MONITOREAL

USER MANUAL 1.6.0

Thank you for choosing the Monitoreal Video Security Assistant!

This user manual consists of a Quick Start Guide and a continuation of the User Manual with all the additional settings and tips. The Quick Start Guide goes through the basic setup procedure of adding the Monitoreal Video Security Assistant to a camera system and it links to sections of the User Manual for additional details. This user manual refers to your Monitoreal Video Security Assistant as MR for short.

TABLE OF CONTENTS

QUICK START GUIDE

The Quick Start Guide covers the procedures outlined below followed by a continuation of the user manual. You may also view the 5-minute Monitoreal Installation & Set Up video overview. Please note that the video shows a previous software version.

1. **POWER UP AND UPDATE**

2. **CONNECT YOUR CAMERAS**

   a. **Add Cameras Automatically**

   b. **Add Cameras Manually**

3. **CUSTOMIZE ALERT AND ACTION RULES**

4. **SET UP ALERTS**

1. POWER UP AND UPDATE
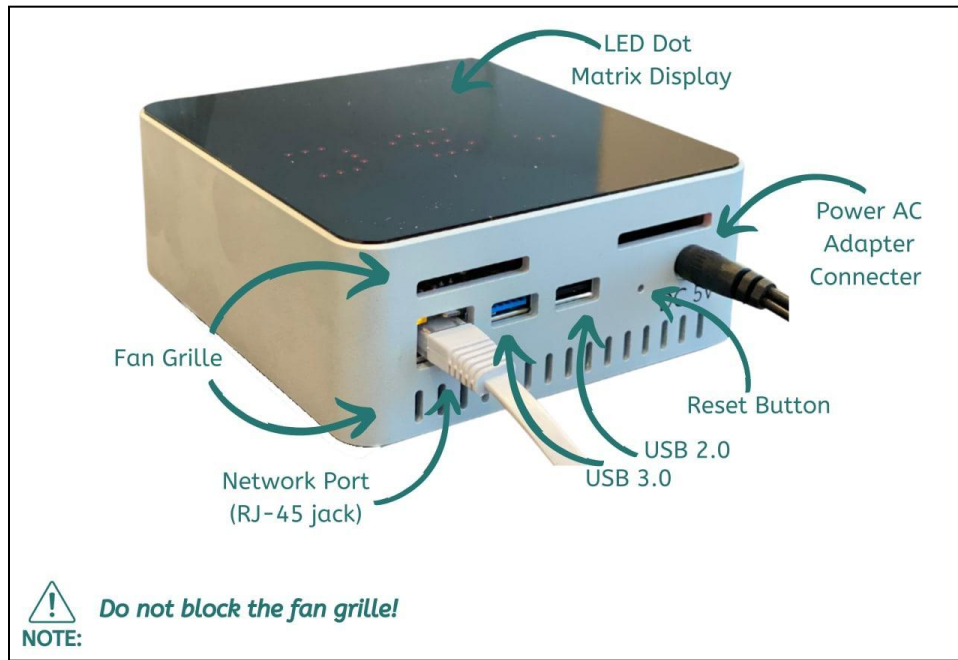
The Monitoreal Video Security Assistant (MR) and its parts

a. Connect your unit to your local area network (LAN). An Ethernet cable is included for this.

   i. The LAN must have a DHCP server (typically a router) so that the unit will obtain a working IP address automatically.

   ii. The unit can typically be connected to a router for initial configuration or permanently.

b. Plug in the power adapter to power up the unit. There is no power button.

c. Wait approximately 2 minutes for the unit to start and display its IP address on the LED matrix.

   i. The IP address is displayed every 1-2 minutes on the LED dot matrix display.

d. Using a web browser on a PC on the same LAN as your Monitoreal unit, navigate to

<p align="center">http://<IP-ADDRESS></p>

<p align="center">Example: http://192.168.1.15</p>

Note: MR does not support HTTPS. You might need to disable HTTPS-only mode in your web browser settings.

e. Log in using the default credentials (username: smartview, password: smartview).

   i. We strongly recommend changing your login credentials for improved security. The credentials can be changed in ⚙ **Settings** → **Profile.**

f. Get the latest software version by going to ⚙ **Settings** → 🖵 **System** → **Check for update**. For more details, see [Updating MR](#).

2. CONNECT YOUR CAMERAS

Adding cameras automatically using the camera search feature is the easiest way to add cameras provided that the cameras are ONVIF conformant with ONVIF access enabled. Adding cameras manually comes in handy when the cameras are not ONVIF conformant or you want to use a different stream or snapshot URL for optimization purposes.

With any camera adding method, the cameras must be on the same LAN, or, for more advanced setups, they must be accessible through network address translation (NAT) or port forwarding. If your

cameras are connected directly to an NVR or DVR, then they are usually on an isolated LAN that cannot be reached through your router or main LAN subnet. See Networking Tips for help with networking.

Go to the 📷 **Cameras** page and you will see the options to search or add cameras manually.
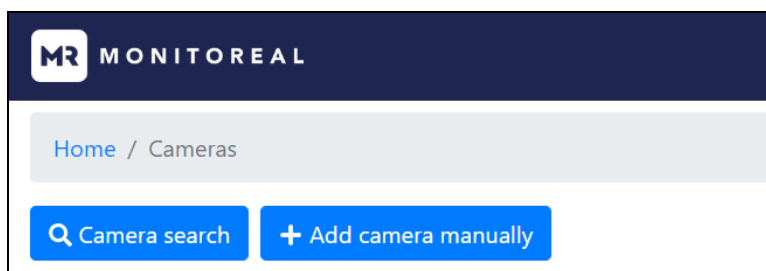
Buttons for adding cameras

Add Cameras Automatically
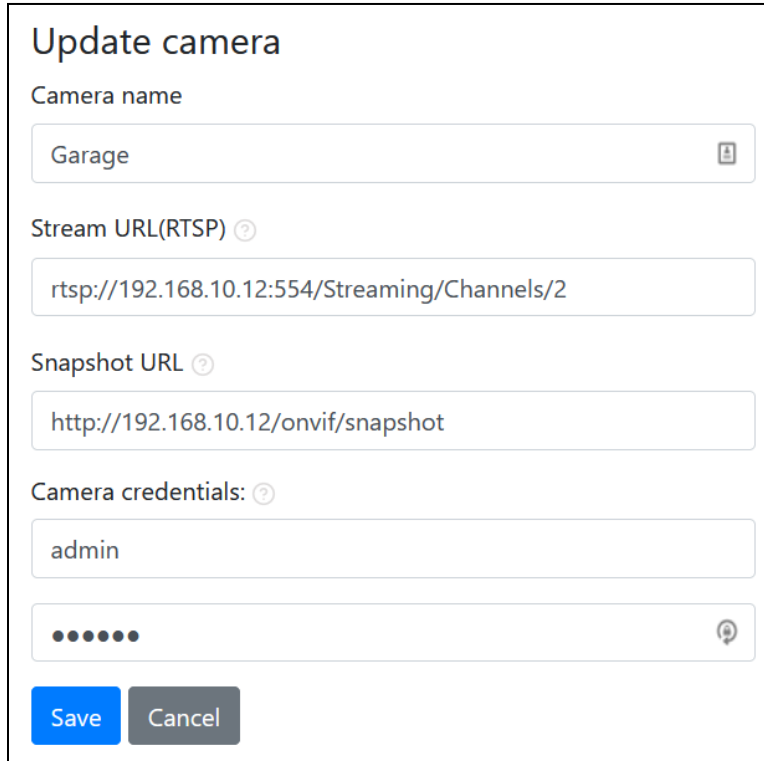
a. Click the 🔍 **Camera search** button.

b. If you are adding Monitoreal cameras that have the default password, check the box labeled "Search Monitoreal cameras", and start searching without a username and password. Otherwise, proceed to the following steps.

c. Enter your camera credentials and, without entering an IP address, click "Start searching" to automatically find ONVIF conformant cameras on the same LAN.

   i. Some ONVIF conformant cameras do not have ONVIF enabled by default. In that case, you must first enable ONVIF in each camera to be added.

   ii. Some cameras also require an ONVIF user to be added.

d. Enter the camera's IP address if any of the following apply.

   i. You do not want to add all cameras on the network.

   ii. The camera is on a different network segment or subnet.

e. Repeat the camera search using different credentials for any additional cameras that have different credentials.

Camera search dialog

Add Cameras Manually

a. Click the **+ Add camera manually** button.

b. Enter your camera's RTSP video stream URL and/or HTTP snapshot URL along with the camera's credentials and your desired name for the camera.

   i. See [Finding Camera Urls](#) for tips on how to do that.

   ii. Using snapshots as the capture source is preferable for cameras and networks that are able to reliably provide one or more snapshots per second. When using snapshots as the capture source, you may still want to add the RTSP stream URL to provide a fallback source and the ability to watch the live stream on the ■◖ **Live stream** page.

   iii. See [Capture Source Considerations](#) for more information and tips.

f. Click **Save** and repeat this process for additional cameras.

Manual camera entry dialog with example values

TIP: Some camera brands may inhibit ONVIF, RTSP and snapshots by default. These will need to be enabled prior to connection.

TIP: Monitoreal units can support more camera channels when using snapshot as the capture source. However, some third-party cameras have difficulty producing and sending several snapshots per second. See [Capture Source Considerations](#) for more information and tips.

NOTE: If you are having problems discovering any of your cameras and help, visit [FAQ & Chat Support](#) and contact Monitoreal for support using the Help button at the bottom-left corner.

3. CUSTOMIZE ALERT AND ACTION RULES

Each newly added camera will appear with default rules. You can edit the rules any time.
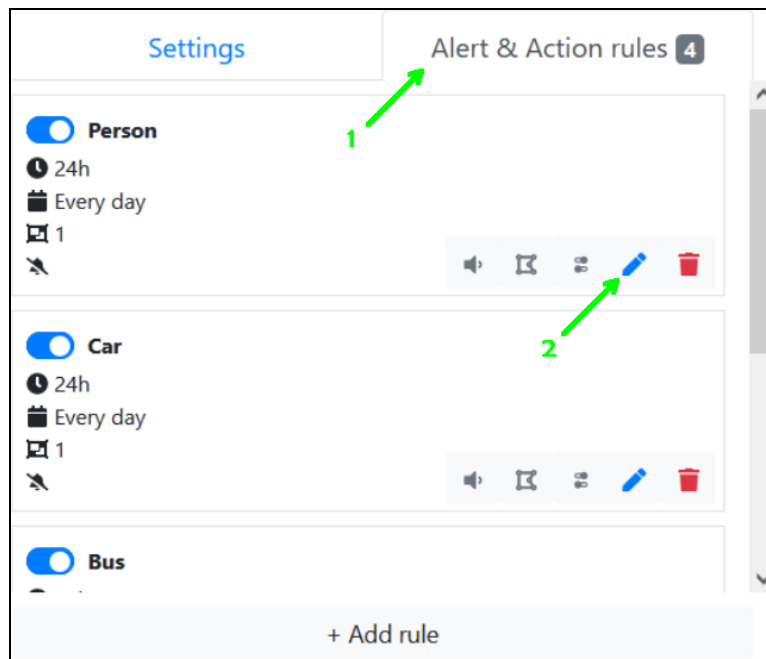
Alerts & Action rules tab under cameras

a. Select the **Alert & Action rules** tab under any connected camera and then click the edit button.

   i. ✏️ Click the pencil icon to edit the rule settings.

   ii. 🗑️ Click the red trash can to delete an unwanted rule.

   iii. ⊠ Click this icon to configure zones and bounding box settings for this rule.

   iv. ≣ Click this icon to configure relay actions.

   v. 🔊 Click this icon to configure audio actions.

   vi. Click the **+ Add rule** button at the bottom to add a new rule.

Rule settings

b. **Object:** Choose from a list of 21 objects to detect.

    i.   You may use multiple rules to detect multiple types of objects.

    ii.   You may also use multiple rules for the same object type.

c. **Density control** defines the minimum number of objects of the selected type that must be present at any time to trigger an alert.

    i.   When using loitering delay, notice that the number of objects specified here must remain present without any one disappearing for the duration of the delay to execute the rule.

d. **Schedule alerts** by entering the start and end time and selecting the days for which you need alerts during that time period.

    i.   The start and end time period may cross midnight from one day to the next. For example, if you set the start time to 08:00 PM and the end time to 08:00 AM, then the rule will be active from midnight to 8:00 AM and 8:00 PM to midnight on every day that is selected.

e. **OD minimal accuracy** can be enabled to adjust the minimal object detection accuracy specifically for this rule.

    i.   For each camera there is a global "OD minimal accuracy" setting that applies to all the rules that do not adjust this value.

f. **Loitering delay** is useful for detecting when people or other objects loiter or remain in an area for an abnormally long time, and you don't want an alert or action upon initial detection. Enter the number of seconds that the object must remain in the zone for the rule to be executed.

g. **Loitering reminders** can be enabled to receive alerts periodically while the object remains present in the zone without disappearing. Define the reminder interval by a number of seconds.

  i. This can be enabled with or without **Loitering delay**. In either case, the reminder counts from the initial detection.

  ii. These reminders are only alerts. Any other configured actions are not executed with loitering reminders.

h. **Alert on object detection:** This option toggles detection alerts for the rule being configured. Disabling object detection alerts can be useful when:

  i. You want an event archive or automatic action without real-time alerts for this particular rule.

  ii. You only want to know when the object has disappeared.

i. **Alert on object disappearance:** This option toggles disappearance alerts for the rule being configured. Please note that if disappearance alerts are not sent, then you will not receive a "get report" button for the event in Telegram with the current software version. Disabling object disappearance alerts can be useful when:

  i. You don't want to receive alerts when objects disappear.

j. **Alert when the number of objects changes:** This option is useful when an object remains tracked on one camera and you want to know when another object of the same type appears or disappears. For example, if you set up car detection and a car parks where it is detected, then any additional cars would not trigger an alert unless this option is enabled.

k. **Profile:** Make the rule active while MR is Armed, Disarmed, or all the time (Armed&Disarmed).

  i. Rules are normally active when MR is armed; However, you may have a special situation where you want some rules to become active when MR is disarmed, or you may want some rules to remain active whether MR is armed or disarmed.

4. MONITOR AND CONTROL VIA WUI

Using the web user interface (WUI) is one of the options for viewing live stream video and events, browsing and downloading the archive, and arming or disarming MR.

Arm and Disarm via WUI

a. Go to the 📷 **Cameras** or 🎥 **Live stream** page.

b. Click **Armed** or **Disarmed** near the top of the page to change the arming status.

  i. The colored option indicates the current status. When armed, the Armed option has a red background. When disarmed, the Disarmed option has a green background.
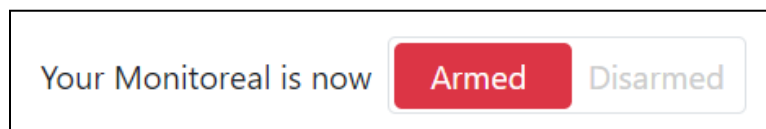
Arming status and control on the 📷 Cameras page

View Live Stream and Recent Events via WUI

a. Go to the 🎥 **Live stream** page.

b. Click any of the camera previews under **Live stream** to view the live video.

  i. The stream URL must be configured for the camera in MR.

  ii. The stream codec must be H.264 for live streaming to work.
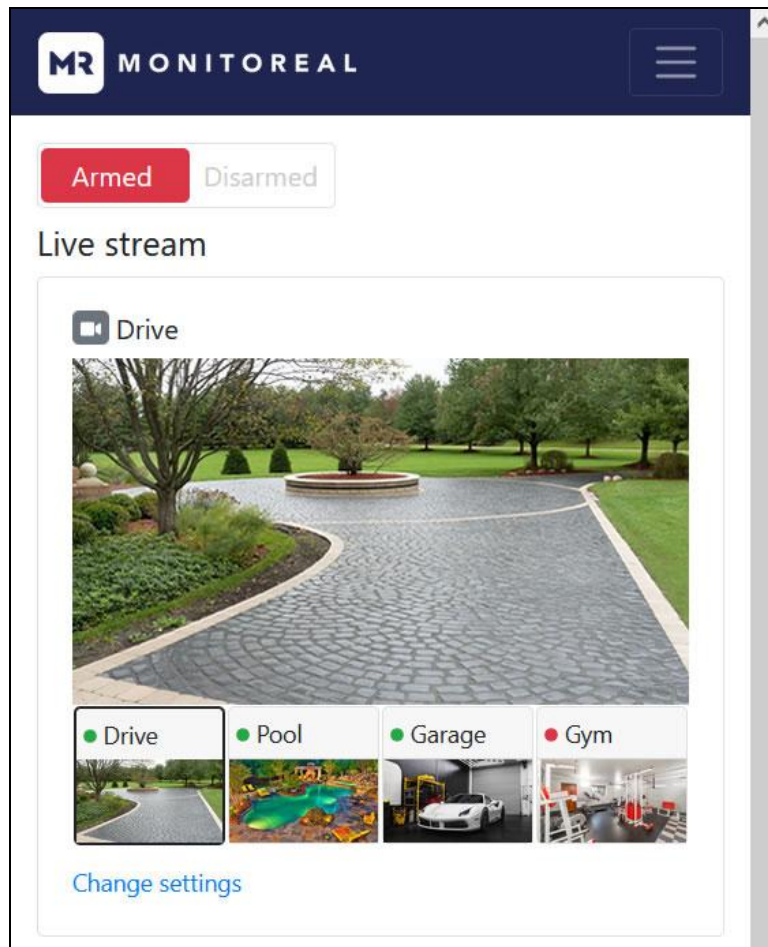
View live video on the 🎥 Live stream page

c. View the live log of **Recent events** shown below or to the right of the **Live stream** pane depending on your browser window width.

    i. The object(s) that triggered the alert will have a thicker bounding box than other objects that may have already been detected and remained preset.

    ii. Object detection and disappearance events include a snapshot and video play and download buttons if MR was set to record the camera.

    iii. Object disappearance events include one or more snapshots and a **Details** button. Click the **Details** button to view the group of snapshots for the event.

        Note: The **Details** button will be unavailable if *alert on object disappearance* is disabled.

    iv. You may download any image by right-clicking (long-press on touch screens) and selecting the save image option.

