User Manual for PIPS P500 Camera Range

Title:	User Manual for PIPS P500 Camera Range
Revision:	1.5
Author:	D. McConnell, D. Yates, A. Jacques, N. Arnell
Date:	January 2021

UM-P500

Contents

Change History

Date	Reason for Change	Revision No.
31 August 2018	First issue	1.0
5 June 2019	• Update author and date • Added Change History • Added info on where to download Toolkit • Added reference to relevant section in Installation Manual re: connecting power and ethernet. • Added section for WiFi • Updated modem section for PAP option • Added note regarding IPSec firewall	1.1
28 June 2019	Added Appendix with technical details for trigger and relay connections	1.2
6 November 2019	Updated Security section to address: • User Account management • Use of SSH Keys for authentication • Physical Security Updated with modem section to reference IPv6	1.3
6 March 2020	Updated security section with details of new firewall functionality, and encrypted filesystems.	1.4
21 January 2021	FCC statement and safety information added	1.5

Safety Information

Please read and follow all safety information contained in these instructions prior to the use of this camera system. Retain these instructions for future reference.

Explanation of Signal Word Consequences

⚠ **WARNING**: Indicates a hazardous situation which, if not avoided, could result in serious injury or death.

⚠ **CAUTION**: Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury and/or property damage.

NOTICE: Indicates a situation which, if not avoided, could result in property damage.

Explanation of Safety and Related Symbols

⚠ **Warning**: Hazardous Voltage

⚠ **Caution**: Lifting Hazard

⚠ WARNING

- **To reduce the risks associated with hazardous voltage, fire, and impact:**
  - Read entire installation guide prior to installation, maintenance and service.
  - Only qualified personnel should install, maintain, or service the system.
  - Installation and service activities must follow all local, regional, and national applicable building and electrical codes.
- **To reduce the risks associated with hazardous voltage and fire:**
  - Disconnect all AC power to the system when connecting or disconnecting components of the system.
  - Ensure that power cannot be restored inadvertently.
  - If excavation is required, understand which local utilities are present prior to starting installation. Caution shall be taken when digging.
- **To reduce the risks associated with hazardous voltage:**
  - Use only with Neology-approved power supplies listed in manual.
  - System has not been evaluated for safe use with any power supply not specified by Neology.
  - Always disconnect power prior to installation, maintenance and service.
  - Ensure that the connection to the mains has no exposed connections.
  - Neology recommends that when the power supply unit is removed, a sealing cap be installed (not supplied).
  - In the event of rain, place a tarpaulin over the cabinet. Secure the tarpaulin around the base with elastic cords.
- **To reduce the risks associated with impact, sharps or fire:**

- Contact manager if the site has been vandalized, there is immovable rubbish, an obstruction or for any unplanned traffic incident on site.

- **To reduce the risks associated with fire:**
  - Leave sufficient space around all electrical components for cooling.
  - Do not mount any electrical components directly above a heat source.
- **To reduce the risks associated with impact:**
  - Install using Neology supplied mounting brackets only.
  - Ensure that all hardware is firmly tightened before loading.
  - Installation and service activities must be in compliance with all applicable building and electrical codes.
  - Any mounting surface must be able to support a minimum static load of equal to the maximum weight of the fixed camera system plus any additional live load due to environmental conditions.
  - Always pay attention to the road.
  - When required work in a team of two or more and ensure line of sight or contact over walkie-talkies (radio) at all times.
  - Always appropriately secure the ladder to the pole.
  - When appropriate use suitable safety harness and lanyard for securing installer to pole.
  - For United Kingdom installations, ensure Approval In Principle (AIP) is signed off by designer and Highway Agency to ensure design meets current standards.
  - Appropriate sign off and approvals shall be obtained prior to installation, maintenance and service.
  - Use only lanyards that are properly installed and inspected to hold tools.
  - Ensure length of lanyard prevents tools from contact with pedestrians or vehicles.
  - Always deploy traffic management in accordance with applicable local and government regulations. - Do not perform work if installer considers conditions unsafe.
  - Wear appropriate PPE on site at all times.

⚠ CAUTION

- **To reduce the risks associated with impact, muscle strain:**
  - Use appropriate PPE and follow safe workplace practices during installation.
- **To reduce the risks associated with muscle strain:**
  - Use appropriate mechanical or human assistance when lifting system components.
- **To reduce the risks associated with environmental contamination:**
  - Dispose of all system components in accordance with applicable local and government regulations.

NOTICE

- **To reduce the risks of property damage:**

  - Do not modify or attempt to service the camera. Return to Neology authorized service centres for repair or service.
    There are no user serviceable parts.
  - Do not use solvents or harsh cleaners on camera.
  - Do not use abrasive materials on camera window.

Federal Communications Commission (FCC) statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Neology is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that might cause undesired operation.

