creating New Site

Sites are created through Smart Layouts. For more information on using Smart Layouts, see Smart Layouts. To create new Site in Smart Layouts, do the following:

1. Navigate to **Sites.** Click on ⋮ and click on **Add New Site** to create a new location. In the **Info** tab of the **Add New Location** dialog do the following:
   a) Provide a name for the location.

      Note: We recommend following a naming convention that will apply to all locations in your environment.

   b) Set the location's address.

      Note: This step is required only if you are using Floor Plans. In that case, enter the following:

   – Street address
   – City
   – State/province/region
   – Zip code
   – Country
   c) (Optional) Select if the location is the default for your account. Otherwise, leave it empty.

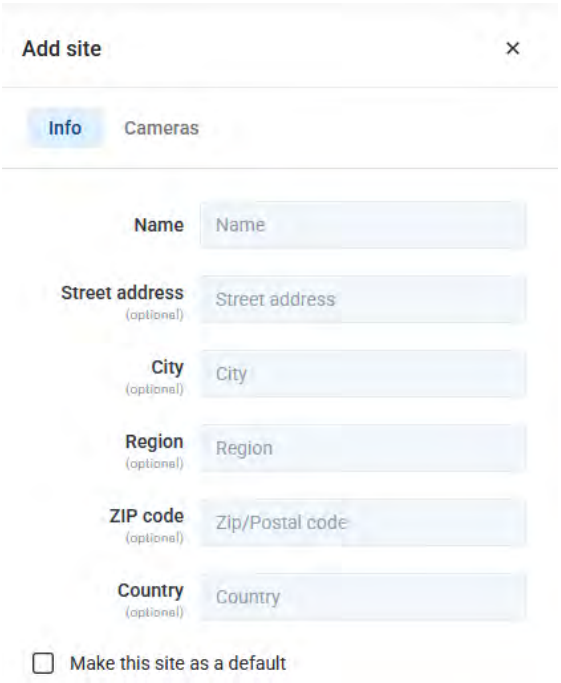


Figure: 60. Enter Site Details

2. Go to the **Cameras** tab to assign cameras to this new location by selecting them from the list.

Tip: You can use the **Filter** field to search for cameras or check the **Hide Cameras** already in location box to hide cameras already assigned to this location. See Figure: 61.

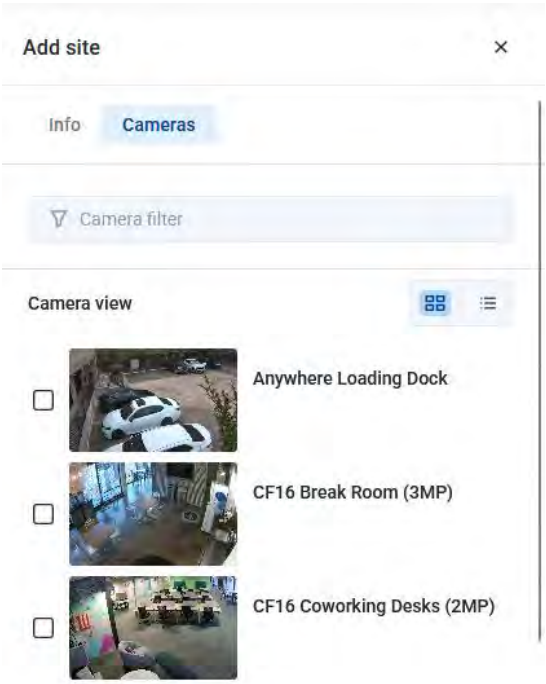


Figure: 61. Add Cameras to the Site

Using Sites

To use Sites in Smart Layouts, do the following:

1. Go to **Sites** for a dashboard view of locations.

   Note: On the dashboard, each location provides useful insights on the status of that location's cameras.

Figure: 62. shows that **Example Location** has 5 cameras online, 2 offline, one completely off, and 2 bridges online. Table 1 defines of Smart Layout statuses.

Figure: 62. Viewing Sites in Smart Layouts

Table 1 describes Smart Layout statuses.

Table 1. Smart Layout Statuses

Status	Description
Green	The device is online
Red	The device is offline (due to camera offline, bridge offline, or internet offline)
Yellow	The device is off (not recording video)

2. To see a layout of the location's cameras, do one of the following:
   a) Click the location's name.
   b) Click the eye icon .
3. For more settings, click the three-dot icon .
   c) Go to the **Location Details** tab to change the address or select whether the location is the default location for the account.
   d) Go to the **Edit Cameras** tab to search for and select or deselect cameras you would like to add to or remove from the location.

Floor Plans

Floor Plans offer end users a way to monitor larger, more complex, locations or even multiple locations by presenting cameras in a visual manner on a floor plan within the Cloud VMS.

Prerequisites

Before you begin with configuring and using Floor Plans, confirm the following:

- The Professional or the Enterprise edition is enabled.
- Sites are set up in the Mobotix Cloud VMS, including the address fields.

  Note: The address fields are not required by default when adding a new Site.

  – If Sites are not set up, see Creating New Site.
  – Even if you previously set up Sites, perform the following check:
    - Go to Sites.
    - Click the three dot icon next a Site to edit it.
    - Confirm that all the address fields are filled.

What to do next:

- If the address fields are properly filled, you can proceed to Configuring Floor Plans
- If the address fields are not properly filled, see Creating New Site

Configuring Floor Plans

The following sections describe how to add new floor plans and map cameras onto floor plans.

Adding a Floor plan

Use the instructions below to upload a new floor plan. See Figure: 63. .

1. Go to Floor Plans.
2. Add a new floor plan by doing either of the following:
   – Click the button and choose **Add New Floor Plan**.

   Note: The following screen only shows up if no floor plan has been added to the chosen location yet.

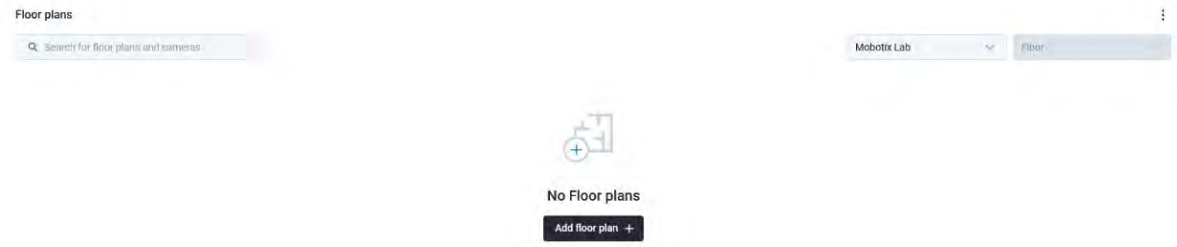


Figure: 63. Uploading a Floor Plan

Tip: You can go forward in the **Add New Floor Plan** page by clicking **Next** and double-check your settings by clicking the blue check icon above each completed step.
Important: If you made changes in previous steps, some of your more recent settings updates may be lost.

3. Select the Site from the drop-down list.
4. Select the floor level from the drop-down list.

   Note: You can choose a floor level between - 5 and 100.

5. Upload a floor plan either by dragging and dropping it on the screen, or by clicking **Browse Files**.

   Note: The file format of the floor plan must be PNG or SVG. The file size limit is 10 MB. You can only select and upload one file at a time.

   Tip: Using larger images with minimal white space around the floor plan helps to maximize available space for camera placement and improve the overall visual clarity of the image. If you are working with a large number of cameras, upload images that allow for proper placement of cameras without overcrowding the floor plan.

6. (Optional) Rename your floor to something more descriptive. See Figure: 64. for an example.

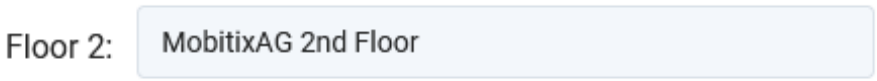


Figure: 64. Naming a Floor Plan

Note: You can change the name of the floor plan any time in Settings. See Managing Floor Plans.

1. Set the location on the map.
2. Click **Confirm** to finalize your setup or **Cancel** to exit the page.

   Important: If you exit without confirming changes, all your changes are lost.

   Result: Your floor plan has been added to the location.
   What to do next: Either continue by Adding Cameras to a Floor Plan, or repeat the same procedure for the rest of your floor plans.

Adding Cameras to a Floor Plan

To add cameras to a floor plan, do the following:

1. Go to Floor Plans.
2. Select the location from the first drop-down list, then do either of the following:

a) Select the floor plan from the second drop-down list. See Figure: 65. .

Figure: 65. Selecting a Floor Plan

b) Search for the floor plan in the search box on the left. See Figure: 66. .

Figure: 66. Searching for a Floor Plan

Note: Only the floor plans on the selected location will show up in the search.

3. Click the ⋮ button and choose **Edit Floor Plan**.
4. Click the + button to add a new device.
5. Choose the camera to add from the Add Devices panel.

   Note: Browse through the list of devices or search for the exact device you want to add. Once you have found the device you want to add, drag and drop it onto the floor plan.
6. Choose how to display the camera on the floor plan. See Figure: 67. .

Tip: The camera icon indicates a regular camera, the fisheye icon indicates that it is a fisheye camera.

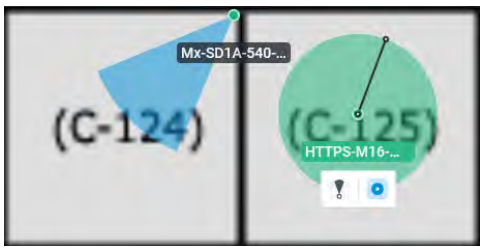


Figure: 67. Locating Devices on a Floor Plan

7. (Optional) To move a device on the floor plan, click the device pin and drag it to the desired location. You can also adjust the range the camera covers by dragging the dot until you achieve the desired size. See Figure: 68. .

Figure: 68. Moving Devices on a Floor Plan

8. Repeat this process until you have added all the devices to the floor plan, then click **Done**.

Tip: You can always come back later, add more cameras, remove cameras, or make changes. Read more in Managing Floor Plans

Using Floor Plans

Finding Floor Plans

1. Go to Floor Plans.
2. Select the location from the first drop-down list, then do either of the following:
   – Select the floor plan from the first drop-down list. See Figure: 69. .

Figure: 69. Finding Floor Plans from Drop-down List

   – Search for the floor plan in the search box on the left. See Figure: 70. .

Figure: 70. Finding Floor Plans using Search Box

Note: Only the floor plans of the selected location will appear in the search results. See Figure: 71. .

Figure: 71. Viewing Locations of all Cameras on a Floor Plan

Figure: 71. shows the cameras on a floor plan with their names and their coverage areas.
Tip: By using the icons on the bottom right corner, you can zoom in, zoom out, or view the floor plan in full screen mode.

Finding Cameras on a Floor Plan

To find cameras on a floor plan, do the following:

1. Hover over the camera marker on the floor plan for a preview. See Figure: 72. .

Figure: 72. Accessing Preview of Individual Cameras on a Floor Plan

2. Click the camera marker for a larger preview. See Figure: 73. .

Figure: 73. Previewing Feed of Individual Camera

3. Click the button to see the camera location on the floor plan. See Figure: 74. .

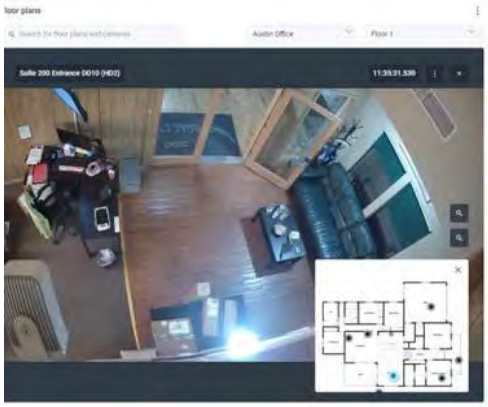


Figure: 74. Finding the Location of a Live Camera Feed on a Floor Plan

4. Click the button to open the Live View of the camera. See Figure: 75. .

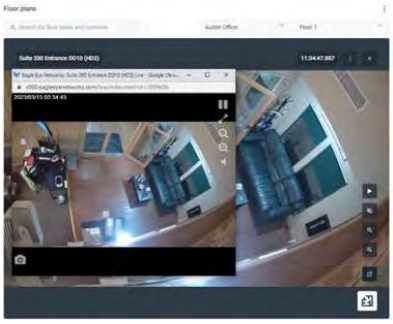


Figure: 75. Opening Live View of an Individual Camera on a Floor Plan

5. To access the camera's history, click the button and choose **History Browser.** See Figure: 76. .

Figure: 76. Accessing the History Browser of an Individual Camera on a Floor Plan

The rest of the icons allow for the following:

- Exit this view.
- Stop the livestream.
- Zoom in and out.
- Open Live View.

Tip: While on the **Floor Plans** page, you can easily switch between cameras, floor plans, and locations any time, even while reviewing video in Live or History view.

Managing Floor Plans

Changing the Name of a Floor Plan

1. Click the button and choose Settings.
2. Change the name of the floor plan.
3. Click Save Changes.

Showing or Hiding Camera Names on a Floor Plan

You have the option to show or hide camera names on floor plans.

1. Click the button and choose Settings.
2. Toggle the Show Camera Names on Floor Plan switch on or off. Important: This setting affects all your cameras, floor plans and locations.
3. Click Save Changes.

Removing Cameras from a Floor Plan

1. Click the button and choose Edit Floor Plan.
2. Select the camera, then click the button to remove it from a floor plan.
3. Click Done to finalize the changes.

Deleting a Floor Plan

Click the ⋮ button and choose **Delete Floor Plan**.

Updating a Floor Plan

If there is any change in a floor plan, you must delete and add it again.

1. Click the ⋮ button and choose Delete Floor Plan.
2. Add the new floor plan as described in Adding a Floor plan.
3. Add the cameras to the floor plan again as described in Adding Cameras to a Floor Plan.

Automations

Actions performed within the VMS are logged as audit events and saved in the audit log. These events are saved for one year for auditing purposes, showing which user did or changed what thing at what time. Automations control which of these events notify people and who is notified. For example, as an administrator, you may want to know when camera settings are changed. You can set up an Automation to email if changes are made and let you know who is making those changes. See. Figure: 77.

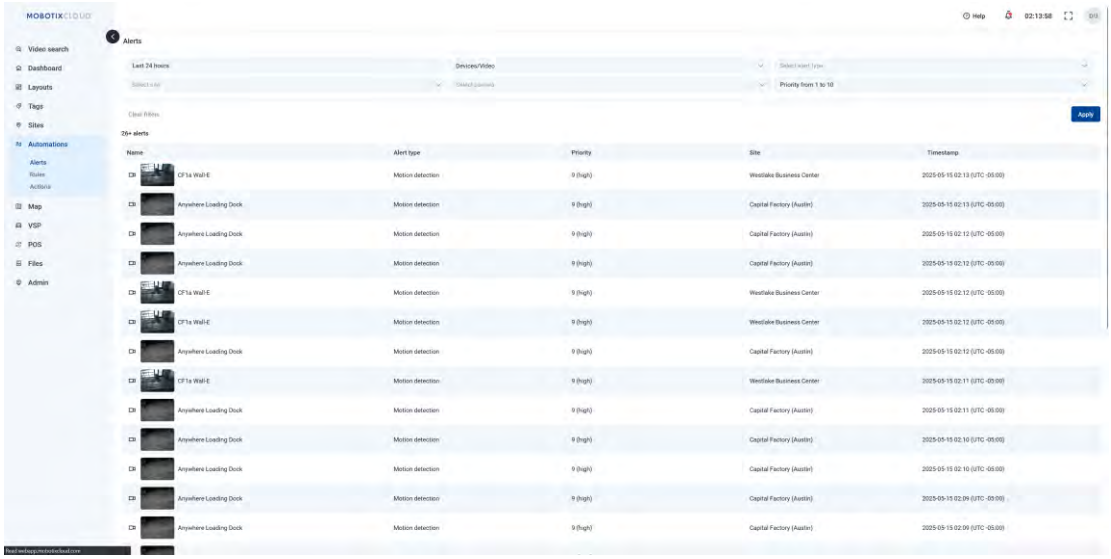


Figure: 77. Automations

Alerts

You can view all Alerts added to the VMS on this page.

- **Time**: Select a time range to view alerts.
- **Source**: Select the source to apply the rule. Choices are Devices/Video and VSP.
- **Alert Type**: Select the Alert Type you want to view.
- **Site**: Select a site you want to view.
- **Camera**: Select a camera if you want to view alerts only on that camera.
- **Priority**: Set the priority from 1 (low) to 10 (alarm) for the rule

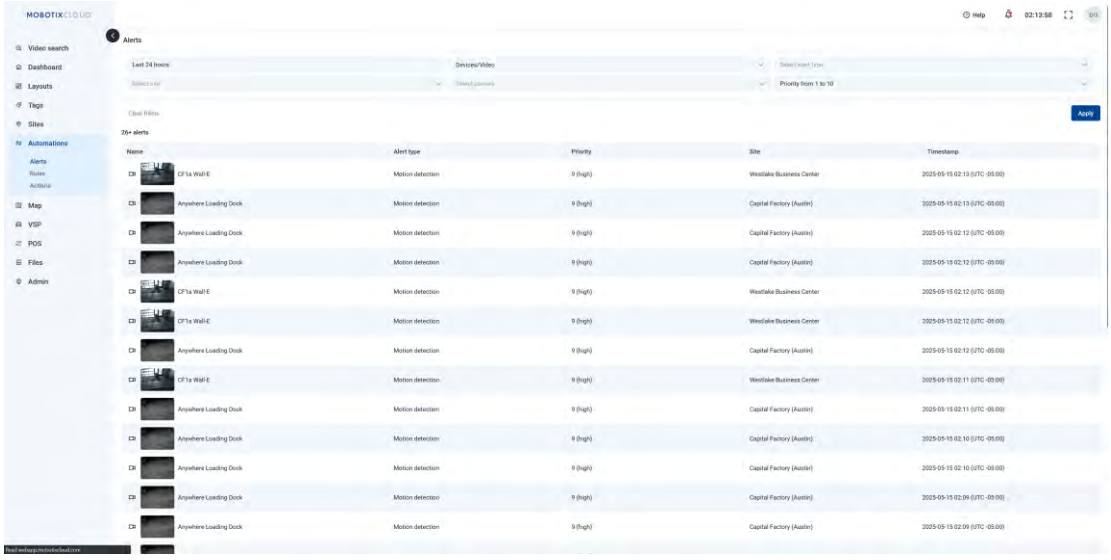


Figure: 78. Automations Alerts

Rules

You can search, view, and edit Rules in Automations.

- **Device/Video or VSP** - Select the type of Rule to view.
- **Select Alert Type** - Select the Alert Type to view.
- **Priority from 1 to 10** - Select to priority level (from 1 to 10) to view.

The results list contains the following fields:
Name - The name of the alert.
Alert Type - The type of alert detected.
Priority - The alert priority from 1 to 10.
Devices - The number of devices where the alert was detected.
Status - Use the slider bar to enable or disable the rule. If the rule is disabled, you will not receive an alert.
Details - Use the three dots icon to view details about the rule.

Add Rule

You can add rules to the Rules section of Automations to your account so that you can receive alerts through various communication platforms.

- **Rule Name** - Enter the rule name.
- **Source** - Select the source to apply the rule. Choices are Devices/Video and VSP.
- **Priority** - Set the priority from 1 (low) to 10 (alarm) for the rule
- **Notes (optional)** - Add any notes about the rule.

Conditions (if) - Use the selections in this section to add conditions where the new rule applies.

- **Alert Type** - Set the Alert Type from the list. Be sure that the camera selected for the rule has the correct analytic enabled.
- **When** - Select the time range that the rule applies. You have the option to set custom hours.
- **Cameras** - Select the cameras on the VMS to apply the rule

Actions (Then) - Use the selections in this section to add actions that the VMS should perform when the conditions set are met.

- **Add Action** - Select actions from the list that the VMS should perform when the conditions set are met.
- **Remove Action** - Remove any previously selected actions.

Edit Rule

Use the selections in this section to edit a rule.

- **Rule Name** - Displays the rule name.
- **Source** - Select the source to apply the rule. Choices are Devices/Video and VSP.
- **Priority** - Set the priority from 1 (low) to 10 (alarm) for the rule
- **Notes (optional)** - Add any notes about the rule.

Conditions (if) - Use the selections in this section to add conditions where the new rule applies.

- **Alert Type** - Set the Alert Type from the list. Be sure that the camera selected for the rule has the correct analytic enabled.

- **When** - Select the time range that the rule applies. You have the option to set custom hours.
- **Cameras** - Select the cameras on the VMS to apply the rule

Actions (Then): Use the selections in this section to add actions that the VMS should perform when the conditions set are met.

- **Add Action** - Select actions from the list that the VMS should perform when the conditions set are met.
- **Remove Action** - Remove any previously selected actions.

