Forecaught

Petrol Station Loss Prevention

Version 1.11.1.0

Table of Contents

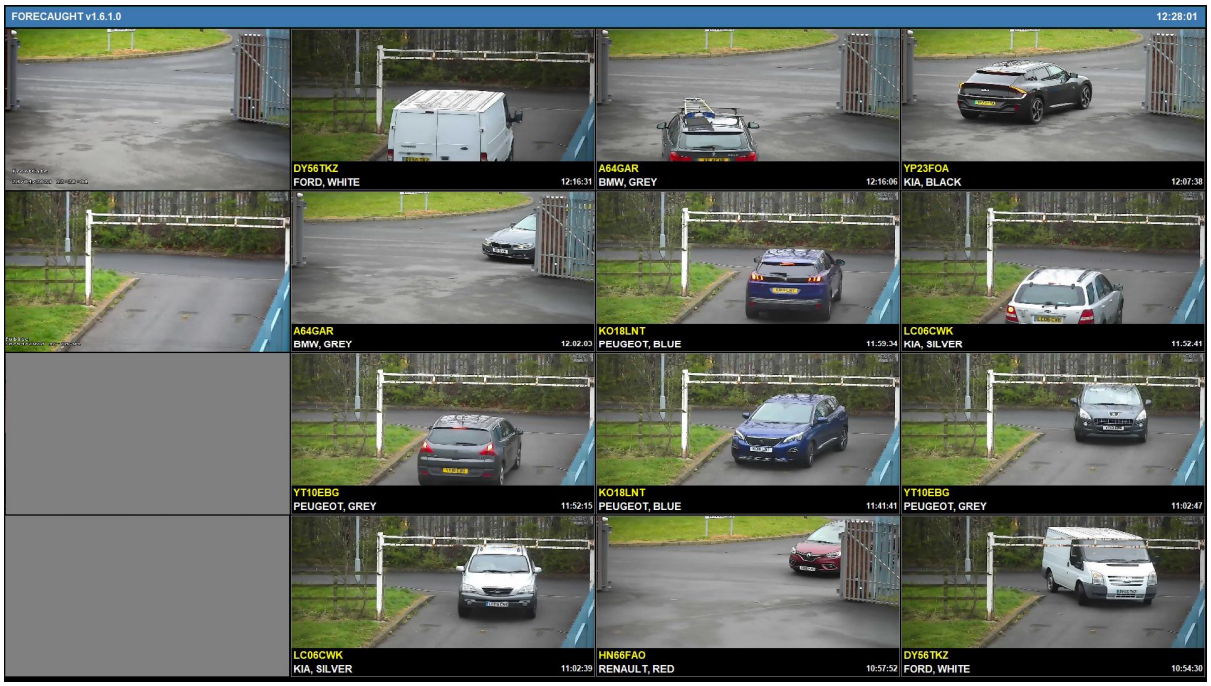
Overview

Forecaught is a Windows application capable of receiving ANPR results from up to 4 x *RoboPlate* branded cameras, it displays live video down the left hand side and snapshots from those cameras in an image grid to the right.

As results are received they are compared against a locally maintained blacklist (which results in an on-screen warning subject to a match) or, are used to make a DVLA query to determine the make & model. Information returned from the DVLA is displayed under the corresponding image for operator comparison.

Prior to using the DVLA lookup service, you must contact them requesting an API access key, this process takes about a week.

Contact: https://register-for-ves.driver-vehicle-licensing.api.gov.uk/



Enigma Protection

This application uses *The Enigma Protector*, a third party tool that offers copy protection, registration and activation features to commercial applications.

All our software products are code signed and we are confident they are virus free at the time of compilation, however, some antivirus programs detect *Enigma* and warn against it.

If your antivirus display s such a warning, you are advised to examine the *Forecaught* executable and satisfy yourself that it has not been tampered with since it left us, you can do this by right clicking on the program itself, select Properties > Digital Signatures, then click on *System Q Ltd*, then “Details” button which should confirm “This digital signature is Ok”.

The *Forecaught* executable is normally located in either;

C:\Program Files\SoftCCTV\Forecaught Unlimited

C:\Program Files (x86)\SoftCCTV\Forecaught Unlimited

Preliminaries

The entire system is IP based so both the PC and cameras must be networked correctly onsite, we recommend a pre-install configuration check before mounting cameras externally on any building.

- Configure a PC and check it has Internet access
- Configure the cameras, check the PC can connect to each in turn and collectively
- Check camera-to-PC connectivity before installing on the building.

You must first decide what network settings are to be applied to the PC, then decide upon network settings for each camera in turn.

Ask the IT support team for the following details or, with knowledge of the site, assign them yourself.

If self-assigning the IP addresses, use the router to guide you:

- Use its subnet mask for the PC and cameras
- Use its IP address as both the gateway and DNS server for the PC and cameras
- Use its IP address range changing the last digit to assign addresses to the PC and cameras.