Introduction

PIPS Technology's new generation number plate recognition cameras are currently available in 2 models. These are the P520 and the P525. The only difference between the two is image dimensions. Specifically:

1. P520 captures images of 2064x1184 pixels.
2. The P525 captures images of 2464x1280 pixels.

The cameras have the following common features:

3. Designed for use in the highest performance applications providing accurate reads for the highest speeds and/or volumes of traffic ever likely to be encountered.
4. Integrated unit containing 2 sensors (colour and monochrome), 2 lenses, LED illumination, CPU and FPGA in a single sealed unit.
5. Motorised zoom lenses supporting the redeployment of cameras.
6. Hardware accelerated H264 video encoding to support H264 streaming video
7. Hardware accelerated Jpeg image compression to support MJPEG streams.
8. Ethernet/WiFi
9. Integrated GPS unit for precise time and location
10. Optional integrated 4G modem

Applicable Documents

1. Installation Manual
2. User Manual (this document). Describes configuration and operation of the camera
3. Reference Manual (full details of all settings and commands)
4. Developers Manual (details of interface protocols and operations to support software developers looking to integrate the camera into their software products.

Quick Start

It is recommended that you familiarise yourself with the operation of your P500 camera in an office or lab environment before attempting a roadside installation.

Required Software

A desktop PC or laptop running Windows 7, Windows 8.1 or Windows 10 is required.

The PIPS ANPR Toolkit (referred to as "Toolkit") is assumed to be installed. Toolkit (and other downloadable software) is available from http://dl.anprlicense.eu/release/public.xml.

Connecting to Power and Ethernet

Please see the P500 Installation Manual, Section: "8. Electrical Connection".

Network Connection to the Camera

To connect to the camera via TCP/IP it is best to start with the camera connected to the same Ethernet LAN segment as the PC running Toolkit. There are two possibilities for a quick start:

1. Set the cameras IP address as appropriate to the local network using Toolkit IP Discovery (recommended).
2. Modify the PC network settings for example by changing its IP address (and netmask if necessary) or assigning a second IP address (with appropriate netmask). The chosen new (or second) IP address must match the subnet corresponding to the factory assigned IP address of the camera.

If none of the above work for you, you will need to connect to the camera via a serial cable and serial terminal to configure the network via the bash shell.

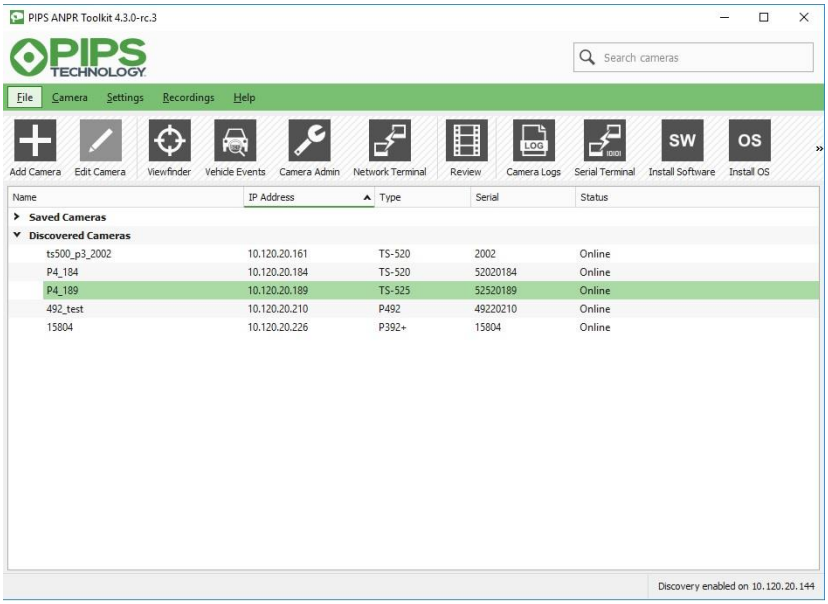
Setting the Cameras Network (IP) Address using IP Discovery

The easiest way to set the cameras network (IP) address is by using the Toolkit camera "discovery" feature. In order for this to work the camera must be on the same LAN segment as the PC running Toolkit.

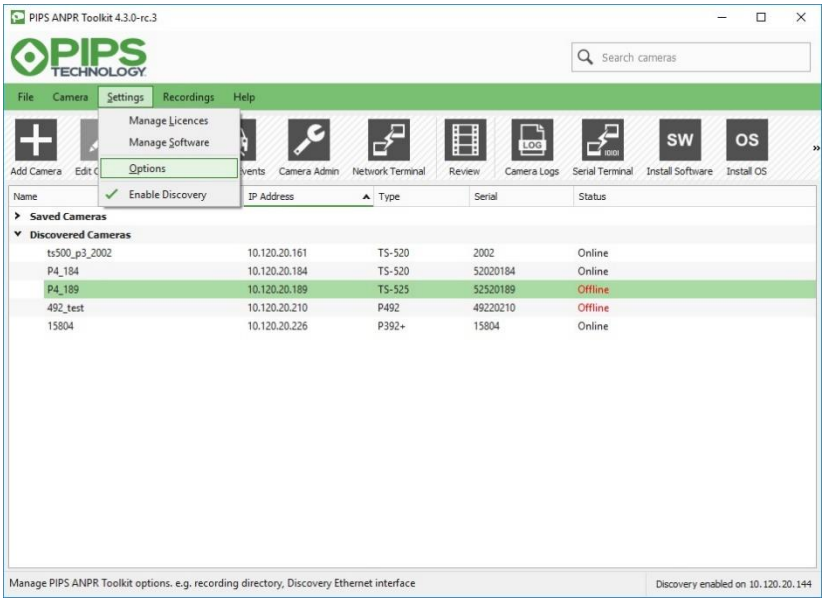
Use discovery to set the cameras IP address and netmask. Be sure to select an address that is available (alternatively isolate your camera and PC onto a private LAN segment).