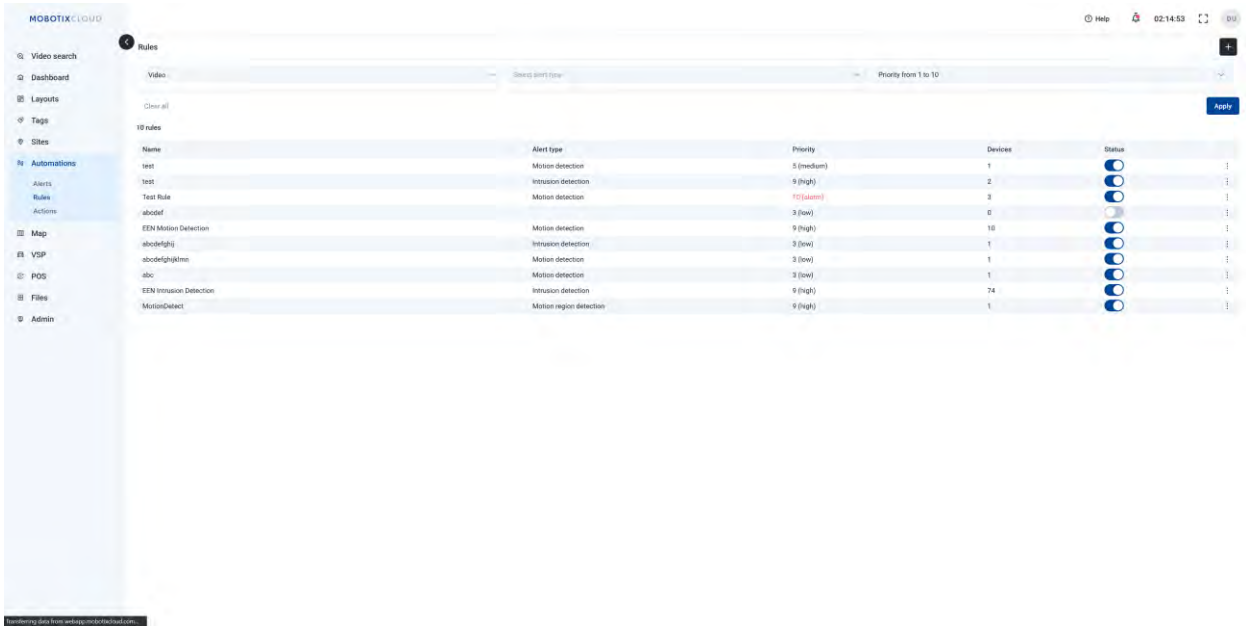


Figure: 79. Automations: Rules

Actions

Click the plus icon in the top right of the window to open the **Add Action** panel.

Add Actions

Action Name - Enter the action name.
Action Type - Select an action type from the menu.
Action types are described below.

- **Immix**: Triggers a webhook or automation after any specific event takes place notifying the user.
- **Notifications**: Fill in the following fields to create a new notification.
- **Re-Arm**: Set when the alert will notify people again; use this to limit the number of notifications people receive
- **Max Per Hour**: Enter how many maximum notifications to be sent in an hour.
- **Notification Type**: Enter the type of notification to send to the user. You can choose from Email or Push Notification or Both.
- **Recipients**: Enter the name or email addresses of the people who are alerted when this notification triggers
- **Webhook**: Trigger a webhook whenever any event occurs.
- **Site URL**: Enter the API URL to trigger after the events occurs

Edit Actions

Click the three dots icon next to an Action name to edit the Action.
Action Name - Displays the action name. This field is not editable
Action Type - Select an action type from the menu.
Action Settings - Use the selections in this section to make changes to your action. The settings vary according to the Action Type.

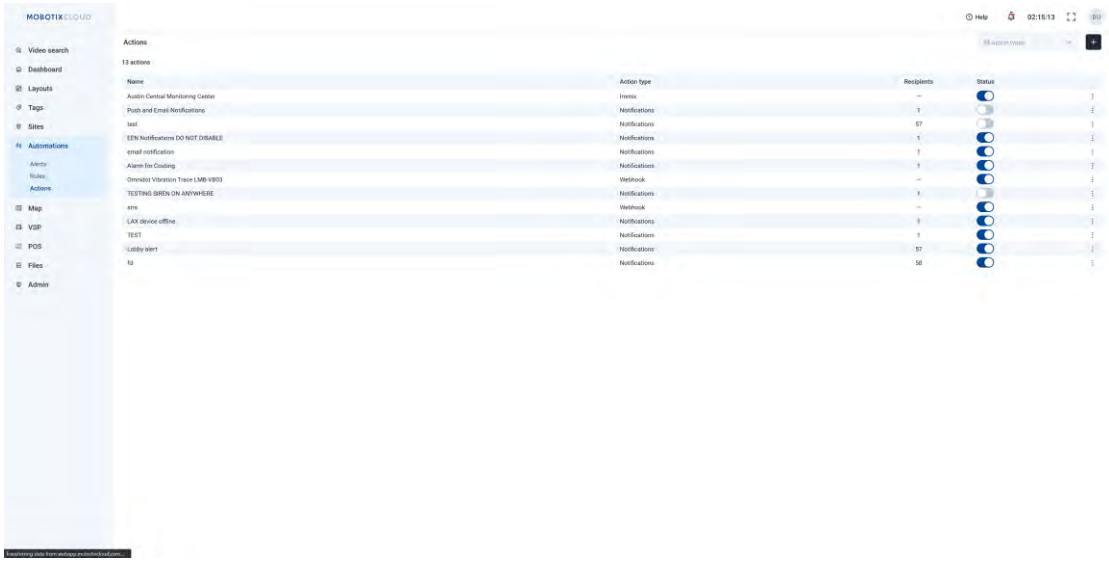


Figure: 80. Automations Actions

Map

The Map feature provides a way to view your cameras based on their physical location with the camera overlaid on Google Maps.
You can also set the correct angle, range, and field of view to have an accurate display of your camera coverage. Clicking a camera on the map brings up the preview video of the camera. Once the preview is visible, the same controls are available as viewing cameras from **Layouts** or the **Dashboard** page.
Multiple floors can be set up with separate views or viewed all at once. The drop-down menu in the upper-right corner of the map allows selecting which floor to view or **All Floors** to see all cameras.

Add Cameras to the Map

There are two ways to add cameras to the map.

- Add the address to a camera by going to **Camera Settings → Location**.

  Note: Entering a street address adds the camera to the map and automatically fills in a latitude and longitude. By default, the cameras are added to the 1st Floor. Changing the number in settings will move the floor a camera is on. Floors from -10 to 100 can be added to the map.

- The second method involves adding cameras directly from the map and offers much more immediate customization. The next section contains instructions for this procedure.

Adding Cameras Directly to the Map

Figure: 81. shows how to access the map edit functions.

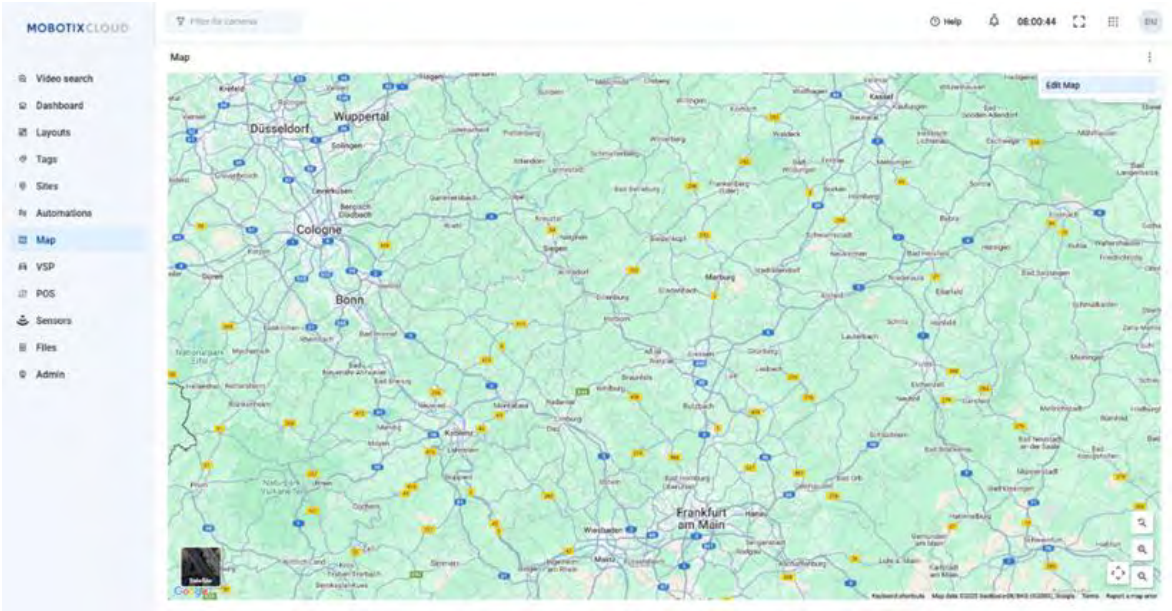


Figure: 81. Accessing Map Edit Mode

To add cameras directly to the map, do the following:

1. Go to the map and click the **Map** drop-down button at the upper left, then select **Edit**. This will add a red outline to the map indicating you are in Edit mode. A new set of buttons will appear at the top of the map. See Figure: 82. .

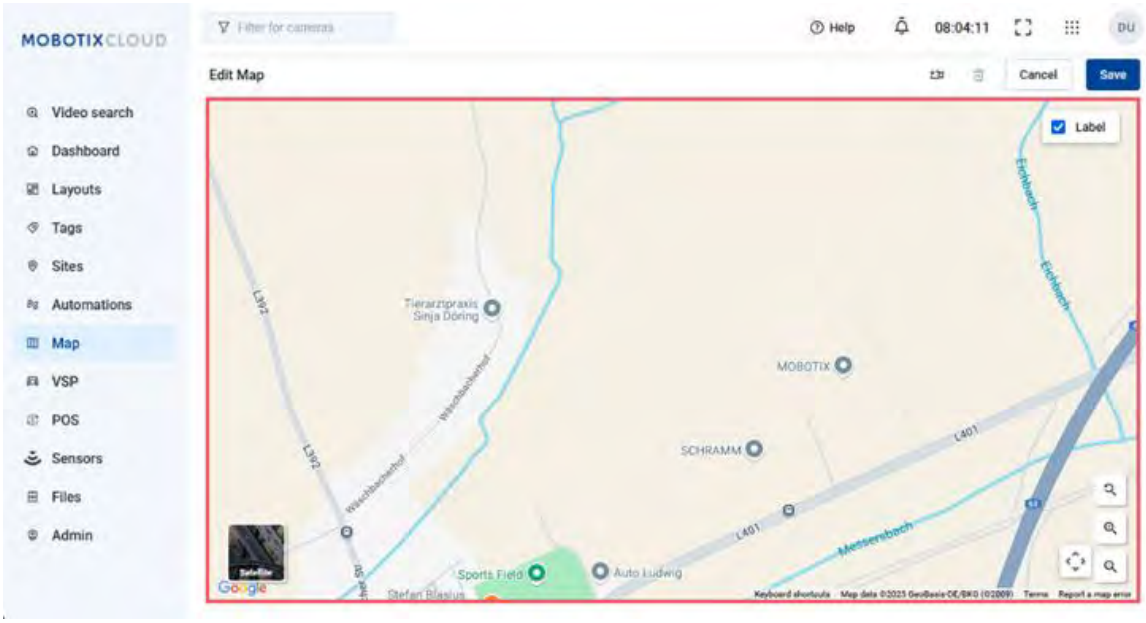


Figure: 82. Adding Cameras in Map Edit Mode

2. Enter the address of the location in the search bar. This will zoom the map to the address location. This is an embedded Google Map, so all expected functionality is available, including pan and zoom using a mouse or touch pad.
3. Use the Add Camera drop-down, which presents a list of the available cameras. Select the camera and it will be added immediately to the map.
4. (Optional) Move the camera by clicking and dragging the circle directly on the camera. Change the direction and range of the camera by clicking and dragging the circle farthest away from the camera. See Figure: 83. .

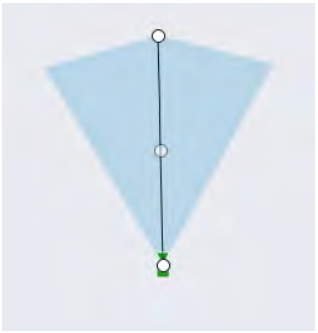


Figure: 83. Camera on Map in Edit Mode

5. Add additional cameras and floors and then click the green **Save** button.

When cameras are added to the map, data is automatically populated in the camera's location value. See Figure: 84. .

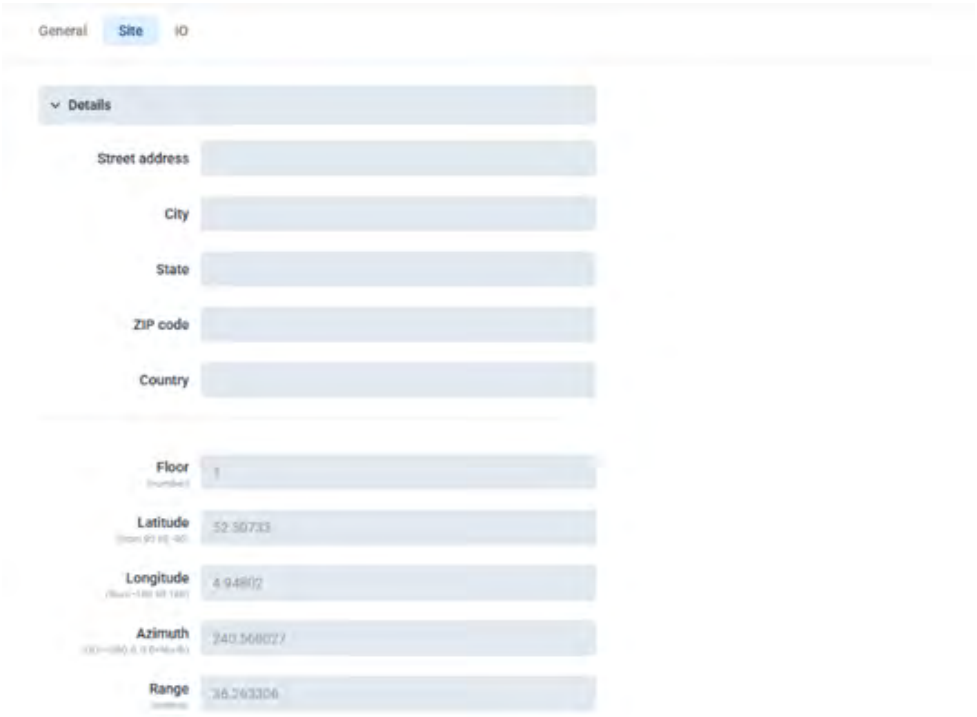


Figure: 84. Viewing Location Values that are Automatically Populated by Map

Editing Camera Locations in Map

Any edits to the camera's physical location need to be done in **Camera Settings → Location**. This includes changing the **Floor** value of the camera.

Removing Cameras from the Map

To delete a camera from the map, delete the street address in **Camera Settings → Location**.

Analytics

Analytics are advanced features of the VMS. They are mostly used by Resellers and admins. There are several types of analytics for your cameras, including:
The analytics run on the bridge/CMVR, so you can enable them on any camera added to the VMS. Analytics may be enabled separately and are billable per camera.

Important: Vehicle surveillance currently requires a specific supported camera.

Note: Analytics use considerable resources on the bridge. Limit the amount of analytics enabled on each bridge to the number stated in that bridge's data sheet.

Tip: For the most accurate analytics, use cameras for analytics that are capable of 16 frames per second (fps) for the MJPEG preview video stream used for analytics. 12 fps can work, but 8 fps does not give adequate results. Make sure that in **Camera Settings → Resolution → Preview Video**, the **Quality** field is set to **Analytics**.

Enabling Analytics for a Camera

Important: Each analytic is separately enabled and billed per analytic for each camera. To enable analytics for a camera, do the following:

1. Open the Camera Settings of the specific camera.
2. Go to the Analytics tab.

Result: A new tab appears for each analytic when enabling them, as shown in Figure: 85. .

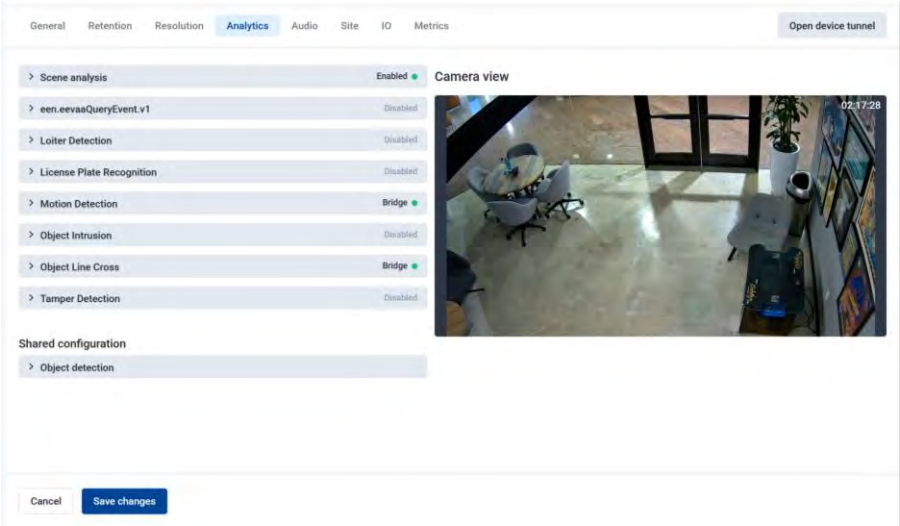


Figure: 85. Enabling Analytics

Setting up Analytics

Use the instructions in this section to set up analytics in the Cloud VMS.
Note: You must create a line or region for an analytic to be enabled.

Loiter Detection

Loitering allows you to define a region in the video output to generate alerts if a person or object enters and remains in that area for a given amount of time. You can check the total loitering counts per day in the analytic graphs. To learn how to access them, see Accessing Analytics
The daily count for the graphs resets at 2:00 a.m. in the configured time zone.

Setting up a New Region

To add a new region, do the following:

1. Add an area by clicking the plus Add region + button.

Note: Create a custom shape by clicking on the area where you want to analyze for object intrusion. You can generate a vertex by clicking anywhere on the screen.

2. Click and drag the shape at its vertices to adjust the size of the detection area.
3. Name the area to complete the setup. See Figure: 86. .
4. Set the **Duration** to define how long a person/object needs to remain in the area to be considered to loiter.
5. Name the area to complete the setup, then save the changes.
6. (Optional) Add multiple loitering areas to the camera by repeating the above steps. See Figure: 86. .

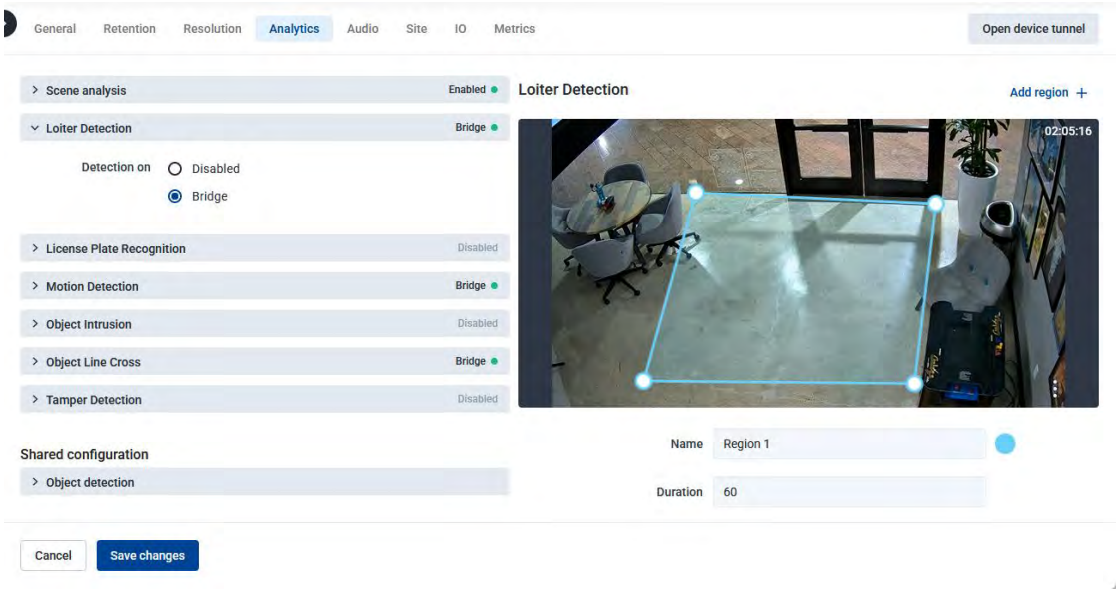


Figure: 86. Analytics: Setting Up Loiter Detection

What to do next: To learn more about setting up an alert associated with analytics, go to Automations.

Motion Detection

Motion detection allows you to define a region in the video output to generate alerts if any motion is detected within the defined area. There is no limit for the number of areas. You can check the total intrusion counts per day in the analytic graphs. Read more about it in Accessing Analytics

Setting up a New Region

To set up Motion detection, do the following:

1. Add an area by clicking the plus Add region + button.

   Note: Create a custom shape by clicking on the area where you want to analyze for object intrusion. You can generate a vertex by clicking anywhere on the screen.

2. Click and drag the shape at its vertices to adjust the size of the detection area.
3. Name the area to complete the setup and then save the changes. See Figure: 88. .