  Example:
  If the router has IP address 192.168.1.1, then it's easy to visualise theses IP addresses:
  - PC = 192.168.1.100
  - Camera 1 = 192.168.1.101
  - Camera 2 = 192.168.1.102
  - Camera 3 = 192.168.1.103
  - Camera 4 = 192.168.1.104

Its is a good idea to write down the PC and camera settings once assigned:

PC	
IP Address	
Subnet Mask	
Gateway	
DNS Server	

	Camera1	Camera 2	Camera 3	Camera 4
IP Address				
Subnet Mask				
Gateway				
DNS Server				
NTP Server				

Camera Defaults

RoboPlate branded ANPR cameras ship with the following settings:

- IP Address = 192.168.10.1
- Admin password = 777777

Tip ➢

If you change your PCs IP to a '10' address, eg: 192.168.10.100, you should be able to connect to and configure each camera in turn.

Camera configuration is via a web interface, most features are accessible via Chrome, some require Internet Explorer.

Upon initial connection, the web interface will request a new admin password, after which it will reboot.

Camera Configuration Tasks

The following list identifies the essential steps to be performed camera-side via a browser; it assumes that you have set a new admin password as described above.

Set the Camera Number & Event Server Port

1. Login via the web interface
2. Navigate to Configuration > System > General
3. Enter device name appropriate for the site, eg: Camera1
4. Select from the drop-down list the number to reflect the camera number
5. Click Save
   At this point the camera will assign itself an Event:Server port number based on the camera number selected, port numbers for this function start at 5000 plus the camera number selected, hence, the first camera assumes port 5001, the second 5002 and so on.
6. Allow the unit to reboot

Scheduled Reboot

1. Login and navigate to Configuration > System > Maintenance
2. Enable Auto reboot
3. Select Everyday
4. Specify a quiet time of day in the early hours
5. Save

Set Date & Time

1. Login via the web interface
2. Navigate to Configuration > System > Date & Time
3. Ensure an NTP time server is set (the camera ***must*** have access to a time server, it will not operate without one).
   If you do not have a local NTP server onsite, you should use an Internet based sever such as *time.google.com*
4. Click Save

Disable UPNP

1. Navigate to Configuration > Network > UPnP
2. Clear the ‘Enable’ tick box

Check / Adjust Video & Audio Options

1. Navigate to Configuration > Video & Audio > Video Encoding
2. Disable mainstream & substream audio if not required
3. When using a low-spec PC we suggest dropping the substream settings ..
    a. Resolution = 352x288
    b. Frame Rate = 6
    c. Bit Rate = 256

Event Server Configuration

1. Navigate to Alarm > Event Server
2. Choose Type = HTTP
3. Enter the server address, this is the IP address of the PC onto which you have installed the Forecaught software
4. Set the port number according to the camera number ..
    a. 5001 .. if this is camera number 1
    b. 5002 .. if this is camera number 2, and so on
5. Enter a username and password, as expected by the *Forecaught* software for this camera.

    Note:
    Both a username and password are required, these are not optional.

    To avoid confusion, some suggestions are;

    a. To use the same username and password for every camera
    b. To use the last few digits of the camera’s IP address for the username and password, eg: if your camera has an address 192.168.1.101, then using 101 for both the username and password helps you identify the camera easily.
6. Leave the POST URL as-is.
7. Click Test “only” when the listener PC, (that is the PC running *Forecaught*) is up and running in a listener state.
8. Click Save

Apply ANPR Options

1. Navigate to Configuration > Smart video > ANPR

Basic Settings ..

1. Ensure ANPR is “Enabled”
2. Click & drag to draw the area of interest, vehicles must appear in this box.
   Try to size and position this box such that attention is focussed on the vehicle in view, it will be beneficial to try and eliminate vehicles further away.
3. Ensure GBR is set for bias to UK plates
4. Save

Barrier Mode:

For our purposes, barrier mode should not be enabled.

Normally, when a plate has been recognised, the vehicle must leave the scene and re-appear in order for a second recognition to happen, this isn’t always possible when a vehicle is waiting for a gate/barrier to open (perhaps the driver stalled the car) so ‘barrier mode’ introduces a wait time after which another recognition is generated without the vehicle moving.

Schedule ..

1. Note: scheduling operates independently for black, white & grey (unlisted) plates
2. Default = 27*7 for each.
3. If you make any change;. Save

Action

Note: actions operate independently for black, white & grey (unlisted) plates

1. Select the ‘grey’ list radio option at the top
2. Enable the Event Server option
3. Enable the image option, with the Event Server
4. Save