To use IP discovery:

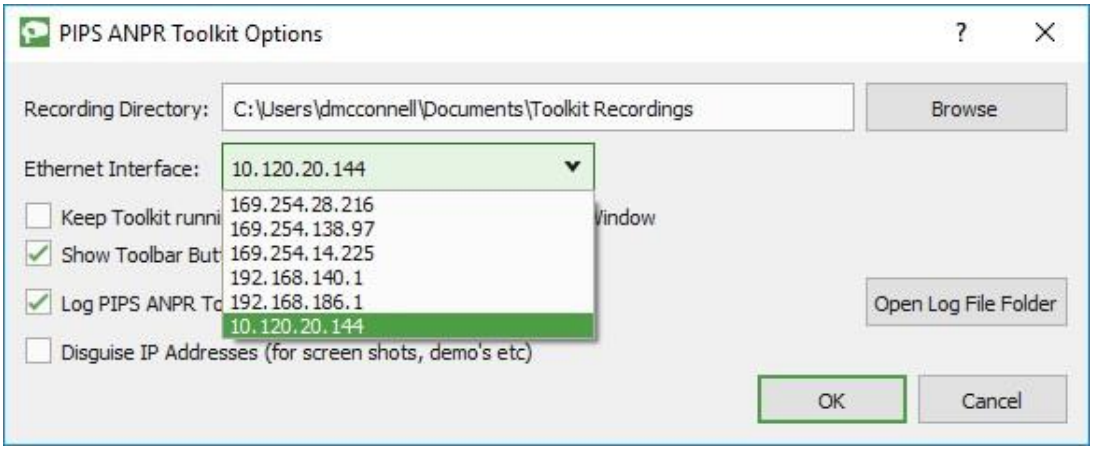
1. Ensure your camera is powered up and connected to the same LAN segment as the PC running Toolkit. Run Toolkit. You should see a screen similar to below.



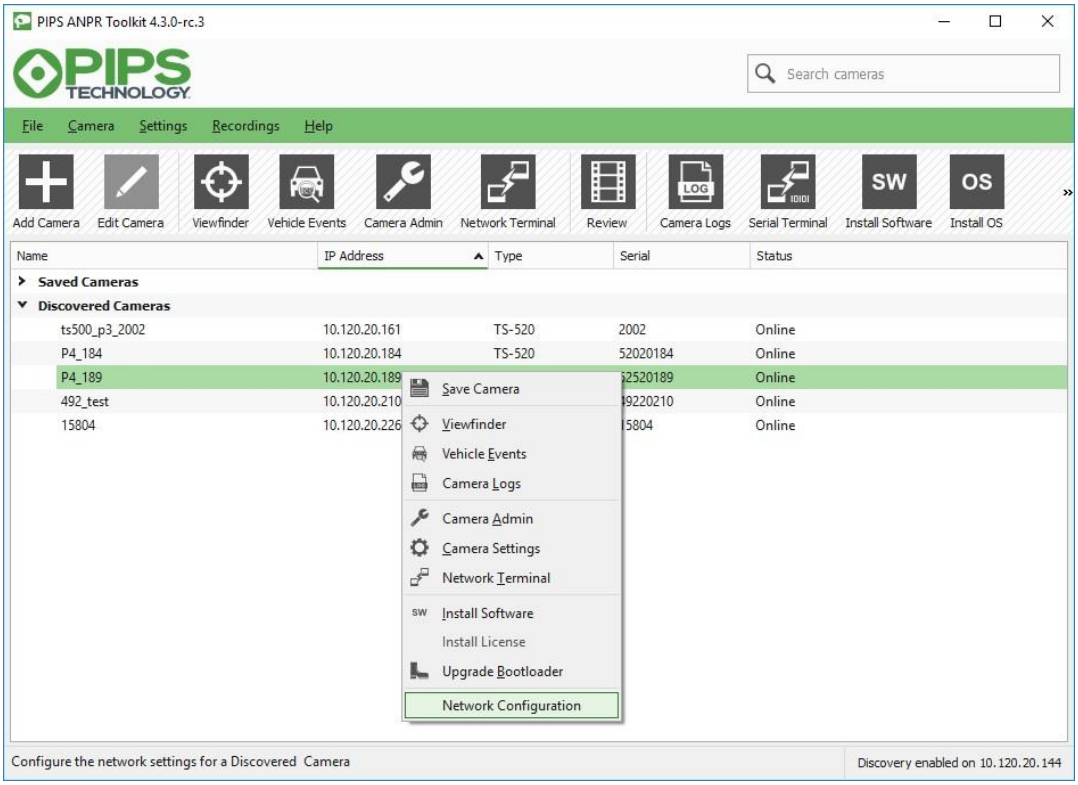
2. If you don't see your camera listed under "Discovered Cameras" you may need to set the network interface that discovery uses. Select "Settings" on the menu bar and then Options.