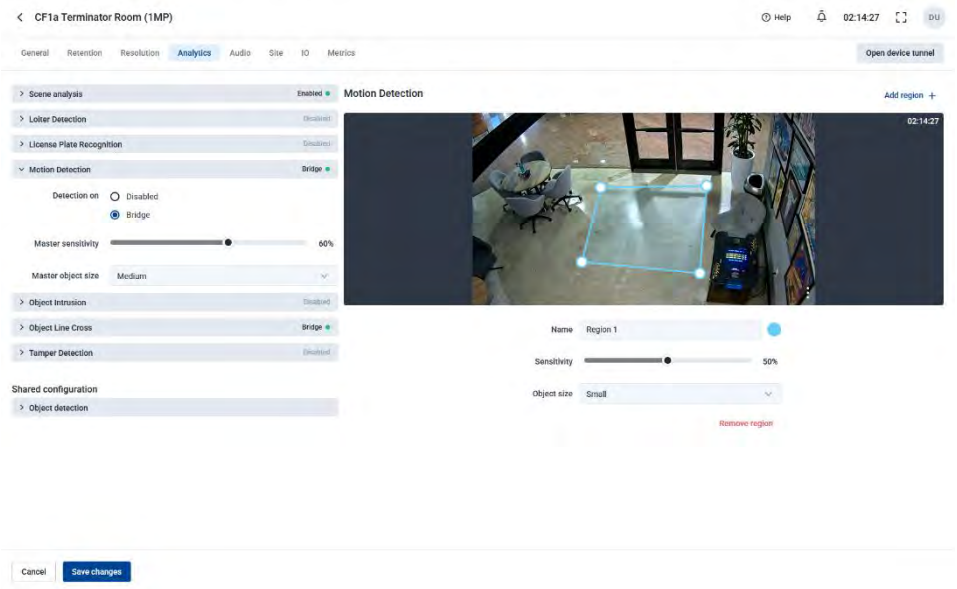


Figure: 87. Analytics: Setting up a New Area for Motion Detection.

4. (Optional) Add multiple detection areas to the camera by repeating the steps above

What to do next: To learn more about setting up an alert associated with a region, go to Automations.

Object Intrusion

Intrusion detection allows you to define a region in the video output to generate alerts if that region is entered. There is no limit for the number of areas. You can check the total intrusion counts per day in the analytic graphs. Read more about it in Accessing Analytics

Setting up a New Region

To set up Intrusion detection, do the following:

1. Add an area by clicking the plus Add region + button.

   Note: Create a custom shape by clicking on the area where you want to analyze for object intrusion. You can generate a vertex by clicking anywhere on the screen.

2. Click and drag the shape at its vertices to adjust the size of the detection area.
3. Name the area to complete the setup and then save the changes. See Figure: 88. .

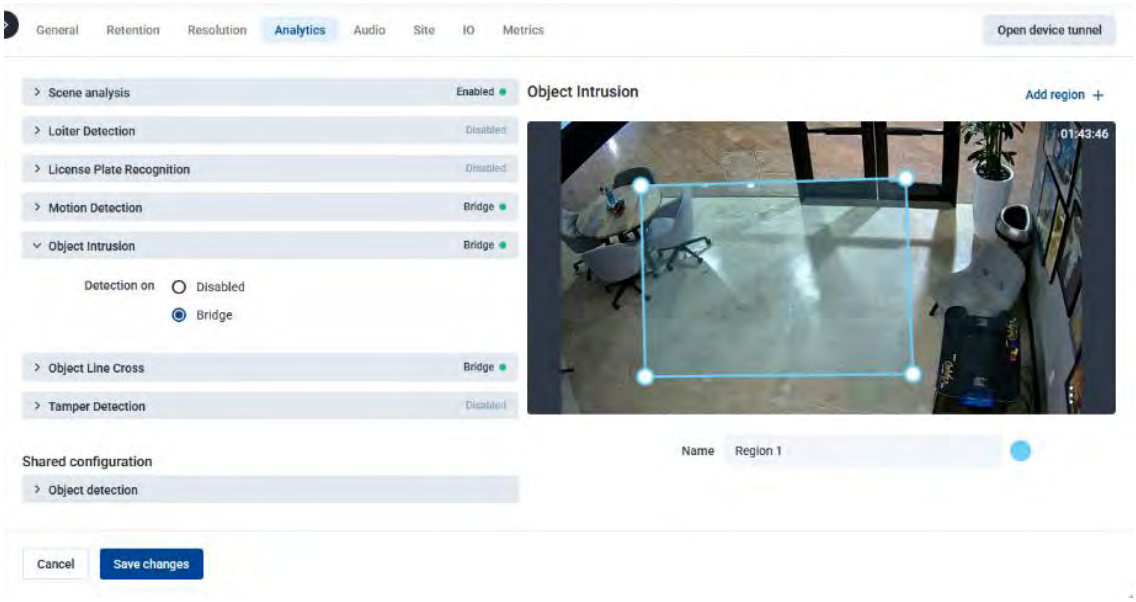


Figure: 88. Analytics: Setting up a New Area for Object Intrusion.

4. (Optional) Add multiple intrusion areas to the camera by repeating the steps above

What to do next: To learn more about setting up an alert associated with a region, go to Automations.

Object Line Crossing

Object Line Crossing allows you to define a line in the video output to generate alerts if that line is crossed. A running count of objects crossing both directions across the line is also graphed, but the count is not displayed in the preview or history browser. Read more in Accessing Analytics

Setting up a New Line

To set up line crossing, do the following:

1. Click on the dropdown icon to open the Object Line Cross.
2. Adjust the line according to your needs.
3. Use the directional arrows to dictate the direction the objects cross the line.
4. Name the line, then save the changes. See Figure: 89. .

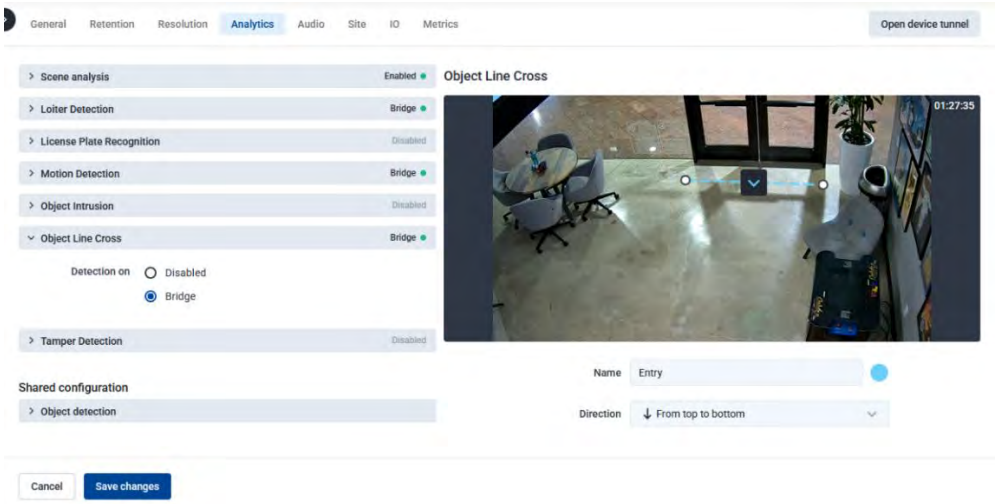


Figure: 89. Analytics: Setting up Object Line Cross

What to do next: To learn more about setting up an alert associated with this line, go to Automations.

Editing the Line

You can expand the size of the line by dragging its ends and adjusting it to your specifications. You may also adjust the direction of the line when the object crosses it by clicking on the arrow or using the direction drop down.

Camera and Line Positioning

For the highest accuracy, use a dedicated camera for the counting and line crossing analytics, mounted with a top- down view in which persons/objects remain the same size as they travel through the image. To be counted, the object/person must be tracked prior to crossing the line, and at least 50% of it must cross the drawn line. Lines must be placed in such a way to allow the object to cross and should not be placed near the edge of the image if parallel to the edge.
Tip: Place the line as close to the center of the image as possible. This may require the repositioning of the camera.

Tamper Detection

Tamper Detection generates alerts if the camera's view is blocked or if the monitored area drastically changes (i.e., someone swivels the camera to point elsewhere). You can check the total tampering counts per day in the analytic graphs. To learn how to access them, see Accessing Analytics

Setting Up Tamper Detection

Set the sensitivity for the camera. See Figure: 90. .

Note: We recommend using the default value when first enabling tampering. After a few days, you can make an assessment on the number of alerts generated and adjust the sensitivity from there. If you are not getting enough alerts, move up the sensitivity. If you are getting false positive alerts, lower it.

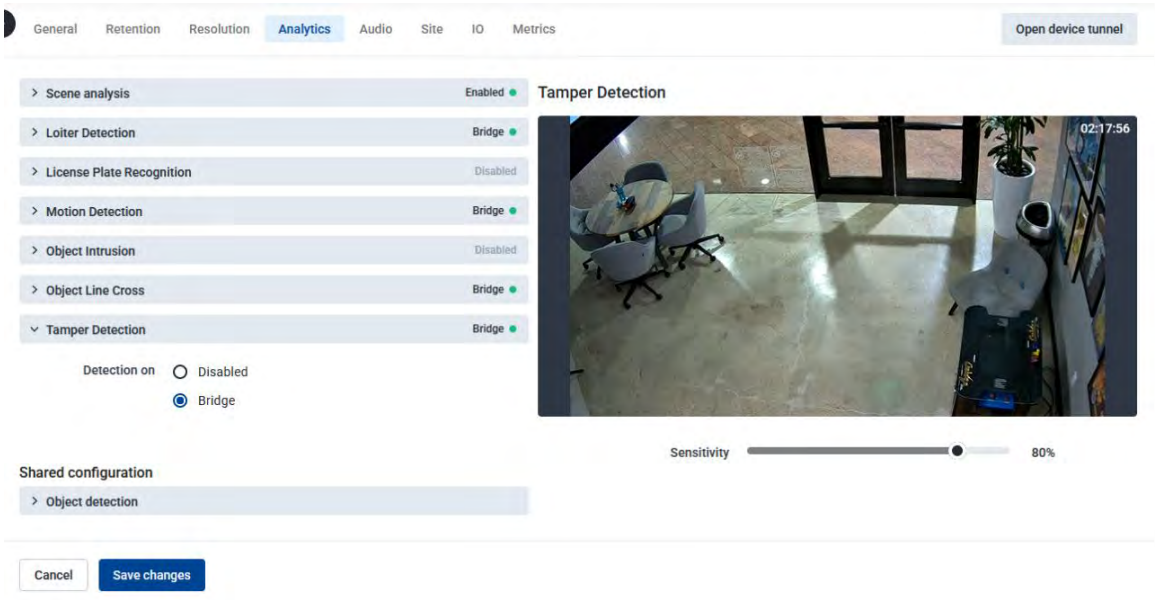


Figure: 90. Analytics: Setting Tampering Sensitivity

What to do next: To learn more about setting up an alert associated with tampering, go to Automations.

Object Detection Settings

Click the icon ⌄ to open object detection settings. See Figure: 91. .

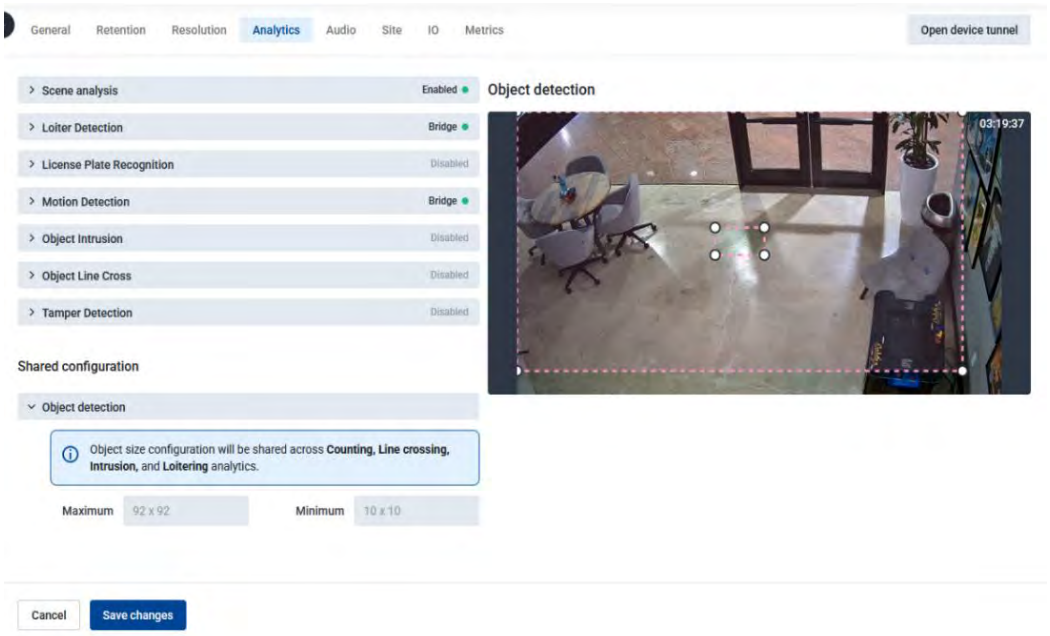


Figure: 91. Analytics: Setting up Object Detection

Note: These settings apply across all analytics except Tampering.

Available object detection settings are:

- **Min Size**: Defines the minimum size of an object to be counted by adjusting the box that appears with the help of its vertices.

  Tip: If the default value is not working for you, we recommend setting this value to be half the height and width of the average object size you expect to count.

- **Max Size**: Defines the maximum size of an object to be counted by adjusting the box that appears with the help of its vertices.

  Tip: If the default value is not working for you, we recommend setting this value to approximately 130% of the object's height and width.

Accessing Analytics

Analytics provide counts and graphs for detailed analysis.

1. To access the analytics graphs of a camera, do either of the following:

   – Go to your chosen camera on the **Dashboard** and click the analytics graph button.

   – Go to your chosen camera in **Layouts**, click the arrow icon and choose **Analytics** from the drop- down list. See Figure: 92. .

Figure: 92. Accessing Analytics

2. Choose the relevant tab to access any of the following:
    - Loiter Detection
    - Motion Detection
    - Object Intrusion
    - Object Line Cross In
    - Object Line Cross Out
    - Tamper Detection

Figure: 93. shows the analytics for objects crossing a line in the given direction, during the given date and times, for a one-hour duration.

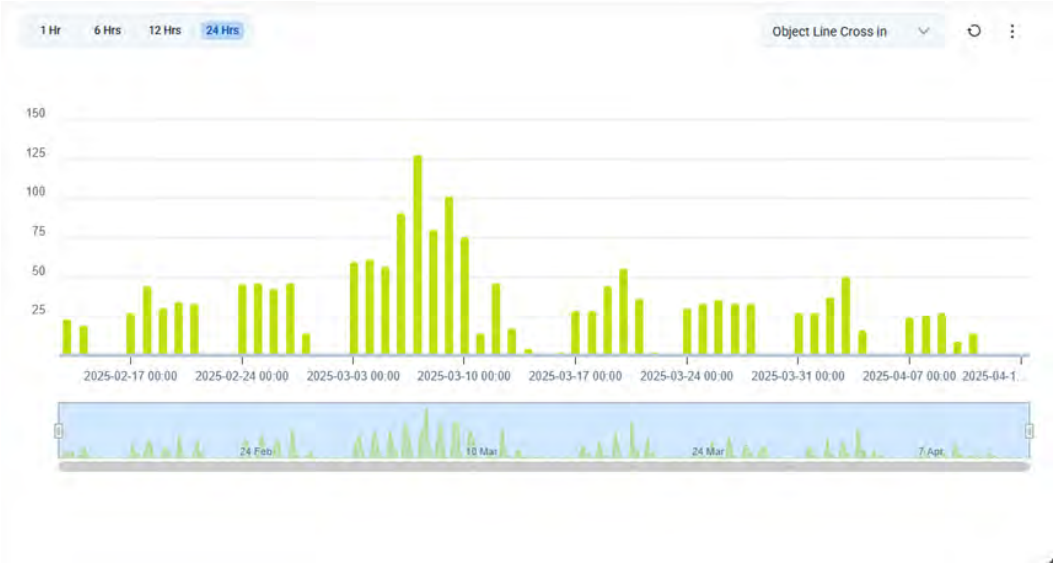
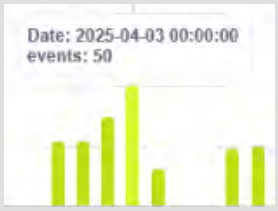


Figure: 93. Analytics: Viewing Line Crossing Data

Table 2 contains descriptions of analytics controls.

Table 2. Analytics Controls

Element	Description
Object Line Cross in	From the drop down select the analytics of which the data should be displayed.
1 Hr 6 Hrs 12 Hrs 24 Hrs	Choose the duration for the displayed data.
24 Feb 10 Mar	Get a quick overview of the flow of the count.
	Adjust the time interval by dragging.

Element	Description
	Hover over the graph for the number of events. Click to access the **History Browser** in the selected time period.
	Print or export graphs to various formats.

License Plate Recognition (LPR)

Mobotix License Plate Recognition (LPR) is a cloud-managed solution from Mobotix Networks for the accurate detection and recognition of license plates. Using the Mobotix LPR, any ONVIF camera connected to a compatible bridge can function as a license plate reader. The Mobotix LPR runs on the bridge, and the data is visualized in the VSP (Vehicle Surveillance Package) feature of the Mobotix Cloud VMS.

Prerequisites

Before you begin, make sure you have the following:

- A compatible bridge – for more information, see the *Mobotix LPR Data Sheet.*
- The LPR feature enabled in the Mobotix Cloud VMS – for more information, see Enabling LPR.
- A compatible camera installed – for more information, see the *Camera Installation Considerations for LPR/ANPR* application note.
- Mobotix LPR - Brivo Integration
  - USB to RS485 Converter - One piece per door
  - A cable for physical connection between the bridge and the panel
  - **Important**: Only use a cable recommended for OSDP, e.g., a shielded twisted pair cable.
- Mobotix LPR - Moxa Integration
  - A Moxa IOLogik e1214 I/O module
  - Power supply for the Moxa module
  - A Cat 6 cable to connect Moxa to the network
  - A cable to connect the Moxa I/O output to the barrier/output port

Recommended Bridge/CMVR Configurations for VSP

While VSP can run on any bridge or CMVR with an LPR compatible camera attached, the number of cameras supported by the bridge or CMVR varies by model. See Table 3 for a list of bridge/CMVR configurations for VSP.

Table 3. Bridge/CMVR Configurations for VSP

Bridges/CMVR	Max Cameras[1]	Max LPR Cameras for Gate/Street Configurations	Additional Analytics[2]	Local Display
304+/324+	5	1/0	0	No
401/403/420	5	2/1	0	No
406+/426+	10	2/1	2	No
524+/504+	10	4/2	2	No
501/520	15	4/2	5	Yes
620e/701/820e/901	50	8/5	10	Yes

1. The number of supported cameras changes when LPR is activated. Reference the latest datasheet and discuss with your sales representative before purchasing.
2. Number of additional analytics supported on the same bridge running LPR.

Enabling LPR

To enable Mobotix LPR analytics in the Mobotix Cloud VMS, do the following:

1. Navigate to the **Camera Settings** of your LPR camera, go to the **Analytics** tab, and check the **License Plate Recognition (LPR)** box to enable it for the account as shown in Figure: 94. .

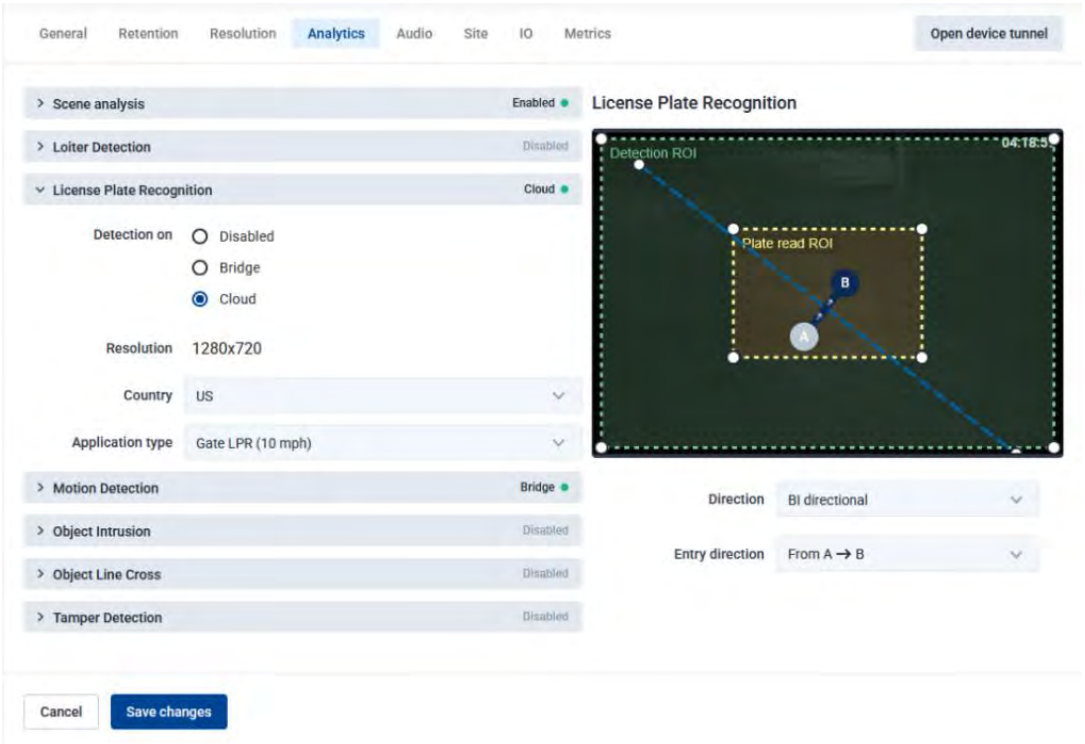


Figure: 94. Enabling License Plate Recognition

Note: If either of the fields you would like to edit are not present, contact support to have them enabled for your account.
Result: The Mobotix LPR is successfully enabled, and now you are able to see the LPR tab as shown in Figure: 94. .