View recent events on the ▉◀ Live stream page

Search the Archive via WUI

a. Go to the ▦ **Archive** page.

b. Set your search filters including the time range, camera and object type, and click **OK** to search.
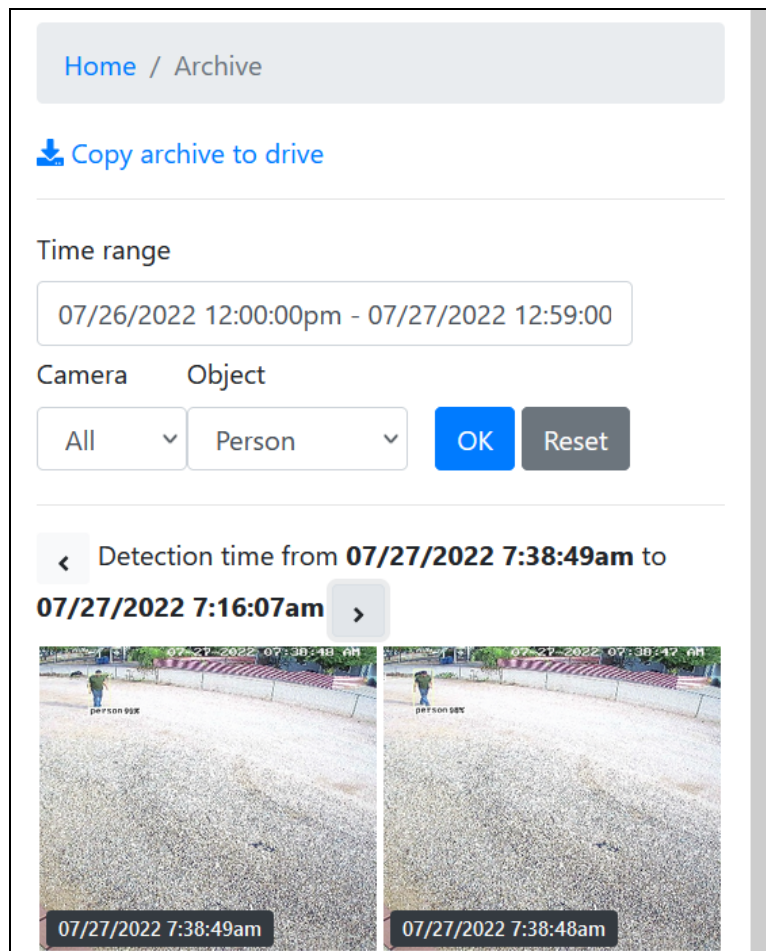
Search and browse the archive of detected objects

c. Click any of the images to view the group of snapshots for the selected event.

d. Use the left and right arrows above the results to see additional pages of results.

e. For cameras that are recorded, you may click the blue buttons below the snapshot to play and download video of the detected objects.
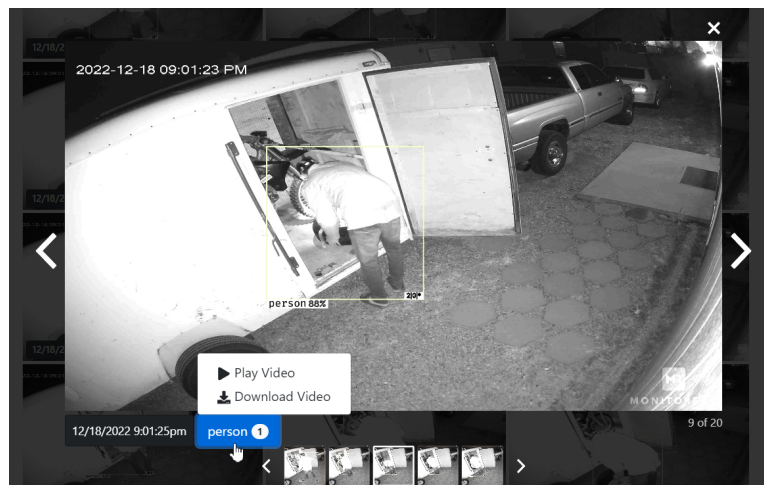
Search and browse the archive of detected objects

Copy the Archive via WUI

a. Insert a USB storage device into a USB port on MR. For a speedy archive copy, it is best to use a USB 3 drive with at least 32 GB of storage, and plug it into the blue USB 3 port on MR.

b. Go to the ⊞ **Archive** page.

c. Click **Copy archive to drive** near the top of the page.

d. Select the desired drive after MR scans for attached external drives, and the copy will begin.

   i. The archive copy could take hours to complete depending on the number of files in the archive and the speed of the storage device.
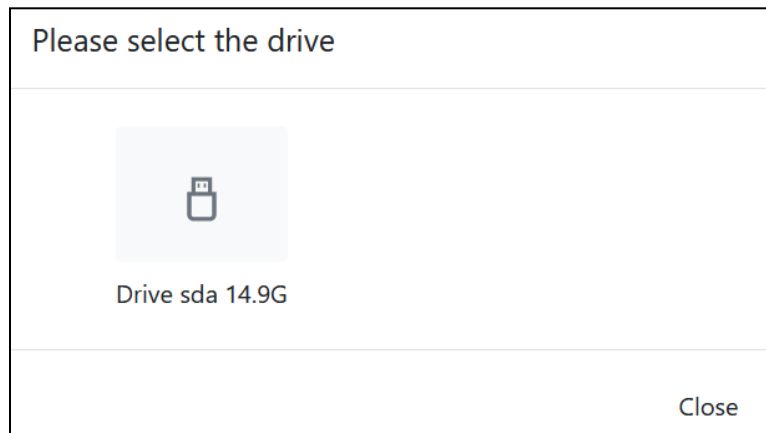
Example of drive selection for archive copying

5. SET UP ALERTS

There are a variety of ways to receive real-time alerts about detected objects and system events. Alerts can be sent to individual users, groups, 3rd party applications, and alarm receiving centers or central monitoring stations. Alerts can be sent to the Monitoreal Secure Guard mobile app and the receivers shown below. Monitoreal recommends using the Monitoreal Secure Guard mobile app or the third party messaging application Telegram.
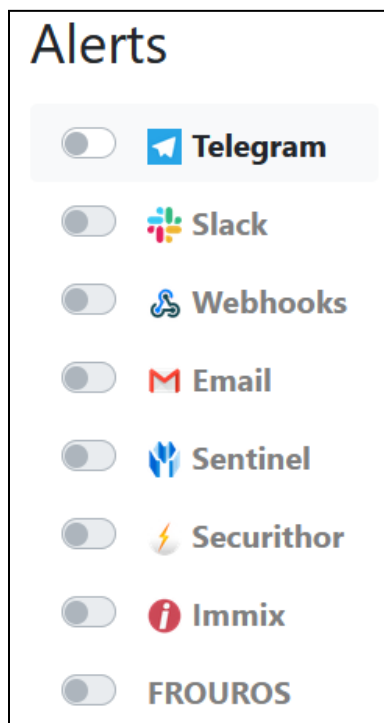
Alert methods available on the Alerts page

The Monitoreal Secure Guard app works on iOS and Android, and it can be used to set up and control MR, receive alerts, and view live streams. Go to Mobile App: Monitoreal Secure Guard for setup instructions.

Telegram works on nearly all platforms (iOS, Android, Windows, macOS, Linux, Web-browsers) and it is focused on security, speed, and a variety of other free benefits. While Telegram cannot be used for initial

setup or live streaming, it does support control of MR. For example, you can change camera settings, request current camera snapshots and video reports, control relays and speakers, and update MR via Telegram. Go to Telegram Alerts for setup instructions, or go to one of the other subsections of ALERTS for other alert methods.

6. GET SUPPORT

If at any time you run into an issue with your unit, we ask that you download the logs within 1 day and share with our support team at support@monitoreal.com. You can download logs through Telegram using the **/logs** command or from the Monitoreal web user interface (WUI). In the WUI, Go to ✿ **Settings** → 🖥 **System** → **Download logs** near the bottom-left corner.

Have Questions? visit our FAQ & Chat Support or email support@monitoreal.com.

Continue reading for additional tips to help you get the most out of your Monitoreal unit!

USER MANUAL (continued)

ALERTS

You have options to send alerts to Monitoreal Secure Guard (mobile app), Telegram, email, Webhooks (HTTP POST), Slack, and a variety of alarm receiving center softwares.
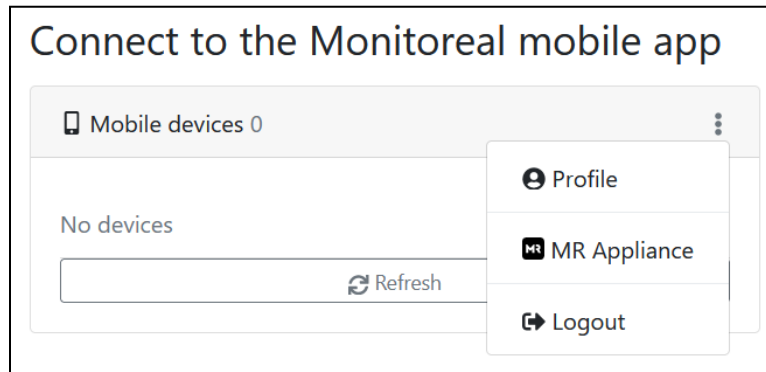
Mobile App: Monitoreal Secure Guard

Monitoreal's native mobile app client for MR Security Assistant appliances is called Monitoreal Secure Guard. The app is developed for iOS and Android mobile devices. Mac models with an Apple M1 or M2 chip can al1so run the iOS app. Monitoreal Secure Guard communicates with the MR appliance via an encrypted, truly direct peer-to-peer (P2P) connection using WebRTC. Initial connection between the app and the appliance is facilitated by Monitoreal's signaling servers, but none of your images or video pass through Monitoreal's servers.

Multiple appliances can be added to each user account. The main steps are to register for a Monitoreal account using the mobile app or MR WUI and sign the MR and mobile app into the same account. Follow the steps below to create a Monioreal account and sign in MR using the MR WUI.

1. Register for a Monitoreal account using the MR WUI.
   a. Go to ✿ **Settings** → **Mobile**
   b. Click **Login**, and a new tab will open with the login page.
   c. New users may click Register at the bottom, or simply sign in using an existing Apple or Google account.
      i. If you register with an email address and password, you will need to verify your email address by clicking a link in the verification email that will be sent to you.
      ii. Close the login/registration/verification pages when finished.
2. Return to the MR WUI Mobile page, and your MR should now be logged.
   a. You may modify the name of the appliance and **Continue**.
   b. Next, your connected mobile mobile devices will be shown. No device will be connected until you sign in to the same account on the Monitoreal Secure Guard app.
   c. The name of the MR appliance can always be changed by going to **MR Appliance** in the menu ⋮ on the **Mobile** page.

d. Click **Profile** in the **Mobile** menu ⋮ to see and manage all connected MR appliances and mobile device sessions in your account.

Connect to the Monitoreal mobile app

📱 Mobile devices 0 ⋮

👤 Profile

MR MR Appliance

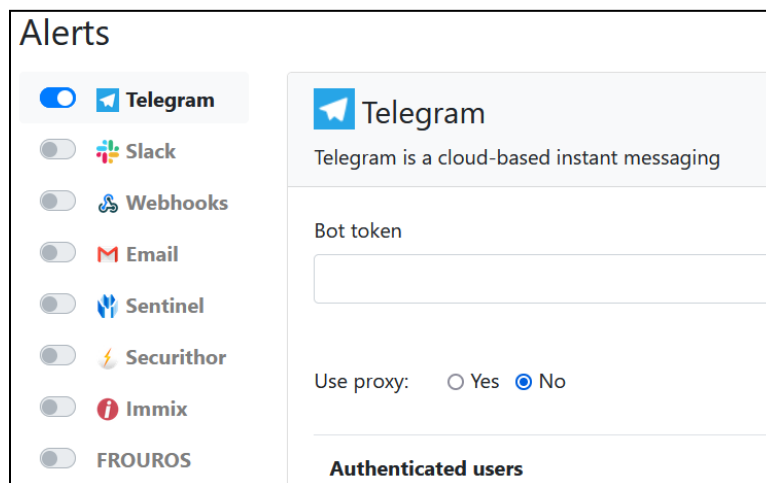No devices

↻ Refresh

➡ Logout

MR WUI Mobile app page with opened menu after login

3. Sign in to the same account on the Monitoreal Secure Guard app. See **Guide to the Monitoreal Mobile Application** for help using the mobile app.

Telegram Alerts

Telegram is good for its simplicity, privacy, security, speed, interactivity and free and unlimited use. You can remotely control your Monitoreal system through the Telegram app. You may set up Telegram alerts by following the steps below.

a. Go to ⚙ **Settings** → 🔔 **Alerts**, and then enable the Telegram toggle switch and click on **Telegram**.

Alerts

Telegram
Slack
Webhooks
Email
Sentinel
Securithor
Immix
FROUROS

Telegram

Telegram is a cloud-based instant messaging

Bot token

Use proxy: ○ Yes ● No

Authenticated users

Telegram is the preferred channel for alerts

b. If you do not have a Telegram account then you will need to get the Telegram mobile app and register there before being able to use the PC, Linux, macOS, or web versions.

   i. iPhone/iPad users can only get apps from the App Store.

   ii. Android users can get the app from the app browser of their choice or from telegram.org.

   iii. Telegram registration only requires your country, mobile number and first name.

c. After registering, you may want to use Telegram on another device from which you are configuring MR so that you can easily copy and paste the API token. Get the Telegram desktop or web app from https://telegram.org/apps

d. Log in to the Telegram app of your choice and search for the "**BotFather**" with the exact spelling and capitalization and the verified badge (white/blue checkmark) as shown below.

The official Telegram BotFather (underlined in yellow)

e. Select the official BotFather and click **START** to begin chatting.

f. Create a new bot by sending the **/newbot** command and follow the onscreen steps.

    i. Enter a display name for your bot such as "MR".

    ii. Enter a unique username for your bot. The username must end with "bot". If the username is already taken, it will let you keep trying different usernames.

    iii. Click the API token in the following message (in your chat) to copy it to your clipboard.
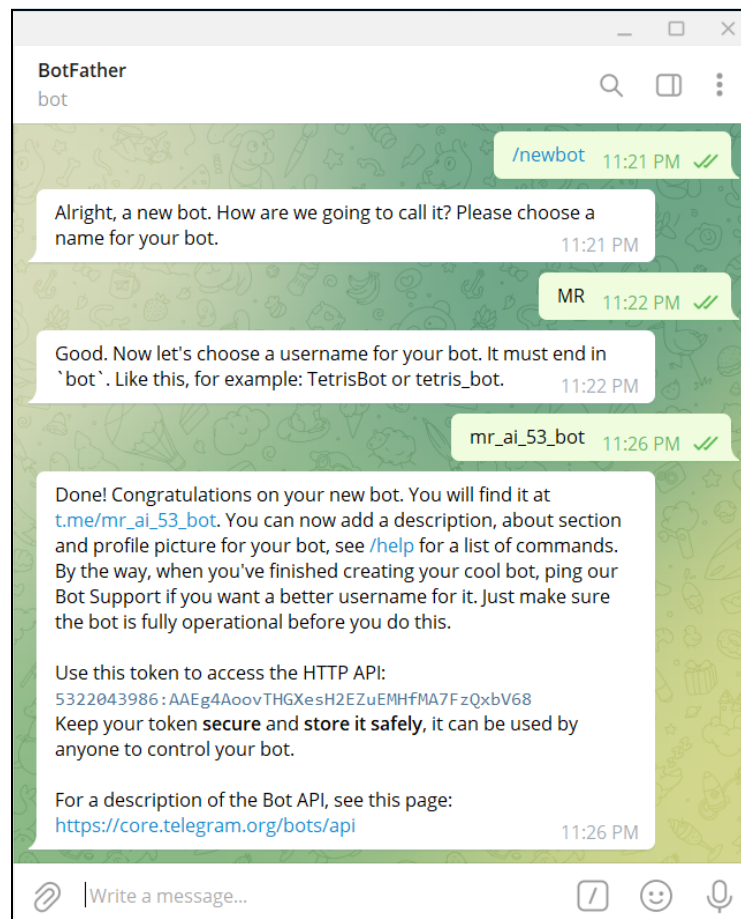
Steps to create a Telegram bot

g. Go back to the MR WUI 🔔 **Alerts** page and enter your new Telegram bot token.

    i. Leave **Use Proxy** set to **No**.

    ii. Click **Save**.

h. Using the link provided by BotFather (e.g., t.me/example_bot), open a chat with your new bot in Telegram, and click **START**.

i. Your MR will ask you to enter the credentials for your MR WUI account. Once you log in, will start receiving any alerts from your MR. You will receive alerts on every device on which you are logged in to the same Telegram account.

j. Your MR system can be managed via Telegram using [Telegram Commands](#).

k. You may also allow additional Telegram users to receive alerts and manage your MR. See [Multiple Telegram Users](#).

Multiple Telegram Users

Individual Chats with Bot

You can have another user connect directly to your bot (using your bot's username) and log in so that they can receive alerts and send commands. Each user will receive the system generated alerts. However, the commands from each user and the bot's responses will not be seen by the other users. That can be a good thing as long as they are trusted with the access and settings.

Group Chat With Bot

Using Telegram on any supported device, you can create a group chat and add the bot and all the users you want, or you can add the bot to an existing group.

Create a Group

a. Click the new message button ✏️. If the new message button is not available, as in the desktop app, then click on the menu button ☰ at the top-left corner.

b. Select 👥 **New Group**.

c. Search for and select your bot and all the users to be in the group and click next ➡️.

    i. You may want to wait to add human users after logging in through the group chat or change your MR password after logging in through the group chat.

d. Name your group and click next ➡️.

Note: Some versions of Telegram may have you name the group first, then select the users, and then "create" the group.

Add Bot to Existing Group

Follow the steps below for the Telegram app you are using.

Using Web Telegram App

e. Go to the group where you want to add your bot and click on the top bar where your group name is shown. The **Profile** panel will open on the right side.

f. Select Edit ✏️ (top-right) → 🛡️ **Administrators** → add users 👤 (bottom-right) → enter your bot's username in the search field → Select your bot.

g. Ensure all admin rights are enabled (except "Remain Anonymous") and click save ✅.

h. Say "Hi" (or anything) in the group chat and your bot will prompt you to log in.

i.   Go to the group where you want to add your bot and click on the top bar

j.   Open the more options menu ⋮ at the top-right.

k.   Select ⇌ **Manage Group** → 🛡 **Administrators** → **Add Administrator** → enter your bot's username in the search field → Select your bot → **OK** → **Save** → **Close** → **Save.**

l.   Say "Hi" (or anything) in the group chat and your bot will prompt you to log in.

Using Mobile Telegram App

m.   Go to the group where you want to add your bot and click on the top bar where your group name is shown. The member list will appear.

n.   Select ⊕ **Add Member** → enter your bot's username in the search field → Select your bot → save ✓ → **ADD.**

o.   Long-press on your bot in the group's member list and select **Promote to admin**.

p.   Select save ✓ at the top-right and then go back ← to the group chat.

q.   Say "Hi" (or anything) in the group chat and your bot will prompt you to log in.

**NOTE:** If for some reason groups are not already enabled for your bot, you will need to rectify that first. Open the [BotFather](#) channel and send the **/mybots** command. Select your bot → **Bot Settings** → **Allow Groups?** → **Turn groups on**. It will tell you if groups are already on.

TIP: Because you will type your MR login credentials into the group chat, it is recommended to either (1) add human members after logging in, or (2) change your MR password after logging in. The chat history for new members should be hidden by default, and you can also ensure that the credentials are deleted by selecting and deleting those messages prior to adding members.

TIP: If you are also logged in through an individual chat with your bot, you can disable duplicate alerts to that chat. Go to the MR WUI → 🔔 **Alerts** → **Telegram** → and toggle off alerts for your Telegram username under **Authenticated Users**. Note that the group chat may not have a name under Authenticated Users, and you should keep that user on. Authenticated users with disabled alters will still be able to send commands to your bot; they just will not receive MR initiated alerts.

Telegram Commands

Simple commands sent to MR via Telegram allow you to request current snapshots, event video reports and control your MR from anywhere without the need for port forwarding. Commands are specific text messages that you can send to your Telegram bot. Your Monitoreal unit will read the messages and do as you command. Commands that require more information are interactive, meaning that you will be presented with buttons so that you can easily select what you want.

Telegram commands are rather intuitive and easy to remember, but if you forget a command, you can easily access a list of options by sending **"/help"** to your MR bot. Here are the available commands.

