AiHomeGuardPro6 Linux Setup

Note: this USB drive will install AiHomeGuardPro6 Linux (Ubuntu 16.04) to a dedicated drive. If you prefer AiHomeGuardPro6 for Windows 10, you may download it from https://aihomeguard.com, and use the same key for its activation.

1 Connect PC to Home Router

You should connect your PC to your home router via its Ethernet port (preferable 1 Gb Wifi or Ethernet switch and ports) so that the link has enough bandwidth to receive aggregated traffic from all cameras.

2 Camera Setup

Follow the camera manufacturer's setup manual to connect them to your home router. Most IP cameras allow you to set them up using a web browser with a URL http://camera-local-ip (e.g. http://192.168.1.12). You'd better configure a static IP address for your cameras because they may reboot automatically, obtaining a different IP addresses from your router.

Set the frame rate and bitrate on cameras: **frame rate to 4 FPS; bitrate to 2048K.** Setting frame rate or bitrate higher than the recommended values may cause the streaming frames getting dropped, causing unstable object detection.

3 Install AiHomeGuardPro6 Linux to Hard Drive

Ensure that your computer has Legacy Boot enabled. Please check your PC's manual or Google its brand/model on how to enter BIOS mode while booting in order to enable its legacy boot. Once the legacy boot is enabled, press F9, F12 or another key, depending your PC manufacture/mode, to enter the boot selection screen, and then select the USB drive containing AiHomeGuardPro6 software. When prompted any input, enter "homeguard" as the password (ignore any error messages on screen).

You will be prompted for your confirmation to copy AiHomeGuardPro software image to hard drive which may take up to 500 GB of disk space. If your PC has more than one hard drive, then you will be asked to select a hard drive for installing AiHomeGuardPro. Warning: the installer will erase all data on the disk you have selected for AiHomeGuardPro6. if you are unsure which hard drive on your PC will be overwritten, please exit the installation process by selecting "No" for the confirmation prompt, and the PC will shutdown. To avoid mistakenly erasing a useful hard drive, you may open your PC cover, and disconnect the cable from the hard drives you want to preserve before trying the installation again.

After successfully installing the software, press Enter, and your PC will shutdown. Power on the PC after removing the USB drive to boot from the hard drive. Login with user "homeguard" and password "homeguard". Change your login password soon by using the main menu item.

Click on the network icon  at the bottom right and select "Auto Ethernet" (Figure 1). The PC will obtain an IP address from your home router. You will see  once the PC is connected to the network via the Ethernet port.

You'd better watch the setup demo video. To do so, select "Web Browser" from the main menu (by right-clicking anywhere on the screen). The browser home page is the local documentation folder. Please open the demo video MP4 file. The video goes through the setup process, including searching ONVIF cameras, drawing monitored areas, selecting and verifying AI inference backend, and so on.