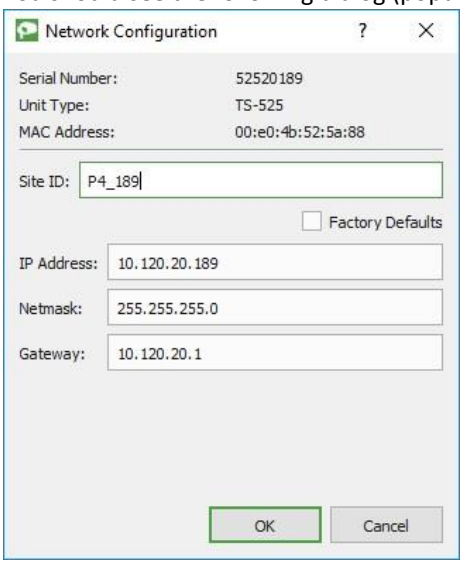
On the displayed dialog, use the “Ethernet Interface:” dropdown to select the appropriate IP address corresponding to the LAN to which the camera is connected.



3. Your camera should now appear in the list of detected cameras. Select your camera, right click and select “Network Configuration”.

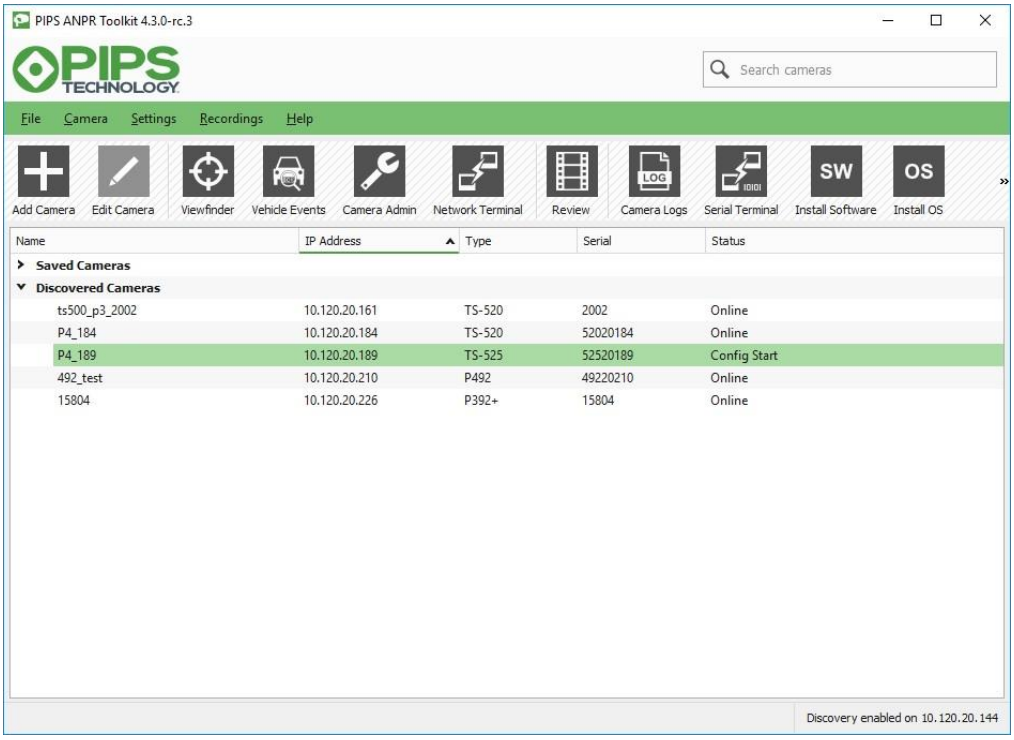


4. You should see the following dialog (populated with the values that your camera is currently set to):