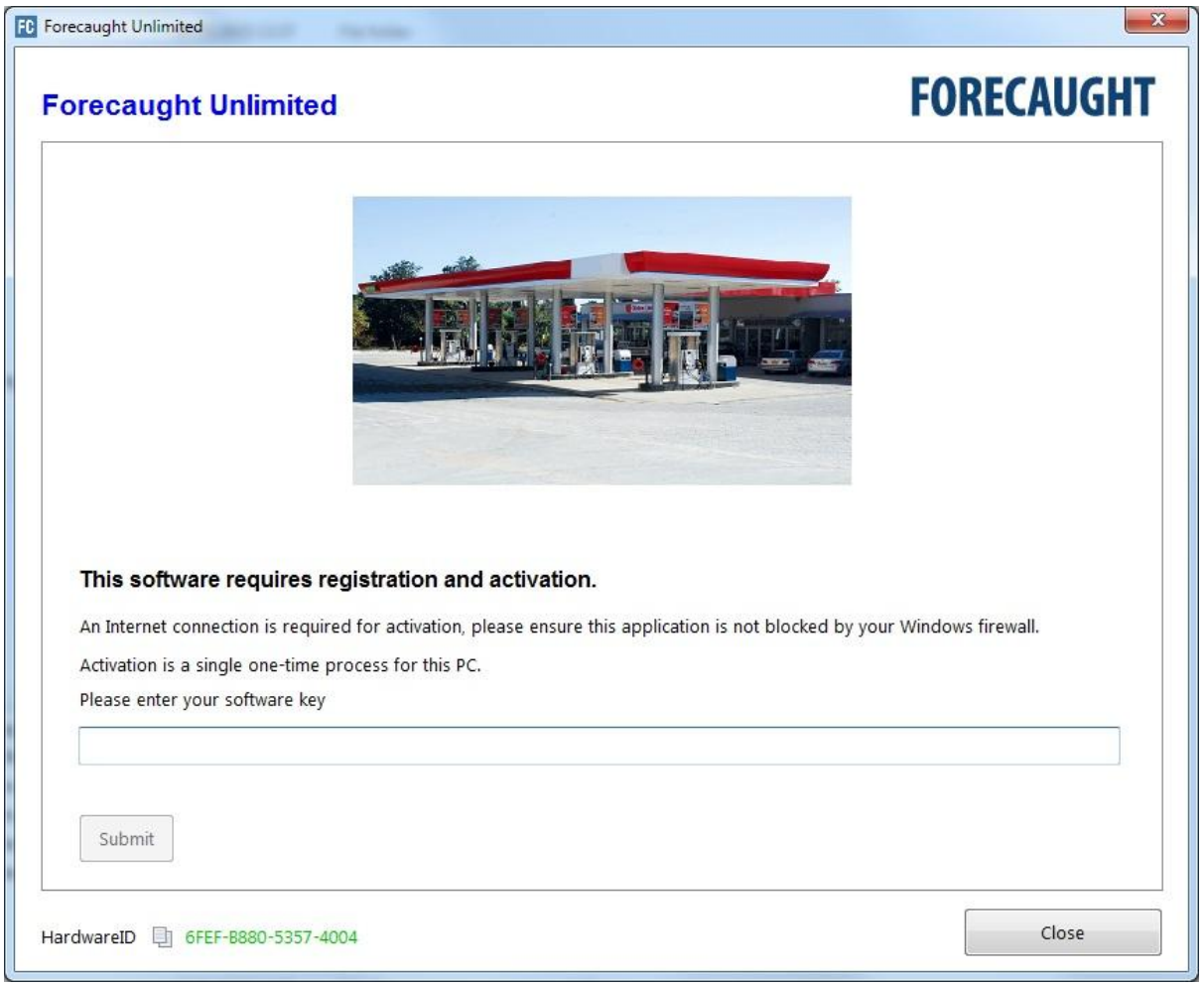
Application Setup

Installation, Registration & Activation

Follow the instructions supplied on the software certificate card to download the installer (setup.exe) used the install this software.

After running the setup.exe an information screen is presented requesting a software key, you will find this on the certificate or it may have been supplied by email.

The PC must be online at this point as the next step requests name and address details for registration purposes.