Camera settings

- **/camera** - edit camera settings including active status
- **/notify** - enable or disable alerts for any camera
- **/arm** - activate all cameras
- **/disarm** - deactivate all cameras

Reports

- **/report** - get a video report of a recent event. You will receive a video report of all events that occurred within the timeframe selected.
- **/now** - get a current snapshot from any camera

Relays

- **/relay** - turn relays and outlets on or off

System

- **/system** - display system and network information
- **/update** - check for system update
- **/restart** - restart system
- **/logs** - download system logs
- **/mobile** - connect/disconnect mobile app
- **/help** - list available commands

If at any time you run into an issue with your unit, we ask that you download the logs and share with our support team at support@monitoreal.com. You can download logs right from your telegram using the **/logs** command.

Add a Command Menu

You can make commands easier to use by having them appear from a menu button in the message entry bar. Commands will also appear when you type forward-slash (/), and they will be filtered by the letters you type after the slash. The video below shows how to add the command menu and the results.
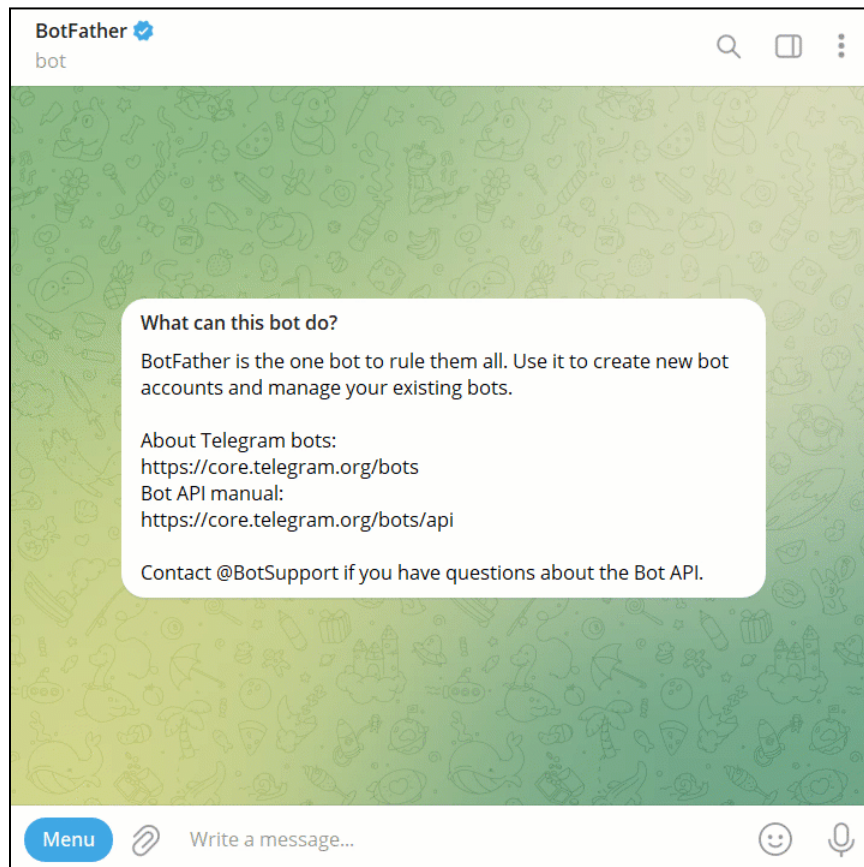
Menu of commands

1. Go to the BotFather in Telegram and send the command /mybots.

2. Select your MR bot.
3. Select **Edit Bot**.
4. Select **Edit Commands**.
5. Copy, paste and send the following list of commands.

```
camera - adjust camera settings
notify - toggle alerts from cameras
arm - arm the system
disarm - disarm the system
report - get video report of detections
now - get current snapshot from camera
relay - control relays
system - get system information
update - update system
restart - restart system
logs - download system logs
mobile - connect/disconnect mobile app
help - list commands
```

Telegram command list to copy and paste

Email Alerts

Alerts can be sent via email (SMTP) after configuring MR to connect to an external email server. You can connect MR to any public or private email service such as gmx.com, outlook.com, yahoo.com, and gmail.com. Search the Internet for the SMTP settings for your mail service. Be aware that some services, including gmail, yahoo and gmx, require external access to be turned on before it will work. For example, with gmx, log in at gmx.com, go to the E-mail tab, go to POP3 & IMAP, check the box labeled "Enable access to this account via POP3 and IMAP", and save. You should also be aware of your email storage quota and any email frequency limit. Sent emails will accumulate on the server taking up storage space, thus requiring periodic deletion. Some email services temporarily block your outgoing emails if too many emails are sent in some period of time.

4. Using a web browser, go to the IP address of MR and log in.
5. Go to ⚙ **Settings** → 🔔 **Alerts**.
6. Enable Email using the toggle on the left as shown below.
7. Enter a name for the sender or site to help you identify which site the alerts come from.
8. Enter the SMTP settings for your email service.
    a. Set the security option to **Automatic** in order to use SSL/TLS or STARTTLS encryption.
    b. Set the security option to **None** if you are using a port that does not support encryption.
9. Enter one or more recipient email addresses, separated by commas.
10. If desired, you can make replies to the alert emails automatically go to a different address.
11. Select **Save** when finished and wait for the success verification message.

Configuration of email alerts

Webhook Alerts

Webhooks allow real-time data to be sent from one application to another application whenever a given event occurs. In this case, MR sends alert data to any URL you provide whenever an alert is triggered. Webhooks allows developers to integrate MR with other systems. The alert data is sent via HTTP(S) POST in JSON format. The Monitoreal webhooks documentation is available online at https://monitoreal.com/guide/Monitoreal_Webhook_Notification.pdf

1. Using a web browser, go to the IP address of MR and log in.
2. Go to ⚙ **Settings** → 🔔 **Alerts**.
3. Enable Webhooks using the toggle on the left as shown below.
4. Click the **Add new webhook** button.
5. Enter the payload destination URL and optional token, and then **Save**.
6. You may add multiple payload URLs and you may toggle individual URLs at any time.
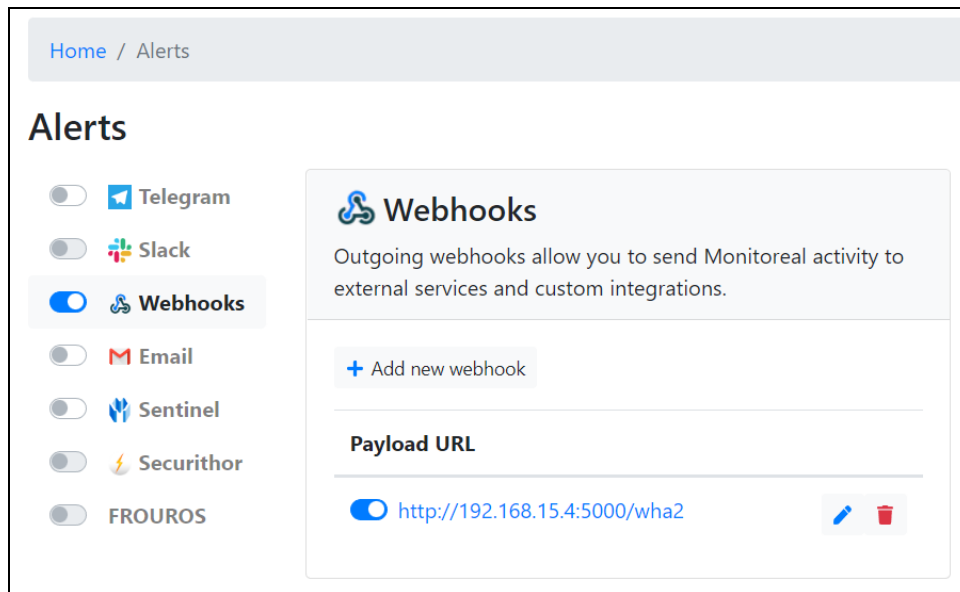
Configuration of Webhooks

Slack Alerts

Slack is a messaging app intended for business, and it is available for iOS, Android, macOS, Windows, Linux, and web browsers including Firefox, Safari, Chrome, and Microsoft Edge. Setting up alerts with Slack is only recommended if you are already using Slack and you need to receive alerts in Slack. You must have a Slack account and workspace as a prerequisite. This setup process is performed in a web browser and preferably on a desktop or laptop computer. Please note that Monitoreal alerts are one-way with Slack. This means that you will not be able to request reports or control your Monitoreal system through Slack.

Log In

7. Using a web browser, go to the IP address of MR and log in. Refer to initial setup instructions if you have not logged in before. Remember that your computer and MR must be connected to the same network.
8. Go to ⚙ **Settings** → 🔔 **Alerts**.
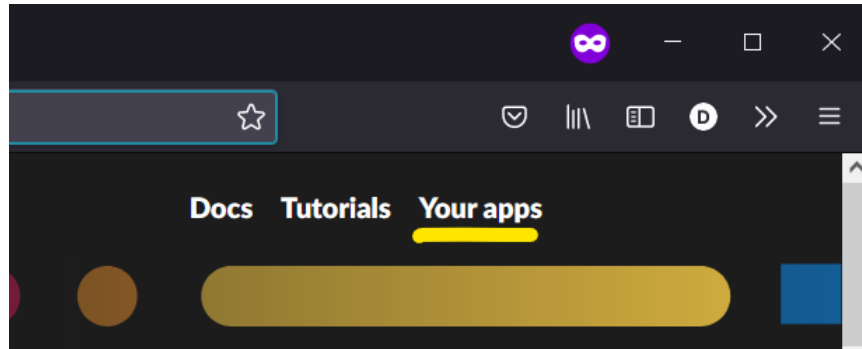9. Enable Slack as shown below, and then leave this browser tab open for later.
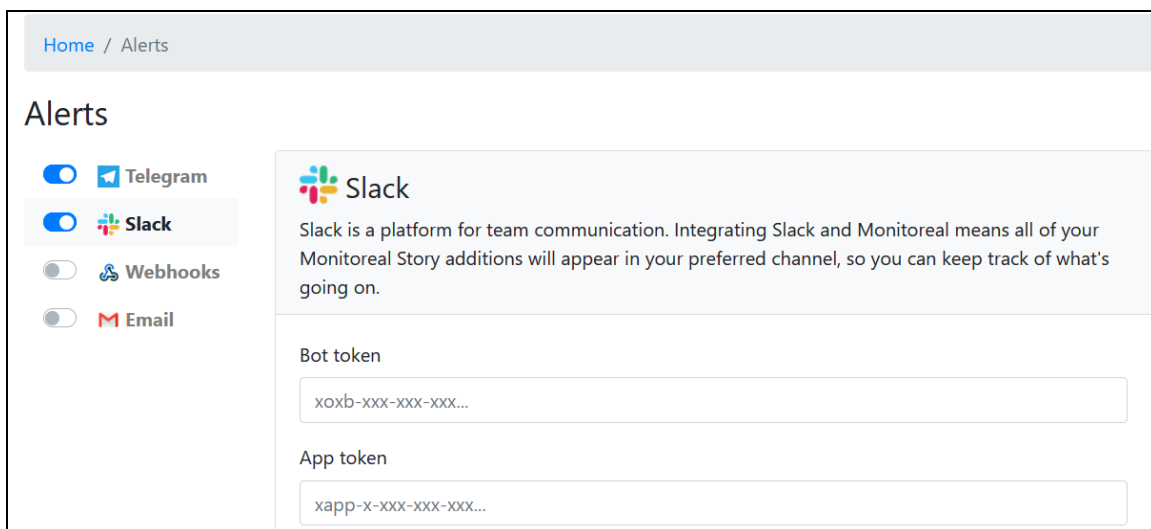
Enable Slack on the Alerts page so that the toggle switch is blue

10. Go to https://slack.com in another web browser tab and log in.

Create a Slack App

1. Go to https://api.slack.com and go to **Your apps** at the top-right.

*Location of **Your apps** link*

2. Click the **Create an App** button.
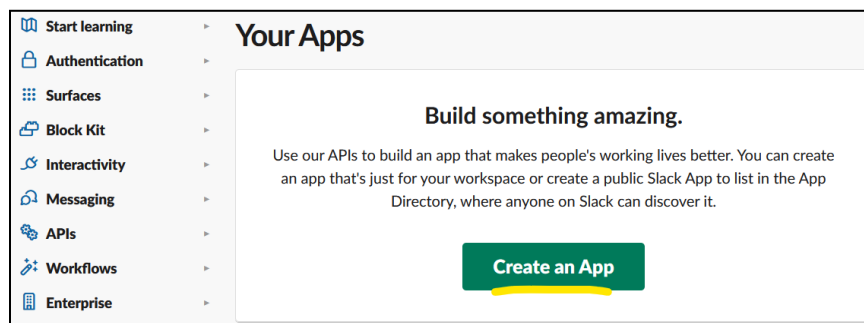
*Location of the **Create an App** button*

3. You will have the option to create an app **From scratch** or **From an app manifest**. Choose the manifest option.
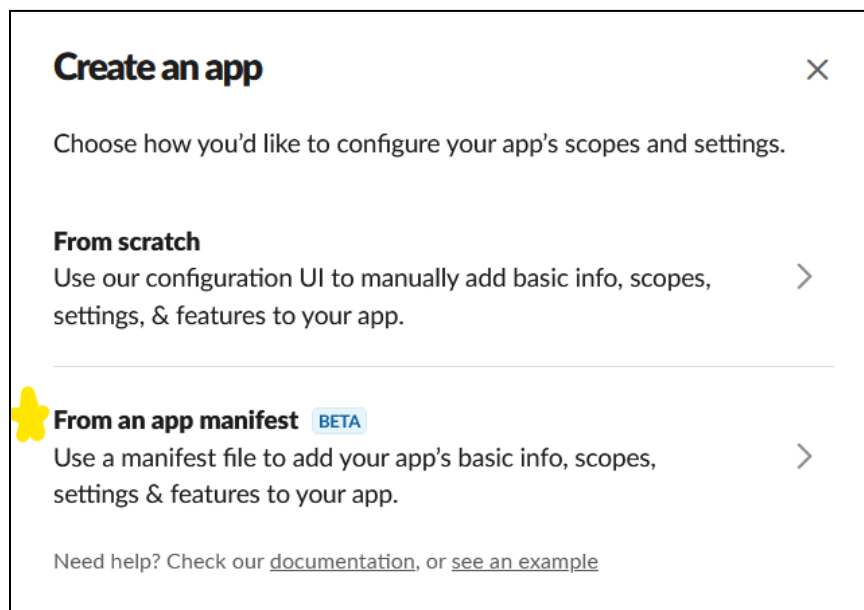
Choose to create an app from an app manifest

4. Select the workspace where you want the app and alerts to go and click **Next**.
5. Now, you will enter the app manifest in YAML form. First, select all the prefilled text under YAML and delete it. Then, copy and paste the following text into the same field. Optionally, you may change the app name from MR to something else on lines 2 and 5.

   Note: It is important not to change any of the line indentations.

```
display_information:
  name: MR
features:
  bot_user:
        display_name: MR
        always_online: false
oauth_config:
  scopes:
        bot:
        - chat:write
        - files:read
        - files:write
        - im:history
        - users:read

settings:
  event_subscriptions:
        bot_events:
        - message.im
  interactivity:
        is_enabled: true
  org_deploy_enabled: false
  socket_mode_enabled: true
  token_rotation_enabled: false
```

The app manifest

6. Click **Next** after you have entered the app manifest as shown below.

The YAML app manifest entered on Slack

7. Click **Create**.
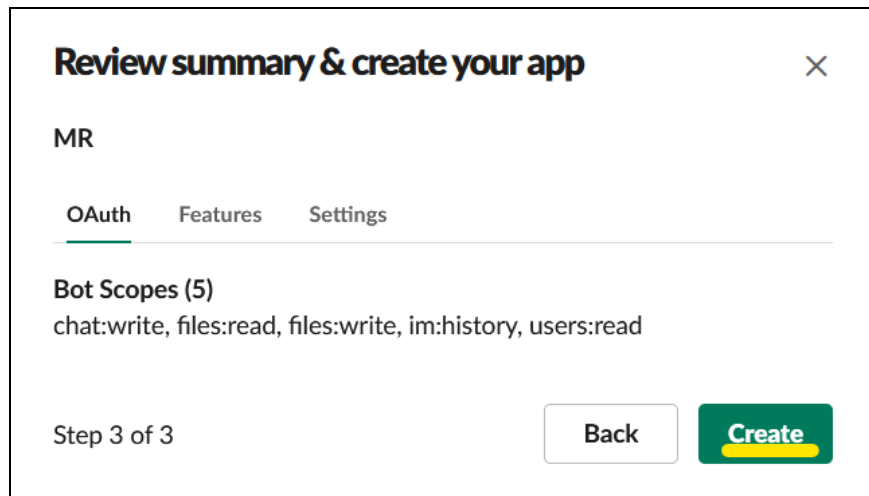
*Location of the **Create** button*

Install the App

1. You will arrive on the app's **Basic Information** page. Click **Install to Workspace**.
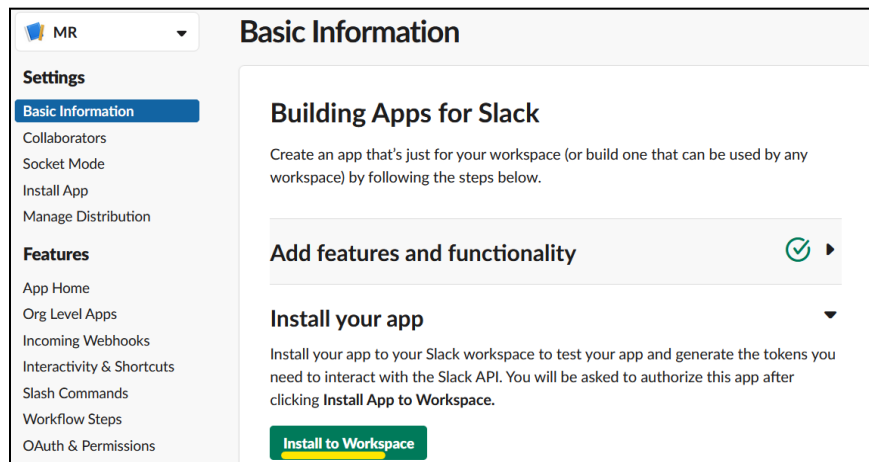
*Location of the **Install to Workspace** button*

2. Review the app's requested permissions if desired and then click **Allow**.
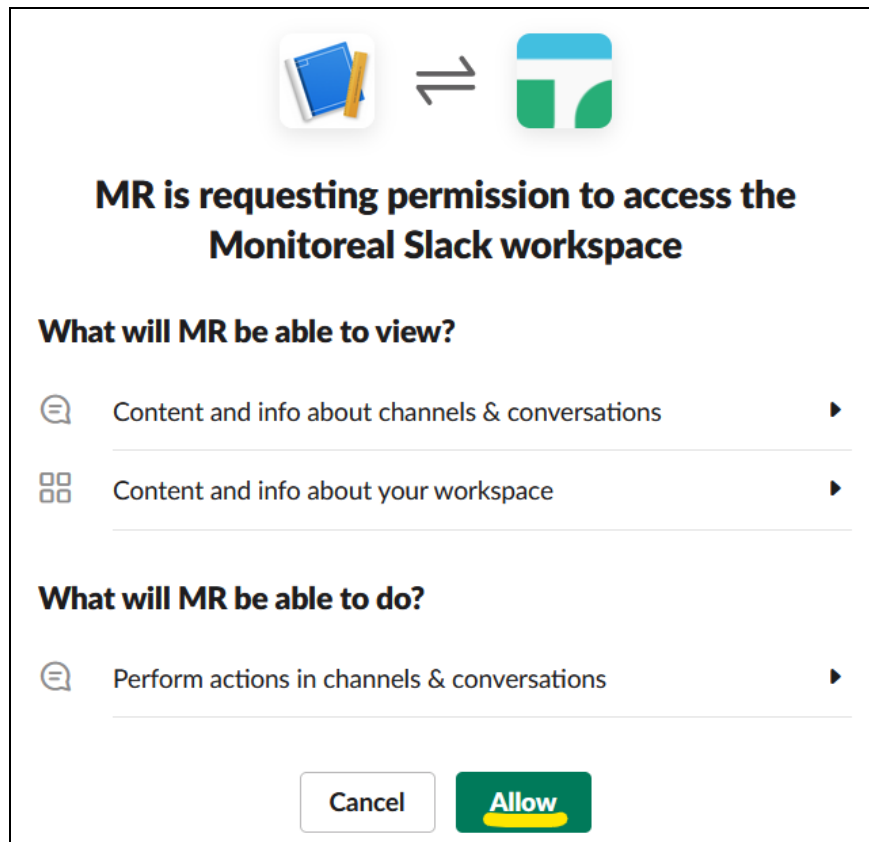
Allow the app's requested permissions

Generate an App-level Token

1. On the same page, scroll down and click **Generate Token and Scopes**.
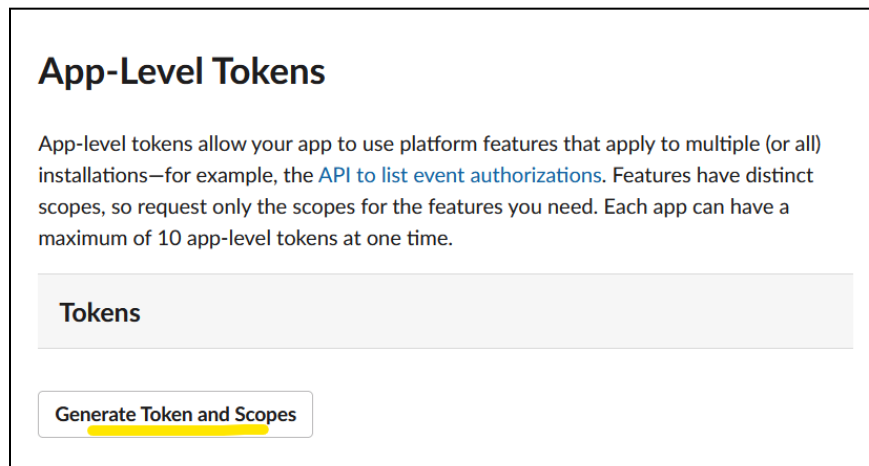
*Location of the **Generate Token and Scopes** button*

2. Enter a token name such as "mr".
3. Click the **Add Scope** button and select "connections:write".
4. Click the **Generate** button as shown below.