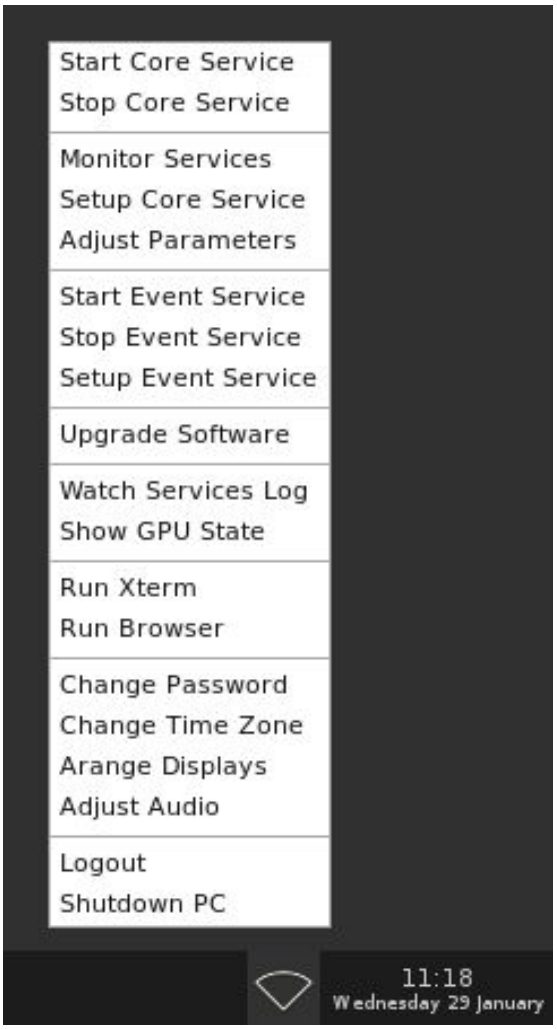


Figure 1.Main Menu

4 Core Service Setup

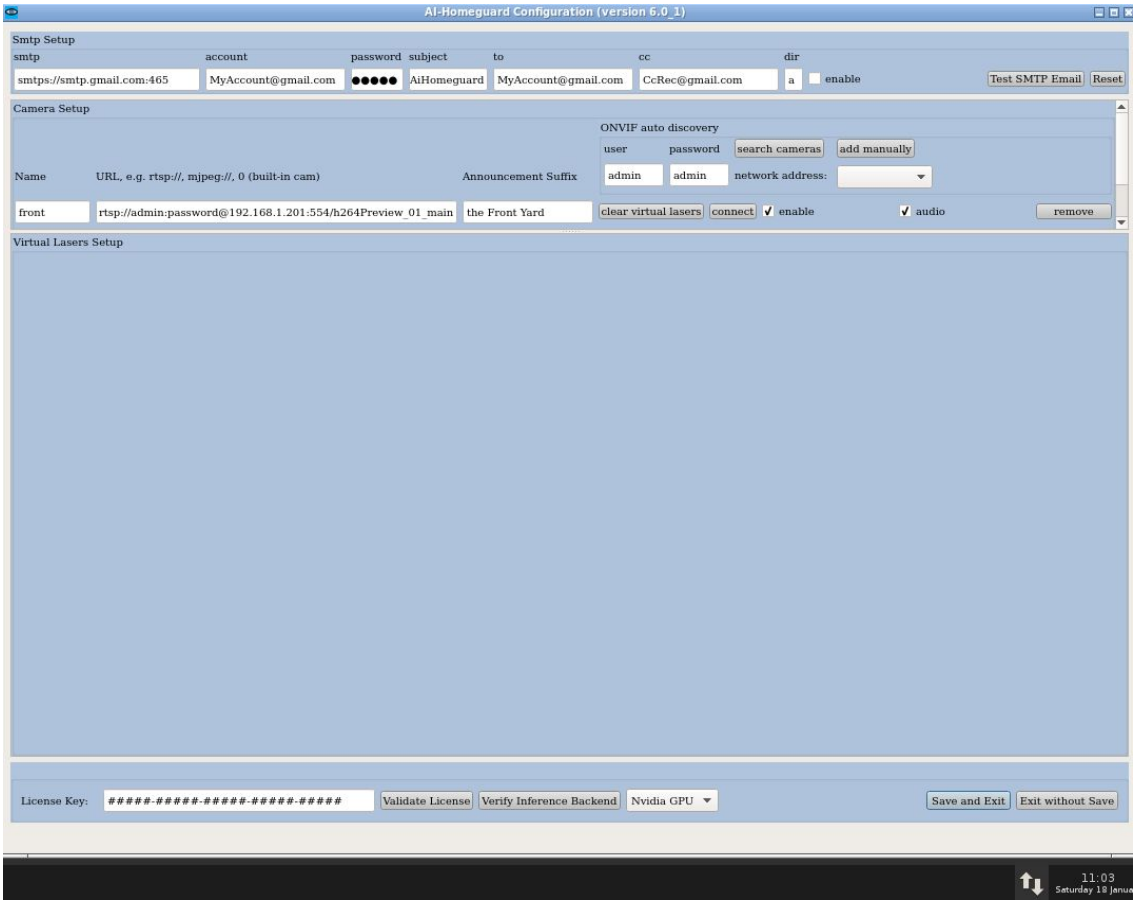


Figure 2. Core Service Setup

4.1 Setup Cameras URL(s) and their Monitored Areas

Open the Main Menu and select “Setup Core Service” (Figure 1) to enter the screen (Figure 2). Press the “search cameras” button to add your cameras automatically, or you may add cameras manually by clicking on “add manually”. Note: the auto discovery feature may need a correct password in the “password” field. You can do the search multiple times if your cameras have different passwords, each time the new discovered cameras will be added to the list.