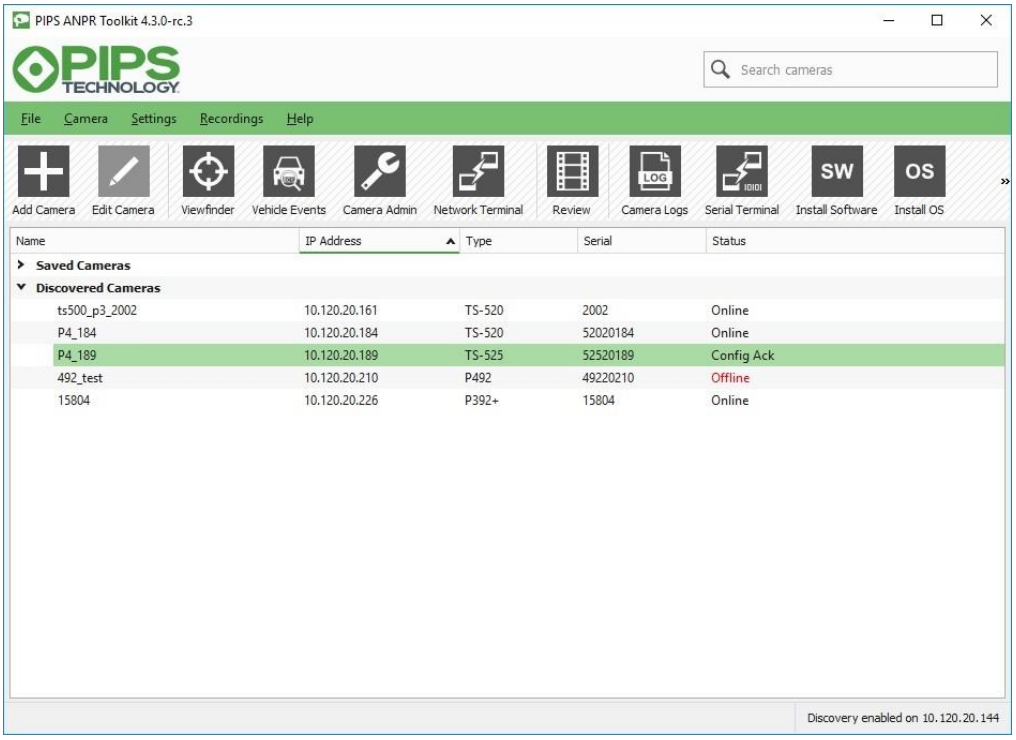


Change the IP Address (and if necessary the Netmask) to values appropriate to your network. If you wish, you may also set the Site ID and Gateway at this time. If you are happy with your changes click OK to have them applied to your camera. Otherwise click Cancel.

5. The Discovered Camera should briefly display Status: “Config Start”

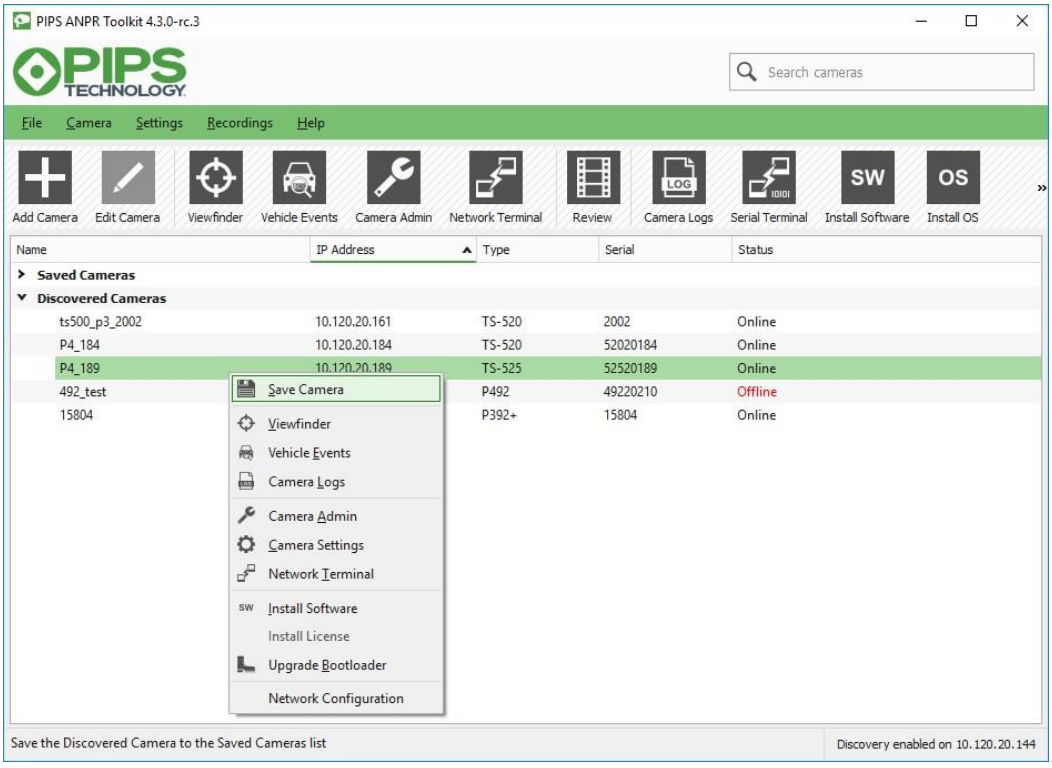


followed by Status: “Config Ack”