*Location of the **Generate** button*

5. The app-level token will be presented. Click the **Copy** button as shown below, which will copy the token to your clipboard.

*Location of the **Copy** button*

6. Switch to your "MONITOREAL - Alerts" browser tab, and paste the token into the "App token" field. Do not click "Save" yet.
7. Switch back to the Slack API browser tab, and click "Done".

Enable Messages to the App

1. Go to **App Home** in the left-hand menu as shown below.
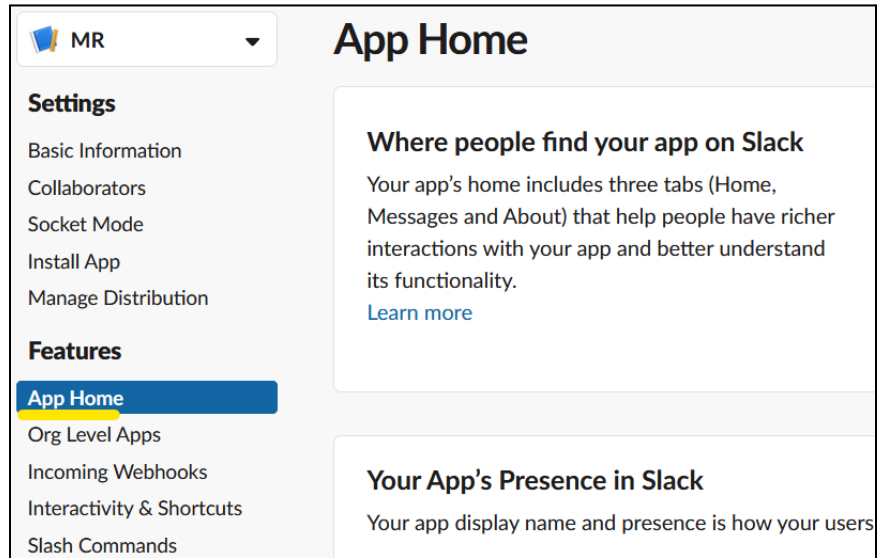
Location of the App Home link

2. Scroll down to the **Show Tabs** section. Under **Messages Tab**, check the box labeled "Allow users to send Slash commands and messages from the messages tab".
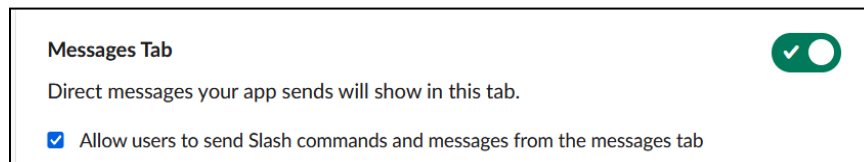
Allow users to send messages to the app

Copy the Bot Token

1. Go to **OAuth & Permissions** on the left-hand menu.
2. Find the **Bot User OAuth Token** and click **Copy.**
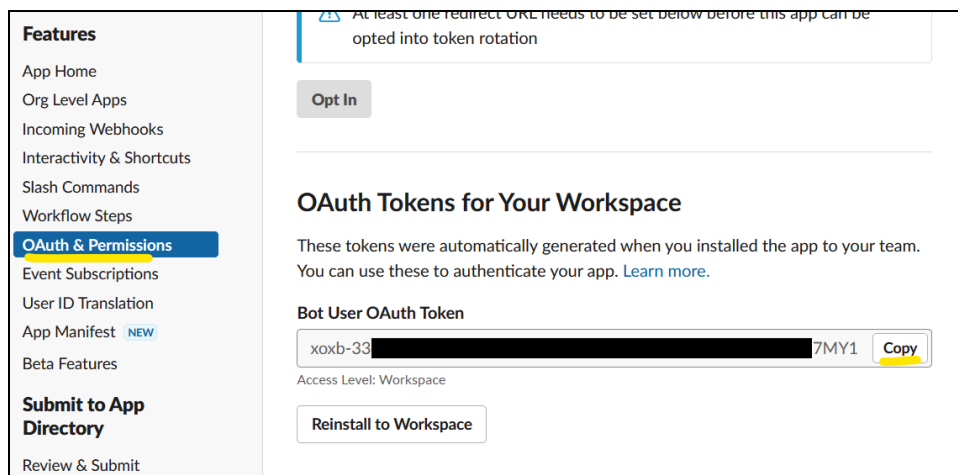
Locations of the OAuth & Permissions link and the Copy button

3. Switch to your "MONITOREAL - Alerts" browser tab, and paste this token into the **Bot token** field.
4. Click **Save** as shown below.

*Example of entered tokens and location of the **Save** button*

Authenticate Slack User

1. Go to slack.com or open your Slack app and launch the workspace in which you installed the app that you just created.
2. Select the app, and you should arrive on the **Messages** tab.
3. Say hello to the app and it will prompt you for the username and password of MR.
4. Once you enter the correct username and password, the app will inform you that it has successfully logged. You will now start receiving alerts from MR through your Slack app.
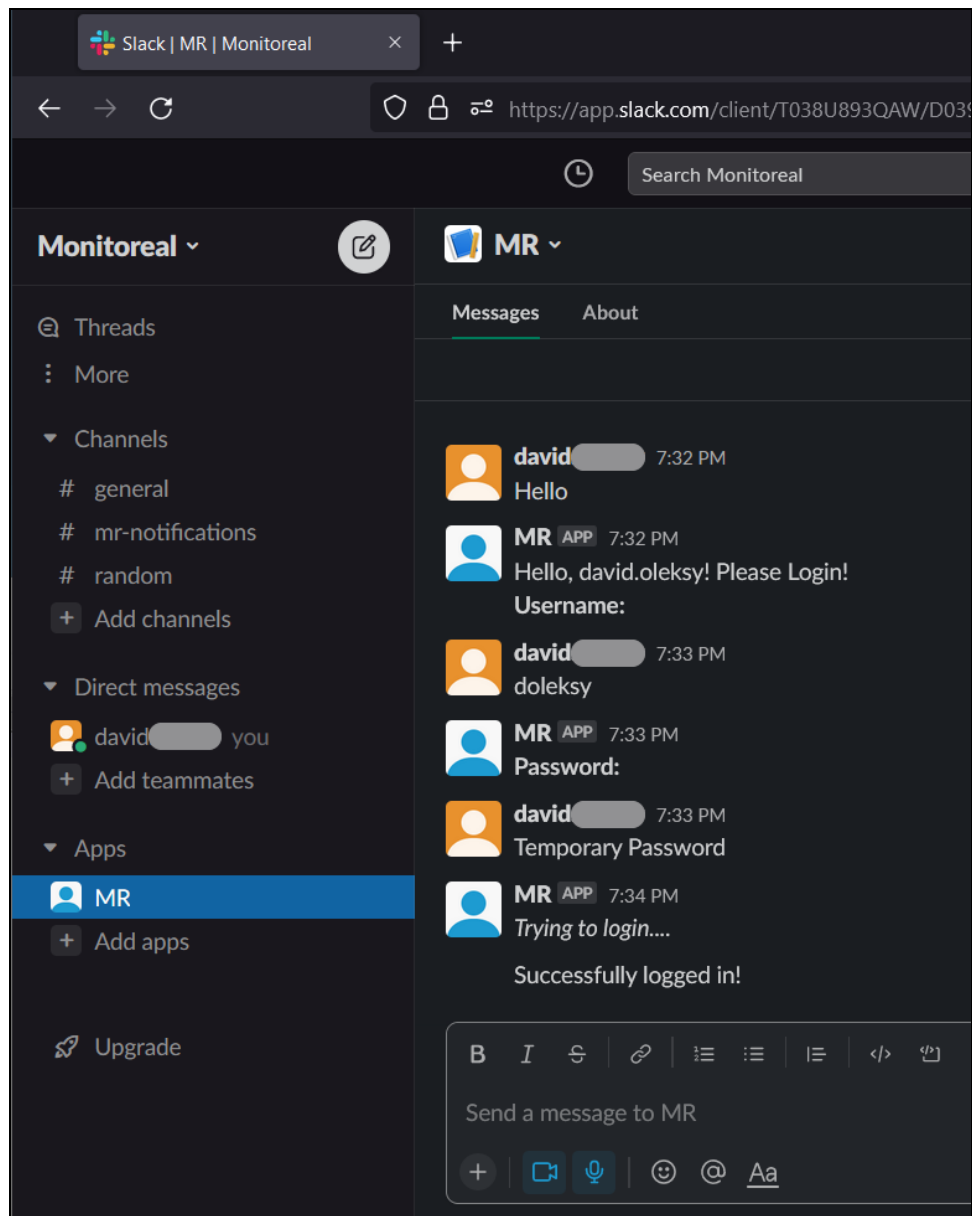
Example of authenticating with MR through the Slack app

CAMERAS

Camera Settings

The default MR settings for each camera should work well in most cases. However, adjustments may be due in some environments to achieve the desired results. The MR settings for each camera are shown on the 📷 **Cameras** page.

Example of camera preview and its MR settings

Stream and Snapshot URLs
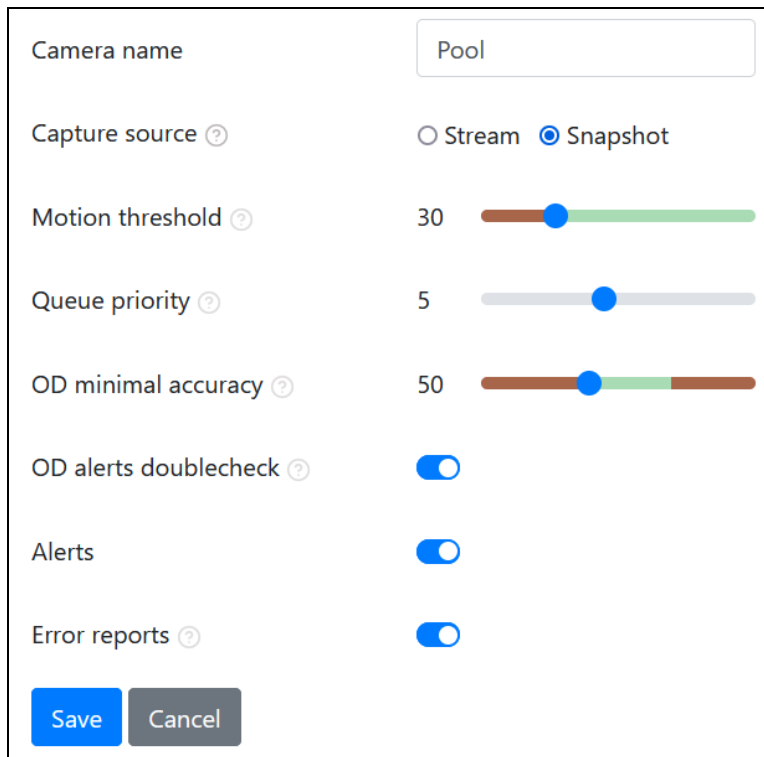
1. If a camera is added manually, there will be a blue edit button, at the top-right of the preview image, that allows you to edit the camera name, URLs, and credentials.

General Object Detection Settings

1. The colored dot left of the camera name indicates the camera's status.
   a. 🟢 Green indicates that the camera is actively being monitored by MR.
   b. 🔴 Red indicates that the camera is deactivated or not working with MR.
2. Each camera can be activated or deactivated using the toggle switch just below the preview image.
3. Open the camera settings editor by clicking **Change settings** under the camera's **Settings** tab, and adjust the following settings as needed.
   a. **Camera name:** Set the name of the camera to be displayed by MR.

b. **Capture source:** The option you choose must be available from the camera and configured in MR either through ONVIF (using camera search) or manual camera entry. See [Capture Source Considerations](#).

c. **Deep sight mode:** This Pro model feature offers enhanced accuracy to detect objects that are smaller, farther away or poorly illuminated.

d. **Motion threshold:** This defines the size of motion that triggers AI analysis. Only decrease the threshold if the objects you need to detect are small and not being detected. Lowering the value below 30% may increase false alerts, overload the system, and cause delayed object detection. Conversely, you may increase the threshold if there are false alerts on objects that are smaller than what you need to detect, and this will help unload and speed up the system.

e. **Queue priority:** Higher priority camera streams or snapshots get processed earlier than those with lower priority.

f. **OD minimal accuracy:** The object detection (OD) minimal accuracy is the object classification accuracy or confidence threshold below which a detected object shall be ignored. If alerts include too many misclassified objects, increase this threshold by 5 and retest before increasing again. Gradual adjustments reduce the likelihood of missed alerts while still improving results.

g. **OD alerts doublecheck:** This setting intends to reduce false positive alerts. When enabled, the object must be detected in at least three frames for an alert to be sent. If less than three frames, then the last frame with the object is analyzed further to decide whether or not to send an alert. When this setting is disabled, the object must be detected in at least two frames for an alert to be sent. When there are not enough frames for an alert, those frames will only appear in the archive.

h. **Alerts:** Toggles all object detection alerts for the camera. When off (leftward position), alerts will not be sent via any method including the WUI ◼◀ **Live stream** page, but objects will still be detected and archived, and any defined actions will still be executed. In other words, turning alerts off decouples alerts from actions and archives. This setting does not affect camera connection notifications.

i. **Error reports:** Toggles error reports about the camera connection. When on (rightward position), alerts about the camera connection status will be sent.

Camera settings edit dialog

Video Recording Settings

1. The **Recorder** button under each camera opens the video recording settings.
   a. Enable or disable video stream recording and **Save**.
      i. The RTSP stream and either a Monitoreal SSD or MR Spartan is required to record video. The capture source can be set to stream or snapshot.
      ii. Video is recorded continuously and detected objects are bookmarked.
      iii. When recording is enabled, the recording status will be indicated at the bottom-left corner of the camera preview image as 🔴rec (recording) or 🟡rec (not recording).

Camera recorder settings dialog

Alert and Action Rules

1. See CUSTOMIZE ALERT AND ACTION RULES in the quick start guide section.
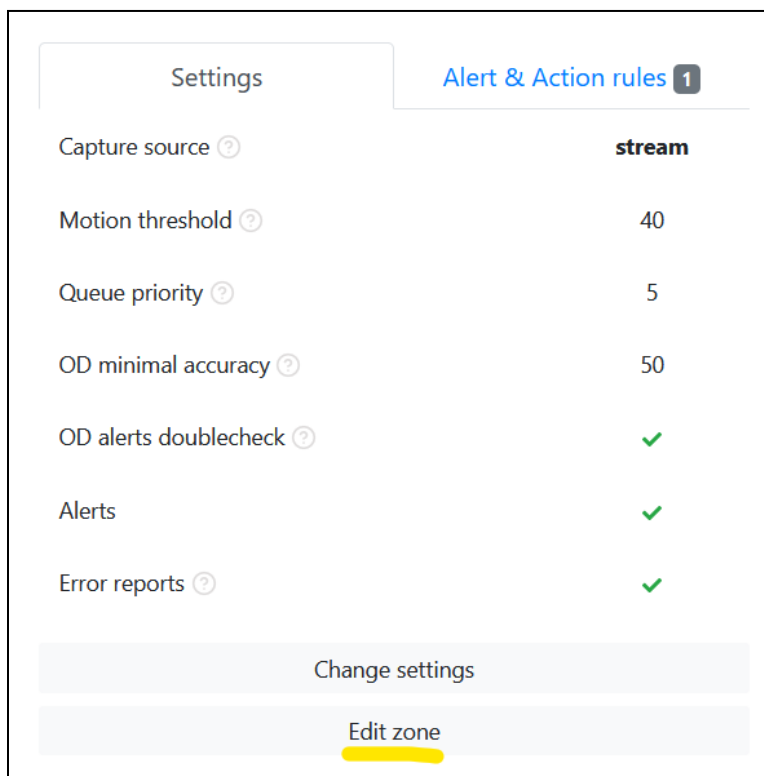
Zones

   A zone is a definable region of the camera's field of view in which object detection shall or shall not execute rules (alerts and actions) depending on whether the zone is inclusive or exclusive, respectively. Regarding what zones do, there is a difference between object detection and rule execution. Zones only affect rule execution. Objects may always be detected anywhere in the camera's field of view regardless of configured zones, and all detected objects can be found by searching on the ⊞ **Archive** page. The alerts

or actions of a rule will only be executed when the object pertaining to the rule is detected within an inclusive zone pertaining to the rule. See Camera-level Zones and Rule-level Zones to understand how zones defined at different levels may or may not pertain to a rule. Adding an exclusive zone is an easy way to (1) prevent alerts and actions from being triggered by objects detected in the exclusive zone, and (2) implicitly define an inclusive zone as the remaining area so long as there are no other inclusive zones explicitly defined at the same level. You may add and edit zones at the camera level and at the rule level.