Configuring LPR

To configure the Mobotix LPR, do the following:

1. Go to Camera Settings → Analytics → and click on › License Plate Recognition See Figure: 95. .

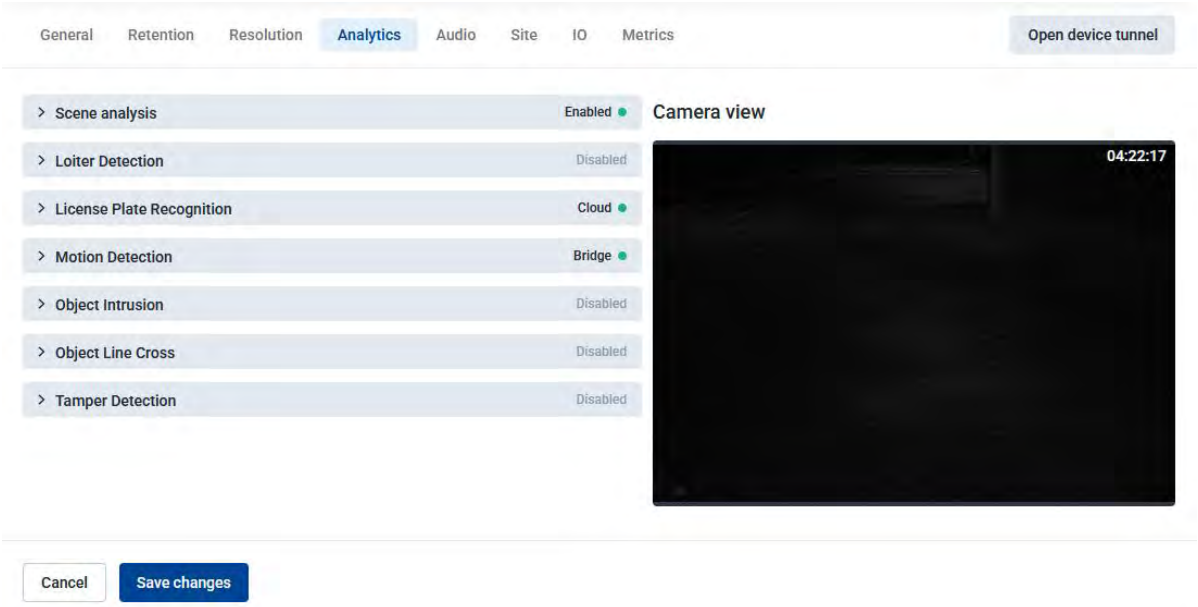


Figure: 95. Open License Plate Recognition Settings

2. Configure settings in the dialog that opens. For more information about the settings and possible configurations, see the LPR Tab Settings and Status Tab Settings sections.
3. Click **Save Changes** after editing the **LPR Settings** and closing the dialog in the **LPR** tab. See Figure: 96.

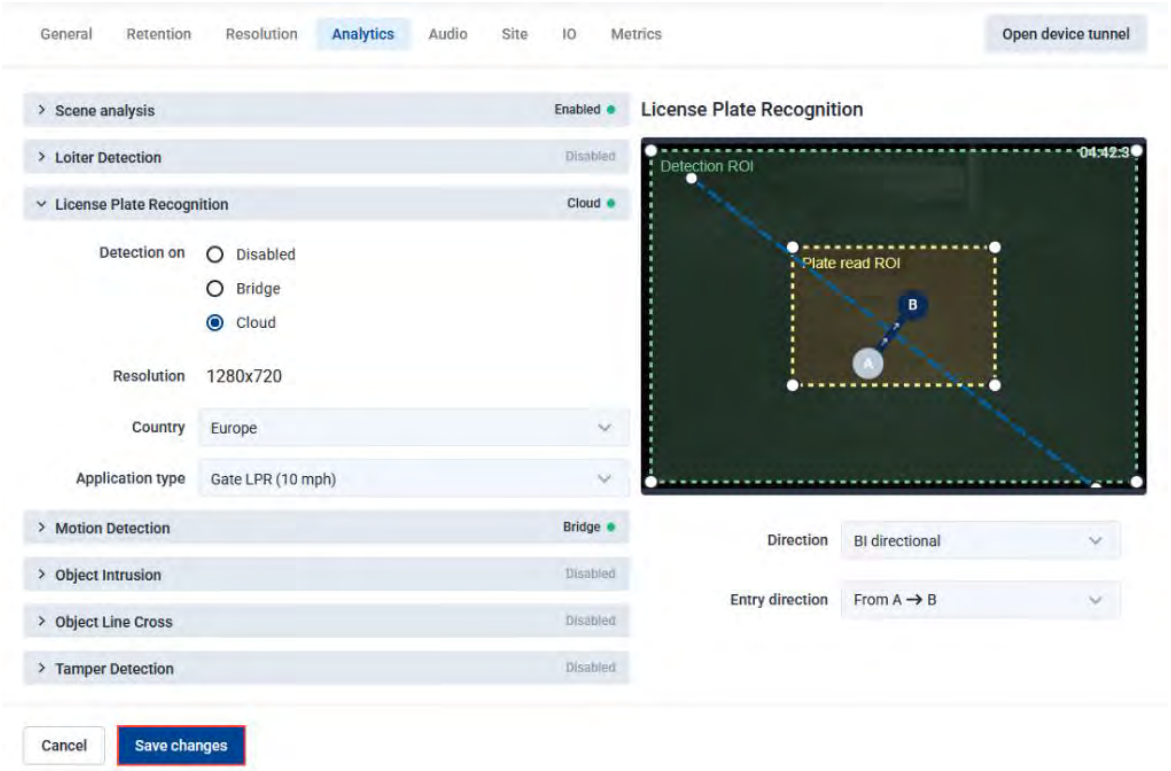


Figure: 96. Analytics → LPR: Saving Changes in the Camera Settings

LPR Tab Settings

This section describes the License Plate Recognition tab settings. See Figure: 97. .

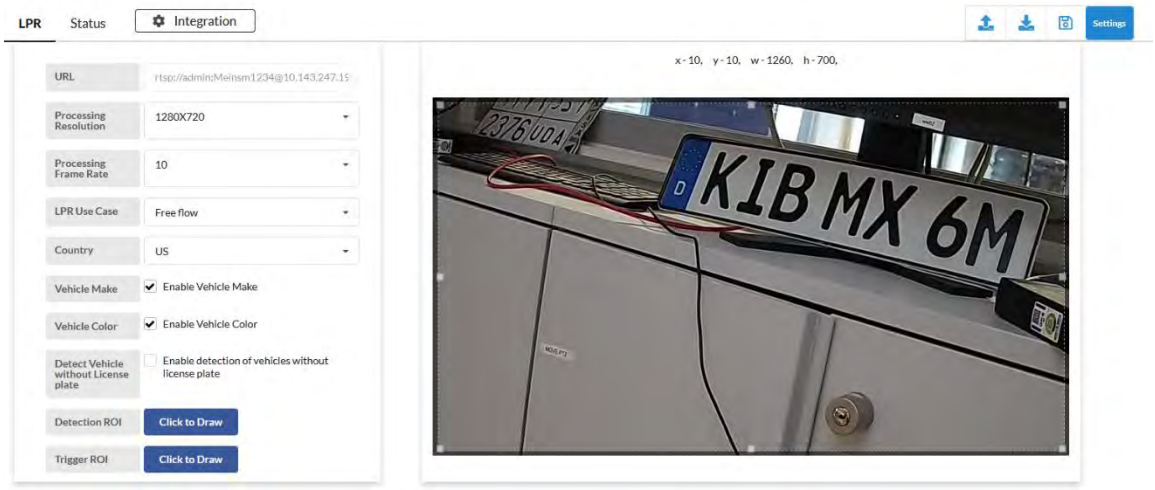


Figure: 97. LPR Settings Dialog

Available LPR settings are:.

- **URL**: This field is automatically populated.
- **Processing Resolution**: The input resolution of the camera video for LPR. A higher resolution increases the load on the bridge. These guidelines can help you select the optimal value:
  - 1280 x 720 – For lane width (camera view) less than 3.5 meters
  - 1920 x 1080 – For lane width (camera view) between 3.5 and 7 meters
- **Processing Frame Rate**: The frame rate at which the LPR is processed. Choose frame rate based on expected vehicle speed. Higher frame rates increase the load on the bridge.
- These guidelines can help you select the optimal value:
  - **Gate** (speed less than 10 MPH) – 10 FPS
  - **Street** (speed less than 30 MPH) – 15 FPS
  - **Highway** (speed less than 70 MPH) – 20 FPS
- **LPR Use Case**: Choose one of two configurations for LPR that align with the use case:
  - **Access Control**: This mode is used in gated garages and gated access control situations. For the best possible user experience, it is ideal to start opening the gate as soon as an allowed vehicle appears in front of the gate. Latency is critical, so detecting vehicles ahead of time is preferred. However, there may not be a long enough passage for detecting vehicles ahead of time, especially in rear-LPR scenarios.
  - **Free Flow**: This mode is used when vehicles can travel freely at varying speeds. This scenario is applicable for surveillance and security applications when the best view closest to the camera can be chosen as the region of interest for reading license plates. Video streams in this scenario must be processed at higher frames than the other modes. Processing FPS is chosen based on the speed of vehicle movement.
- **Country**: The AI model is tuned for a specific country to have an enhanced accuracy and understanding of the pattern of plates from the county.

Note: If the country you are looking for is not listed in the drop-down list, select the US as the country.

- **Vehicle Make**: The LPR determines the make of the vehicle and includes it in the metadata if you enable this field.
- **Vehicle Color**: The LPR includes the color of the vehicle in the metadata if you enable this field.
- **Detect Vehicle without LP**: The system still detects the vehicle and marks it as an event even if it cannot find or read a license plate because it was covered or missing if this field is enabled.
- **Detection ROI**: The region of interest (ROI) inside which the license plate would be detected.
- **Trigger ROI**: Trigger ROI is specific for customers using LPR for access control. Trigger ROI is a subset of detection ROI and shares the result back when the plate is inside the trigger ROI. Trigger ROI is enabled only in access control mode.
- **Preferential ROI**: Preferential ROI is also a subset of detection ROI and is defined as the region where the plates are clearly visible. With Preferential ROI, the system of the region is informed where license plate reading is most effective.
- **Access Type**: Access Type informs the system on vehicle direction and enables direction filters to ignore vehicles going in the opposite direction. The function is also used for reconciliation.
  - **Entry** – The vehicle enters the premises.
  - **Exit** – The vehicle exits the premises.
  - **Bi-Directional** – Vehicles are expected to move in both directions.
- **Entry Direction**: Entry direction defines the direction of vehicle movement and helps to filter vehicles in opposite directions. The direction mentioned is the trace of the license plate. Users can select multiple options to filter the direction effectively. For example, the user can select top to bottom and right to left to define diagonal vehicle movement from top right to bottom left.
  - Top to bottom
  - Bottom to top
  - Left to right
  - Right to left
- **Repeat LP Detection Timer**: Vehicle congestion and similar issues can cause the same plate to be in front of the camera for a few seconds. This setting can eliminate those repeated results by setting a timer when a plate is read and not saving results for the same plate for the given amount of time.

Provide the value in seconds to ignore the same plate if read.
Note: Only set this parameter if a repeating license plate was observed at the site.
As an example, Figure: 98. shows an LPR configuration with Detection ROI enabled.

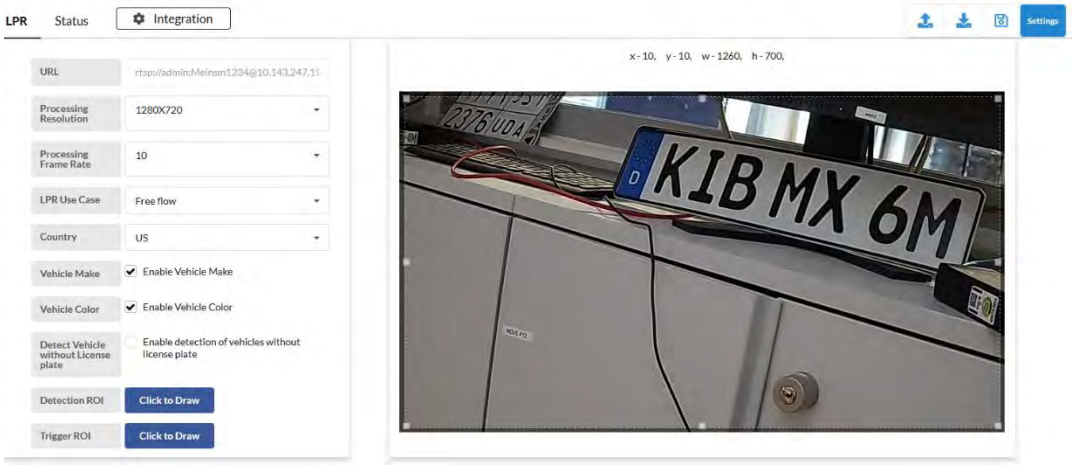


Figure: 98. LPR Configuration with Detection ROI Enabled

Status Tab Setting

Figure: 99. shows the LPR Status Tab settings.

Figure: 99. LPR Status Tab Settings

Available LPR Status Tab settings are:

- **Event Info**: Shows the Mobotix LPR scans for a specified time period to help to compare results with VSP in the Mobotix Cloud VMS. This helps determine if there is a communication issue.
- **System Status**: Presents the number of frames processed to understand how much the LPR engine is working in the background. It also displays the health of the system.
- **Integration**: Supports 3rd party integrations. Please contact Mobotix LPR Support for details and support for integrations.

Learn more about integrations in the Brivo Integration and Moxa Integration sections.

Access Control Integration

Access control integration enables the Mobotix LPR to be used as an authentication system to trigger and open the gate. Mobotix supports access control through Brivo and Moxa I/O Modules.

To change access control settings, go to **Camera Settings → Analytics → LPR Settings → Access Control**. See Figure: 100. .

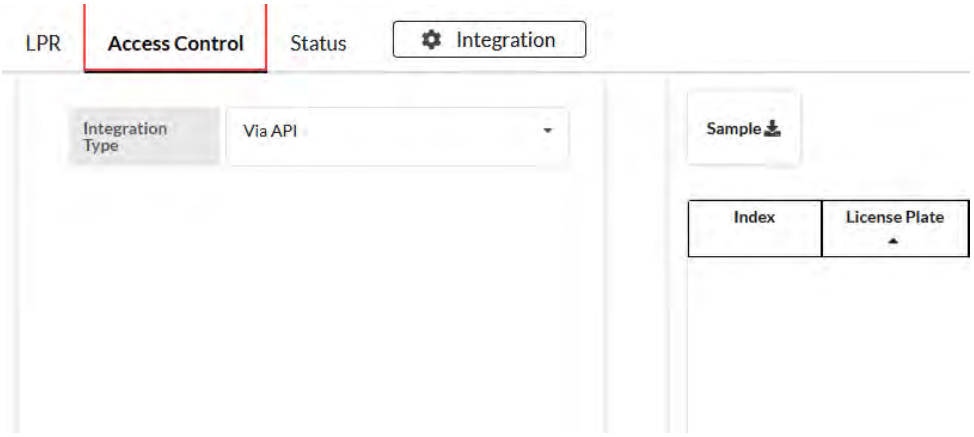


Figure: 100. Access Control Tab under LPR Settings

Note: Make sure that **Local ID** is enabled for access control in **Camera Settings → Analytics**. For more information, see Step 2 in Enabling LPR.

Camera Positioning For access Control

Camera positioning is very important for access control. In the following sections there are recommendations for various capture methods.

Front License Plate Capture

Figure: 101. shows front license plate capture in the LPR system.

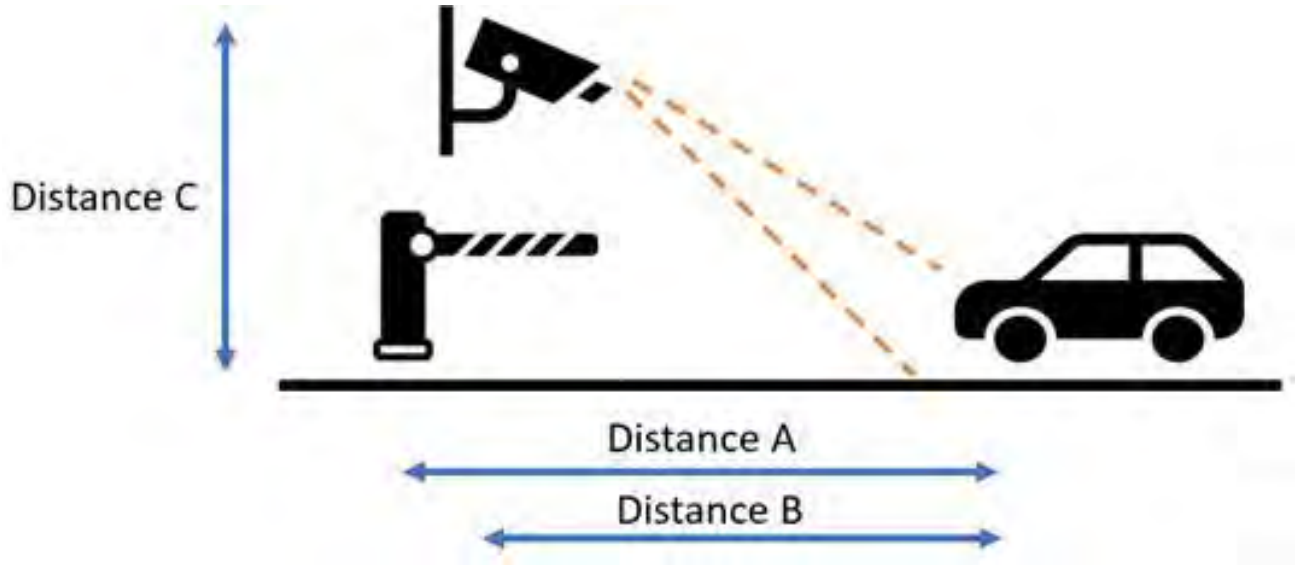


Figure: 101. Front License Plate Capture

Note: Always keep in mind that the barrier should not occlude license plate capture, and best if the camera is ahead of the barrier.

- **Distance A** – The distance between the barriers to the LPR imaging area. The distance is best kept between 6–12 feet (2–4 meters). This is to ensure that vehicle triggers are sent to the barrier promptly so it opens as the vehicle approaches. No space is left to allow for unauthorized vehicle access.
- **Distance B** – The distance between the camera and the LPR imaging area. For Gate Access Control, the distance is best kept between 6–12 feet (2–4 meters). Access control demands high accuracy, which is only possible if plates are imaged best for LPR. A shorter distance allows for better imaging at night as the IR power can best illuminate nearby plates.

- **Distance C** – The height of camera installation. For Gate Access Control, it is best if cameras are positioned between 4–8 feet (1.5–2 meters). The camera should be angled down approximately 30° to avoid direct sunlight.

Rear License Plate Capture

Figure: 102. shows rear licensee plate capture in the LPR system.

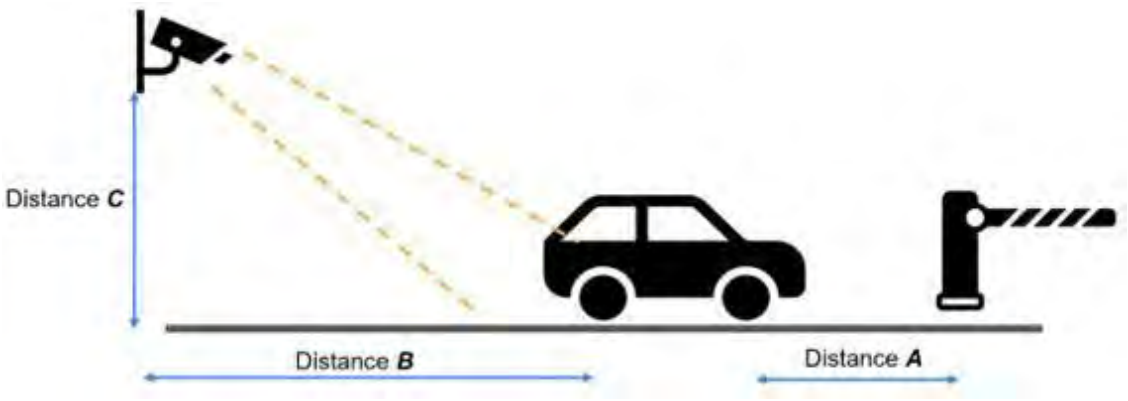


Figure: 102. Rear License Plate Capture

- **Distance A** – The distance between the barriers to the LPR imaging area. The distance is best kept between 20–26 feet (6–8 meters). This is to ensure that vehicle triggers are sent to the barrier promptly so it opens as the vehicle approaches. No space is left to allow for unauthorized vehicle access. Vehicles in different countries usually have a different length, so the recommended distance from the barrier to the imaging area is 3 feet (1 meter) more than the longest vehicles that might enter the site.
- **Distance B** – The distance between the camera and the LPR imaging area. For Gate Access Control, the distance is best kept between 9–15 feet (3–5 meters). Access control demands high accuracy, which is only possible if plates are imaged best for LPR. A shorter distance allows for better imaging at night as the IR power can best illuminate nearby plates.
- **Distance C** – The height of camera installation. For Gate Access Control, it is best if cameras are positioned 4–9 feet (1.5–3 meters), or if side-mounted, 8–10 feet (2.5–3 meters). The camera should be angled down approximately 30° to avoid direct sunlight.