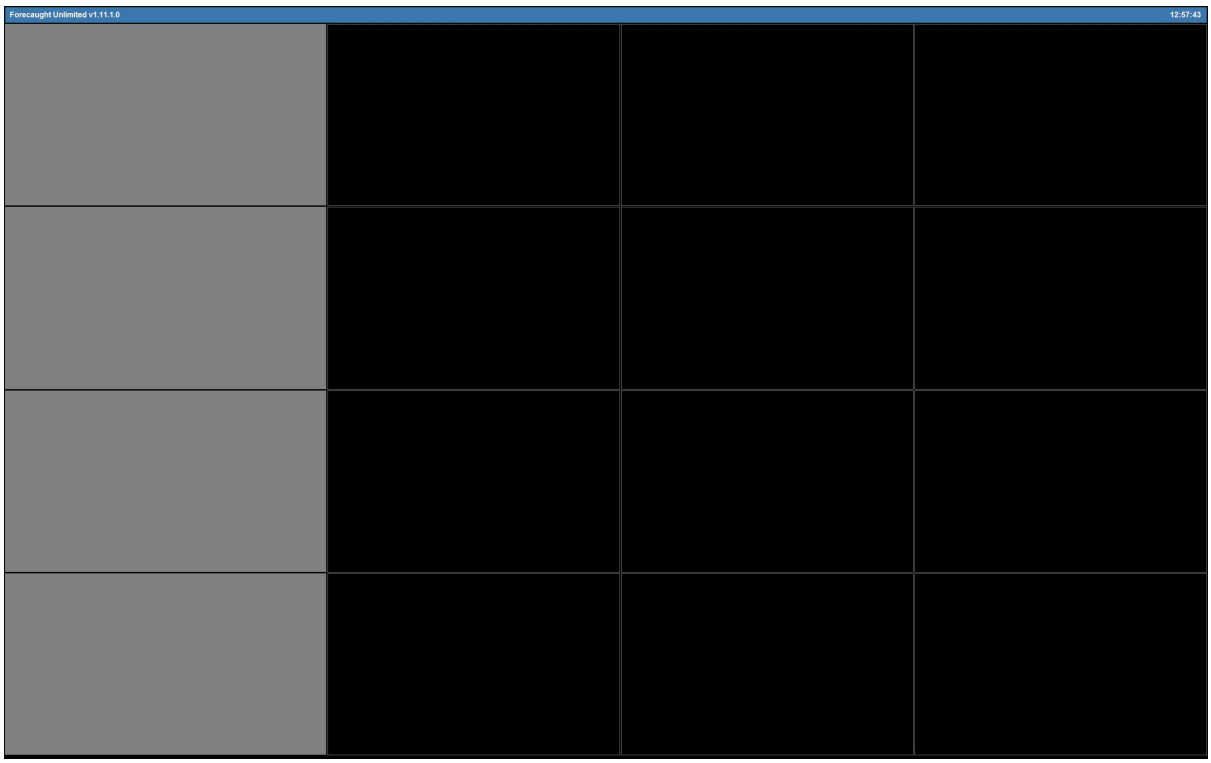


Important:

Be aware that the name and address details entered on the registration screen that follows will be used to identify the registrant. Title to use the software will be granted to that person or organisation. Title is not user-transferrable so it is important to ensure that details entered are correct and valid.

Main Interface

The applications main interface looks like this:



Settings Menu

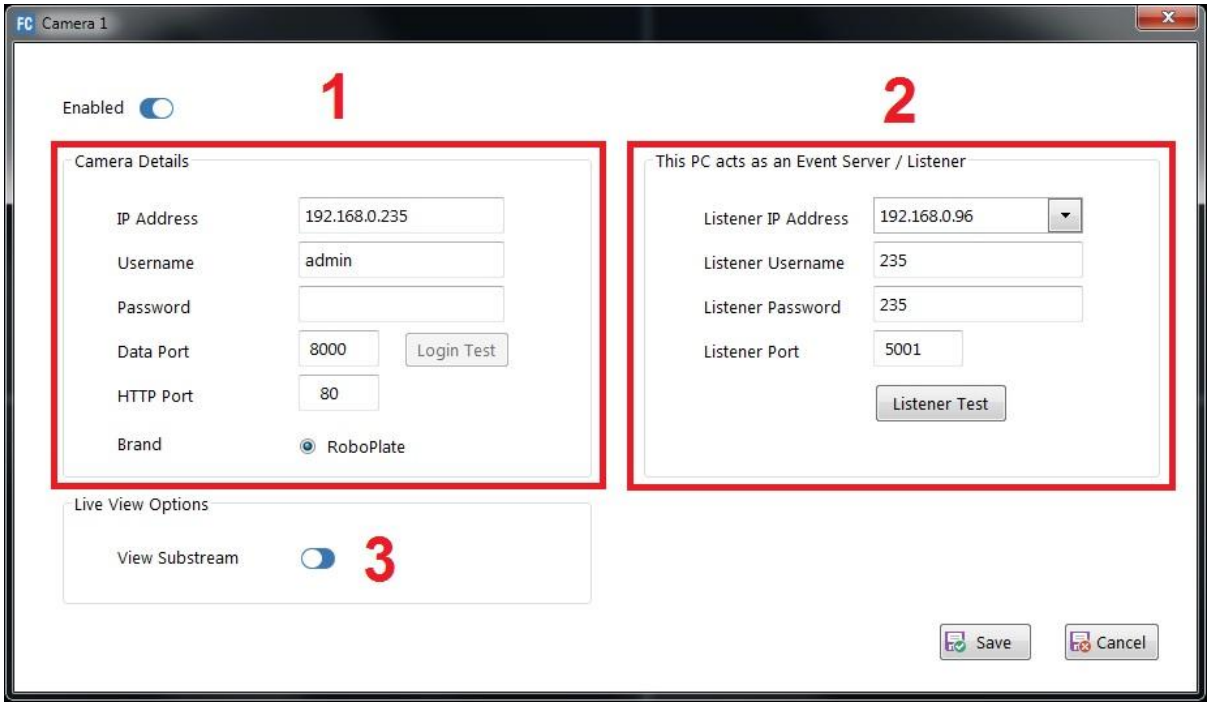
Program settings are accessed via a right click popup menu in the left hand column.

Exit the Program

Close the program via the *Exit* option accessed via a right click popup menu in the left hand column.