If your PC has multiple network interfaces, then you may need to pick an IP address from the pull-down list from which your cameras are reachable. You can initiate auto discovery on one interface at a time if your cameras are reachable from different networks/interfaces. Some cameras might not be searchable if they don’t support ONVIF protocol or ONVIF port is disabled; in such case you can add them manually; you may find the correct RTSP from https://www.ispyconnect.com/sources.aspx.

Once all cameras are discovered, please change the camera names and the announcement suffixes. To setup the monitored area, click the “connect” button on that camera which will

take a snapshot from its view. Draw one or more “virtual laser beams” or red lines that act like a tripwire for the area. If you want to remove a camera from the configuration, press the “remove” button. If you want to setup the monitored area at a later time without removing it, uncheck the “enable” button.

4.2 Select AI Inference Backend

The step is to select and verify AI Inference backend before it can be used for the Core Service:

If you don’t have an Nvidia GPU, but have an integrated HD graphics (e.g. a PC with 5th or newer Gen Intel CPU), select HD Graphics from the pull-down list, and press “Verify Inference Backend”. It may take up to 30 to 90 seconds to validate the backend with its latency number shown in the message bar (on the bottom of the screen).

If you have an Nvidia GPU, select “Nvidia GPU” from the pull-down list, and the latency should be less than 200 ms.

If you don’t have an Nvidia GPU nor a suitable HD Graphics, you can choose “CPU”.

Remember to press the “Save and Exit”, and only the last verified inference backend, once it setup is saved, will be used for Core Service.

Recommendation: using the HD graphics (e.g. a 4th or 5th Gen Intel CPU) is preferred than using the CPU even though the latency with the CPU is lower because AI inference using CPU may compete for CPU with other tasks like camera streamings/recordings. If the inference latency is too high, e.g. higher than 2000 ms, the delay will be longer when an object crosses the red lines triggering sending alert and recording.

You may verify that the Core Service is actually using the specified inference backend from the service log as shown in the demo video.

4.3 Email and SMS Notifications Setup

On the “AI-Homeguard Configure” screen, enter your email service provider URL (a Gmail template is provided). Enter your own email address and password, and add email recipients under “to” and “cc.” Click “Test SMTP Email” to send a test email to the recipient email address. Note: For Gmail, you need “less secure apps” setup for you Google account; you may also need to login to your gmail account from your other device to confirm this device. Here is how to enable “less secure apps” on your Google account:

- Sign in to your Google account, and select Admin console.
- Click Security -> Basic settings.
- Under Less secure apps, select Go to settings for less secure apps.
- In the subwindow, select the Allow users to manage their access to less secure apps radio button.

To receive SMS/MMS alerts, you can use your carrier's SMS/MMS gateway. For example, T-Mobile customers can send the notifications to: *your10digitmobilenumber@tmomail.net*.

Enter your Activation Key from the tag on the USB drive in your shipment. Click "Validate License". Click "Save and Exit" and accept the EULA.

5 Start, Stop and Monitor AiHomeGuard Alerts

5.1 AiHomeGuard Monitor

Open the Main Menu and click "Monitor Services" (Figure 1) to invoke the monitor screen (Figure 3). From the monitor, you can watch the services status, start live streams from cameras, temporarily disable (hibernate) any cameras for a period of time, navigate the detected objects and play the associated recording, and so on.

5.2 Start Core Service

From the main menu, click "Start Core Service". Once the service starts successfully, the monitor button "AI-HomeGuard Service: On" will turn green. Note: the image section on the monitor screen will remain blank until the system detects its first object. If you have modified AI-HomeGuard Configuration, you must stop, and then start AI-HomeGuard Service to make the change effective. Note that once AI-HomeGuard service starts, it will automatically start when OS reboots (e.g. after a power loss) no matter the monitor is shown or not.