Camera-level Zones

Zones defined at the camera level apply to all of the camera's rules that do not have any rule-level zones defined. Any newly added camera will not have any default zones predefined. When no zone is defined, MR will treat the camera's entire field of view as an inclusive zone. To add or edit a camera-level zone, go to the 📷 **Cameras** page and click **Edit zone** beneath the camera of your choice. Then, proceed to Zone Configuration.

The camera-level Edit zone button (underlined in yellow)

Rule-level Zones

Zones defined within a rule apply only to the rule in which they are defined. Rule-level zones allow you to have different zones for different objects or even different rules with the same object. Having rule-level zones and the ability to create multiple rules with different schedules and other settings allows a great deal of control over alerts and actions. Any camera-level zones will be ignored by rules with their own zones. To add or edit a rule-level zone, go to the 📷 **Cameras** page, select the **Alert & Action rules** tab beneath the camera of your choice, and then click the zone configuration button (⧓) for the rule of your choice. Then, proceed to Zone Configuration.

The rule-level zone configuration button (underlined in yellow)

Zone Configuration

The UI for configuring zones is as shown below for all levels of zones.

Editing page for zones of all levels

Zone Settings

These settings apply to all the zones listed on the same page.

1. **React to intersections by:**

a. **Edge of bounding box:** The object is considered to have appeared when any edge of the object's bounding box touches any part of an inclusive zone. The object is considered to have disappeared when no part of the object's bounding box touches any inclusive zone.

b. **Center of bounding box:** The object is considered to have appeared when the center of the object's bounding box touches an inclusive zone. The object is considered to have disappeared when the center of the object's bounding box does not touch any inclusive zone.

Notes: Only inclusive zones, whether explicit or implicit, are used in determining the intersection of the object and the zone. See Zone Tips below for an understanding of implicit inclusive zones.
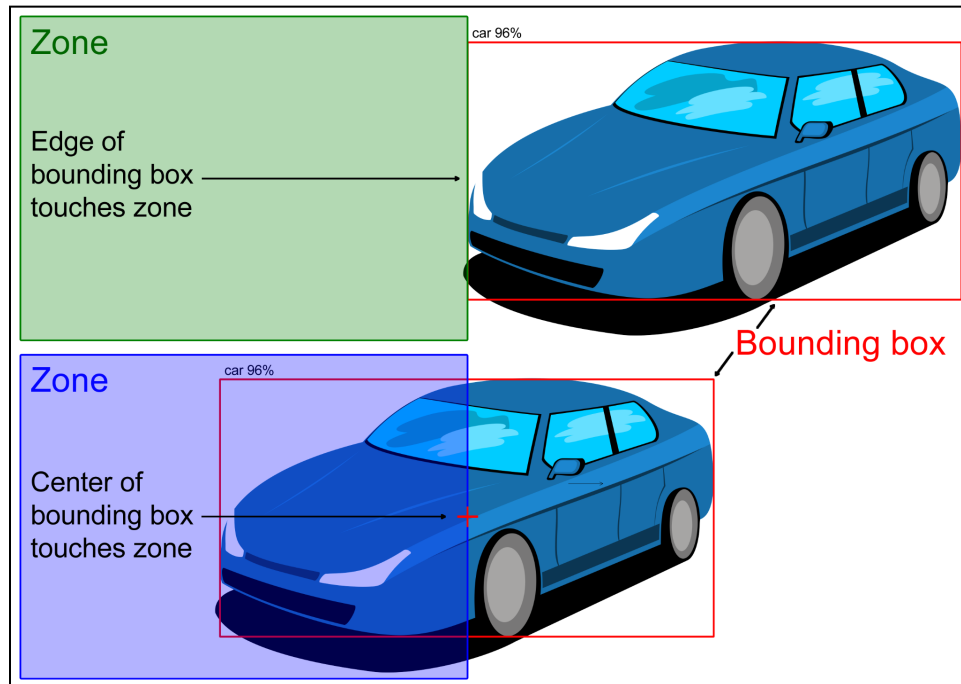
Options for defining when an object enters a zone

2. **Display zone on results:** Enabling this option will display all the zones on the object detection alert images and report video clips. The zone outline and inclusive-area tint will be green or blue depending on your selection of edge or center of bounding box, respectively.

Add a Zone

1. In case the camera view has recently changed, click **Refresh preview** below the image.
2. Click the blue **+ Add Zone** button and a new zone with 8 vertices will appear.
3. Think about the unique purpose of this zone and enter a name in the name field. Having a meaningful name will help you identify the zones when you have multiple zones per camera or rule, and you want to edit them. The zone name will not appear in the alerts.
4. Decide if you will create an inclusive or exclusive zone and make your selection.
5. Click and drag the vertices around on the camera preview to create the desired zone shape.
6. Click the save button: 🔖

Edit a Zone

1. Click the edit button for the zone you want to edit: ✏️
2. Make all needed changes to the name, type, status, and zone vertices.
3. Click the save button: 🔖

Delete a Zone

1. Click the delete button for the zone you want to delete: 🗑

Zone Tips

1. If there are one or more areas you want to ignore, you can create exclusive zones and the remaining area will automatically be an implicit inclusive zone provided that you do not draw any inclusive zones. If you choose to display the zone on the results, the implicit inclusive zone will be displayed.

   a. If you want to ignore some or all object types in those areas, or you have multiple rules for the same object type, then it may be easiest to create the exclusive zones at the camera level. Remember that the camera-level zones will not apply to any rules that have rule-level zones.

   b. If you only want to ignore one type of object in those areas and you only have one rule for that object type, then you may create the exclusive zones in the rule for the object type you want to ignore.

2. In some cases, it may be easiest to create a combination of inclusive and exclusive zones at the camera level or within one rule. In this case, an exclusive zone will have no effect unless it overlaps an inclusive zone thereby subtracting from the inclusive zone. That is because all areas outside of the inclusive zones are already excluded. Furthermore, remember that zones from different levels or rules do not ever combine or work together.

3. For each camera, all zones that are set to display on the results will appear on every detected event regardless of whether each zone was part of the detection logic.

Capture Source Considerations

The capture source for each camera can be either **snapshot** or **stream**, and each option has different effects.

Snapshot Mode

- Snapshot mode is preferred for the Base and Pro models, because those models support more cameras and higher resolution in snapshot mode.
- MR can capture multiple frames per second in JPEG format.
- It is best to get snapshots directly from each camera rather than from or through an NVR.
- The snapshot resolution should be 2 MP (1920x1080) or less to reduce processing load on the cameras, network, and MR. This is not to say that higher resolution snapshots cannot be used; they just might be less stable depending on the devices.
- With higher resolution cameras check for a way to request snapshots at a lower resolution.
  - You need to manually add a camera to specify an alternate snapshot URL.
  - Some cameras only provide snapshots in main-stream resolution.
- If the high-resolution snapshots do not work well (the camera cannot send them fast enough for a stable connection), consider switching to **stream** mode and use a sub stream.

Stream Mode

- Stream mode is preferred for the Spartan models, because those models have the processing power to support all cameras in stream mode, and RTSP video streams are generally more available, configurable, efficient and stable.

- For the Base and Pro models, the number of supported channels is reduced when using stream mode. Two (2), three (3) and twelve (12) streams up to 2 MP each are supported by the Base, Pro and Spartan units, respectively.
- The video stream should be H.264 encoded with any special smart/ultra/zip/+ encoding options disabled. Use the "main" encoding profile rather than the "high" profile.
  - Technically, H.265 streams and some special encoding options are supported for object detection, but the increased processing required may reduce the number of channels that can be processed, and live view of H.265 video is not supported by the WUI or mobile app.
- Turn on **Key frame mode for streams** in the MR 🖵 System Settings (with MR software version ≥ 1.2.5) to enable 5 or 6 streams to be processed on the Base and Pro units, respectively. You should configure the streams to produce key frames (I-frames) at a rate of 1 to 2 per second. This means that the I/key-frame interval (also known as GOP or GOV) should be 1 to ½ of the frame rate. For example, if the frame rate is 12 [fps] then the key frame interval should be 12 to 6 [frames]. Note that a higher key frame rate increases the video bit rate and recording space usage.
  - It is preferable to use a lower resolution auxiliary stream that is not being recorded.
  - Add a camera manually to specify an alternate stream URL.

Finding Camera URLs

To add a camera or video server manually, you will need the RTSP stream URL and/or the JPEG snapshot URL along with the username and password. Here are some ways to get those URLs.

1. Try adding the camera or video server automatically using the camera search. This will work if the device is ONVIF conformant.
   a. After the video server is added, open its **Details** to see the URLs.

Location of camera/encoder connection details

   b. You can try the same URL templates for similar models even if the device is not found with the camera search. You will need to modify the IP address and possibly the port, channel and stream numbers in the URLs for other cameras/devices of the same brand or manufacturer.

Example of camera/encoder connection details

2. Ask the manufacturer, or search their support documents.
3. Use one of the following databases.
   https://www.ispyconnect.com/cameras
   https://camlytics.com/cameras

   a. Select the vendor of the video server.
   b. Find (Ctrl-f) your video server model and click its row.
   c. Enter the IP address of your video server in the URL Generator
   d. Delete any prefilled username and password and leave them blank. These will be entered separately in the MR WUI.
   e. Set the desired video channel if needing a channel other than the first.
   f. Generate the URL as shown below.

Example of finding stream and snapshot URLs using ispyconnect.com

Axis Video URL Generator

FFMPEG

IP	192.168.1.20
Username	
Password	

Note: Use your camera credentials, not your ispyconnect login.

| Channel | 0 |

rtsp://192.168.1.20/onvif-media/media.amp
Copy

Close   Generate

The URL generator dialog on ispyconnect.com

Networking Tips

The cameras must either be on the same LAN, or they must be accessible through network address translation (NAT) or port forwarding. When using the automatic camera search, the cameras must be on the same LAN. When manually adding camera URLs, it is possible to connect to cameras through NAT or port forwarding. If your cameras are connected directly to an NVR or DVR, then they are usually on an isolated LAN that cannot be reached from your router or main LAN subnet. Examples and tips for various network configurations are given below.

Cameras on Network Switch

1. Connect MR Video Assistant via Ethernet to the network switch having internet access.
2. Connect any MR smart plugs and relays to the same network via WiFi or Ethernet.
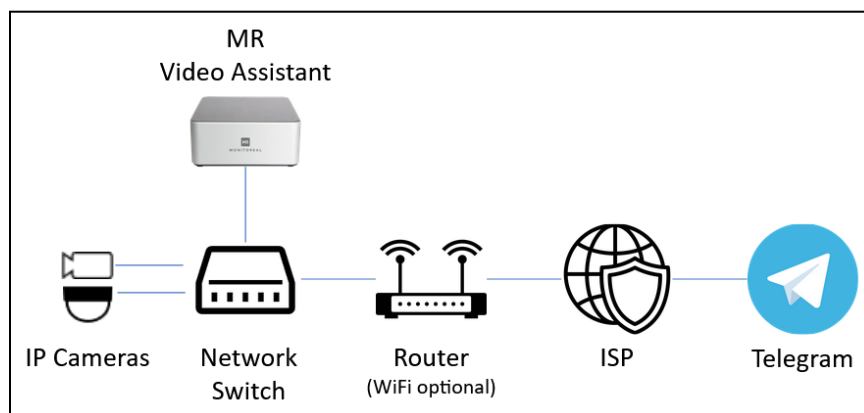
Example with IP cameras connected to a network switch having internet access

Cameras on General WiFi

1. Connect MR Video Assistant via Ethernet (preferred) or WiFi to the router.

2. Connect any MR smart plugs and relays to the same network via WiFi or Ethernet.
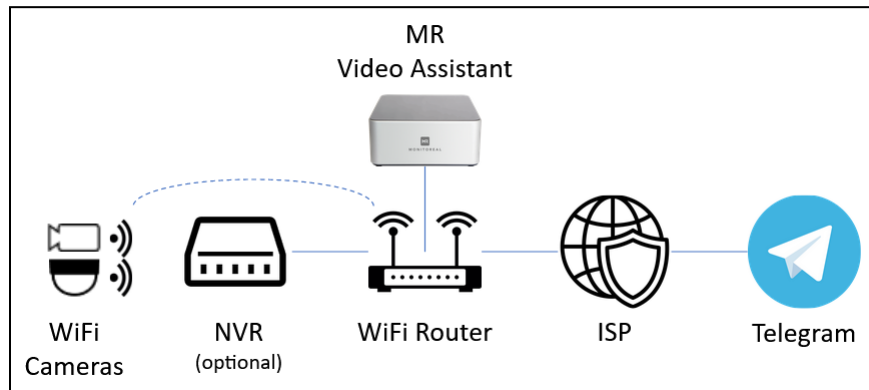
Example with WiFi cameras connected to the general network

Cameras on PoE-NVR or WiFi-NVR

The challenge with having the cameras connected directly to a plug and play PoE NVR or WiFi NVR is that the cameras are usually on a separate network that is isolated from the rest of your network. If the MR unit is connected to the same isolated camera network, then it can function with the cameras, but it will not be able to send notifications outside of the camera network without a secondary network connection. There are three options in this case.

1. Dual NIC Option: Connect the MR unit to the isolated camera network and internet using two network interface cards (NIC) on the Monitoreal unit
2. Single NIC Option: Change camera connection points and use a single NIC.
3. Add video channels from a video server. Jump to Cameras on DVR, NVR or Encoder.

Dual NIC Option

1. Connect MR Video Assistant via Ethernet to a camera port on the NVR.

    a. If your NVR does not have an open camera port, then you can add a PoE switch to the camera network (to add ports), or use the Single NIC Option (preferred) or see Cameras on DVR/NVR.

2. Also connect the MR video assistant to an internet gateway via WiFi or USB-Ethernet adapter (USB-Ethernet adapters available from third parties).

3. Connect any MR smart plugs and relays to either of the networks.
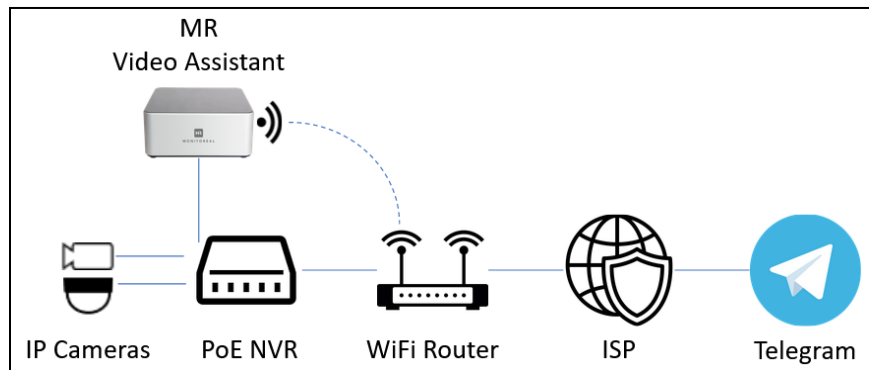
Example of dual NIC (Ethernet + WiFi) connection where cameras are connected to NVR subnet
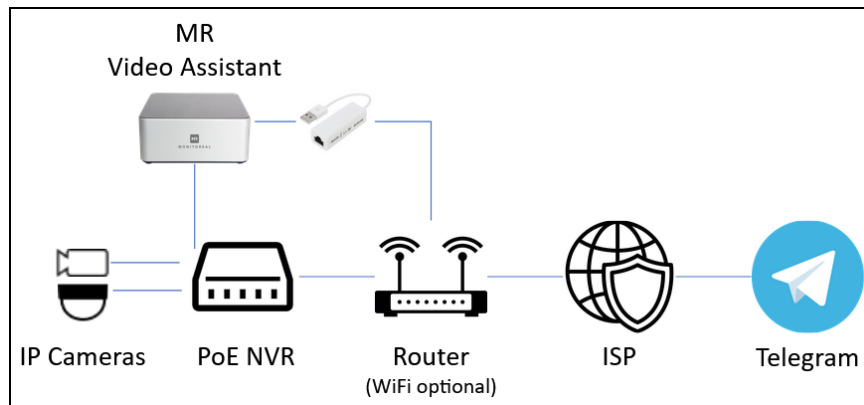
Example of dual NIC (Ethernet + USB-Ethernet) connection where cameras are connected to NVR subnet

Single NIC Option

1. Change how the cameras are connected to use the single NIC option.

   a. **WiFi Cameras:** Connect the cameras to a general WiFi network with internet access instead of the NVR's isolated camera network.

   b. **PoE Cameras:** Connect all the cameras to a PoE switch (sold separately) that is connected to your internet gateway.

2. Connect the NVR to the network switch (preferred) or router.

3. Re-add the cameras or update their IP addresses in your NVR.

4. Connect the MR unit to the same switch or router that the cameras are now connected to.

5. Connect any MR smart plugs and relays to the same switch or router.
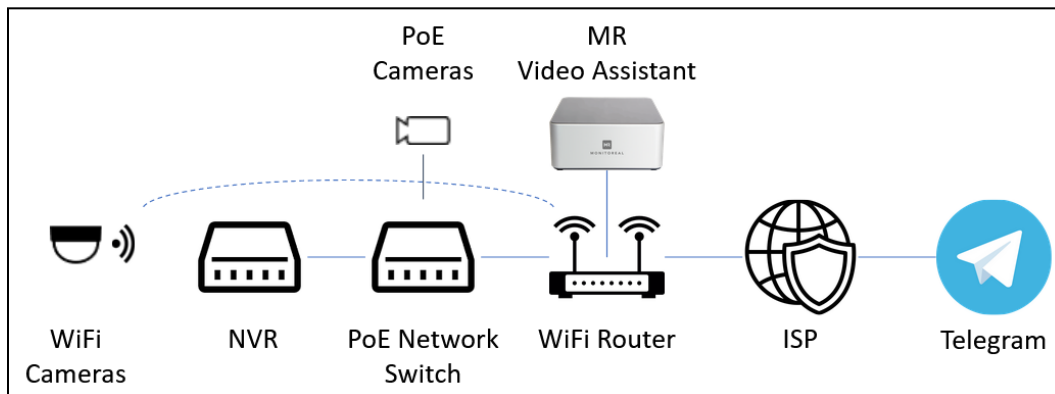
Example of single NIC MR connection where cameras were connected to NVR subnet

Cameras on DVR, NVR or Encoder

If your cameras are connected directly to a DVR or video encoder, then they are analog cameras, which must be encoded by the DVR or encoder to be accessed via network. If you have IP cameras connected to an isolated subnet of an NVR, then they cannot be reached from your router or main local area network subnet. In both cases, the cameras can be added to a Monitoreal Security Assistant (MR) by adding the video channels served by the DVR, NVR or encoder (video server). The network should resemble the following diagram.
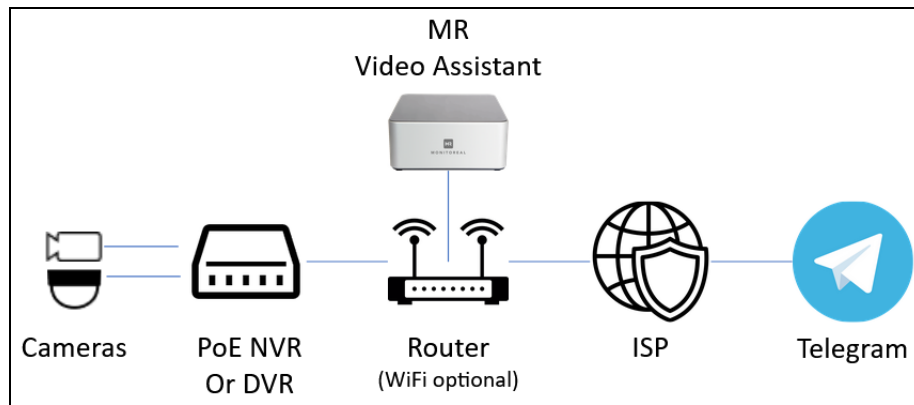
Example with analog cameras on DVR or IP cameras on NVR subnet

1. Connect MR via Ethernet to a switch or router that is also connected to the video server.

2. Add cameras using stream and snapshot URLs provided by the video server.

   a. Try adding the video server automatically using the camera search. This will work if the device is ONVIF conformant. You will need the username and password for the video server. Enter the IP address of the video server to avoid searching the entire network for additional ONVIF devices.