Camera Settings

Select each camera in turn and configure them as follows:



It is important to appreciate what the entries defined here are used for:

Camera Details: tells the program how to connect outbound to a camera (in order to display a picture)

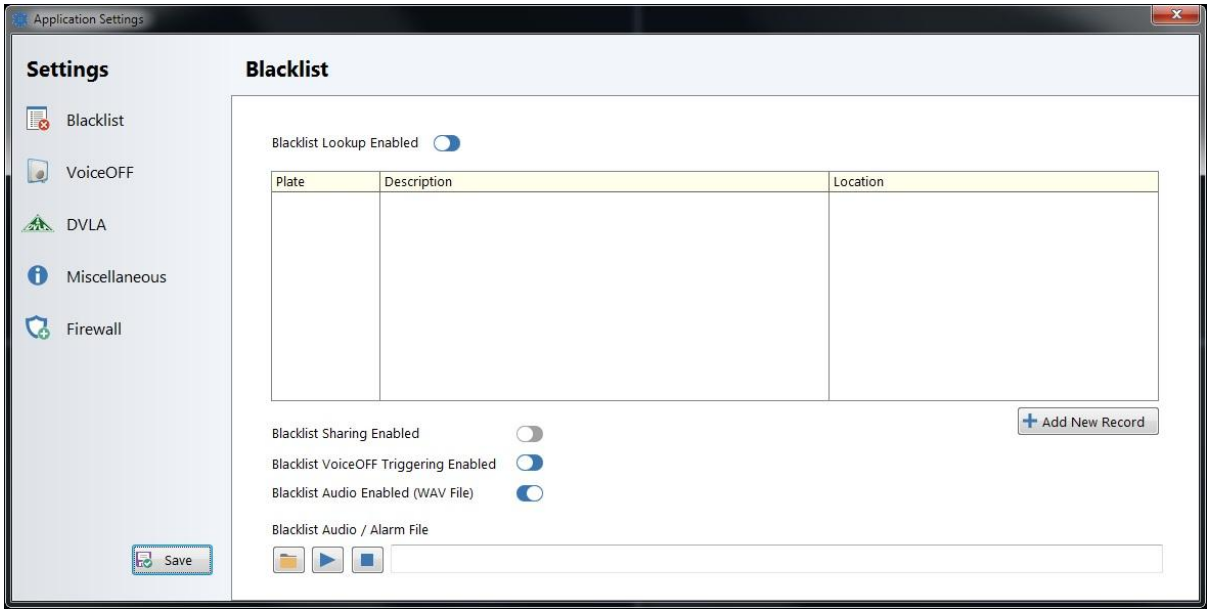
Listener Details: tells the program how to listen for inbound connections from a camera (in order to receive results from each camera)

1. Camera Details, you need to specify:
    a. The camera's IP address
    b. The username required when logging onto the camera (typically *admin*)
    c. The password associated with the username
    d. The data/login port
2. Listener Details, you need to specify:
    a. An IP address; the address of the PC's Ethernet card
    b. A username, the camera must use this during connection
    c. A password, the camera must use this during connection
    d. A port number, the camera must connect to this port

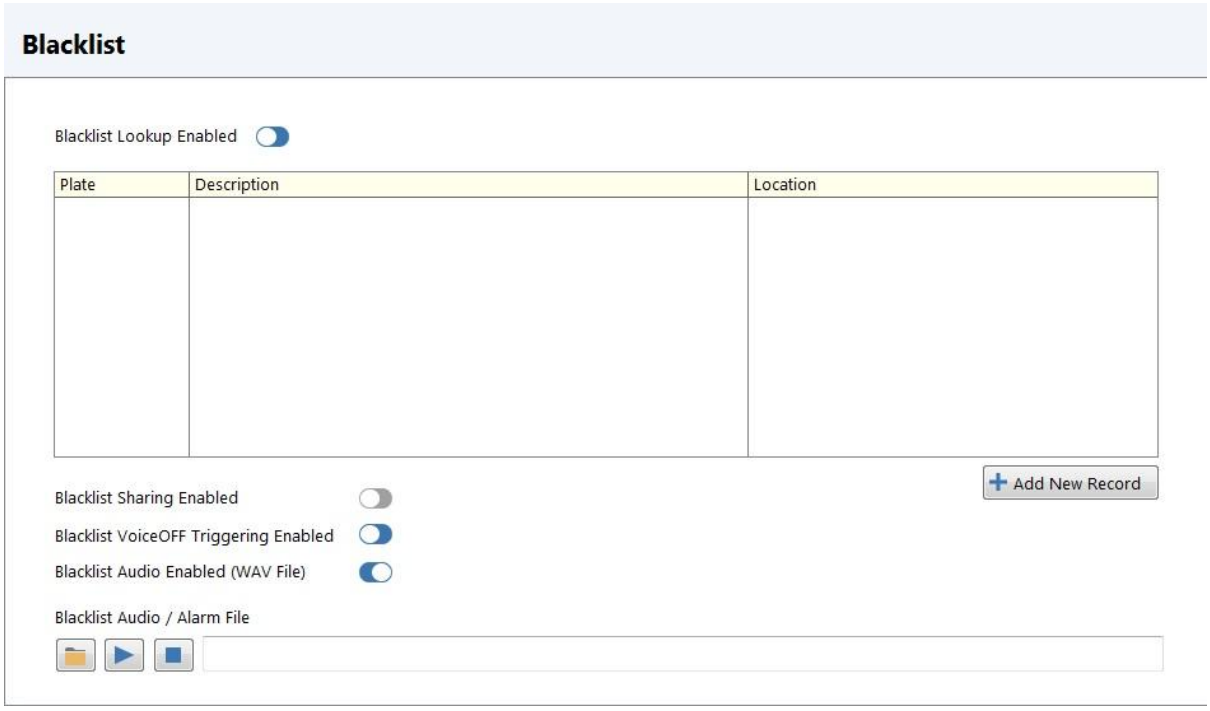
    Usernames and passwords are required, they cannot be blank, in the camera configuration section, we suggested the same username/password for every camera, or, the last few digits of the camera's IP address for both, eg: 101
3. View Substream ?
    a. Yes .. if using a relatively low spec PC and/or switch
    b. No .. if you have a high spec PC and good high spec switch