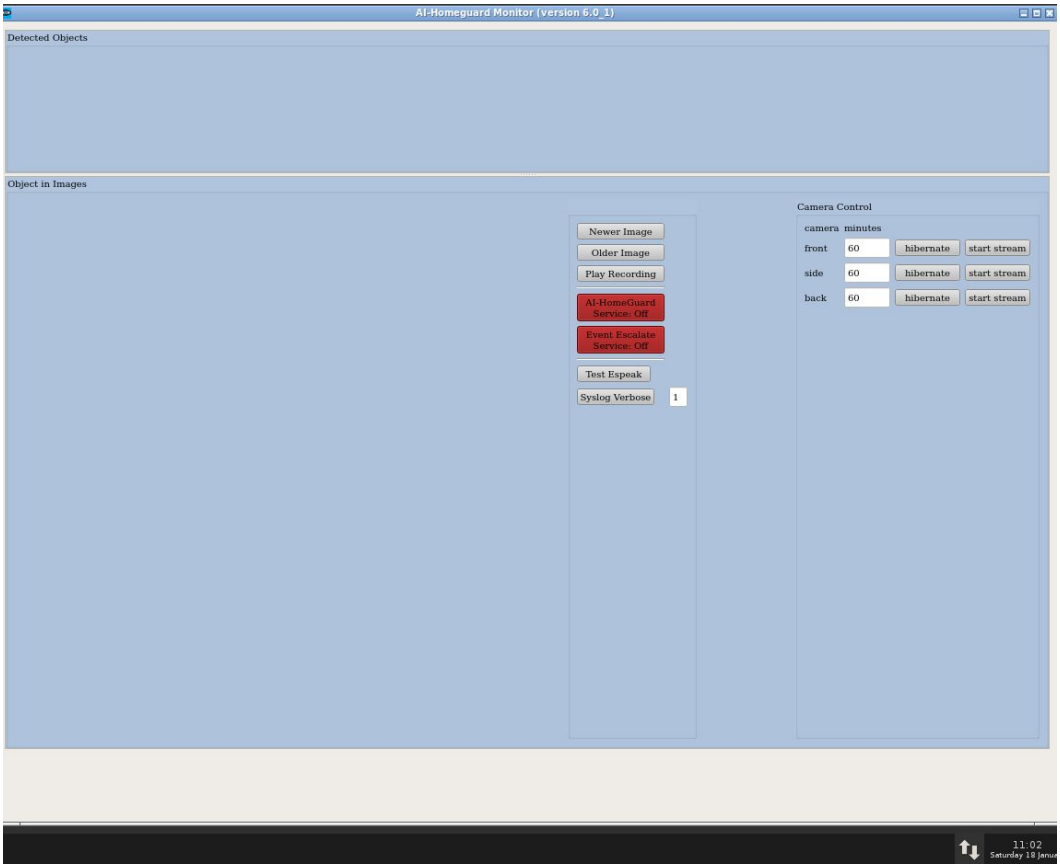


Figure 3. AI-HomeGuard Monitor

5.3 Viewing Images and Video Clips

Thumbnails of detected objects are at the top, with the leftmost being the most recent event. To view the full image, click on a thumbnail. Scroll through your images by clicking “Older image” and “Newer image” for those not shown in the thumbnails.

Your email alert also contains a link to a web page (HTTP port 8000) where you can view the full images from your device as long as they are on the same LAN (or WiFi router) as AI-HomeGuard server.

Click the “Play Recording” button to view the video clip associated with the full image.

You may watch video recordings from other devices (Android phone, iPhone or iPad, Windows PC or MacBook) via any App supporting Microsoft Samba protocol, such as VLC (free download from your device app store).

5.4 Temporarily Disable Object Delections on Cameras

You can temporarily disable (hibernate) the detection function on any cameras. Next to the desired camera, enter the number of minutes you want to disable and click “Hibernate.” To resume the hibernation, use the value “0.”

5.5 Live Streaming from Cameras

Press the “Start Stream” button to get a live stream screen for that cameras. Starting streaming from cameras may cause your PC consuming more CPU, and may reduce the total number of cameras the system can support. Please watch your CPU utilization to decide if the CPU is overloaded.

5.6 Service Log

You can monitor the core service and event service logs by pressing the “Watch Services Log” on the Main Menu. If you need any customer support, please provide the service log messages to help diagnose the problem. You may setup log level (0 ~ 9) by pressing the “Syslog Verbose” on the services monitor with the desired log level number.

6 AiHomeGuardPro Software Upgrade

AI-HomeGuard software version number is shown on top of “AI-HomeGuard Monitor” or “AI-HomeGuard Configure” screens. You can do an online software upgrade for AI-HomeGuardPro. The newer versions contain new features, bug fixes (e.g. for more certified cameras) and performance improvements. To start software upgrade, choose “Upgrade Software” from the main menu (Figure 1) after shutting down the core service. You will be prompted for the login password, and then asked for confirmation for the upgrade if the installed version outdated. The upgrade will not change your current camera configurations, nor the license key.