Adding an encoder using camera search

   b. The first camera from the video server will be added to MR. Open the **Details** of the first camera.
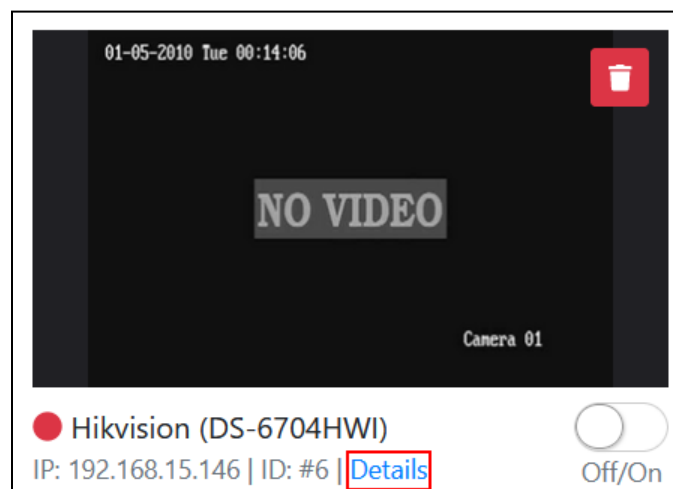
Location of camera/encoder connection details

   a. Copy the stream and snapshot URLs to a notepad.

Example of camera/encoder connection details

c. Manually add more cameras from the video server using the copied URLs with modification of the camera channel. To get the 2nd camera in this example with an old Hikvision digital video server (encoder), change the number 101 in the stream URL to 201, and the number 1 in the snapshot URL to 2.

    i.   Hikvision devices address the channel (C) and stream (S) with a four-digit number formatted CCSS. For example, channel 1, stream 1 is 0101, and the leading 0 can be omitted. Channel 16, stream 1 is 1601. For streams, 01 is mainstream and 02 is substream.

    ii.   Devices from other manufacturers may use a different convention.

    iii.   See [Finding Camera URLs](#) for other options.

Manually adding 2nd channel from encoder with modified URLs
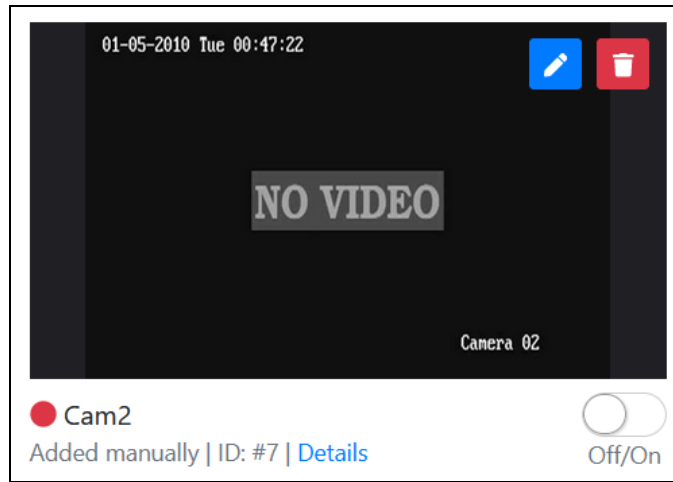
2nd channel from encoder successfully added

    d. Activate each camera added to MR by flipping the toggle switches to the On position.

3. Connect any MR smart plugs and relays to the same network as MR via WiFi or Ethernet.

Network Segmentation

Network segmentation is a network architecture approach that divides a network into multiple segments often referred to as subnets, each acting as its own smaller network. A segmented network can improve security and performance. Network segments can be created for different categories of devices and users. For example, one could have subnets for family/employees, guest access, IoT/smart devices, and security devices. Use multiple routers and/or virtual LANs (VLANs) to create network segments.

In the basic example below, MR and any WiFi cameras, NVR/DVR, smart plugs and relays connect to Router 1. Other personal devices such as PCs and smartphones can connect to Router 2. Connect a Router 1 LAN port to the Router 2 WAN port and ensure the routers have different subnets. This way, your personal devices can access your IoT devices, but the IoT devices cannot initiate access to your personal devices.
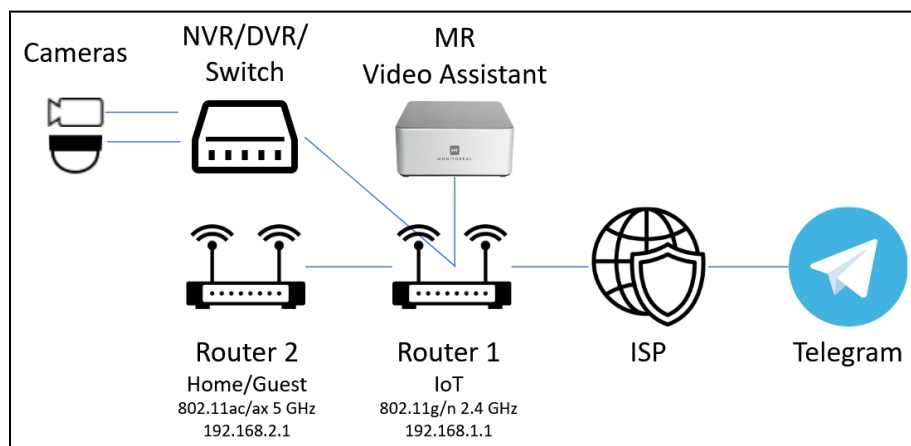
Example of segmented security and personal networks

Minimum Object Size

How small of an object can the Monitoreal Base Unit detect?

As a general guideline for achieving consistent detection accuracy, each object of interest should fill at least 15% of the image frame.

What is 15% of the image frame?

For example, a 2 MP image frame has pixel (px) dimensions of 1920 ×1080 px.
15% of the image frame width = 1920 * 0.15 = 288 px.
15% of the image frame height = 1080 * 0.15 = 162 px.

The objects in the following images have widths and/or heights that are 15% of the corresponding dimension of the containing image frame.
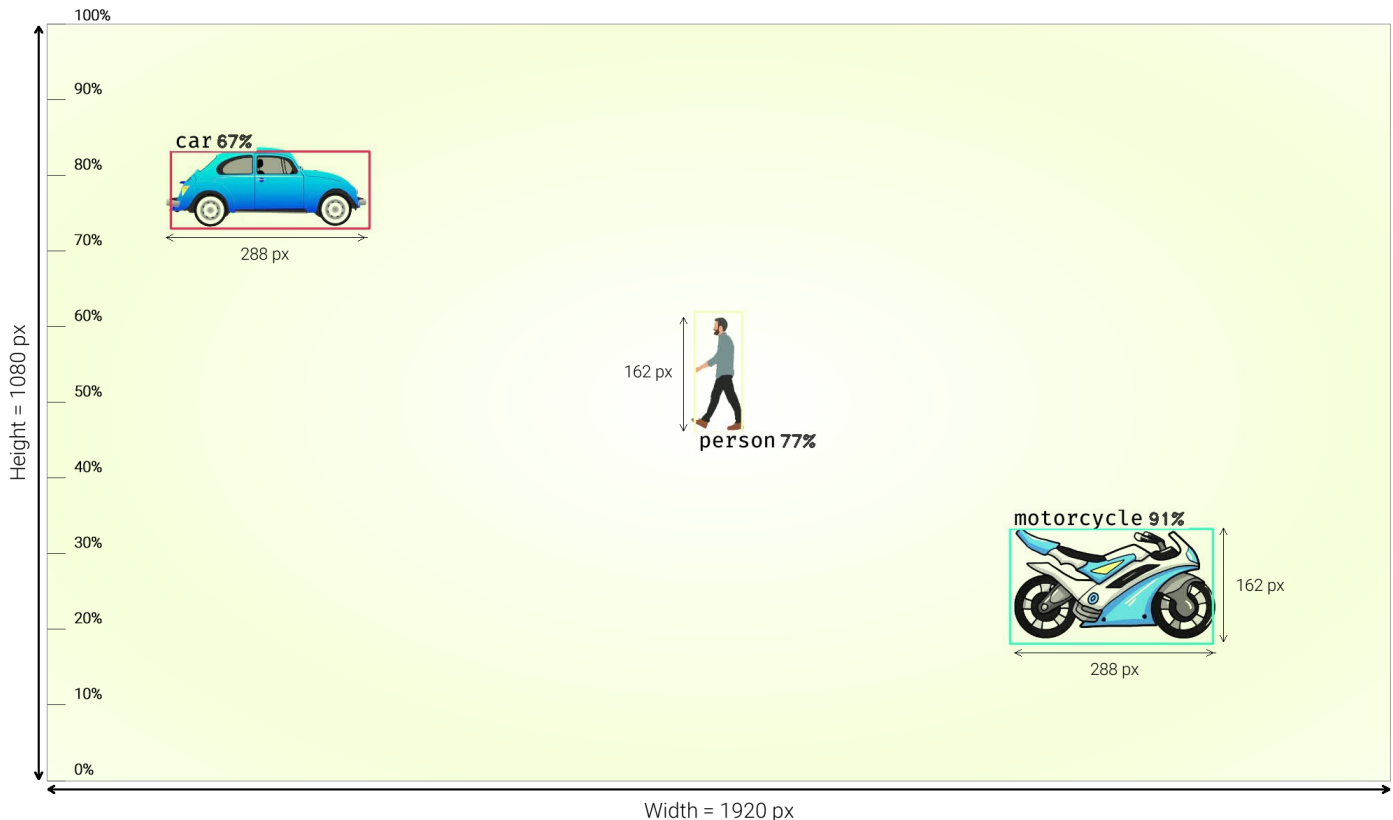
Example of objects that fill 15% of the image frame

How can a camera system be designed to ensure that the objects will be large enough?

Use an image calculator to determine the pixels per foot (or any unit distance) on a target captured by a camera at the farthest distance of interest. Multiply that linear pixel density with the real size of the object to get the object's image size in pixels and determine if it is at least 15% of your image frame size. If it is not, then you need a camera with a longer range lens.

For example, with a goal of detecting people greater than or equal to 5 ft tall at a distance up to 25 ft, and a camera that captures 33 px/ft at 25 ft (based on image calculations), multiply the linear pixel density on target by the target's linear size using the same unit of distance for each:

$$33 \text{ px/ft} * 5 \text{ ft} = 165 \text{ px}$$

This means that a 5 ft tall person standing 25 ft away from the camera will have an image height of 165 px, which is greater than 15% of the 1080 px image frame height (162 px). Your results will vary due to any difference in camera resolution, field of view, or object size and distance.

Note: Sometimes slightly smaller objects can be detected, and sometimes the object needs to be slightly larger. There are many parameters affecting how large an object appears in a camera image and whether or not the object is detected. Adjustments to the detection settings can improve detections.

RECORDER

The **Recorder** page provides playback of recorded video. Note that recorded video of object detections can also be played from the **Live stream** page under recent events and from the **Archive** page. The Recorder page provides access to all of the continuously recorded video whether or not there was an object detection. Refer to Video Recording Settings to enable video recording. This section explains the Recorder page.

1. Go to ⚙ **Settings → Recorder**.
2. Select a camera and date to review.
3. Click **OK**, and the video for the selected camera and date will load.
4. There will be a 24 hour playback timeline that is split into ~5 minute video segments. The number of each detected object type in each video segment will be graphed with color coding. Click on any segment to play the video.
5. You may zoom in anywhere on the timeline.

    a. ⬓ Click this icon to zoom in by dragging a click or touch across the region you want to see. You may zoom in multiple times.

    b. ⬒ Click this button to go back to the previous zoom level.

    c. ↻ Click this button to restore the full timeline.
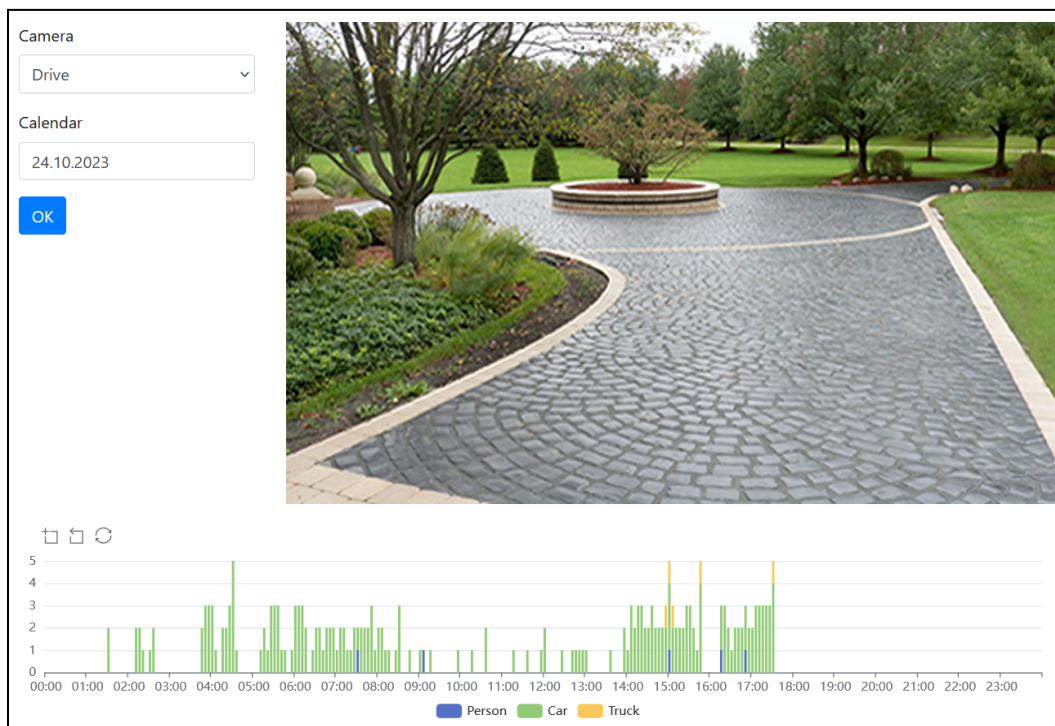
Video playback on the Recorder page

AUDIO

MR models can connect to speakers and play sound files when an object is detected or disappears. This feature can be used for various purposes such as audial alerts for the occupants of the building, or automated deterrence of intruders using pre-recorded sounds or voice messages with indoor or outdoor speakers. All MR models can connect to Bluetooth® receivers and speakers. Additionally, MR Spartan models have a 3.5mm analog audio output.

1. Connect Wired Speakers

MR Spartan models have a 3.5mm headset audio jack on the front of the appliance, which can be connected to various audio systems and speakers including public announcement (PA) systems, home

and pro audio systems, A/V receivers, and speakers with an integrated amplifier. Depending on the audio receiver you intend to connect, you might need to purchase or make an adapter cable. Audio cables with 3.5mm connectors are available with lengths up to 200 ft (70 m) or more. The audio can also be transmitted over ethernet cable by using baluns.

a. The MR side of your audio cable must be a 3.5mm connector (type TRS, TRRS or TS). Plug this side into the headset jack on the front of MR.
b. Connect the other end of your cable to the audio receiver of your choice. In case you need and have bare wires on this side and there are more than two wires, you need to use the left or right channel (one or the other) and ground. The ground wire is typically the larger wire that is bare within the outer sheathing. If you do not know which of the other wires are for the left or right channel, try using one at a time until you find one that works by playing an audio clip on the 3.5mm output.
c. Proceed to Upload Audio Files.

2. Connect Bluetooth® Speakers

a. Prepare your Bluetooth® speaker by bringing it in working range with MR, turning it on, disconnecting any other devices that may be connected, and enabling pairing mode.
b. In the WUI of MR, go to ⚙ **Settings →** 🔊 **Audio.**
c. Click the blue Search button to search for Bluetooth® devices.
d. Click **Connect** next to the desired speaker
e. The device will appear under **My devices** upon successful pairing.
f. The speaker should remain powered on all the time, or whenever needed.
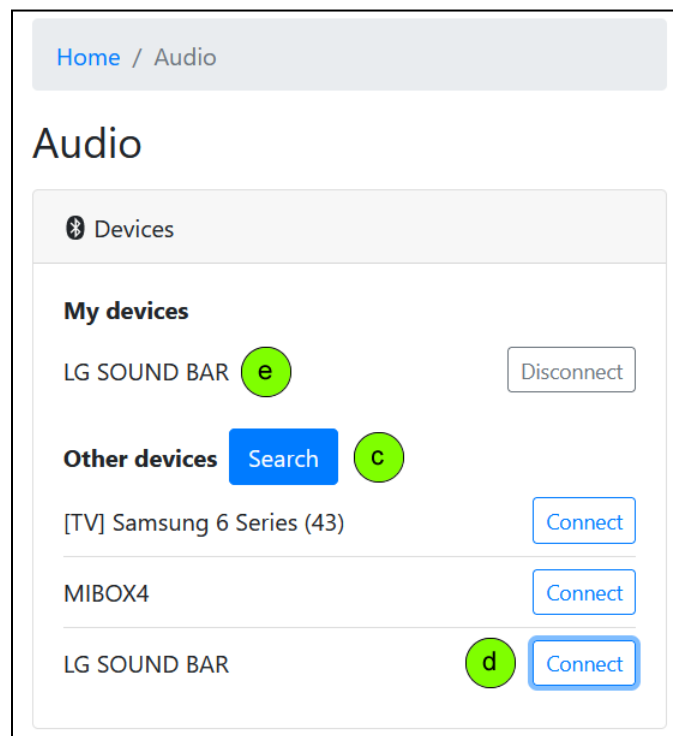
Example of pairing a Bluetooth® speaker

3. Upload Audio Files

a. Remaining on the 🔊 **Audio** page, click the **Browse** button and select the audio file that you want to upload. MR accepts nearly any audio file format.
b. Click the blue **Upload** button, and the file will appear below as a WAV file once the upload and conversion is complete.
c. You may then test play the audio file on the speaker of your choice by selecting the speaker below the file input field and then clicking the play button next to the desired audio file.
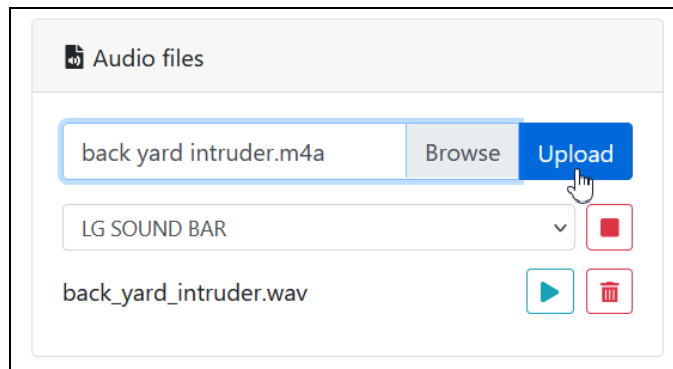
Example of uploading an audio file

4. Add Audio Actions

a. With a Bluetooth® speaker connected to MR, audio actions can now be configured in **Alert & Action rules**. Go to the 📷 **Cameras** page, find the desired camera to link with the relay, and select the **Alert & Action rules** tab.

b. Click the audio button for the rule that should play the audio file: 🔊
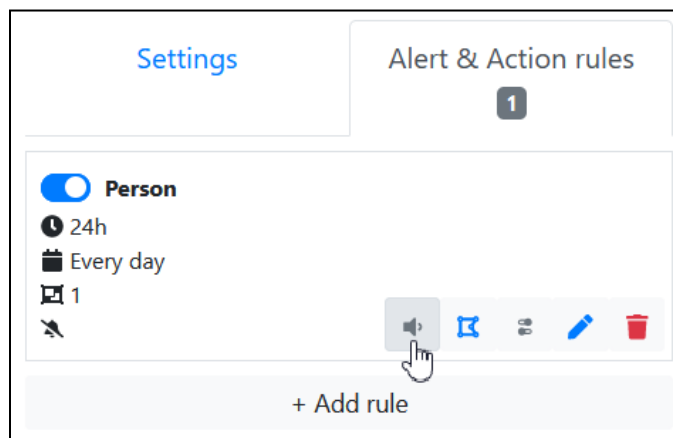
Click the audio button for the rule that should play the audio file: 🔊

c. The **Audio actions** dialogue will appear. Click **Create action** on the **Object detected** tab and/or the **Object disappeared** tab depending on your needs.

d. Enter a name for your own reference.

e. Select the device (speaker) to play the audio file.

f. Select a previously uploaded audio file to play.

g. Enter a trigger delay of 0 or more whole seconds. Note that there is already an inherent delay with playing the audio on a Bluetooth® speaker.

h. Click **Save** and then **Close**.