Brivo Integration

The section explains the physical connection between the Mobotix Bridge and the Brivo panel, and how to configure the LPR on the Mobotix LPR side.
To integrate the LPR with the Brivo panel, do the following

1. Insert the USB to RS485 converter to the USB port of the bridge and complete the wiring. See Figure: 103. .

Figure: 103. Connection between the Mobotix Bridge to the Brivo Panel using an USB to RS485 converter

2. Make sure that you use the right cable (a shielded twisted pair cable) to avoid lossless transmission.
3. (Optional) If required, you might need to connect a Backup Reader. See Figure: 104. .

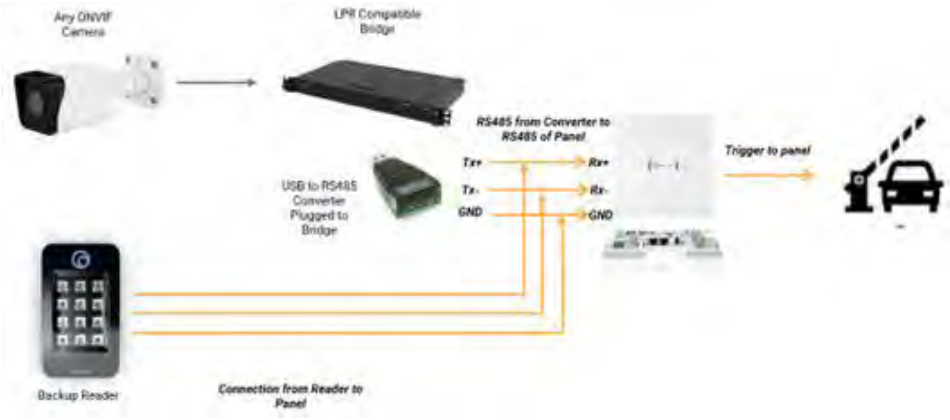


Figure: 104. Connection between the Mobotix Bridge to the Brivo Panel using an USB to RS485 converter and a Backup Reader

To enable Brivo Integration, go to **Camera Settings → Analytics → LPR → LPR Settings → Access Control** and select Brivo from the list in the **Integration Type** field, as shown in Figure: 105. .

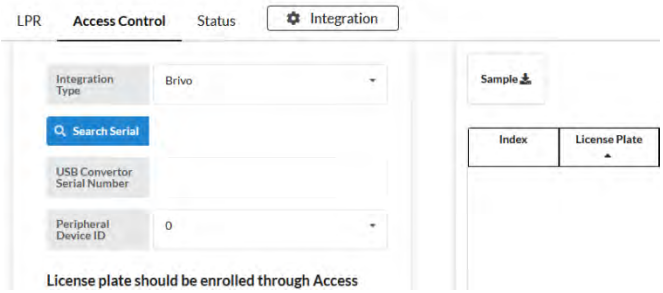


Figure: 105. Integration Type – Brivo

Available Brivo integration access controls are:

- **Search Serial**: Finds the serial numbers of the USB Converters attached to the bridge. Select the S/N of the USB Converter corresponding to the door (LPR Lane). See Figure: 106.
- **USB Converter Serial Number**: Displays serial number of components selected in **Search Serial**.

For troubleshooting, verify the serial number here.
If the USB Converter is interchanged or replaced with a new USB Converter, the user should change the serial number of the USB Converter attached to the camera during configuration.

- **Peripheral Device ID**: Indicates the following:
  - If no other reader is connected to the door
  - If any other reader is connected to the door

Figure: 106. Searching Serial Numbers

Moxa Integration

Communication with Moxa IOlogik e1214 module is over IP. The Moxa module is connected to the WAN port. The device has to be powered separately with the DC power adapter provided. See Figure: 107. .

Figure: 107. Moxa Connection to a Barrier/Shutter

In case of a connection to a light or a buzzer, the output from Moxa I/O to light is as shown in Figure: 108. .

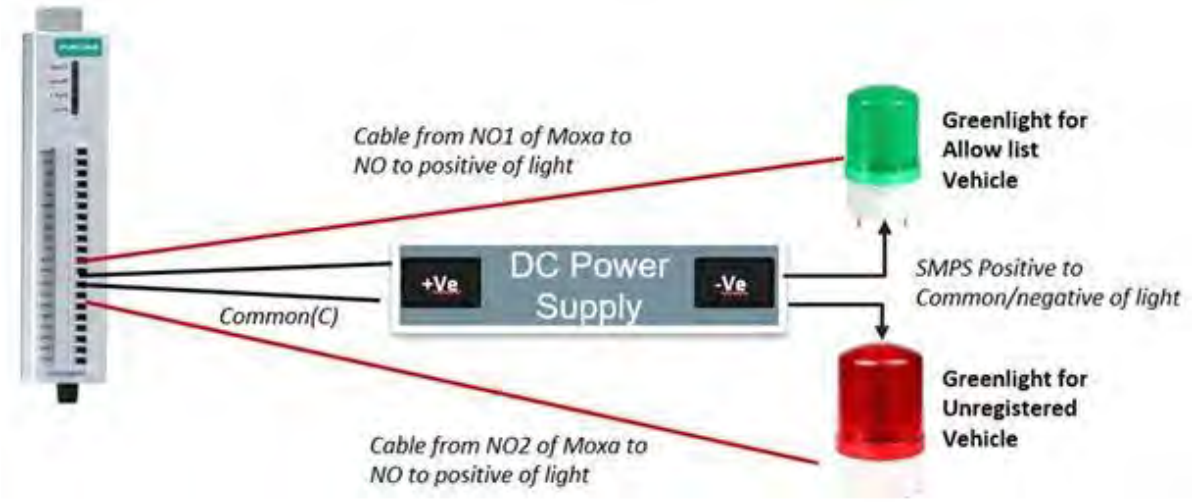


Figure: 108. Moxa Connection to a Light or Buzzer

Note: Make sure that the power supply and light are compatible before purchasing.
To enable Moxa Integration, go to **Camera Settings → Analytics → LPR → LPR Settings → Access Control** and select External I/O Moxa from the list in the field Integration Type, as shown in Figure: 109.

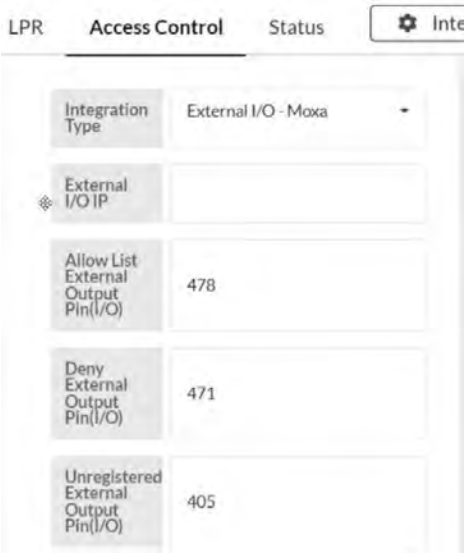


Figure: 109. Integration Type – Moxa

Available Moxa integration access controls are:

- **External I/O IP**: Provide the IP address of the Moxa I/O module here. Ensure that the Moxa I/O module is made to static IP to avoid the IP getting changed in the future.
- **Allow List External Output Pin(I/O)**: Provide the PIN information of Moxa.
- Deny List(Hotlist) External Output Pin(I/O): Provide the PIN information of Moxa.
- **Unregistered External Output (I/O)**: Provide the PIN information of Moxa.

Note: The database of vehicles can be uploaded or entered through the LPR Configuration UI, as shown in Figure: 110. .

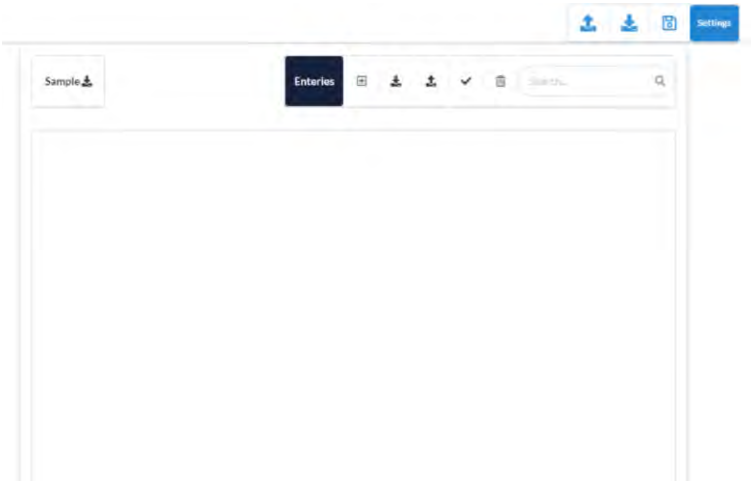


Figure: 110. LPR Configuration UI

Table 4. Camera Specifications for Optimal LPR Readings

Specification	Gate LPR 10 MPH (20 KM/H)	STREET LPR 30MPH (50 KM/H)	HIGHWAY LPR 70MPH (110 KM/H)
FPS	10	15	20
	Important: For an optimized performance, the FPS of the camera and the LPR processing FPS have to be the same.		
Day and Night Settings	Switching from day mode to night mode should be Auto. If the camera supports profile mode, then two profiles can be set, one for day time and one for night. If a monochrome image is acceptable, then night mode can be set permanently.		
Specification	Gate LPR 10 MPH (20 KM/H)	STREET LPR 30MPH (50 KM/H)	HIGHWAY LPR 70MPH (110 KM/H)
Maximum Exposure/ Shutter	1/250 If motion blur is observed, this can be changed to 1/ 500.	1/500 – 1/1000 Depends on motion blur. Shutter can be set to 1/1000 to prevent motion blur.	1/1000 - 1/2000 Depends on motion blur. Shutter can be set to 1/2000 to prevent motion blur.
	Note: If plates are saturated, you may reduce shutter speed.		

Specification	Gate LPR 10 MPH (20 KM/H)	STREET LPR 30MPH (50 KM/H)	HIGHWAY LPR 70MPH (110 KM/H)
HLC	Turned on		
Gain	Needs to be kept below 10% to minimize noise in the image. Different cameras have different settings, so you may need to adjust the Gain to have proper imaging.		
IR Power	Set to **Full**. It is always advised to keep IR power to maximum and reduce gain.		

Testing the Clarity of the License Plate Image

Follow the steps below to make sure you have the correct setup.
Note: You should perform these steps in both day and night environments.

1. Park a vehicle in the camera's view and adjust the settings as described in Enabling LPR.
2. Adjust the settings to have the optimal image quality.

   Note: Exposure may be limited as mentioned in Table 4.
3. Drive the vehicle at the maximum speed expected at the site and make sure there is no motion blur.
4. Adjust the gain as required to have clear images of the plates.
5. Verify the results for the next 24 hours, and adjust the settings as needed to make sure that all plates are clearly visible.

Vehicle Surveillance Package (VSP)

The Mobotix Cloud VMS Vehicle Surveillance Package (VSP) takes traditional License Plate Recognition (LPR) and adds analytic features such as marking tags as allowed or denied, watchlisting, and search. This package combines on-camera LPR tools (from supported devices) with the analytic power included in the Mobotix Bridges and CMVRs, then uses the cloud to make the resulting information available anywhere with an internet connection, via the VMS.

VSP is only available on Enterprise and Professional editions of the VMS. It is primarily used by resellers and admins rather than end users.

Summary

The VSP Summary page provides an overview of the Vehicle Surveillance Package activity on the account, starting with a high-level summation of all license plate reads, then showing the most recent alerts, and detected plates.
See Figure: 111. for an example VSP Summary Page.

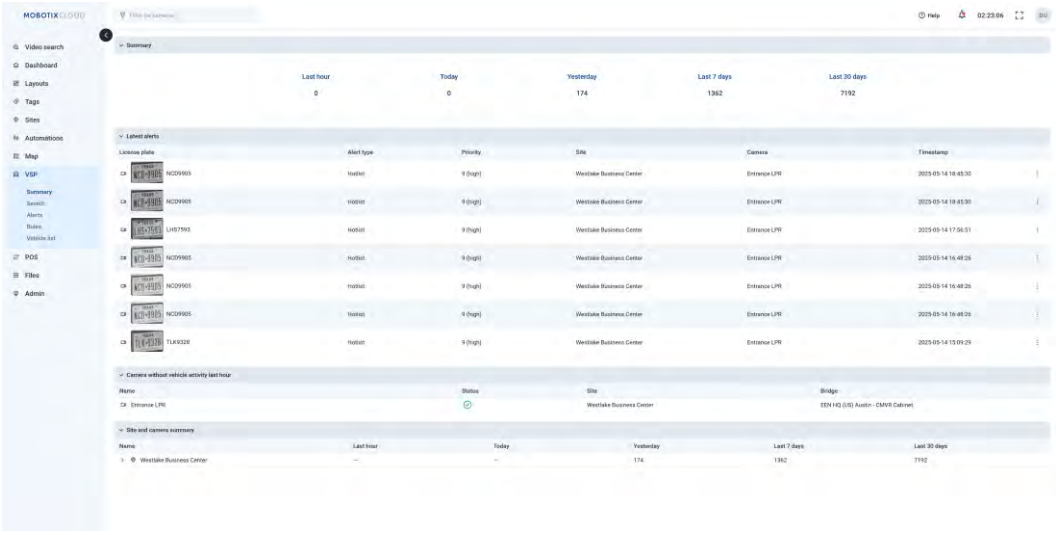


Figure: 111. VSP Summary Page

Summary

The **Summary** page shows the number of plates detected in several time periods: last hour, today, month to date, year to date, total. These fields cannot be configured.

Latest Alerts

The five most recent alerts are displayed here. More alerts can be viewed and filtered by clicking the **Alerts** link at the top of the **Summary** page. Alerts are governed by rules that can be created, modified, or deleted on the **Rules** page, accessible at the top of the **Summary** page.

Cameras without Vehicle Activity Last Hour

This section displays the cameras that have not detected any vehicle activity for the last hour. It includes the Camera Name, Status, Location, and Bridge.

Location and Camera Summary

This section displays the license plate reads on a per camera basis, showing the statistics for each one (reads in the Last Hour, Today, Yesterday, Last 7 Days, and Last 30 Days). Using these numbers, over or under-active cameras can be identified in order to determine any necessary remediation.

Search

Vehicle Surveillance Package records all plates detected by a compatible camera in the VMS. This might lead to the accumulation of a larger number of license plates to skim through. License plate search makes it easier to find the car you're looking for in the database.
You can search certain areas, partial plates, or a specific plate at any site where you have a compatible camera. See Figure: 112. for an example VSP Search page.

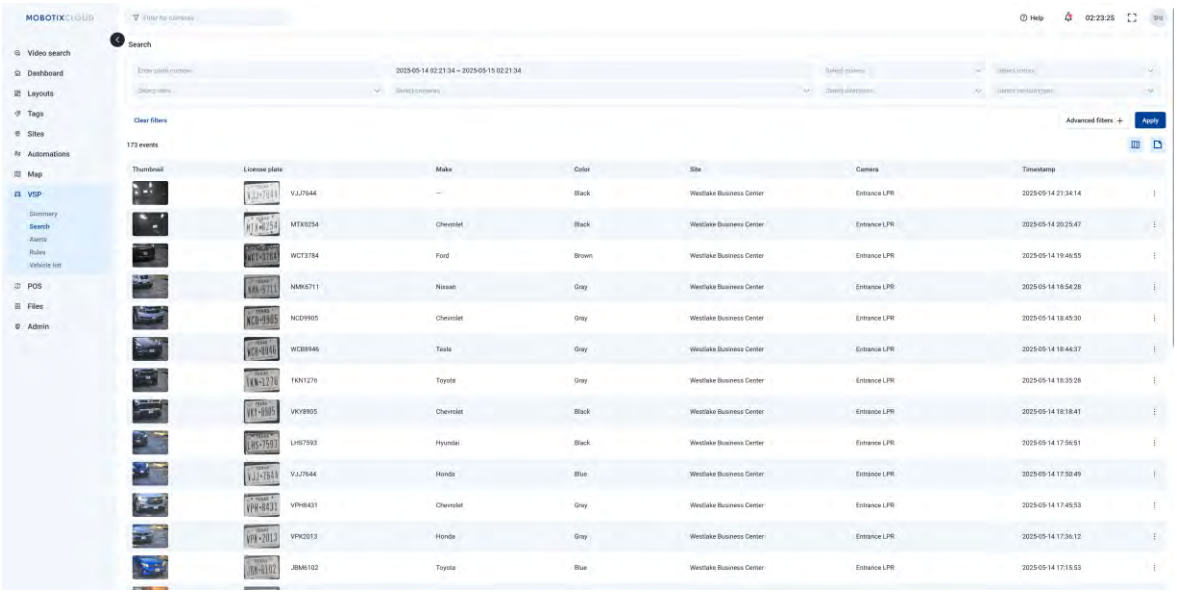


Figure: 112. VSP Search Page

Search Parameters

Use the following fields to refine the search parameters for the user:

- **License Plate** – This field accepts any alpha-numeric set of characters that pertain to the license plate sought. Fuzzy search is also supported. Users can introduce an asterisk (*) in place of an unknown character.

  Example: To search for plate starting with AB, users can type AB* to find results for plates starting with AB. Similarly, to find plates ending in 23, users can search for *23 to find plates ending with 23.
  Fuzzy search also allows searching for specific characters. Search A*1*3 would return plates having characters A,1,& 3 in the given order.

- **Date Range** – Enter specific start and stop dates and times to filter results, or use predefined time periods (e.g. the current day, the previous day, the previous week, the current month, and the previous month).

- **Site** – Search for specific sites. This shows results from any compatible camera at the given site.

  Note: This requires the site to have been configured in the camera's settings within the VMS. Alternatively, **Any Site** can be selected to view results from all compatible cameras.

- **Camera** – Search for results from a specific camera, or from all compatible cameras.

Search Results

When clicking the search button, the map updates with license plates that match the search parameters, and a list of potential matches is displayed. Each potential match contains the following information:

- **Thumbnail** – A screenshot of the license plate as seen by the VMS. Click the thumbnail to open the History Browser to view the clip.

- **License Plate** – A cropped image of the license plate, skewed to display head-on, and the license plate value read by the camera.

  Note: There may be some discrepancies in these entries, most likely because of an improperly positioned camera. The camera should be positioned so that the vehicles are approaching head-on, and slowly.

- **Camera** – The name of the camera where the license plate was seen.
- **Site** – The name of the site where the license plate was seen.
- **Timestamp** – The date and time that the clip was taken.

  Note: The timestamp shown here is adjusted to the Timezone value set for the user in the VMS. When viewing the clip in the History Browser, the History Browser shows the timezone of the camera.
- **Actions** – The **Sites +/- 15 min** button repopulates the search results to all plates read at that site fifteen minutes before and after the time that plate was read.

Alerts

The License Plates Alerts page gives the user an opportunity to view a historical listing of all license-plate-related alerts received on the account, sorted by the time received. The alerts can also be filtered by a number of parameters to only view those related to the specific issue the user is investigating.
See Figure: 113. for an example VSP Alerts page.