Start the service again after the upgrade completes.

7 System Parameters Adjustment

7.1 About System Parameters

The default system parameters are sufficient for most all deployment scenarios. However, if you want to fine tune the system behavior, such as increase or reduce motion sensitivity or choose to ignore some particular objects (e.g. cat, dog), you may run “Adjust Parameters” setup (figure 6) from the Main Menu. Press the “Help” button regarding the parameter’s value and function in that screen. Press the “Save/Exit” button to save the changes. You must restart the core service to have the change effective (via main menu).

7.2 Set Archive and Purge Image and Video Files

A Linux cron job will archive and purge old image and video files automatically with default 20 days for archiving and 60 for purging at 1 a.m every day. If you want to change the values, please change the system parameters on the “System Parameter” setup screen.

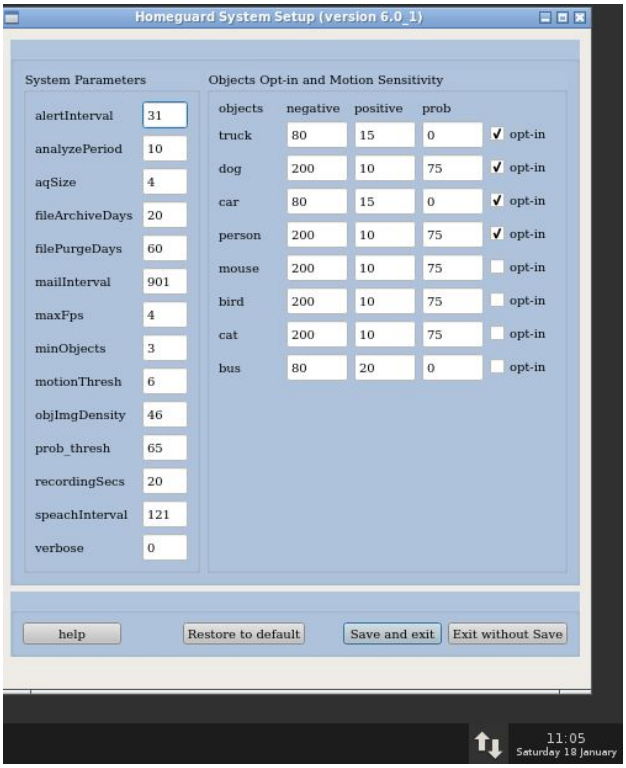


Figure 4. System Parameters Adjustment

8 Event Service

8.1 Event Service Overview

AI-HomeGuardPro offers an Event service, which can control smart switches or plugs when the AI engine has detected an object entering or leaving your area. With this capability you can add additional protection on your home area. For instance, you can plug a siren to the smart plug and configure the service to trigger the siren when a car or person enters your yard, and simultaneously trigger another smart plug to turn on the bedroom light. Another use case is to have the hallway lights connected to a smart switch, and have it turned on or off periodically when an intruder has touched red lines on a camera view.

The service configuration app offers a variety of ways to define the “filter” and the action associated with it; where “action” controls one or more smart plugs to respond with a defined pattern. Here is an example as how this “filter” and “action” can be configured: If the “front” camera detected a “incoming” “person” on “normal” schedule, then turn on smart plug “FrontSiren” for 30 seconds, and (simultaneously) turn on and off smart plug “AlarmClockRadio” 6 times with 30 seconds interval.