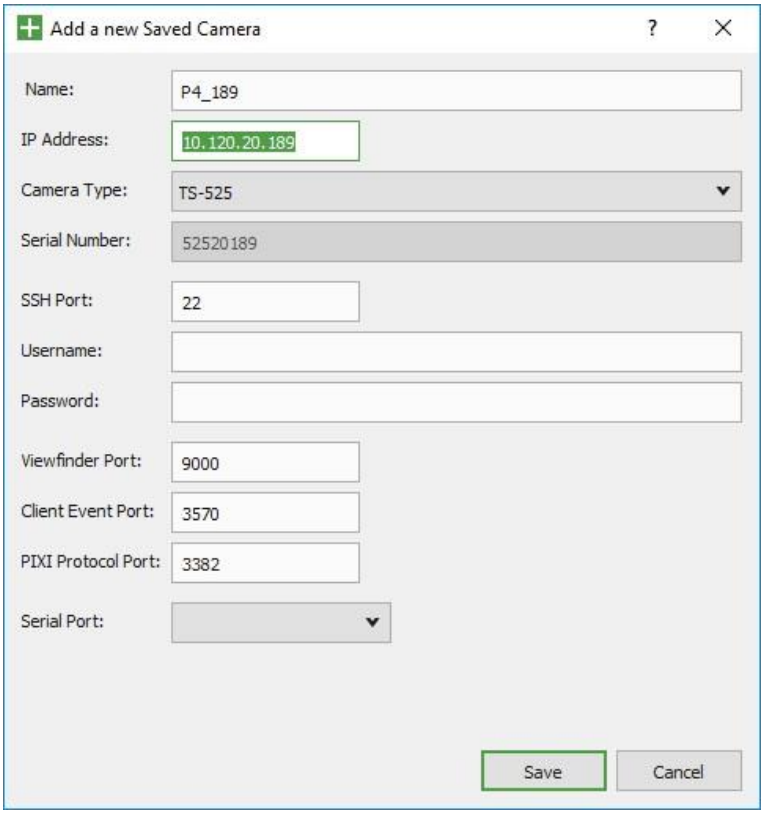


and then a little while later back to Status: "Online".

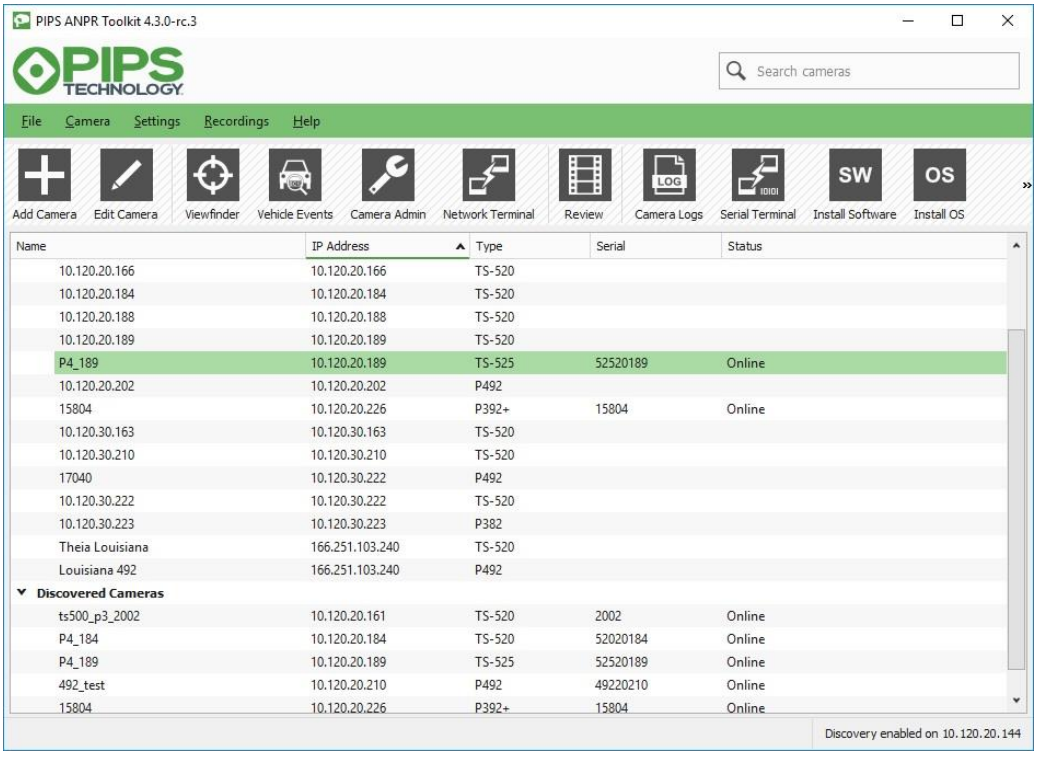
6. At this point you may save the camera to have it appear in the "Saved Cameras" list. Right click on the camera again and select Save Camera



and you will see the pre-populated dialog appear. For convenience you may wish to enter a Username and Password but it is not necessary that you do.