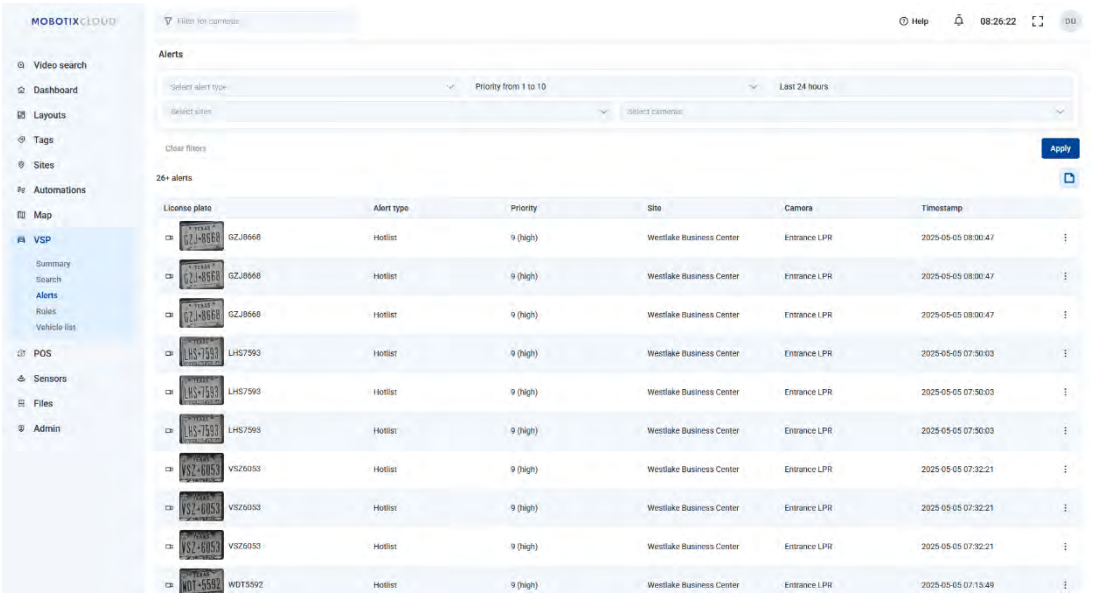


Figure: 113. VSP Alerts Page

Alert Parameters

The search form allows for any license plate alert to be searched and filtered. The following parameters can be specified.

- **Status** – Use this parameter to specify whether the displayed alerts are Active, Cleared, or All.
- **Date Range** – Specific start and stop days/times can be entered to filter results, or predefined time periods can be used (current day, previous day, previous week, current month, and previous month).
- **Type** – Alert types can be filtered by **Allow**, **Deny**, or **Watch**. Plates can be added to these types through Rules.
  - **Allow** – Plates that are allowed to enter the access point.
  - **Deny** – License plates that are denied access to the entry point.
  - **Watch** – Specific plates that entered or left the lot and were not scanned again for a certain amount of time, meaning they stayed in or out for too long.

- **Cleared By** – Alerts can be filtered by the specific user who cleared them, or **Any** can be selected to show all alerts.
- **License Plate** – This field accepts any alpha-numeric set of characters that pertain to the license plate sought. It is not case-sensitive and will work with any number of characters, allowing for partial or specific plates to be searched. Do not enter spaces between search items.
- **Site** – This field is used to specify a specific named site to search. This will show results from any compatible camera at that site. This requires the site to have been configured in the camera's settings within the VMS. Alternatively, **Any Site** can be selected to view results from all compatible cameras.

Alert Search Results

When the search button is clicked, the table below it will populate with the alerts that match the parameters selected. For each alert, the following information is displayed.

- **License Plate** – Displays the license plate that generated the alert.
- **Timestamp** – Reports the day and time the alert was generated.
- **Type** – Lists the alert as being **Whitelist**, **Blacklist**, or **Watchlist**. See the above section for details on these types.
- **Status** – Displays whether the alert is **Active** or **Cleared**.
- **Cleared By** – Lists the name of the user who cleared the alert.
- **Clear Reason** – Shows the reason for clearing the alert, as selected by the user who cleared it. Available selections are **Authorized**, **Incorrect**, or **Overridden**.
- **Cleared At** – Shows the timestamp for when the alert was cleared.
- **Site** – Reports the site where the alert occurred if the site has been defined in the camera's settings.
- **Actions** – Presents a button that will clear the alert with the reason selected by the user.

Rules

License Plate Rules dictate the alerts and notifications for the analytic. You can use these rules to notify certain people if a particular license plate is detected entering a garage, for example. The rules come in one of three varieties: **Allow**, **Deny**, and **Watch**.
See Figure: 114. for an example of a VSP Rules page.

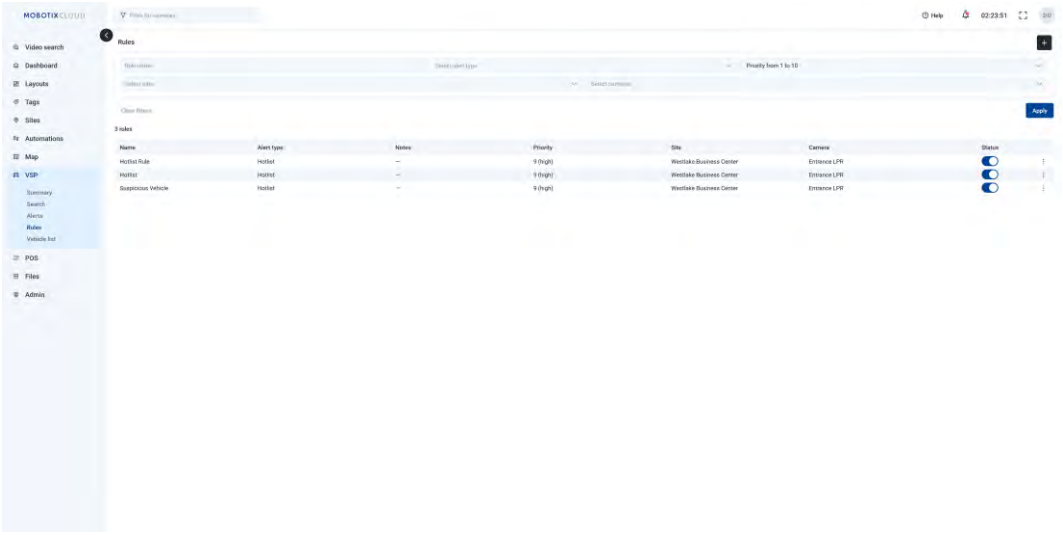


Figure: 114. VSP Rules Page

- **Allow** – License plates that are allowed to enter the access point. All license plates added to this list will be logged when they enter the area.
- **Deny** – License plates that are denied access to the entry point. Any license plate that is on this list and is detected by the compatible camera will generate an alert, notifying specified users that the plate approached the entry point.
- **Watch** – The watchlist allows for the tracking of a specific plate and keeps track of the time between readings. If the time is outside of a set limit, an alert is generated. The time limit can be specified as 15, 30, 45, 60, 75, 90, 105, or 120 minutes.

An example:
A license plate on the list is detected exiting the lot; this begins a timer and creates an alert in the background (no notification is sent yet).
The timer runs until the license plate is detected again, presumably when it is returning to the lot. If the time is within a specified limit, the alert will be automatically cleared.
If the time is outside the limit, a notification will be generated by the alert, notifying all those on the account of the vehicle's status.
Or, if the vehicle has not returned by the end of the set time limit, notifications are sent.

Rule Parameters

The following parameters are required to create a new rule. Enter the value for each field, then click **Save** to create the new rule.

- **License Plate** – This field accepts any alpha-numeric set of characters that pertain to the license plate sought. It is not case-sensitive and will work with any number of characters, allowing for partial or specific plates to be added. Only one entry can be made at a time. Do not include spaces in the search parameters.
- **Site** – Use this field to specify a specific named site to search. This will show results from any compatible camera at that site. This requires the site to have been configured in the camera's settings within the VMS. Alternatively, Any Site can be selected to view results from all compatible cameras.
- **Type** – This can be set as Allow, Deny, or Watch as described in Alert Parameters.
- **Recipients** – This field defines which users are notified when the rule is triggered.

A list of all rules on the account is also displayed on the VSP Rules page. This table shows the license plate, site, type, when the rule was created, recipients, and any action required. Use the **List** field to dictate how many rules are shown per page.

Vehicle List

The VSP Vehicle List lets you search for create lists that search for specific vehicles according to parameters that you set.

Vehicle List Parameters

Use the selections in this section to set up search parameters as follows:

- **Vehicle List Name** – Enter a vehicle list name.
- **License Plate** – Add a license plate to a vehicle list.
- **Select Sites** – Select a site to search for a vehicle.
- **Select Cameras** – Select cameras to search for a vehicle.

Click **Apply** to add a new vehicle to your list. The results appear below.

Add Vehicle List

Click the plus icon at the top right of the Vehicle List window to create a new vehicle list.

- **List Name** – Add a new vehicle list name
- **Site**– Select a site or site for your vehicle list. You may select all sites on your VMS.
- **Cameras** – Select the cameras you want to detect the vehicles on your list. You may select all cameras on your VMS.
- **Status** – Toggle on if you want the vehicle's status to appear on the results.

An example:

- A license plate on the list is detected exiting the lot; this begins a timer and creates an alert in the background (no notification is sent yet).
- The timer runs until the license plate is detected again, presumably when it is returning to the lot.
- If the time is within a specified limit, the alert will be automatically cleared.
- If the time is outside the limit, a notification will be generated by the alert, notifying all those on the account of the vehicle's status.
- Or, if the vehicle has not returned by the end of the set time limit, notifications are sent.

Rule Parameters

The following parameters are required to create a new rule. Enter the value for each field, then click Save to create the new rule.
Rule Name – Enter a Rule name.
Select Alert Type – Alert types can be filtered by Allow, Deny, or Watch. Plates can be added to these types through Rules.

- **Allow** – Plates that are allowed to enter the access point.
- **Deny** – License plates that are denied access to the entry point.
- **Watch** – Specific plates that entered or left the lot and were not scanned again for a certain amount of time, meaning they stayed in or out for too long.

Priority – Use this parameter to specify the alert priority from 1 to 10.
Select Cameras – Use this parameter to search by a specific camera on your system.
Select Sites – Use this field to specify a specific named site to search. This will show results from any compatible camera at that site. This requires the site to have been configured in the camera's settings within the VMS. Alternatively, **Any Site** can be selected to view results from all compatible cameras.

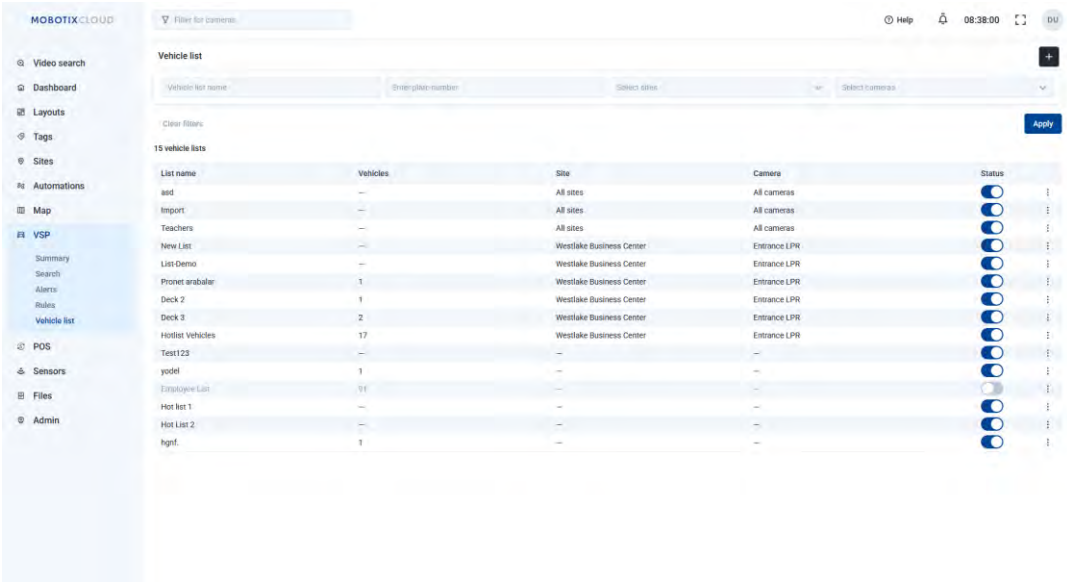


Figure: 115. VSP Vehicle List.

Video Search

Use the information in this chapter to improve your search results in the VMS.

Smart Video Search

Smart video search in the VMS lets you use natural language to quickly and easily find people, vehicles, or objects throughout your camera infrastructure. See Figure: 116. for an example of the Video Search page in the VMS.

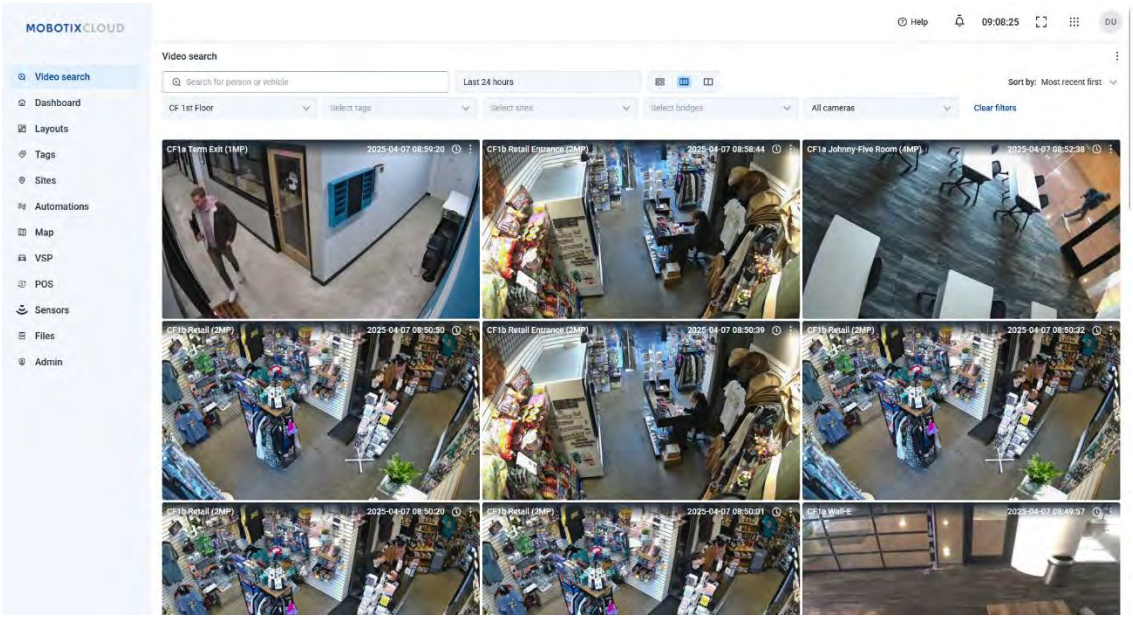


Figure: 116. Video Search

Configuration for Optimal Results

Smart Video Search works on both bridges and CMVRs. When motion is detected, the bridge sends key images to the VMS. These key images are processed by AI models in real-time to identify vehicles/people/objects.
It is important to make sure that CMVRs are not set to “Minimum Bandwidth mode” in order to receive key images for processing.
The recommended preview video resolution is 640x360.

A Note on Search Results

Smart Video Search utilizes a “wide search” to ensure that you do not miss anything that meets your search query. This means that the system may incorrectly label a few shirt colors, car makes, etc. This is to make sure that nothing that does match your query is missed. We think it’s better to have a few extra results to sift through rather than miss any result that matches what you’re looking for.

Button Overview

- Search for person or vehicle Enter search terms here. Can be broad (person) or specific (man in red shirt). You can search for people, vehicles, or objects, depending on the VMS Edition.
- Enlarge the Key Images.
- Cameras Click this button to bring up filters for cameras that are included in the search results. These filters include individual cameras, tags, regions of interests, and, in Pro/Enterprise Editions only, Groups and Sites. Each filter allows you to select multiple individual entries or all.

- Time Click this button to change the day, time, and time intervals that are being searched. By default, search will automatically use the previous 24 hours. You can change the day of the search and the 24 hour period that is being searched, or change the search window to one, four, or twelve hours.
- Person Click this button to search for people. After you click the button, you can access the options below to fine-tune your search by clicking the Person drop-down button.
  - **Trash Can**: Remove the person filter from your search.
  - **Gender**: Specify whether you're looking for Female, Male, or Any.
  - **Upper Body Clothing Color**: Choose the color of the shirt, jacket, or other upper body clothing.
  - **Lower Body Clothing Color**: Select the color of pants, skirt, etc. for lower body clothing.
- Vehicle Click this button to do a general search for vehicles. After clicking this, you can click the newly displayed Vehicle drop-down button to display additional filters.
- Trash Can: Remove the vehicle filter from your search.
- Class: Select whether you want to search for buses, cars, motorbikes, trucks, or any.
- Color: Specify the color of the vehicle to search for.
- Make: Choose the manufacturer of the vehicle you want to search.

Search Results

When you search any terms, or apply any filters, the search results will automatically update. Each camera that has any result in the selected time period will be displayed as shown in Figure: 117..

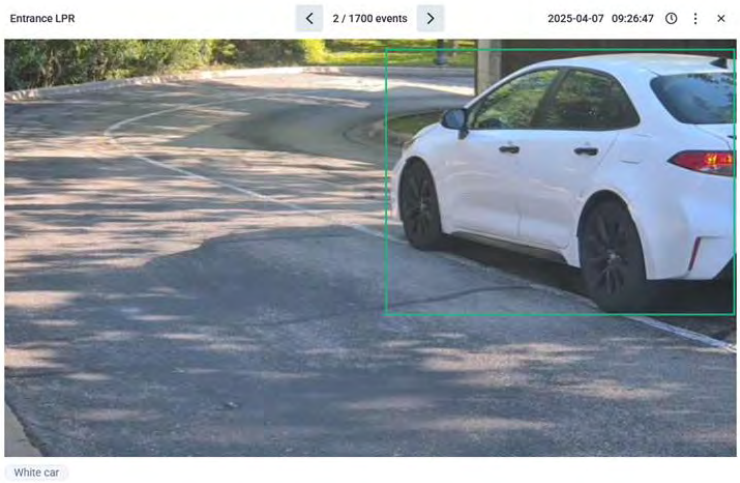


Figure: 117. Search Results

Each of these camera results will show the following:

- Time of the latest result, shown in the top-left corner of the video preview image.
- Click this icon to open the history browser at the time of the result shown in the video preview image.
- Click this icon to open a menu with additional options.

  - Find Similar Images: Click this to search for other images that match the description.
  - Incident Explorer: Click to open the Incident Explorer to dive deeper into the Video Search feature. This feature is only available with Pro and Enterprise Editions. More details below.
  - Live View: Open the camera's live view in a new window.
- Click the video preview image to enlarge the image and look at the metadata.
- 1460 The count shows you the total number of search results in the time period.
-  The series of boxes at the bottom of the image is called the density map. This breaks the time period into equal time frames and gives you an idea of how many times the person, vehicle, or object you searched for appears in that time frame. The darker the blue, the more times the person or thing was detected. More information on the density map below.

Density Map

The density map breaks the search time period into equal blocks of time and shows you how many results for your search occurred in that time block. If you change the time filter to search a smaller time range, the density map time blocks will represent a shorter amount of time. The actual numbers are broken down as:

- 24 Hour Time Period: 1 hour blocks
- 12 Hour Time Period: 30 minute blocks
- 4 Hour Time Period: 10 minute blocks
- 1 Hour Time Period: Approximately 2 minute blocks

The time blocks are color coded to indicate the number of search results for that block.

- - Zero results
- - One result
- - Two to four results
- - Five or more results

You can click on a time block to view images of the search results for that time. Navigation arrows and the total number of results will appear in the bottom-right corner of the image, as shown below. Click the arrows to cycle through the results. See Figure: 118. .

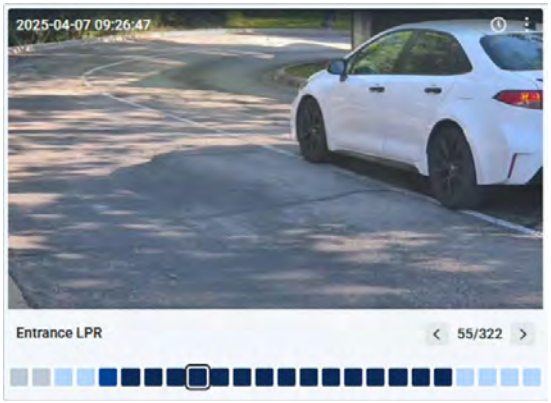


Figure: 118. Search Results for a Time

Incident Explorer (Pro/Enterprise Editions Only)

The Incident Explorer gives you additional capabilities to analyze your search results and expand them to track a person, video, or object throughout your camera infrastructure. See Figure: 119. .

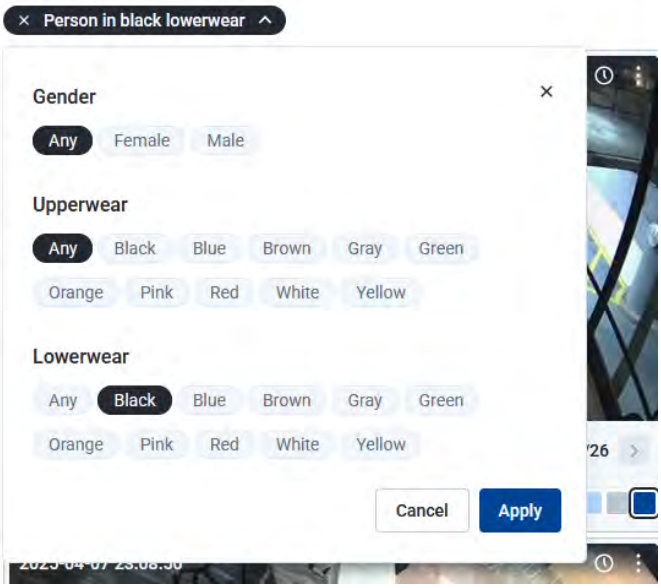


Figure: 119. Incident Explore Homer

Incident Explorer Navigation

See Figure: 120. for an example of the Incident Explorer navigation window.