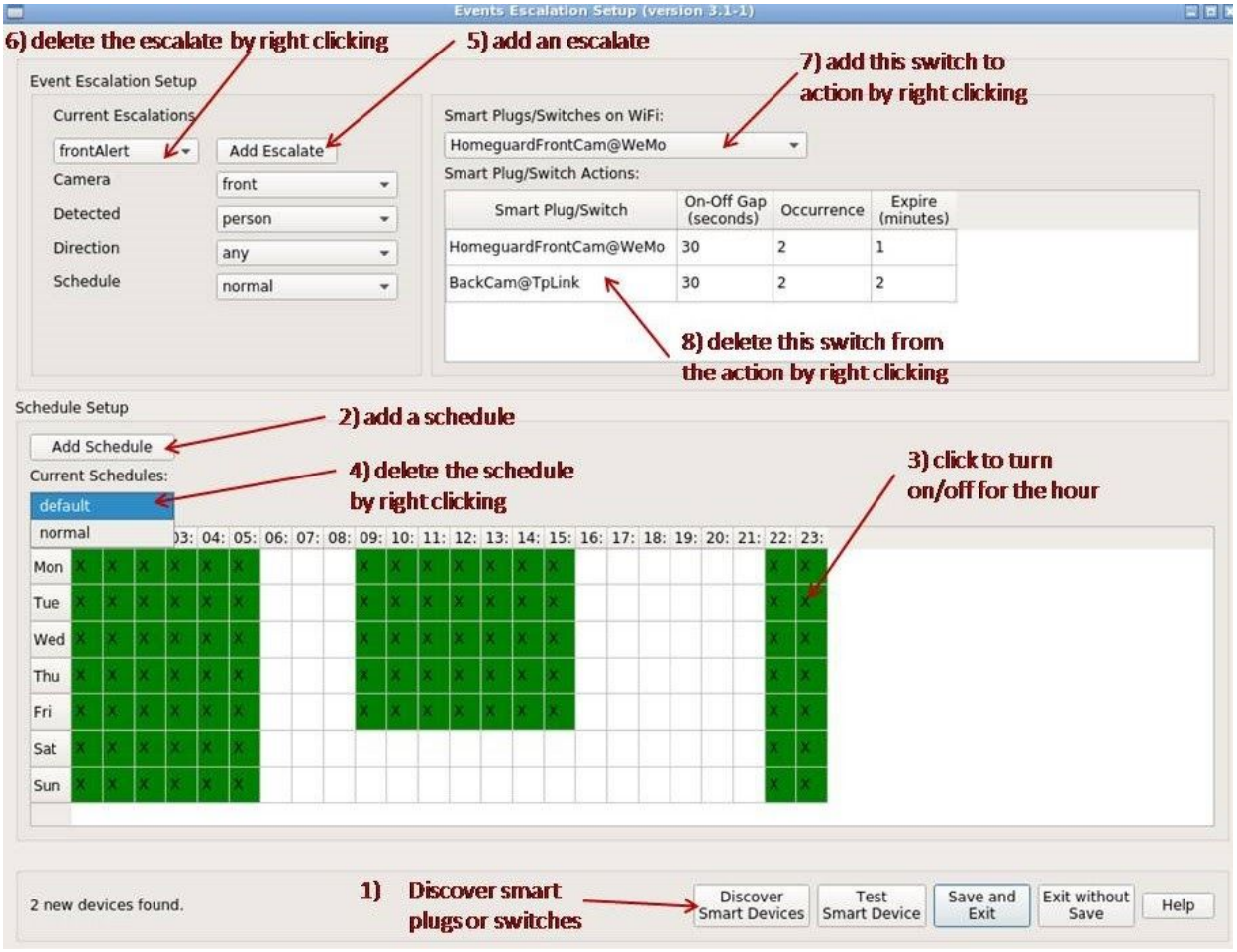
The Event Escalation configuration allows you to define any number of filters, actions, and schedules. A schedule is simply a 24x7 matrix specifying at which hour during the day of the week the filter can be valid.

8.2 Setup Event Service

Select “Setup Event Service” from the Main Menu, and the event setup screen (figure below) will appear. Please follow the red colored steps on the figure:

1. First, you need to discover all smart plugs or switches on your WiFi network. You may try more times if you don’t see the plugs you expected.
2. The system provides a default schedule when you first run the configuration. You may add more schedules for filters (on escalation setup).
3. Click the square to turn on or off that hour for the day of that week.
4. If you want to delete an unused schedule, select it from the pulldown menu, and then right click the mouse..
5. Press “Add Escalate” button to create a new escalation. Then choose other conditions in the filters (camera, object, moving direction, and schedule)
6. If you want to delete an escalation, select it from the pulldown menu, and right click the mouse.
7. Select a smart plug or switch discovered at step 1, and right click the mouse to add it to the action. You may set three values: the interval to turn on or off the switch (in seconds), the total number of On or Off to take; note that an even number will eventually put the switch at Off state, and odd number will put it at On state finally, and the expiration (minutes) is for prohibiting other actions to control the same switch within that period.
8. If you want to remove a switch from an action, right click the mouse at the switch name on the action table column.