Settings Menu

Application settings are accessed via the same right click menu in the left hand column, navigation into individual pages is via the left hand vertical menu.



Settings: Blacklist



Enabled

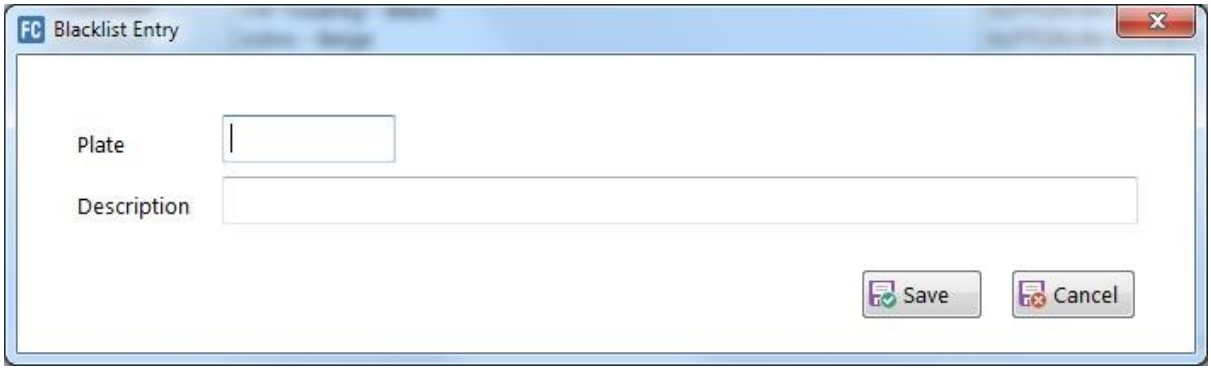
Blacklist lookup has a master switch to enable/disable this feature, if disabled there will be no lookup and no response or warning subject to detection of a blacklisted vehicle.

Add New Record

Plate and vehicle information can added via the editor.

Tip ➢

Do not use spaces in the plate field.



Blacklist Edit Entry

A double click, or right click on a registration plate in the vehicle allows you to edit an entry.

Blacklist Notification Test

Right click on a registration plate in the vehicle list to access a popup menu, select *Blacklist Notification Test* to see the popup window that would normally be displayed when a blacklisted plate is detected. This window must be cleared manually by clicking OK.

Blacklist Sharing

This is a 'work-in-progress' feature, we intend to make it possible for sites to share blacklisted entries via a webserver.

Sites willing to share their own blacklist will be able to download entries shared by others.

We consider this to be mutually beneficial, sites wanting to download shared entries must likewise be willing to share their own data, there will be no "download only" option.

Blacklist VoiceOFF triggering

This software supports the VoiceOFF annunciator, a network addressable MP3 player capable of accommodating up to 9999 audio files on a SD card.

See *Settings: VoiceOFF* below.

Blacklist Audio Enabled (WAV File)

The software is capable of playing a .wav file subject to blacklist vehicle detection. The PC will need either;

- External speakers
- Speakers in a monitor fed by audio, HDMI or display port cables

The file is only played once subject to detection, if a longer continuous play is required, simple replicate the audio in the file using third party software such as Audacity.

There are many download sites offering free downloads, examples include pixabay.com and freesound.org

Blacklist Audio File

Browse for and select the .wav file to be used during audio playback.

Settings: VoiceOFF

Website: www.voiceoff.com

A VoiceOFF unit is a mp3 file player, it is equipped with an audio amplifier and built-in speaker, it has a connection for secondary remote speaker, up to 9999 files may be stored on its SD card.

If placed in the counter area, it can be used to alert staff about blacklisted entries, a secondary/slave speaker can be used to alert staff in another location.

It can be triggered manually via a closing contact switch (to play 1 of 5 files) or programmatically over the network to play any of its 9999 files, *Forecaught* uses this latter method so you need to specify;

- Its IP address
- Its password
- Its port number
- The file number you wish to play

Settings: DVLA

Forecaught can query the DVLA database via an Internet connection to get vehicle information including make and model (as well as MOT and tax status).