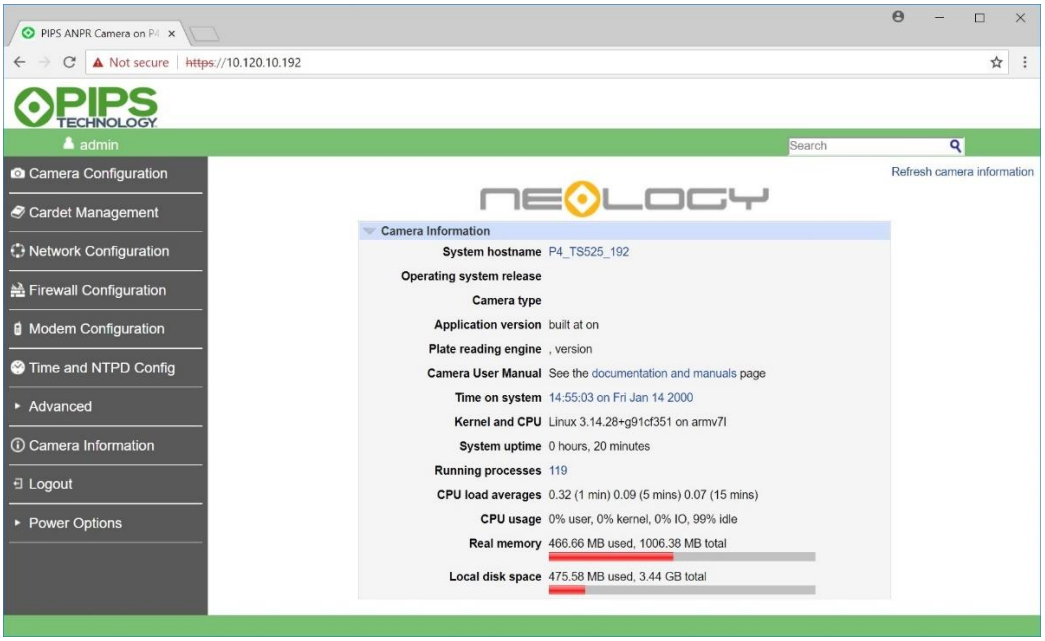
Click Save and your camera will now appear in the Saved Cameras list.



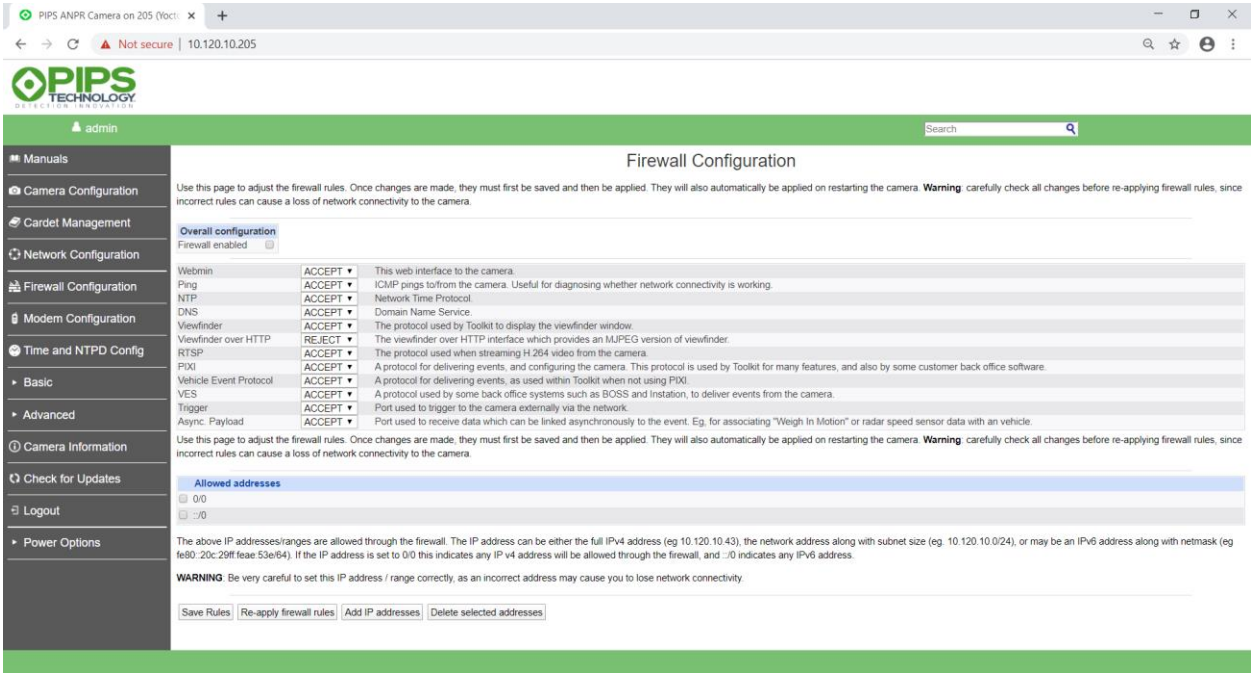
Disabling the Firewall

By default, the camera firewall is setup to block most things. In order to use the Viewfinder and Event Viewer (as described hereafter) you will need to modify some firewall rules. Since this is a quick-start section, the easiest will be to simply disable the firewall. That way when you re-enable it, all the default rules will still be intact.