Once you complete the configuration, remember to press the “Save and Exit” button to make the change effective, the Escalation service daemon will automatically pick up the change.



8.3 Start Event Service

From the main menu, click “Start Event Service”. Once the event service starts successfully, the button “Event Service: On” will be shown on the monitor screen with its color turning to green. The event service will be automatically started when the PC reboots.

8.4 Event Notification API

AI-HomeGuardPro provides an API allowing users to add their down-stream components to react to events on the detected objects. The events are instantly delivered to the event consumer which can determine what kind of object is detected. The events are sent by the AI-HomeGugard core service daemon to a multicast UDP port (43210) on interface “lo” (IP 127.0.0.1) with multicast group address 226.1.1.100. The events are ASCII strings with the following fields:

- notify image image-base-name
- notify video video-file-name

The application that received the “notify image” can parse the image-base-name to get the information about the detected object:

- the type of object (car, person, dog, etc.)
- The camera name which detected the object
- The time at which the object is detected, including year, month, hour, minute, second, and millisecond
- The direction the object is moving (either toward the camera or move away from the camera)

From the base image name, the user application can derive either the full or cropped images file path. The “notify video” gives the video file path once the video file is closed, thus this event will lag the “notify image” event delivery for the same detected object. You may read /home/homeguard/docs/homeguard_event_consumer_sample.py on how the events are handled.

9 Troubleshoot

9.1 Cannot Connect to Camera from “Setup Core Service” Screen

If a camera’s view is not shown after you press the “connect” button, follow the steps below to troubleshoot:

Start a “xterm” session, and ping camera’s IP address (e.g. ping 192.168.1.201). If the ping fails, check the camera setup again using your camera’s manufacturer's app to find its correct IP address. If the ping is successful, ensure that you are using a correct RTSP or MJPEG URL. If you get the URL manually (e.g. ONVIF discovery is disabled on cameras), you may find the correct RTSP or MJPEG URL from the commonly used cameras list in Appendix of this document, from your camera’s manufacturer's home page, or from iSpy site https://www.ispyconnect.com/sources.aspx.

Also, double check that you typed in a correct user/password within that URL. You may need to check if the camera is configured with a standard RTSP (554) or MJPEG port.

Sometimes, a camera can stop working because most it reboots at midnight, and obtained a new IP address from your router. It is advised to setup a static IP address on each of your cameras.

9.3 Fail to Start Core Service

When you press “Start Core Service” from the Main Menu, the status in the Monitor screen should turn to Green; the Core Service may fail to start if there is no camera configured. To find out the root cause, please check the services log (via main menu).

9.4 Fail to Detect Moving Objects

Make sure that your RTSP connection has good quality. On the AI-HomeGuard monitor screen, click the “start stream” button for that camera, and you should see a new window showing real-time video stream for that camera. Be sure that the video quality is good

(constantly clear view). If you observed damaged image frames, recheck the camera setup (section 2) for the correct frame rate and bitrate. The bit rate doesn't need to exceed 2048 Kbps, and the frame rate doesn't need to exceed four frames per second, otherwise your network bandwidth may not be able to support the aggregated rates of your cameras, or you must use a high-end router.

If you still see damaged images, check your WiFi connection quality. You may need WiFi extender if the WiFi signal is too weak at the camera's installed location.

If none of the above are the root cause, set a higher log level, e.g. 6 (via Services Monitor), and then press "Watch Services Log" on the Main Menu. You need to walk to the front view of a camera, and then check the logs and see if there is any clue.

Note: the system will not send alerts on duplicate detections. An alert (email, audio or image shown on the minitor) is considered duplicate if the same camera discovers the same type of object (person, car, etc.) traveling in the same direction within a predefined period, e.g. three minutes for sending email, which can be modified with "Adjust Parameters" on the Main Menu.