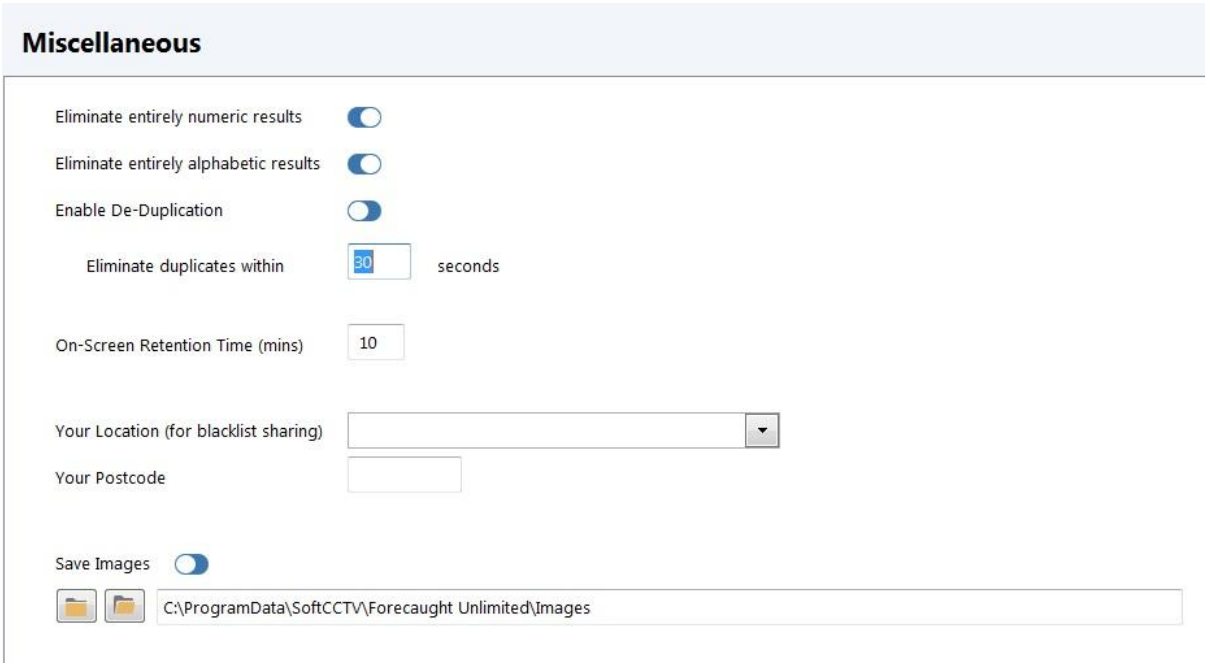
This function requires an access/API key, you must contact the DVLA directly to request your own key via;

https://register-for-ves.driver-vehicle-licensing.api.gov.uk/

Then enter the key received;

The Test button allows you to check that the DVLA query feature is working, it will request entry of a registration plate.

Settings: Miscellaneous



Miscellaneous settings help improve program performance;

Eliminate entirely numeric results

Telephone numbers that appear on some sign written commercial vehicles and vans can be interpreted as valid results, if enabled, this feature helps eliminate those results.

Eliminate entirely alphabetic results

Trading and company names that appear on some sign written commercial vehicles and vans can be interpreted as valid results, if enabled, this feature helps eliminate those results.

De-Duplication

The deduplication feature helps eliminate multiple results and/or warnings from a vehicle seen in rapid succession.

Camera positioning can be quite important as well, too wide a field of view may result in a vehicle further away being detected before it reaches the main pump area.

On-Screen Retention Time (mins)

Specifying an on-screen retention time in minutes determines how long the captured images remain in view before they are removed.

Your Location and Postcode

Please choose your post town and specify your postcode, these will be used during blacklist sharing should you decide to participate in that program. The sharing program is optional but post town and postcode entries are required.

Save Images

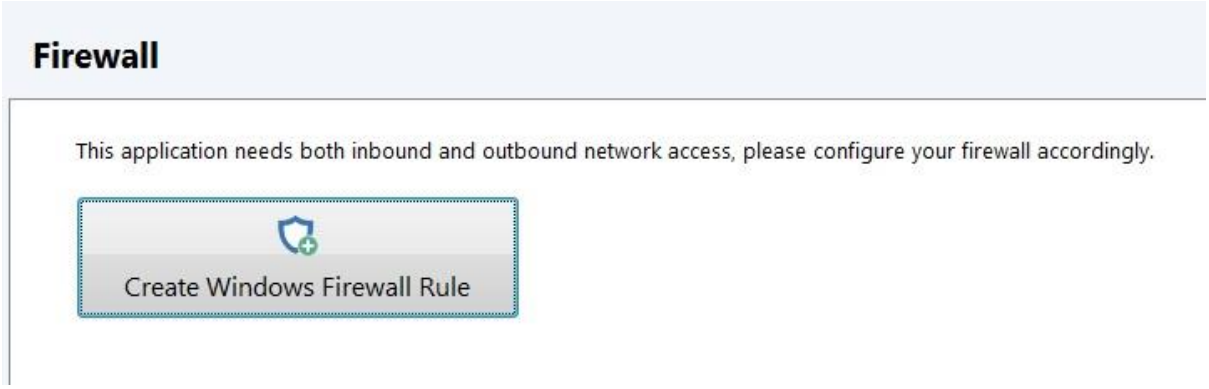
This optional feature allows you to save captured images to disc at a given location.