Example of adding an audio action when an object is detected

RELAYS AND SMART PLUGS

Monitoreal manufactures smart plugs (electrical outlets) and relays that enhance your autonomous Monitoreal system with the ability to control power and logic signals to large and small electrical appliances and devices. The outlets and relays are both compatible with low-voltage and high-voltage loads up to AC 250 V. Unlike many other smart plugs, these Monitoreal accessories do not require or use an internet connection (unless updating), nor do they rely on a cloud service remaining online or in business. Rather, they are controlled locally by MR in an autonomous system with the option for manual control locally via the WUI and physical buttons and remotely via Telegram. These accessories are sold separately.

1. Connect Relay to Network
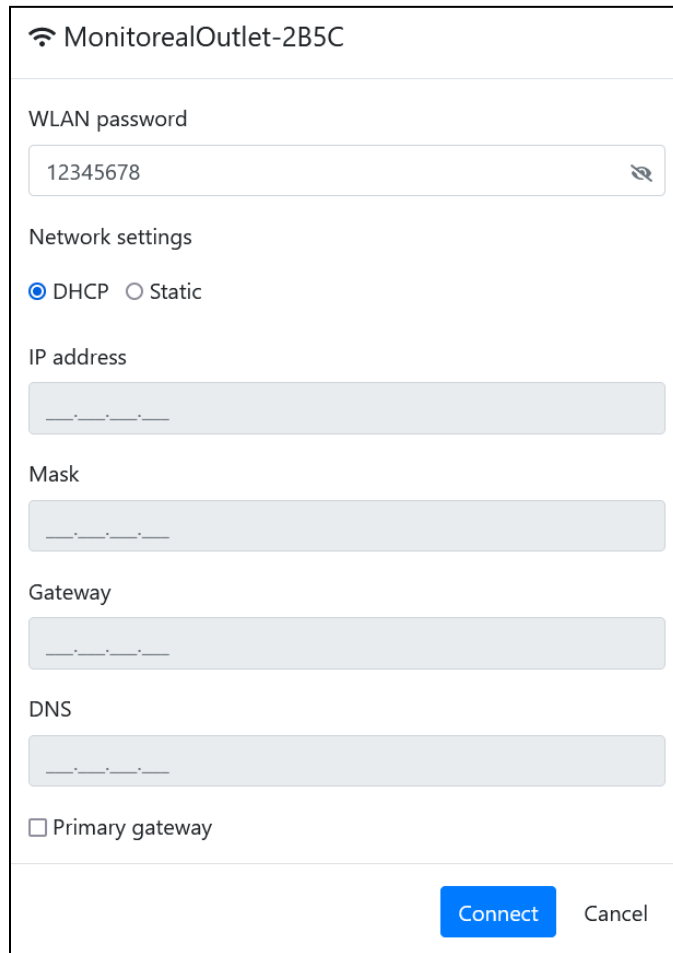
   a. Smart plugs and relays will both be referred to as a relay. Power on the relay with AC 90–240 V. If the relay connects via WiFi, power it on in the same room as MR for initial setup to ensure good WiFi connectivity, and follow the next steps in WiFi Relays; otherwise, skip to Ethernet Relays. Then, proceed to Add Relay to MR.

WiFi Relays

   b. Connect to the WUI of MR using its Ethernet port IP address, because MR will need to connect directly to the relay via WiFi for initial connection of WiFi relays. The relay can then be switched to client mode and connected to your preferred WiFi network.
   c. In the WUI of MR, go to ⚙ **Settings → 🖧 Network** and click the **WiFi networks** button.
   d. Search the available WiFi networks for "MonitorealOutlet-xxxx" and select it.
      i. The 4-channel WiFi relay may be reset by holding the reset button until the light flashes.
      ii. The WiFi smart plug may be reset by holding the power button until the light flashes.

e. Connect to the relay using default password 12345678 and leave the other settings at their default values. You should receive notice of a successful connection.

Default settings to connect to the WiFi relay

Ethernet Relays

f. Connect the relay to the same local area network as MR using an Ethernet cable.

  i. The relay must initially obtain an IP address via DHCP. If the relay does not get an IP address, the power light on the relay will continue to blink. In this case, try connecting the relay to a different Ethernet port or to a different network switch or router.

g. If an Ethernet connection is not available, and if the relay firmware version is 2.11 or greater, the relay may be switched to WiFi mode by holding relay button #3 for 5 seconds (until the power indicator light flashes). Then, follow the preceding instructions in WiFi Relays.

  i. Holding relay button #3 for 5 seconds toggles the relay between the Ethernet and WiFi networking modes.

  ii. Holding relay button #1 for 5 seconds resets the relay to factory settings.

2. Add Relay to MR

After connecting your relay to the appropriate network using the preceding steps, complete the following steps for Monitoreal relays of any type. Each relay cannot be added to more than one MR at the same time.

a. In the WUI of MR, go to ⚙ **Settings** → 🔀 **Relays** and click 🔍 **Relay Search.**

b. Any relays found on networks that MR is connected to will be available for adding. Click the add (**+**) button next to any devices you would like to add. I/O Network Relays with firmware ≥ 2.27 have a PIN feature that allows the relay to be moved from one MR to another without clearing the relay's settings or deleting the relay from the previous MR.

   i. If the PIN has not been set, enter any four digits when adding the relay to set the PIN.

   ii. The PIN can always be changed in the relay's options menu using the MR that the relay is currently connected to without knowing the previous PIN.

   iii. When a relay with a PIN is moved to a different MR, it is disconnected from the previous MR, but not deleted. If the relay is to be moved back to the previous MR, the relay must first be deleted so that it can be found in a relay search.

Relay search

Monitoreal outlet 2B5C 192.168.4.1   **+**

        ⟳ Refresh   Cancel

Example of finding and adding a relay without a PIN to MR

Relay search

Monitoreal relay 8238 192.168.10.115 | PIN | **+**

        ⟳ Refresh   Cancel

Example of finding and adding an I/O relay with a PIN (firmware ≥ 2.27)

c. The relay will appear on the ⇄ **Relays** page. The device name and channel names can be edited clicking the ✏ button that appears when hovering over the names. This is also where the relays can be manually switched via the WUI by clicking the toggle switch next to the channel. The current, voltage, and power relayed by the smart plug can also be monitored here.

● NIO ✏   ⋮   ● Smart Plug   ⋮

◯ Channel 1   ◯ Channel 1

◯ Channel 2   Current(mA) - 2

◯ Channel 3   Voltage(V) - 121

[Input 1] [Input 2] [Input 3]   Power(W) - 0

Example of added network I/O relay and smart plug

3. Relay Firmware Update

   a. Open the more options menu ⋮ on the relay and click **Update firmware**.
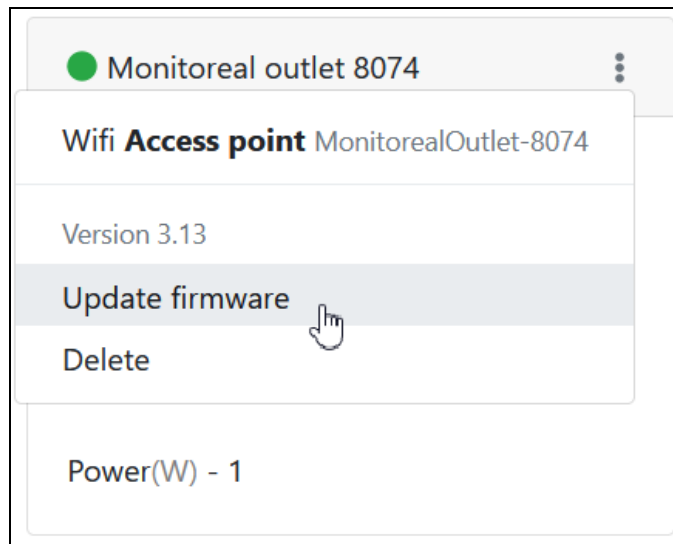
Check for relay firmware update

4. Change WiFi Relay to Client Mode

WiFi relays are initially in access point mode so that MR can connect to them via WiFi and then configure them. It is usually preferable to then change those devices to client mode and connect them to the network, via WiFi router or access point, to which MR is also connected. Relays connected with an Ethernet cable can be switched to WiFi if desired.

a. Open the more options menu ⋮ on the WiFi relay and click "Wifi **Access point**".
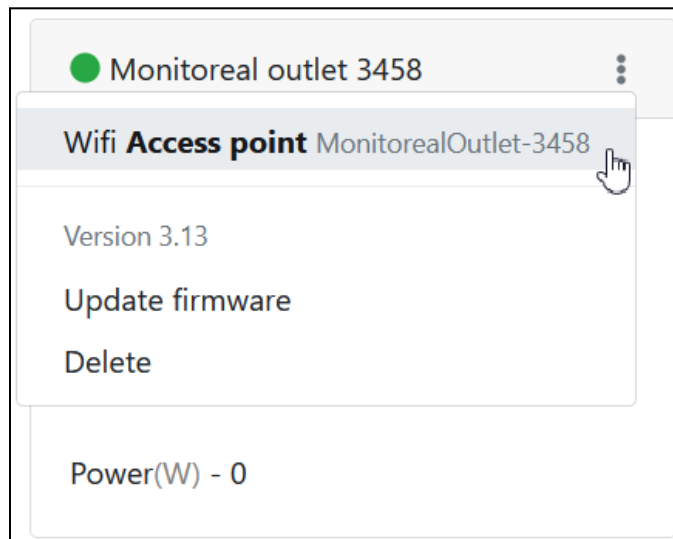
Changing a relay's WiFi mode

b. Select **Client** mode, type or search and select the WiFi network SSID, enter the WiFi password, select the desired WiFi transmission power level, configure for DHCP or static IP address, and click **Save**.

Connecting a relay to a WiFi network as a client

    c. Recall that MR's WiFi NIC was connected directly to the relay for setup. If you have just set the relay to connect to a WiFi network that is separate from the LAN that MR is connected to, then MR needs to be connected (or re-connected) to the same WiFi network to communicate with the relay.

5. Set Relay to Static IP Address

WiFi relays can be set to a static IP address by following the steps in Change WiFi Relay to Client Mode. For relays connected via Ethernet, follow the steps below.

    a. Open the more options menu ⋮ on the Ethernet relay and click the Eth IP address.
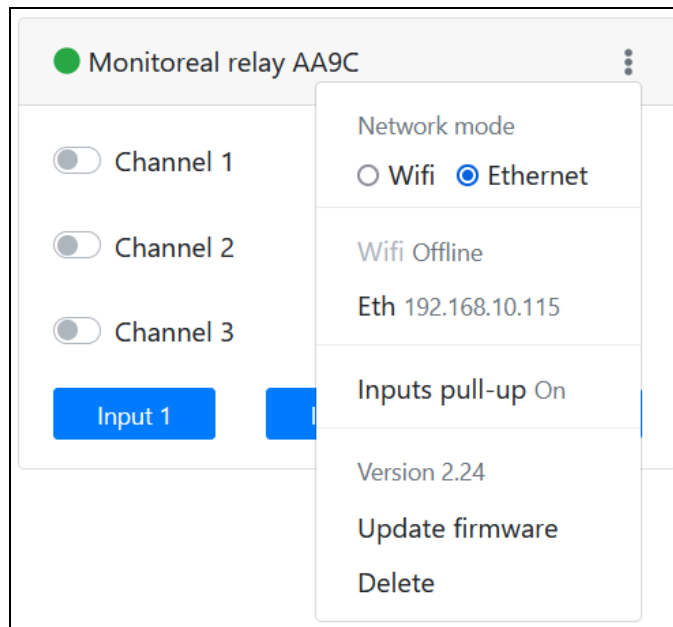
More options menu of Ethernet relay

b. Select **Static** configuration, enter the IP address to be assigned, and click **Save**.

Changing IPv4 configuration for Ethernet relay

6. Add Relay Actions Triggered by Object Detection

a. With a relay connected to MR, relay actions can now be configured in **Alert & Action rules**. Go to the 📷 **Cameras** page, find the desired camera to link with the relay, and select the **Alert & Action rules** tab.

b. Click the relay button for the rule that should trigger the relay:
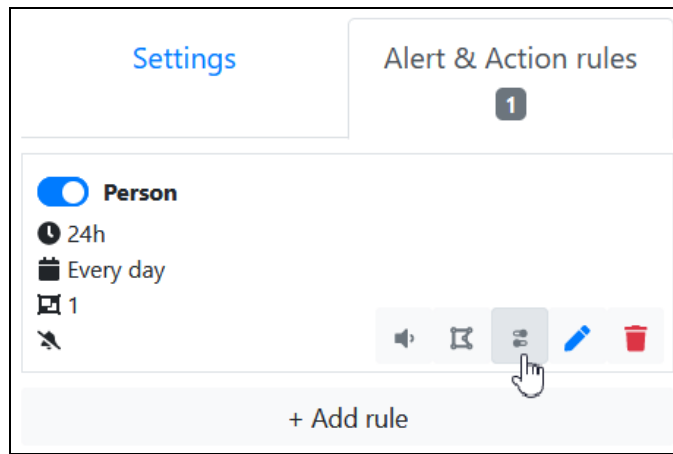
Click the relay button for the rule that should trigger the relay:

c. The **Relay actions** dialogue will appear. Click **Create action** on the **Object detected** tab and/or the **Object disappeared** tab depending on your needs.

d. Enter a name for the device that the relay triggers. This name will be used in the alerts.

e. Select the relay by name and its channel that is connected to the device to be triggered.

f. Select the desired relay action. The **Strobe** option slowly switches the relay on and off repeatedly for the specified duration.

g. Set the mode to **automatic** or **semi-automatic** if you want to confirm the relay action via Telegram before it executes.

h. Set the **duration** in seconds for the relay to remain on or strobing. The relay will return to its previous state after the duration. To turn on indefinitely, set the duration to 0 (this only works for the "Turn on" action).

i. Enter a trigger delay of 0 or more whole seconds. Using a trigger delay can make the action seem more human-like.

j. Click **Save** before switching between object detected and object disappeared.

k. Click **Close** when finished.

Example of relay action settings

7. Add Actions Triggered by Relay Inputs

The Monitoreal I/O Network Relay (IONR) has three relays (outputs) and three inputs. Any of the inputs can be used to arm and disarm MR, send snapshots, and trigger outputs.

- **Armed / Disarmed**

  This allows for integration with alarm systems that have an output indicating the arming status, and it synchronizes the arming and disarming of MR with your alarm system. A simple switch could also be connected to an input to provide a convenient way to arm and disarm MR.

- **Send snapshots**

  Snapshots from all connected cameras will be sent via your enabled alert methods. This allows you to see what is happening and verify alarms when any of your alarm sensors or zones are tripped.

- **Trigger output**

  Any input can trigger any and all of the outputs on the same relay to turn on, turn off, or strobe. A duration can be set for the turn on and strobe actions. An output can be turned on indefinitely by setting the duration to 0.

Follow these instructions to connect inputs and configure actions.

a. Connect your switch or other signal with two wires to one of the IONR inputs and a common contact (COM).

   i. The input may be a dry contact switch or relay, or a binary signal with a voltage up to 5 volts. Do not apply more than 5 volts to any of the inputs. When applying a voltage, ensure that the positive lead is connected to the "INPUT" side and the ground or common lead is connected to the "COM" side of the input. Refer to the input contact labels in the image below.

   ii. The inputs are internally connected to 5 V through a 1 kΩ pullup resistor. Be aware that a small current of up to 5 mA could be driven into your connected electronics/batteries if the applied voltage or resistance is low or zero.
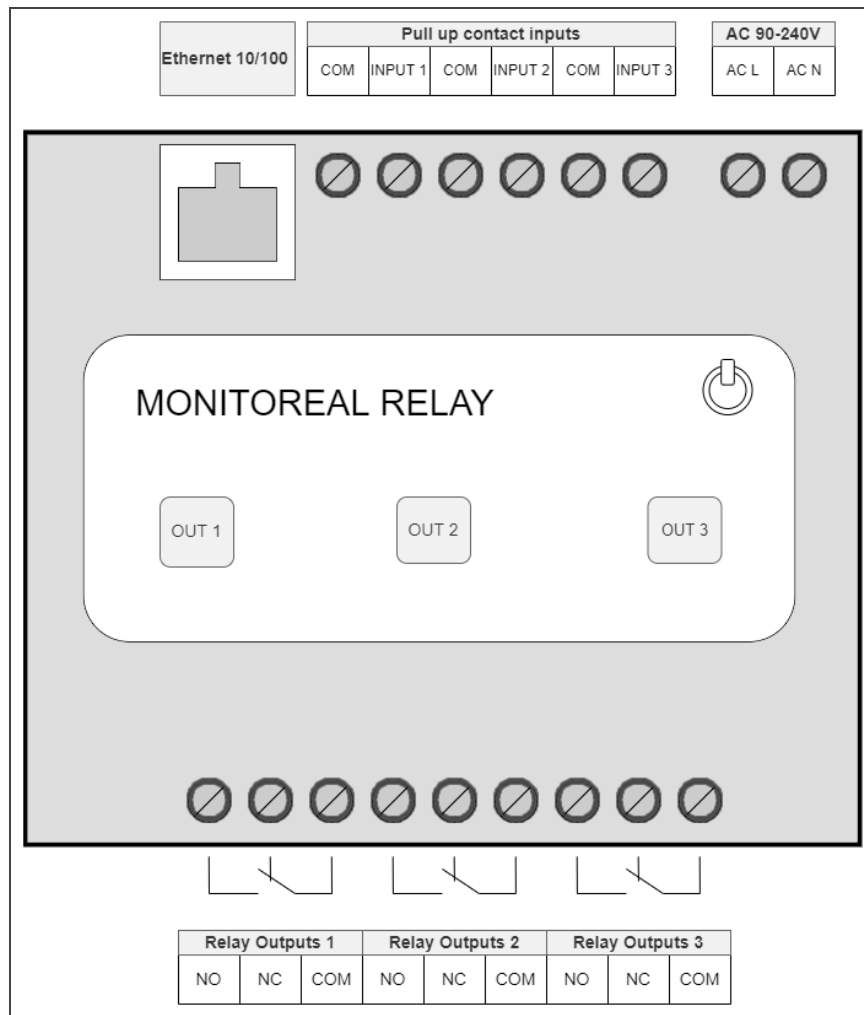
IONR drawing with labeled contacts and buttons

b. Go to ✿ **Settings** → ᠍ **Relays** and click the input button corresponding to the input that you have wired up.

c. Click **+ Add rule** to add an **Input State** that will trigger the **Action** you select.

    i. When using an input for arming and disarming, add two rules so that MR can be armed and disarmed by the input based on the input state.

d. Select the **Action** that you want the selected **Input State** to trigger. The options are Armed, Disarmed, Snapshots, and Trigger output.

    i. For arming and disarming, select **High** for one **Input State**, **Low** for the other **Input State**, and then set the desired action for each state.

    ii. The **Action** is triggered when the input state changes to the corresponding state. When the input contacts are not connected or there is a very high resistance between them, that is a "High" input. When the input contacts are connected together with a very low resistance, that is a "Low" input. For example, if you are using a voltage-free switch, then the input will be Low when the switch is closed, and High when the switch is open.

    iii. In another example, some alarm panels provide an output with a voltage in the Low range for MR when the alarm panel is armed, and an open circuit when disarmed. The low voltage is like a closed switch and the open circuit is the same as an open switch.

    iv. You may click Advanced under the Input State to customize the input range.

e. Optionally, the "Armed" and "Trigger output" actions may be delayed by a number of seconds. This can give you additional time to exit the view of the cameras to avoid tripping the alarm while leaving just after arming the system.

f. Click **Save** and then **Close** after saving succeeds.