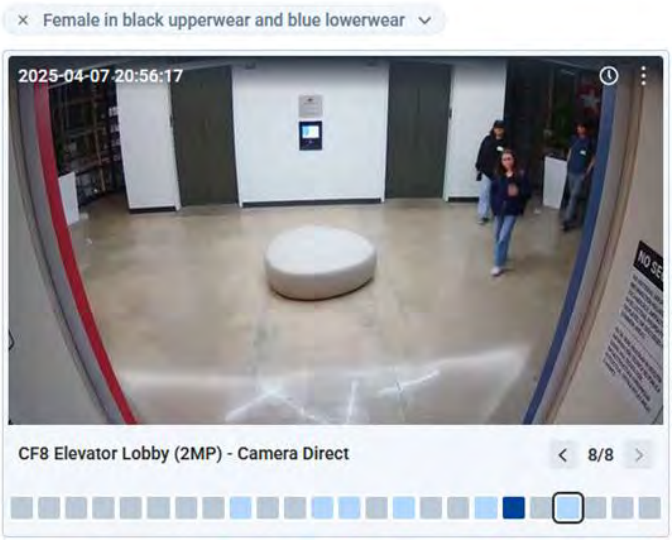
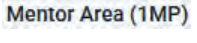
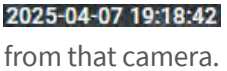


Figure: 120. Incident Explorer Navigation

The Incident Explorer Navigation tools are described in the following section.

- 

When you open the Incident Explorer, it opens a new tab. Click Video search to return to your search query. You can open multiple Incident Explorer instances and cycle through them in the tabs.
- 

Click on the camera name to look at all images from that camera.
- 

Click on a specific time to display all images in that time window from that camera.
- 

This shows the name of the camera you are viewing and the date and time of the image shown.

-  Click this icon to open a drop-down menu that will take you to the live view of the camera or the history browser at that timestamp.
-  Click these arrows to cycle through the search results in this time block. The image data section will update with what was detected in that frame.
-  Cycle through each frame of the video in the time block.
- Image Data - The Image data section displays what video search detected in the frame. You can click on the text to highlight the detection box around the person, vehicle, or object. Click the magnifying glass in the Image data section to run a new search for that description.
- 

The time bar and density map shows you how many detections occurred at each time block. The time bar helps you to get an idea of the time it occurred.

Search Suspicious Person/Vehicle Across Cameras

The Smart Video Search Incident Explorer also makes it easy to track a person/vehicle across all of your cameras. Whenever a detection is made, a unique re-identification ID (reID) is generated for it. This reID is then applied to all instances of that person/vehicle in your VMS.
To track everywhere that person/vehicle has been, click the detection box around the person/vehicle to highlight it. Then, simply click the magnifying glass that appears above the detection box. This will change to the Video Search tab and search for that person's/vehicle's reID, letting you see everywhere it's been caught on your video.

Blocking Unused Areas From Video Search

Some of your cameras may have certain areas that you aren't interested in searching. For example, there could be a window with vehicles driving by outside. You can use motion regions of interest to create a motion mask for that area.

1. Navigate to the Dashboard and find the camera that you need to create a mask for.
2. Click the three dot icon ⋮ next to the camera to bring up **Camera Settings**.
3. Click the **Motion** tab.
4. Click the **+** button to create a new motion region.
5. In this region, adjust the sensitivity to 0.

Now, any motion that occurs in this region will not generate Video Search results.

Files

Archive

Videos in the Mobotix Cloud VMS can be added to the Archive for permanent storage or compiled and uploaded to the Downloads section for downloading to a local device. After downloading, videos can be viewed or shared without internet connection. Before a video can be archived or downloaded, you need to create a clip.
Important: Archived clips can be downloaded and are kept for as long as needed, but clips saved to download expire.

Creating a Clip

Clips can be created in the History Browser.
After reviewing the video and having determined what part you want to save as a clip, do the following:

1. Navigate to the History Browser of the Camera.
2. Click on the  Export button in the bottom right corner.
3. Select the Time Range for which you want to create the clip.
4. Now select the Destination from **Downloads** and **Archive** and click on the Export Button. See Figure: 121.

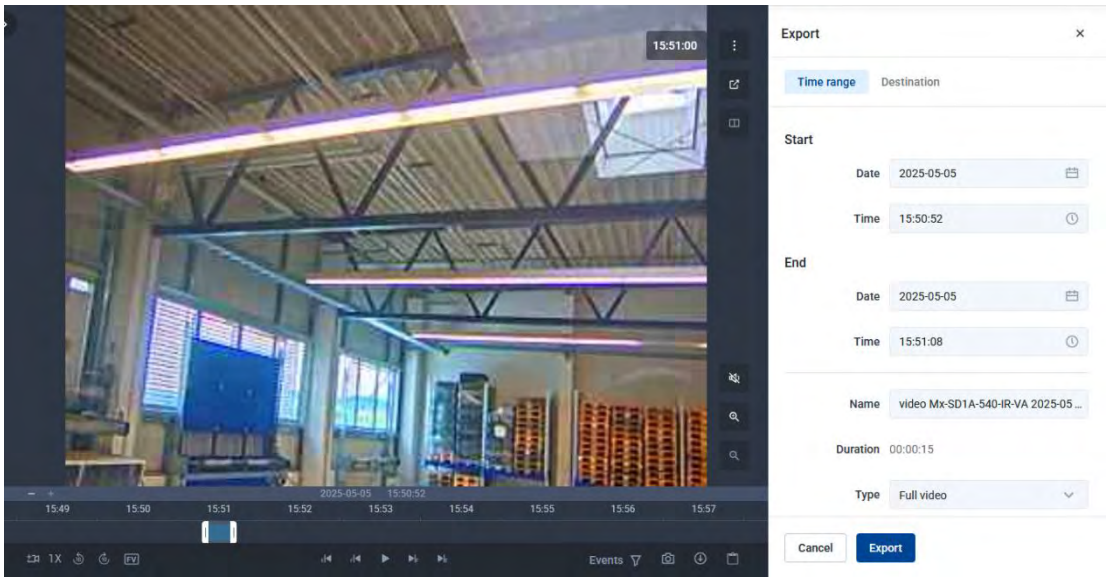


Figure: 121. Creating a Clip

Archiving Video

The Archive allows you to save and store video clips outside of the normal duration of cloud retention. After a clip is archived, it can be viewed directly in the Archive or downloaded to the local device.
The Archive also allows you to provide video clips of a crime or incident to law enforcement or first responders without having to create an account for them. This makes it easier for external users to view the video clip, allowing them to access it directly from their email rather than having to log in to an account and navigate to the archived video.

Navigate the Archive and Share Clips

The Archive is represented in directory form where folders and files can be organized and optionally shared via a secure link to anyone, without requiring a user login. The secure links can be revoked anytime or set to expire on a specific date. Any files and folders that are shared are clearly marked within the Archive. See Figure: 122. .

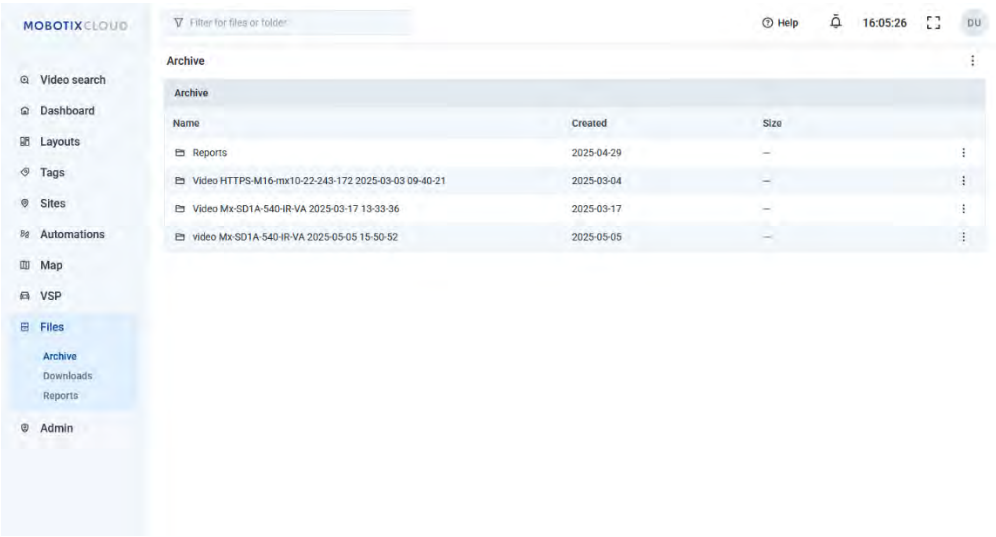


Figure: 122. Navigating the Archive

The Archive feature makes organizing and saving clips quick and easy and allows you to include additional important and relevant documents with the archived video. You can attach a police or incident report with the archived video and store the documents and videos for up to one year without being charged for extra storage.
Also, when providing an archived video link to a third party, an expiration date can be set on the link so that access to the video is revoked after a set time frame. This way, a third party will have access to a video during the period when it is necessary and then access will be removed when the video is no longer needed or relevant to the third party, providing VMS users with complete control over who can view archived video and when.

Using the Archive

You have the following functions available within the Archive. Click on the three dots next to the Archive folder to show the funtions:

- **Add Folder**: Click on the three dots in the upper left corner and click on Add Folder to create a new folder.
- **Trash**: Click on the three dots in the upper left corner and click on Trash to access the recently deleted Archives
- **Details** – Access the details of each archived file by clicking the three dots icon on the right side of the file.
  - **Info** - This tab provides the folder name and the file's date and timestamp. You can add notes and tags to a file.
  - **Share** - This tab allows you to to get a shareable Link, add password protection if desired, add an optional expiration date, and records the date the file was shared.
- **Copy Link** - Get a shareable link immediately by clicking the three dots icon on the right side of the file and choosing Copy Link.
- **Link Share/Unshare** - Click the three dots icon on the right side of the file and click this to start/stop sharing the file.
- **Move** - Click the three dots icon on the right side of the file and click this to move the file to a different Archive folder. You can also create a new Archive folder and move the file there.
- **Copy** - Click the three dots icon on the right side of the file and click this to copy the file to a different Archive folder. You can also create a new Archive folder and copy the file there.

- **Download** - Access the ability to download a video to your system by clicking the three dots icon on the right side of the clip.
- Delete Folder - Click the three dots icon on the right side of the file and click this to delete the file from the Archive.

Archive Permissions

VMS users can be granted read-only access to the Archive or full editing rights.

1. Click Users on the left-side menu, then click the three dot icon ⋮ next to the desired user.
2. Click the Permissions tab, then the drop-down arrow next to Archive.
3. Select whether the user can only View the Archive, has full Edit access to the Archive, or cannot access the Archive at all (make sure neither box is checked). A user with only View permission cannot save clips to the Archive. See Figure: 123. .

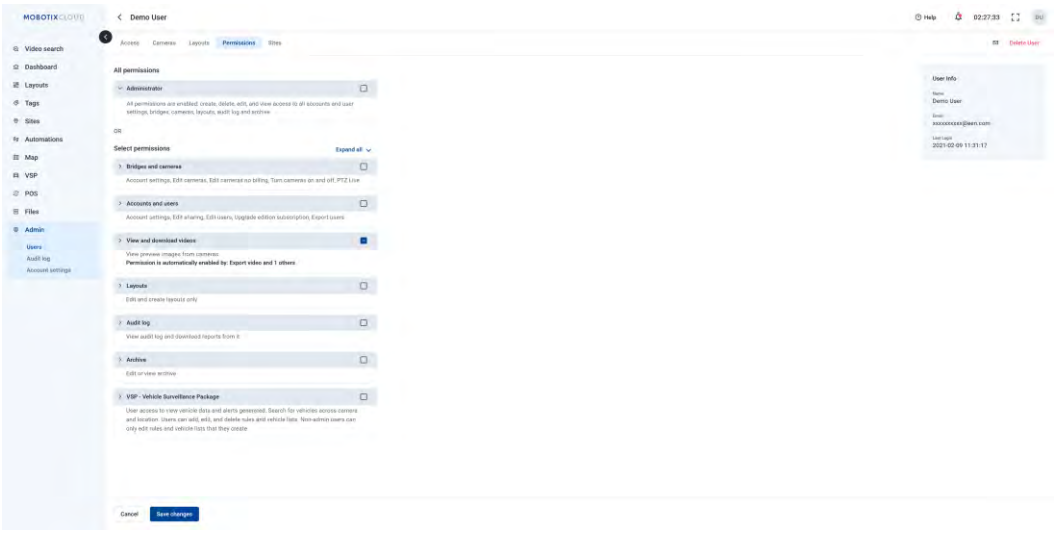


Figure: 123. Setting Archive Permissions

Downloads

When you click **Download** after creating a clip, a window pops up immediately with information that the download is being prepared, and it will estimate the completion time.
To access your downloadable clips, click **Downloads** on the left navigation pane.

- **Name** - This column shows the name of the downloaded file.
- **Download Availability** - This column shows you when the download expires or the date it expired. When a download is created, it is available for 14 days.

  Note: A download might contain multiple clips in a zipped file. If a recording is interrupted, the download will stop and restart with a new clip when recording begins again.
- **Created** - This column shows the date and time the download was created. Use the arrow to sort the clips from oldest to newest or vice versa.
- **Size**: The size of the download able file.
- **Details** - Access the details of each download by clicking the three dots icon on the right side of the clip. The details provided are the camera name, the clip's date and timestamp, and the file size. It also tells you if an expired download is out of its retention period.
- **Download** - Access the ability to download a video to your system by clicking the three dots icon on the right side of the clip.

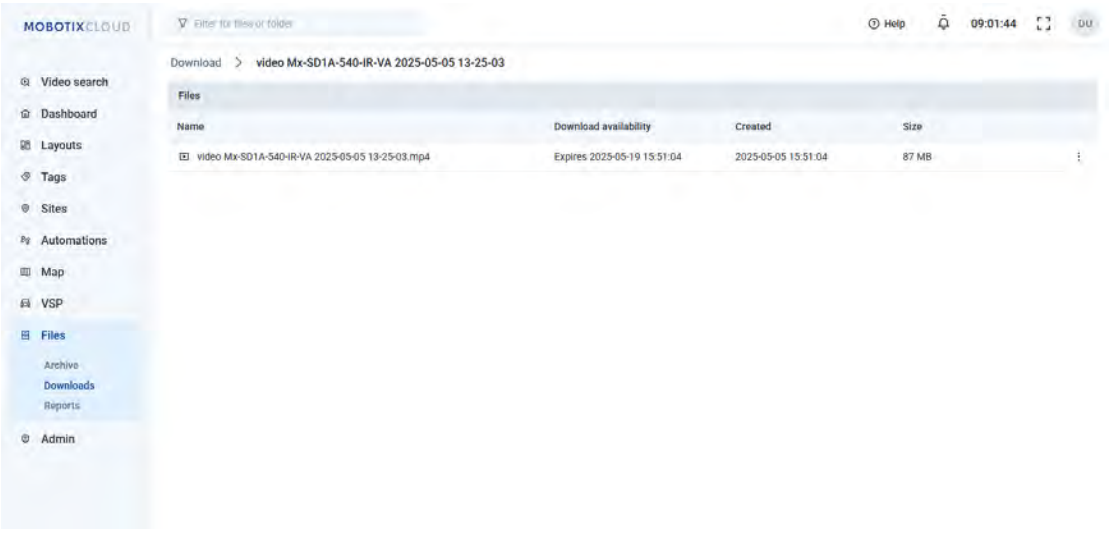


Figure: 124. Downloads

Reports

You can create various reports in the VMS and download them as HTML or CSV files. See Figure: 125. .

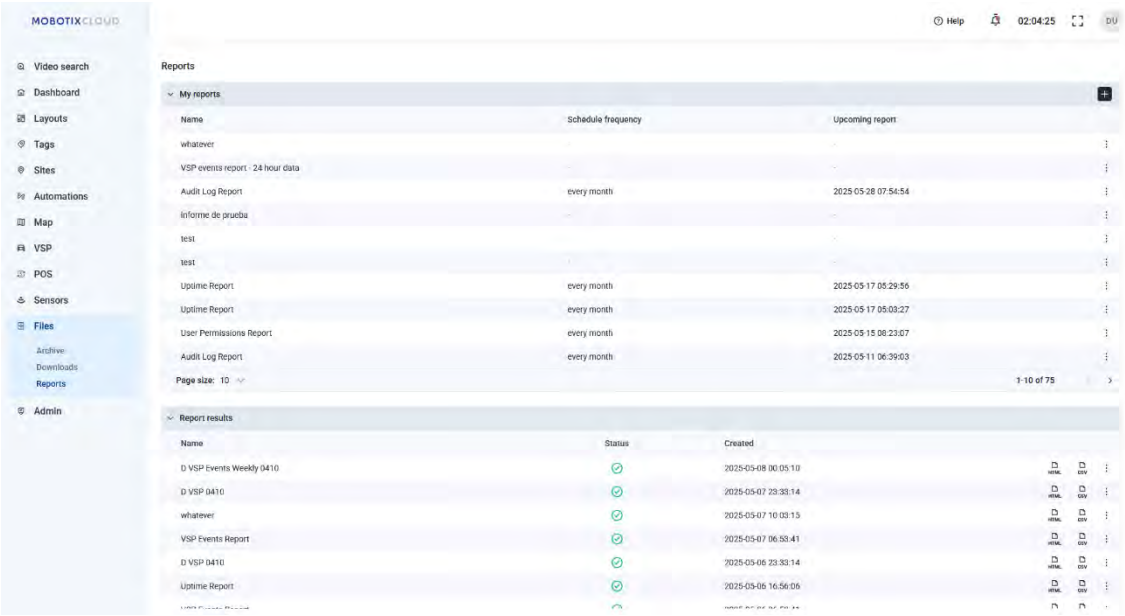


Figure: 125. Reports

Viewing Reports

The **My Reports** section provides a list of all the user-created reports to be run on the VMS. This section has three descriptive (non-editable) fields:

- Name: The name of the report.
- Schedule Frequency: The frequency the report will be run. This can be set to every day, every week, or every month.
- Upcoming Report: The next date and time that the report will be run.

Click the three dots icon ⋮ on the right side of the section to access the following controls:

- Edit: Click to change the report settings.
- Run Now: Click to run the report immediately.
- Delete: Click to delete the report.

Report Results

This section contains the results of the reports that have been run on the system.

- Name: The name of the report.
- Status: A green check mark indicates that the report ran successfully. A red X indicates that the report failed to run.
- Created: The date and time that the report was created.
- Delete: Click to delete the report results. Reports are available for download as HTML or CSV files.

Note: Fields are occasionally missing from the report results due to API inconsistencies.

Creating Reports

To create a new report, click the **Create Reports** button in the top right of the Reports window. The available report settings are:

- **Report Template**: Select one of the following Report Templates:
  - **User Permissions Report**: Contains a list of users and their permissions inside the VMS.
  - **Camera Status Report**: Contains the status information for each camera, including the serial number and whether the camera is online or offline.
  - **Camera List Report**: Contains a list of all the cameras on the system, each camera's MAC address and firmware version. This report is used for inventory purposes.
  - **Bridge Status Report**: Contains the status information for each bridge, including the serial number and whether the bridge is online or offline.
  - **Bridge List Report**: Contains a list of all the bridges on the system, each bridge's MAC address, and how many cameras are attached to the bridge.
- **Report Name**: Enter a name for the report that will appear on the main Reports window.
- **Schedule Report**: Toggle this switch to On if you want to schedule a report. If you want to schedule a reports, enter the following:
- **Start Day**: Enter the day to start the report schedule.
- **Start Time**: Enter the time to start the report.
- **Frequency**: Enter the frequency to run the report: Daily, Weekly, or Monthly.

Choose **Cancel** to close the window without making any changes or **Create Report** to save the new report.

Editing Reports

Use the settings described below to edit a report.

- **Report Template**: Displays the report template type.

  Note: You cannot edit the report templates. The list below provides descriptions of the available report templates.
  - **User Permissions Report:** Contains a list of users and their permissions inside the VMS.
  - **Camera Status Report**: Contains the status information for each camera, including the serial number and whether the camera is online or offline.

  - **Camera List Report:** Contains a list of all the cameras on the system, each camera's MAC address and firmware version. This report is used for inventory purposes.
  - **Bridge Status Report**: Contains the status information for each bridge, including the serial number and whether the bridge is online or offline.
  - **Bridge List Report**: Contains a list of all the bridges on the system, each bridge's MAC address, and how many cameras are attached to the bridge.
- **Report Name**: Enter a new name for the report that will appear on the main **Reports** window.
- **Schedule Report**: Toggle this switch to On if you want to schedule a report. If you want to schedule a reports, enter the following:
  - **Start Day**: Enter the day to start the report schedule.
  - **Start Time**: Enter the time to start the report.
  - **Frequency**: Enter the frequency to run the report: Daily, Weekly, or Monthly.

Choose **Cancel** to close the window without making any changes or **Update Report** to save the new report settings.

Managing Users

User management options are available for anyone with admin or user admin permissions.

Users

The Users window of the VMS allows you to manage user access, roles, and permissions. See Figure: 126. .