Settings: Firewall

This program needs TCP/IP connectivity both inbound and outbound so firewall rules should be created granting this.

- Inbound access = to receive results originating from the cameras
- Outbound access = to connect to, and display a camera image

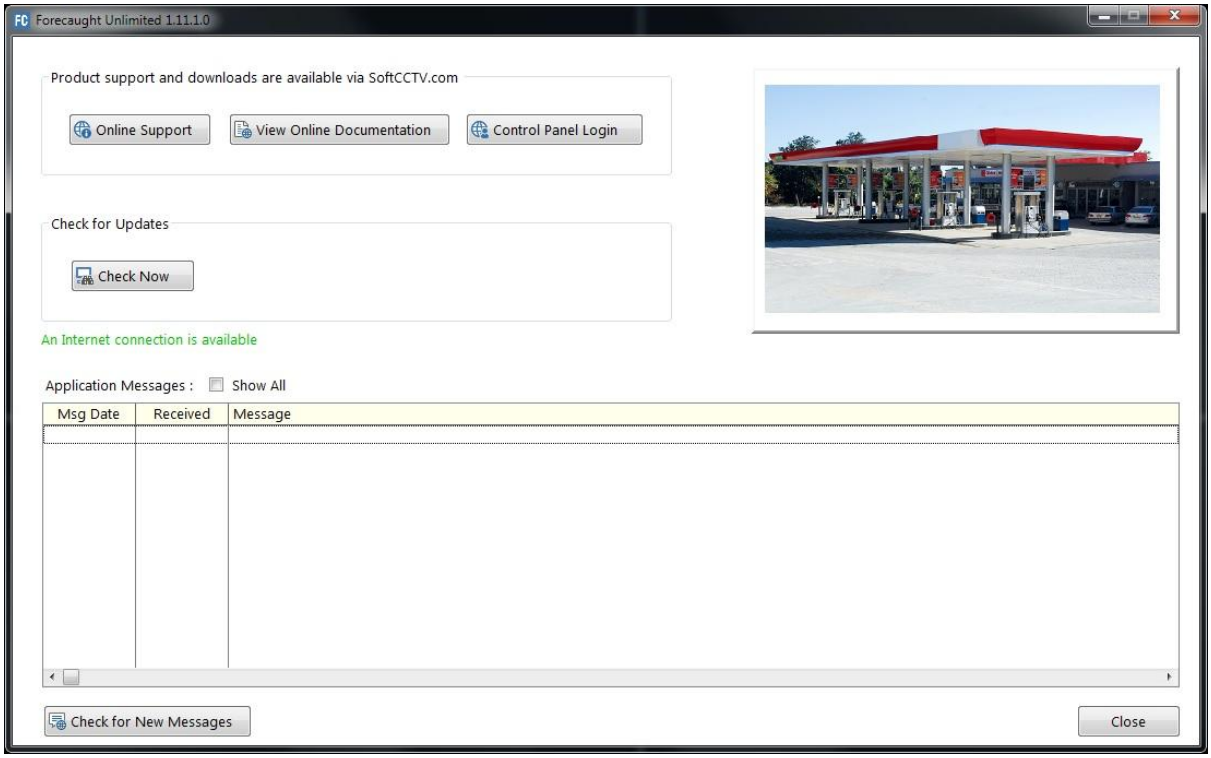
If the supporting tool; runas.exe exists in the application folder then *Forecaught can use* this to create a Windows Firewall rule programmatically.



Note:

This program is not capable of creating firewall rules in third party firewalls, if you use one of these then please refer to the manufacturer's instructions for information how to achieve this manually.

Support



Online Support

Online support in the form of a knowledge base (questions and answers) will be made available via:

systemq.com/helpdesk/kb/faq.php?cid=126

Online Documentation

The latest version of this document is always made available online via:

softcctv.com/pdf/enigma/Forecaught-Unlimited.pdf

Control Panel Login

Software can be downloaded via your personalised *Control Panel,* please refer to the email sent to you post-registration for your username and password.

Check for Updates

Checking for updates is a manual procedure, if an update is available you may download it from your *Control Panel*.

Application Messages

We have the ability to generate application messages via our web server, they are deliberately brief and occasional intending to serve as notifications about new features and/or editions. Individual messages can be flagged as “read” via a right click menu.

Appendix A : RoboPlate Camera Information & Resources

Camera Reset Procedure

RoboPlate cameras have a reset button under the SD card access panel, this can be opened after removing two cross head screws, the reset button clears any user-defined password and resets the camera to factory defaults.

The reset procedure is as follows:

- With the power applied, press and hold the reset button for 10 seconds, then release
- Wait 20 seconds
- Remove the power
- Wait 5 seconds before reapplying the power

Camera Firmware

Firmware for the *RoboPlate* branded camera is available via the *RoboPlate* website via this (case sensitive) link:

www.roboplate.com/support/RoboPlate-ANPR-Camera-Firmware.zip

SD Card Contents

A master copy of the camera license files can be downloaded from:

www.roboplate.com/support/RoboPlate-SD-Card-Master.zip