9.5 False Alarms Observed

- If the alarm is triggered by a stationary object (e.g. a poster containing a human picture or a parked car) you may increase parameter value "minObjs" and "aqSize" via "Set Parameters" button, e.g. set both to 3 or 4 (the default is 2 for minObjs, but minObjs must NOT exceed aqSize). This parameter is used to analyze the motion of a sequence of identified objects so that a stationary object wouldn't trigger an alarm. Note that the larger value of minObjs may increase the response time: it roughly equals the minObj times the Inference latency - you can see the latency from "Verify Inference Backend" in the setup screen. The response time is when the object crosses the red lines until an alert is generated, and the video recording is started.
- If a moving object is mistakenly classified, e.g. take moving shadow as a person - this may occur if the lens of the camera got wet during the night, and get reflections from the infrared light on the camera, you may increase the minObjs above or increase "prob_thresh" for that object.
- You may also see alerts when an object moves toward the redlines without actually crossing them. To avoid such false alarm, you should redraw the redlines a little farther from the traffic area.

Remember to stop/start Core Service once the parameters changes are saved.

9.6 Fail to discover smart switches or plugs by Event Config or Service

● Please press the “Discover Smart Devices” button a few times and see if it can discover more devices (during “Setup Event Service” session).

● Be sure that the switches can be discovered by the manufacturer's apps.

● Also check the WiFi connection quality of those smart switches.

9.7 Fail to turn on smart switches by Event Service

Please run Event Configure, and press the “Discover Smart Devices” button. Once the switches are shown, press the “Test Smart Device” button to see if you can turn it on or off. The problem may be caused by Event Service. Please check the syslog for conditions, schedules or unmatched actions. Be sure that the PC clock is correct, otherwise you

may wrongly configured the schedules.

If your system has tried to rediscover the smart switches after it failed to contact the switch (e.g. the switch has changed its IP address after reboot), then the system should resume to work for the next detection.

9.8 Failed to Send Test Email in Setup Core Service

These tips are for using your Gmail account to send alerts. Other email service providers might have other Smtp URLs for sending email.

If you got “Authentication Failed” error when pressing “Test SMTP Email” button on “AI-HomeGuard Configure” screen, please follow the instructions described in section 4.3 of this document. If you get an error other than “Authentication Failed” when pressing the “Test SMTP Email”, you might have entered invalid (or removed) some needed text in the fields (e.g. in field SMTP). Note that no character “;” in any field is allowed. You may restore the default values by pressing the “Reset” button on the “SMTP Setup” panel, and replace the default values one by one before pressing the “Test SMP Email” to see which field caused trouble.

Appendix

A1 Commonly Used IP Cameras Supporting RTSP/MJPEG

If your cameras don’t support ONVIF but support RTSP, you may search them on https://www.ispyconnect.com/sources.aspx and find out the RTSP or MJPEG URL(s) for your camera brand/model. Here is a list of low-cost wireless cameras. The high-end or wired cameras with the same brands should be working too as long as they support RTSP (H.264) or MJPEG.

- Foscam Outdoor Bullet Camera, FI9800PR 720P, Foscam HD 720P Outdoor WiFi Security Camera (FI9800P), RTSP URI: rtsp://user:password@ip-addr/videoMain
- Wansview 720p, 1080p, RTSP URI: rtsp://admin:password@192.168.1.7/live/ch0
- Amcrest IPM-723 Outdoor 960P, RTSP URI: rtsp://user:password@ip-addr/cam/realmonitor?channel=1&subtype=0
- RLC-410ws (Reolink), RTSP URI: rtsp://user:password@ip-address/h264Preview_01_main
- Microseven 1080P WiFi IP Camera, RTSP URI: rtsp://user:password@ip-address/11
- SV3C HD 960P Wifi Wireless Security Camera Outdoor, RTSP URI: rtsp://user:password@ip-address/11
- Mobotix D15 camera URL (MJPEG): http://admin:pwd@ip:port/control/faststream.jpg?stream=full
- Zmodo (most models), e.g. ZP-IBH15: rtsp://admin:pwd@ip-address/tcp/av0_1
- Lorex:
  - LNR600 Series NVR, RTSP URI rtsp://admin:admin@ip-address/cam/realmonitor?channel=0&subtype=01
  - Lorex LNB8921, rtsp://<username>:<password>@<camera-ip>:554/cam/realmonitor?channel=1&subtype=0

If your camera brand/model is not listed above, you can visit https://www.ispyconnect.com/sources.aspx and search for your camera brand/model for RTSP or MJPEG URL(s).