Rules for input 1
Current input value High (91 %)

An action is triggered when the input state changes to the selected state. When the input contacts are not connected or there is a very high resistance between them, that is a "High" input. When the input contacts are connected together with a very low resistance, that is a "Low" input.

Voltage or resistance can be applied, and the ranges that correspond to digital Low and High are given below.

Low = 0–20% (0–360 ohms, 0–1.3 volts)
High = 21–100% (380–infinite ohms, 1.4–5 volts)

Note: Do not apply more than 5 volts.

Show less

Input State	Action	Delay sec
High	Disarmed	0
Advanced		
Low	Armed	30
Advanced		

+ Add rule

Save   Close

Example of IONR input configuration for arming and disarming

8. Toggle Relay Input Mode

The Monitoreal I/O Network Relay (IONR) has two input modes of operation: Pull-up On and Off.

- **Pull-up On**

Pull-up On is the default mode. Each input is internally connected to 5 V through a 1k ohm resistor. Connect buttons, relays, switches, etc. to the inputs and COM. Close the circuit to trigger the "Low" state. Open the circuit to trigger the "High" state.

- **Pull-up Off**

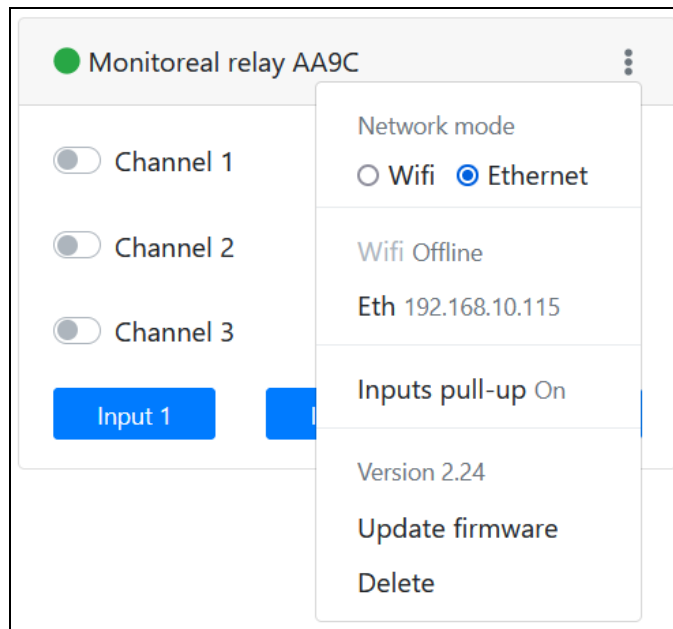Setting Pull-up Off makes it safe to apply voltages up to 30 V DC to the inputs. The inputs can sense voltages between 0 V and 4.2 V corresponding to input values between 0% and 84% following the equations below.

$Input = V_{in}/5 \times 100$ for $0 \leq V_{in} \leq 4.2$

$Input > 84$ for $4.2 < V_{in} \leq 30$

a. To change the mode, open the more options menu ⋮ on the IONR and click **Inputs pull-up**.

More options menu of Ethernet relay

    b. Select On or Off and then Save.

SYSTEM SETTINGS

Troubleshooting

We expect your MR to perform to your satisfaction; however, if at any time your unit is having trouble, we recommend troubleshooting the issue by restarting, running a recovery, or resetting. If the MR is unreachable via WUI or Telegram, then check The Obvious and Not-so-obvious and skip to the Recover / Update option.

The Obvious and Not-so-obvious

1. Ensure MR is plugged into a working power source.
   a. The power adapter's LED should be illuminated.
2. Ensure MR is connected to your network.
   a. The Ethernet port lights on MR should be illuminated.
   b. MR should display an IP address every couple of minutes unless the display was disabled.
   c. Can you see a device named "monitoreal" in your router's list of connected devices?
   d. Can you ping MR's IP address?
3. Ensure that your PC and MR are on the same subnet.
   a. Compare the first three octets of the IP addresses of your PC and MR. For example, if their addresses start with 192.168.1 and 192.168.0 then they are on different subnets, and you need to correct your network configuration. See Networking Tips.
4. Has the IP address changed? You can prevent it from changing using one of these options.
   a. **DHCP Reservation**
      i. Log in to your router's administration website and reserve an IP address outside of your DHCP range for the MAC address of your MR.
      ii. You might need to restart your router or MR for the new address to be assigned to MR.
   b. **Static NIC Configuration**
      i. In the WUI, go to ✿ **Settings** → ⊹ **Network** and **Network settings** under the desired NIC.
      ii. Select the **Static** option.

    iii.   Enter an available IP address that is outside the DHCP range on your network.

    iv.   The other settings should already be filled in and OK if the NIC was previously connected via DHCP. Otherwise, the Mask is usually 255.255.255.0, and the Gateway and DNS can usually be set to the IP address of your router.

    v.   Save the new settings and then refresh the page or go to the new IP address if you changed it.
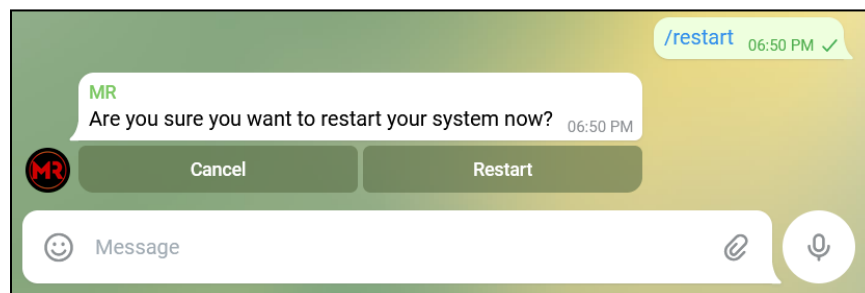
Restart via WUI

In the MR WUI, go to ⚙ **Settings** → 🖥 **System** and click ↻ **Restart**.

CPU load	78.3%
CPU temperature	63 °C
RAM	40.3%
Disk usage	84.2%
↻ Restart	

The MR restart button on the 🖥 System page

Restart via Telegram

Send the **/restart** command to your MR Telegram bot and select the **Restart** button.

Restart MR via Telegram

Recover / Update

1. Use a PC that is connected to the same LAN as MR.
2. Download the Recovery Tool from https://monitoreal.com/downloads/.
3. Start the Recovery Tool, and it will automatically search for MR. Continue when MR is found.
4. Keep **Factory Reset** unchecked.
5. Keep the version on **Main** unless you want to beta test new features in the release candidate.
6. Click Start recovery and wait for notice that it has completed. Do not remove power or internet connectivity from MR during this process.
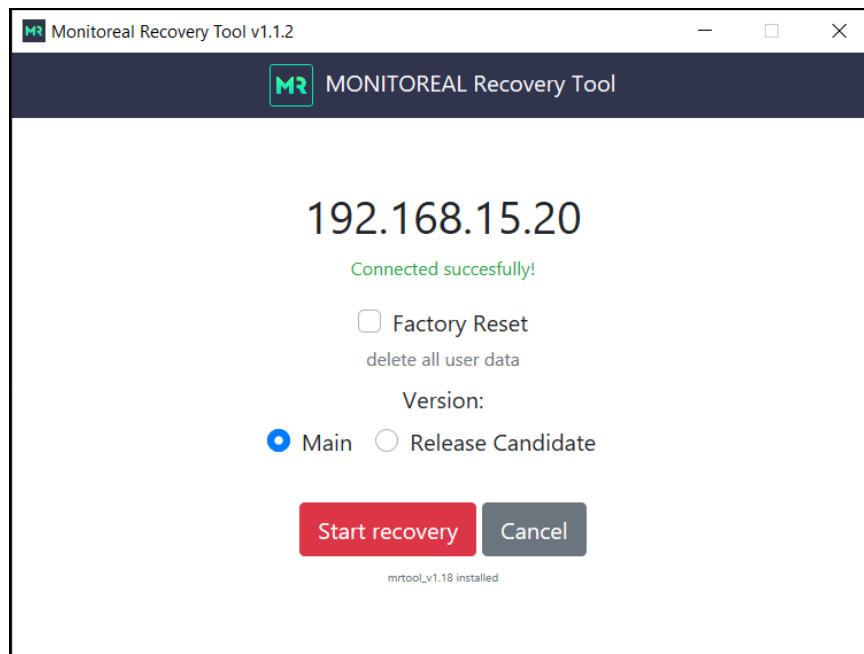
Device found in Monitoreal Recovery Tool v1.1.2

Factory Reset

Performing a **Factory Reset** is not recommended in most cases. If you need to use it as a last resort, please note that it will delete all user configuration and data. A factory reset can be performed using the Recovery Tool or the multifunction button on the MR.

Via Recovery Tool

1. Follow the steps for Recover / Update except at step 3, select the **Factory Reset** option.

Via Multifunction Button

2. Find the pinhole recessed button on the back of MR and use a pin to press it continuously for 10 seconds until the factory reset starts.
3. Wait until the factory reset completes and MR displays its IP address on the dot matrix display.
4. Access the WUI using the new IP address and reconfigure as needed.

Multifunction Button

The pinhole recessed button on the back of MR serves multiple functions. When the button is pressed and held, the LED display will count from 1 to 10. Each of the following functions can be executed by releasing the button when the corresponding number is displayed. If the count reaches 10, then factory reset will start immediately.

0. Display the software version with a quick press of the button
1. Reserved
2. System reboot
3. Run all diagnostic tests (#4, #5, #6, and #7)
4. Test the Intel® Movidius™ Neural Compute Stick (NCS) (exists only in MR Pro model)
5. Test the LED dot matrix display
6. Test the system fan
7. Test the system speaker
8. Perform a recovery with system update
9. Reset network settings

10. Factory Reset (see [Factory Reset](#))

Updating MR

Update via Monitoreal App

1. Open the Monitoreal Secure Guard app and open the burger menu and go to the **Dashboard**.
2. Verify that you are connected to the device that you intend to update by checking the device name at the top. If necessary, select a different device on the **Devices** page.
3. Tap the green menu button at the bottom-center and select **System**.
4. Tap **Check for update** and then start the update if an update is available.
5. Automatic updates can be toggled in the settings ⚙ of the System page.
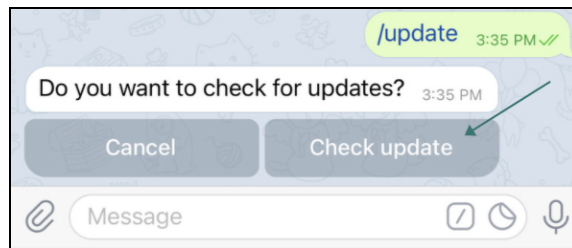
Update via WUI

6. Go to ⚙ **Settings** → 🖵 **System** → **Check for update** under System info.
7. If an update is available, an option to update will appear.
8. Optionally, you may enable **Auto update** under Settings on the same page. You will receive an alert whenever an automatic update completes.
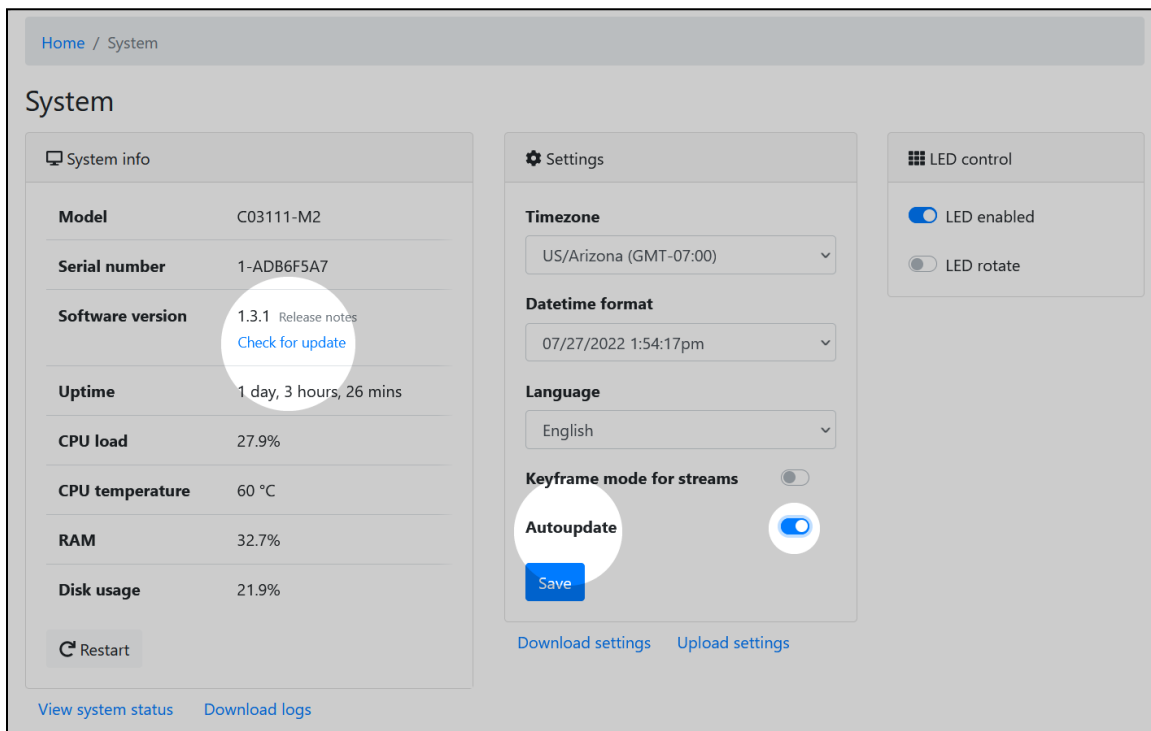
The MR 🖵 System page found under the main ⚙ Settings menu

Update via Telegram

1. Send the **/update** command to your MR Telegram bot and select the **Check update** button to check for an update.
2. If an update is available, then you may choose to update.

Check for an update via Telegram

Update via Recovery Tool

You can update MR without clearing its configuration using the Monitoreal Recovery Tool. See [Recover / Update](#) under [Troubleshooting](#) for instructions.

Backup Settings

Create a backup of your camera settings and restore your configuration if needed in the future. You could also upload settings from one MR to others to speed up deployments where each site is similar. All settings except for login credentials and network configuration will be restored; furthermore, relays cannot be automatically restored to a different MR.

Export Configuration

1. Go to ⚙ **Settings** → 🖥 **System** → **Download settings** under Settings.
2. Choose whether or not to set a password on the settings file. If a password is set, the password will be required when uploading the settings.
3. Click the **Download** button to download the configuration file.
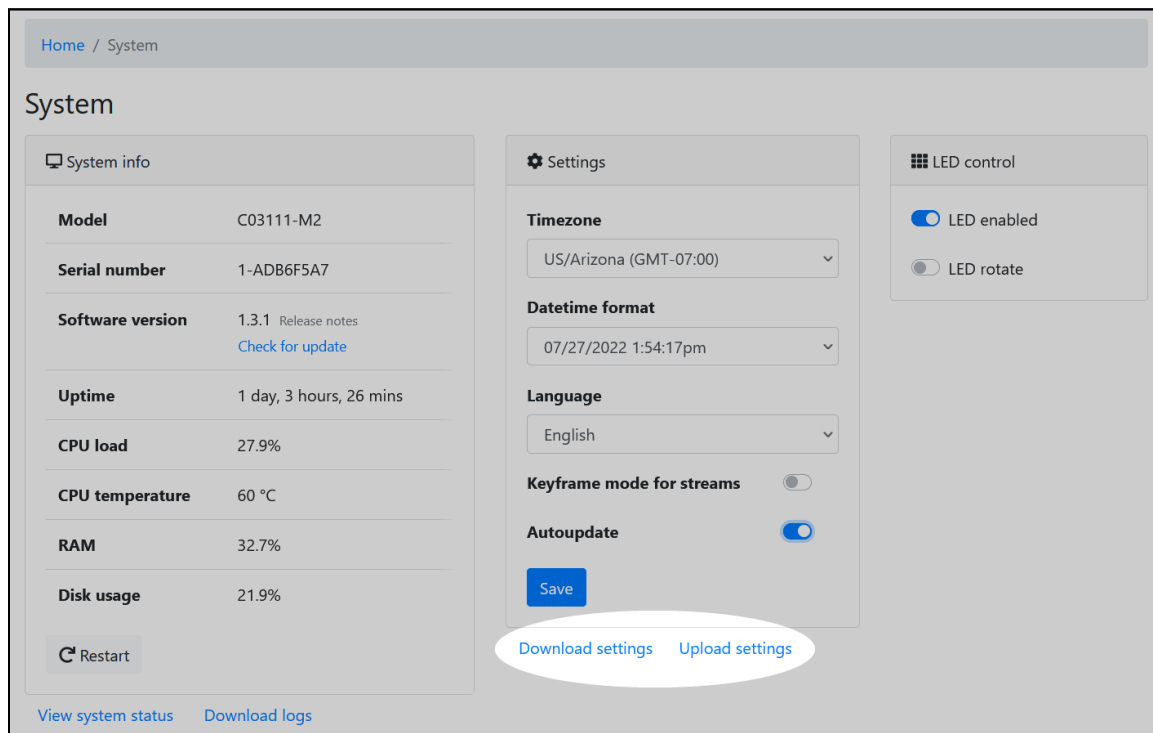
Download and upload settings options on 🖥 System page

Import Configuration

1. Go to ⚙ **Settings** → 🖥 **System** → **Upload settings** under Settings.
2. Enter your configuration password if you set it.
3. **Browse** and select your mrbackup file.

4. Click **Upload**.

Dialog for uploading an MR configuration file

The End