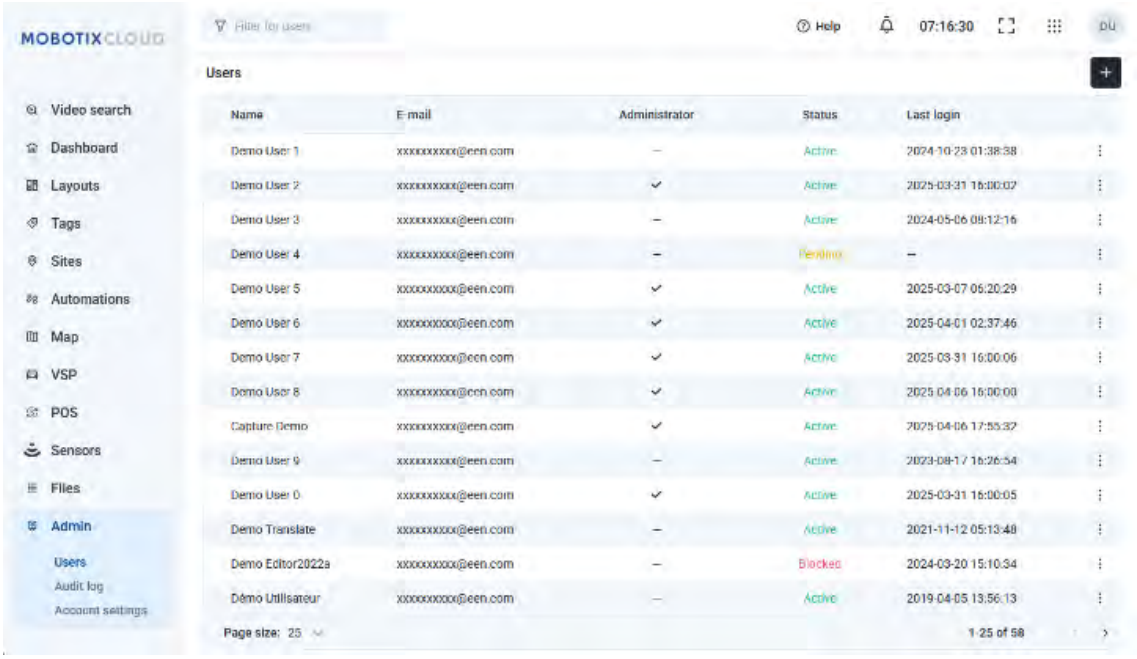


Figure: 126. Users

Adding New Users

Before you begin: You need the following information from the users you would like to add:

- First name
- Last name
- Email address

Note: The email address must be unique, as in not already associated with another Mobotix Cloud VMS account.

To add a new user, do the following:

1. Click Users in the navigation bar on the left.
2. Click the green Add User button.
3. Enter the required information (first and last names and email address)
4. Click Next to go through the Access, Cameras, Layouts, and Permissions to set up new user access.
5. Click Save to add the user to your Mobotix Cloud VMS.

What to do next**:** Once the user has been added, they will receive an email with a link. They need to click this link to validate their email address and choose a password. The email link is only valid for 72 hours and can be resent if needed.

Deleting Users

To revoke a user's access to the Mobotix Cloud VMS, delete them from the Users table.

1. Click Users in the navigation bar on the left.
2. Find the user in the list that you want to delete, then click the three dot icon ⋮ next to the user and click on the Delete User button.
3. After reading the warning message, finalize the deletion by clicking Delete.

Granting and Denying access to cameras and layouts

Access control to cameras and layouts within the Mobotix Cloud VMS allows specific choices. It is possible to grant or deny access to individual cameras, layouts, and other settings.
Access can be granted either when initially adding the user to your Mobotix Cloud VMS or at any time in the **User** Settings dialog.

1. Click Users in the navigation bar on the left.
2. Find the user whose access needs to be edited in the list.
3. Click the three dot icon ⋮ next to that user and click the Settings button.
4. Use the Cameras and Layouts tabs to edit the access.
5. Drag and drop cameras or layouts to the appropriate column (No Access or Access).
6. Click Save Changes to finalize the access changes.

Result: The changes will immediately go into effect.

Granting Permissions

Permissions can be granted in many configurations in the Mobotix Cloud VMS. In the **Permissions** tab, it is possible to do either of the following:

- Grant users administrator status with permission to control access to everything in the Mobotix Cloud VMS.
- Set permissions on a per user basis.
  - Click Users in the navigation bar on the left.
  - Find the user whose permissions you want to edit in the list.
  - Click the three dot icon ⋮ next to that user.
  - Click the Permissions tab to edit the permissions.
  - Go through the list to view each permission. Click the arrows to expand each section.
    - Check the box next to a permission to grant it.
    - Uncheck the box next to a permission to revoke any previously granted permissions.
  - Once all changes have been made, click Save Changes to implement them.

Audit Log

Audit Log shows the record of events that were taken by users for the selected period of time. See Figure: 127. .

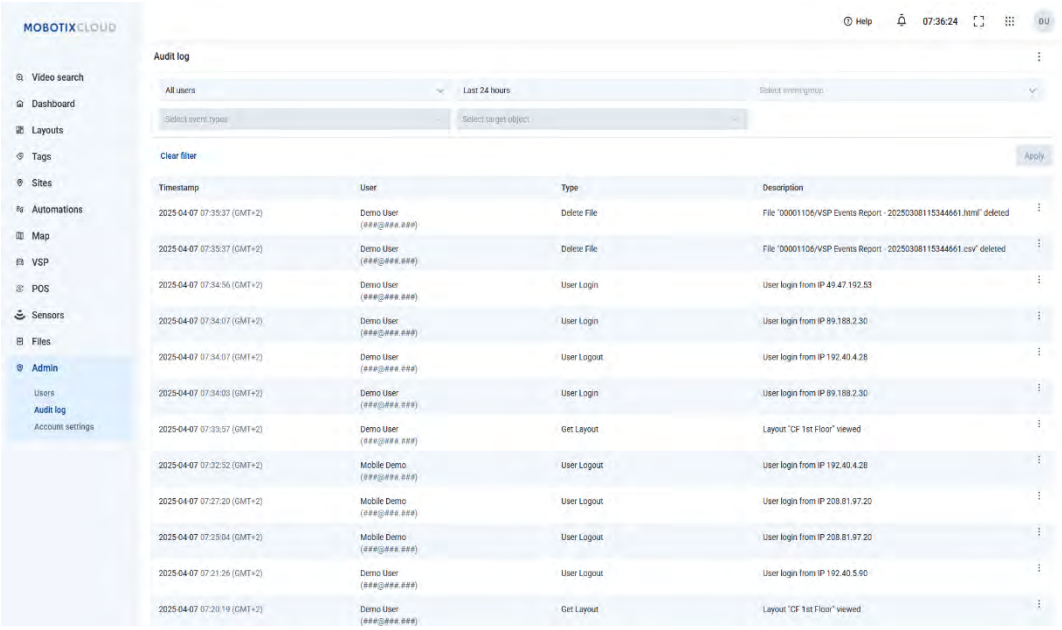


Figure: 127. Audit Log

The audit log settings are described below.

- **Date Range**: Select the start date of the event to show in the audit log list. Both start and end dates are inclusive.
- **Actor Filter**: Select to see the audit events from any user on the system.
- **Event Filter**: Select to see all of the events or any specific event from the list:
  - User Login
  - User Logout
  - User Add
  - User Update
  - User Delete
  - Switch Account
  - Update Account
  - Password Reset Request
  - View Live Video
  - View Video Start
  - View Video End
  - Download Request
  - Download Save
  - Device Add
  - Device Update
  - Device Off
  - Device On

  - Device Delete
  - Control Managed Switch
  - Update Managed Switch
  - Layout Add
  - Layout Update
  - Layout Delete
- **Target Filter**: Select to see audit events from the targets listed below.
  - All
  - Accounts
  - Devices
  - Layouts
  - Locations
  - Users
  - Video
- **Go**: Performs a search for the selected inputs.
- **CSV**: Downloads all of the registered events for the selected inputs to the CSV format file.
- **Total**: Shows the total count of registered events for the given search.
- **Limit**: Select between 10, 25, 50 or 100 entries per page.
- **Timestamp**: Date and time of the entry.
- **User**: Name and email of the user that performed the action.
- **Event**: Name of the registered event that the user has performed.
- **Detail**: Short description of the event. Click on the entry in order to see more details.
- **Previous**: Open previous page of the results.
- **Next**: Open the next page of the results.

Using the Mobotix Cloud Application

To use the Mobotix Cloud VMS platform from a mobile device, download the **Mobotix Cloud** from the Google Play store for Android devices or the Apple App Store for iOS devices.

Downloading the Mobotix Cloud Application

To access the Mobotix Cloud mobile application, click the QR code for your type of mobile device. See Figure: 128. .

iOS **Android**

Figure: 128. Accessing the Mobotix Cloud Mobile Application

Download the Mobotix Cloud Application to your mobile device.

Logging in to the Mobotix Cloud

Before using the Mobotix Cloud, users must configure a password within Mobotix Cloud VMS web interface. This authentication method can be secured using MFA (multi-factor authentication) via SMS or email for further security.
After opening the Mobotix Cloud, there are two options:

1. Shake your mobile device to enter the demo account. Mobotix Clouds' demo environment provides a safe place to learn the mobile application functions without impacting a live system.
2. Click Sign In to log in to your own account. Enter your email address and password into the authentication system. See Figure: 129. .

Figure: 129. Signing into you Mobotix Cloud Account

Using Layouts in the Mobotix Cloud Application

After logging in, the Layouts interface opens. Layouts are a user-configured collection of cameras with access configured on a per user basis. All layouts assigned to your user account can be accessed by touching the name of the layout across the top of the interface. See Figure: 130. .

Figure: 130. Using Layouts on the Mobotix Cloud Application

Creating a New Layout

With the proper user permissions to create layouts, you can create your own custom set of cameras to be displayed in a layout. To create a new layout, do the following:

1. Press the three dots icon ⋮ at the top right of the screen and select **New Layout**. See Figure: 131. .

Figure: 131. Creating a New Layout in the Mobotix Cloud Application

2. Name the layout, choose how many cameras to display in each row, enable or disable the camera title bars, and select **Add Cameras**. See Figure: 132. .

Figure: 132. Selecting Cameras for a New Layout in the Mobotix Cloud Application

3. From the list of available cameras, check the boxes of those you wish to add to the layout, then press Save. See Figure: 133. .

Adding Cameras to a New Layout in the Mobotix Cloud Application

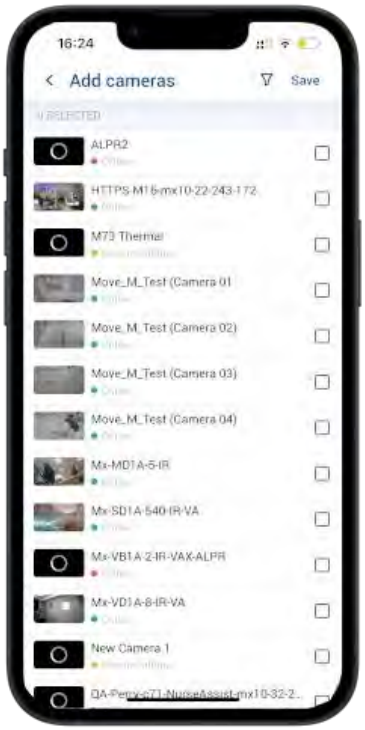


Figure: 133. Adding Cameras to New Layout

Editing A Layout

Edit the order of the cameras within the layout by pressing the three dots icon ⋮ and selecting **Edit Layout**. In edit mode, a long press on any camera in the layout allows you to drag it to your preferred position within the layout.

Remove cameras from the layout by pressing the red delete icon ⊖ at the top right of each camera. See Figure: 134. .

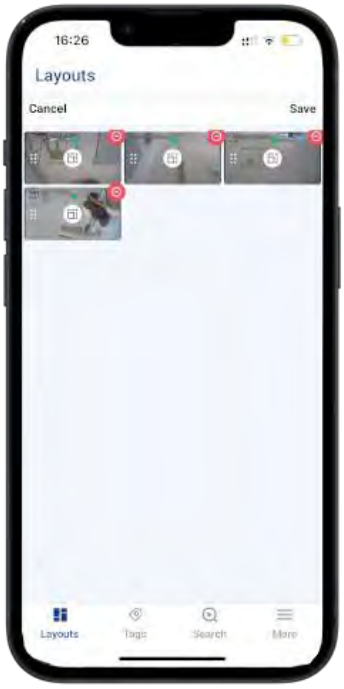


Figure: 134. Editing a Layout in the Mobotix Cloud Application

Viewing Live Video in the Mobotix Cloud Application

Cameras viewed within layouts in the Mobotix Cloud Application are displayed in preview quality, with the video shown at lower resolution and frame rates to minimize the impact of viewing multiple cameras at once on both the mobile device and the on-site system transmitting the video stream. To view high-quality video for any camera within a layout, press the camera. See Figure: 135. .

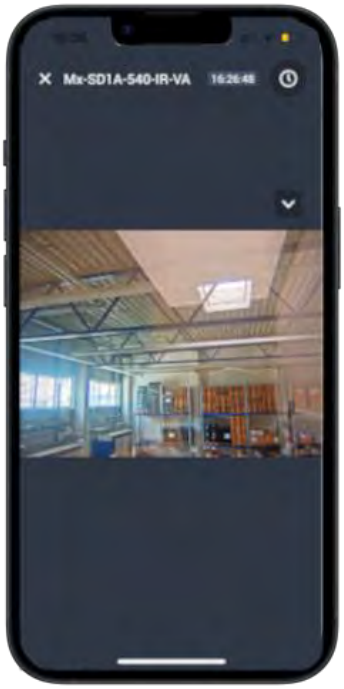


Figure: 135. Viewing Live Video in the Mobotix Cloud Application

Accessing Recorded Video

To access recorded video from any camera, press the clock icon in the top right of the live view for the camera to open the history browser. Within the history browser, pressing and dragging on the displayed timeline will allow you to navigate through recently recorded video. See Figure: 136. .

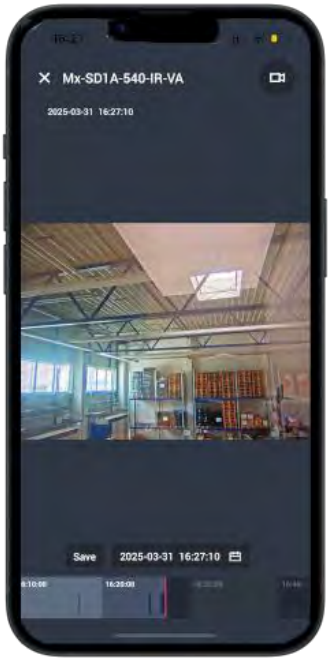


Figure: 136. Opening the History Browser in the Mobotix Cloud Application

If you know the date or time of the recorded video you want to view, press the calendar button shown next to the date and time to enter your desired time. See Figure: 137. .

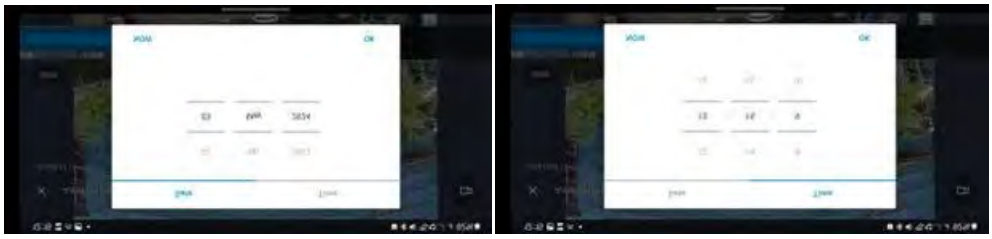


Figure: 137. Entering the Date and Time of Recorded Video

Once the appropriate time has been found on the timeline, press once on the camera view to play the video.

Exporting Video from the Mobotix Cloud Application

To export or save a piece of footage for external sharing, press the **Save** button shown next to the date and time in the History Browser. See Figure: 138. .

Figure: 138. Exporting Video from the Mobotix Cloud Application

The **Save** interface where you can configure export settings opens. You can configure the following settings:

- **File Name**: Enter a name for the exported video file.
- **Download** Type: Select the format of the exported file.
- **Video**: Show a continuous high quality video of the entire time frame selected.
- **Bundle**: Collect all high-quality and preview video recorded within the specified time range.
- **Preview Timelapse**: Exports the preview quality video for the entire time frame selected.

- **Save To**: Select where the exported video will be saved to.
- **Start Time**: Select the beginning time for the video clip.
- **End Time**: Select the end time for the video clip.
- **Time Stamp**: Embed the date and time into the exported video clip.
- **Notes**: Include any notes you wish to attach to the video file. See Figure: 139. .

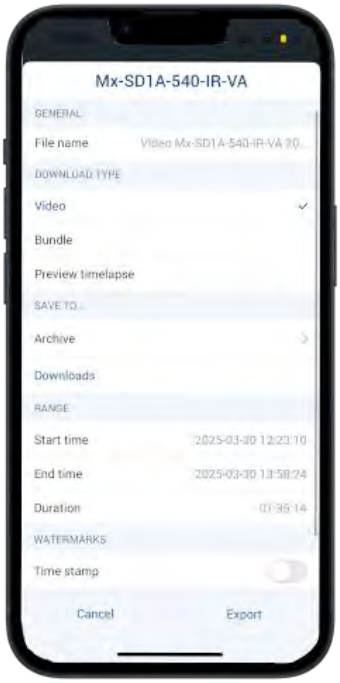


Figure: 139. Configuring Export Settings in the Mobotix Cloud Application

After entering details, press the **Export** button. The exported video appears in the *Downloads* section of the Mobotix Cloud Application. To access downloaded video, go to **More > Downloads**. See Figure: 140. for the workflow.

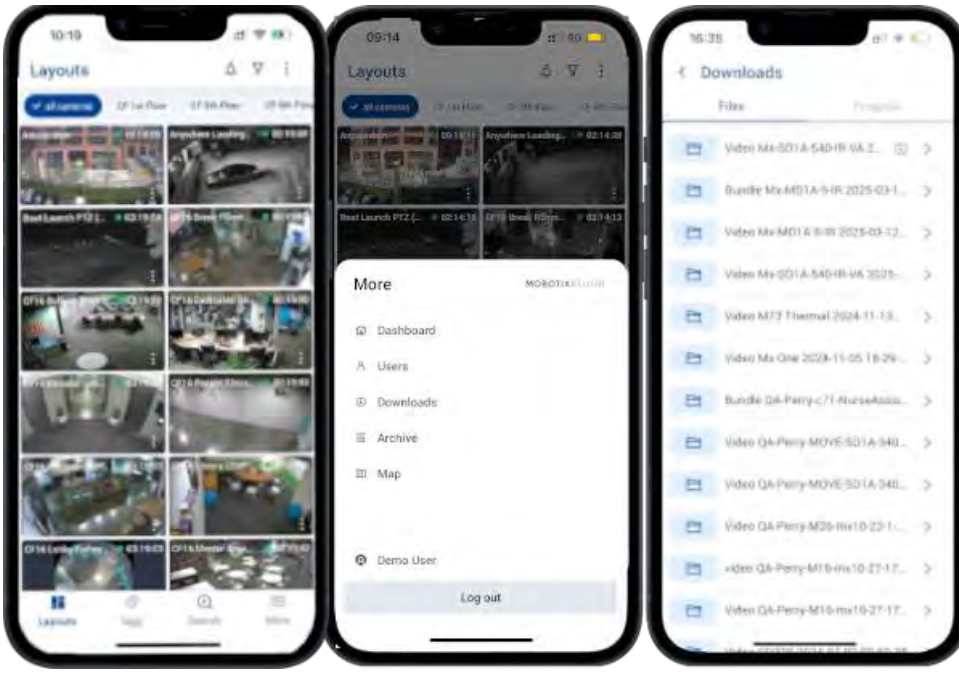


Figure: 140. Accessing Exported Video in the Mobotix Cloud Application

Video Search in Mobotix Cloud Application

Mobotix Cloud VMS includes smart video searching functionality to allow its users quick and convenient methods to find video using natural language searches. Mobotix Cloud Applications' AI engines automatically analyze all recorded video for people, vehicles and objects and certain attributes as described in Reports . To access the video search functionality within the Mobotix Cloud Application, select **Search** from the bottom of the UI. See Figure: 141. .

Figure: 141. Searching for Video in the Mobotix Cloud Application

Use the search box to enter a description of a person, vehicle, or object. See Figure: 142.

Figure: 142. Entering Search Terms in the Mobotix Cloud Application

Use the drop-down menus at the top of the search interface to filter the video search to particular cameras, sites, camera tags, or regions of interest. Videos found through Video Search can be viewed in the History Browser and exported as described in Exporting Video from the Mobotix Cloud Application.

Getting Help

How to Get Help with the Cloud VMS

If you need technical support, please contact your MOBOTIX dealer. If your dealer cannot help you, he will contact the support channel to get an answer for you as quickly as possible.
If you have internet access, you can open the MOBOTIX help desk to find additional information and software updates. Please visit:
www.mobotix.com > Support > Help Desk.

MOBOTIX

BeyondHumanVision

EN_15.05.2025

MOBOTIX AG • Kaiserstrasse • D-67722 Langmeil • Tel.: +49 6302 9816-103 • sales@mobotix.com www.mobotix.com