In order to disable the firewall, you will need to login with webmin. See Webmin Web Interface for instructions on logging in to Webmin. Once logged in you will see the following:



Click on “Firewall Configuration” and you will see:



Deselect (untick) “Firewall enabled” and click “Save Rules”, and then click “Reapply firewall rules”.

Note this disables all the cameras firewall rules and therefore is a security risk. You should re-enable the firewall before the camera is deployed. You may of course need to adjust the firewall rules to suit your needs. Please see this section: Firewall.

Viewing the channel with Viewfinder

The P500 has two sensors, a colour and a monochrome. It is therefore in fact two cameras in one body.

The monochrome sensor also normally has an Infrared bandpass filter in place and relies on Infrared flash from the LEDs for illumination. For this reason, the monochrome sensor is often referred to as the **IR** Sensor (or "IR Camera").

Unless there is a retro reflective plate in the field of view, the IR camera normally sees very little, so we will start with the colour camera.

Double clicking on your camera in the "Saved Cameras" list will bring up the Viewfinder. The dropdown on the top left will show which camera (colour or IR) is being displayed. If it is IR, use the dropdown to select the colour camera.

It is likely that the view you first see will be out of focus. However, you should see something, even if it is just a blur.

Setting Focus and Zoom

In order to focus the colour camera, select the “Lens Control” tickbox on the top right of the Viewfinder screen.

The slider bars that appear may be used to adjust the focus and zoom. Suggest adjusting the focus first so you can properly judge the field of view, and then adjust the zoom. Since changing the zoom will cause loss of focus, you may want to make several zoom adjustments, refocusing after each, until you are satisfied with both the field of view and the focus.

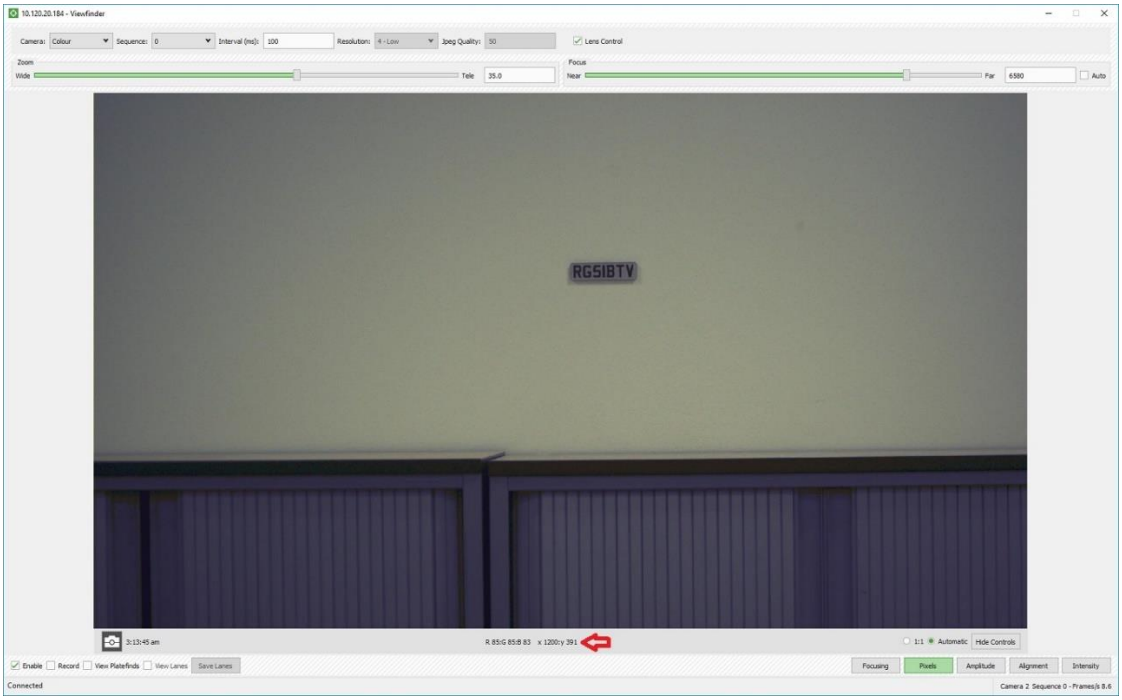
Note, if a slider bar is selected (a selected slider has an green handle as for the Focus slider above), then the left and right arrow keys may be used to single step the focus (or zoom if that slider were selected). It is also possible to type specific numbers into the text entry fields adjacent to the slider bars.

Reading a Plate

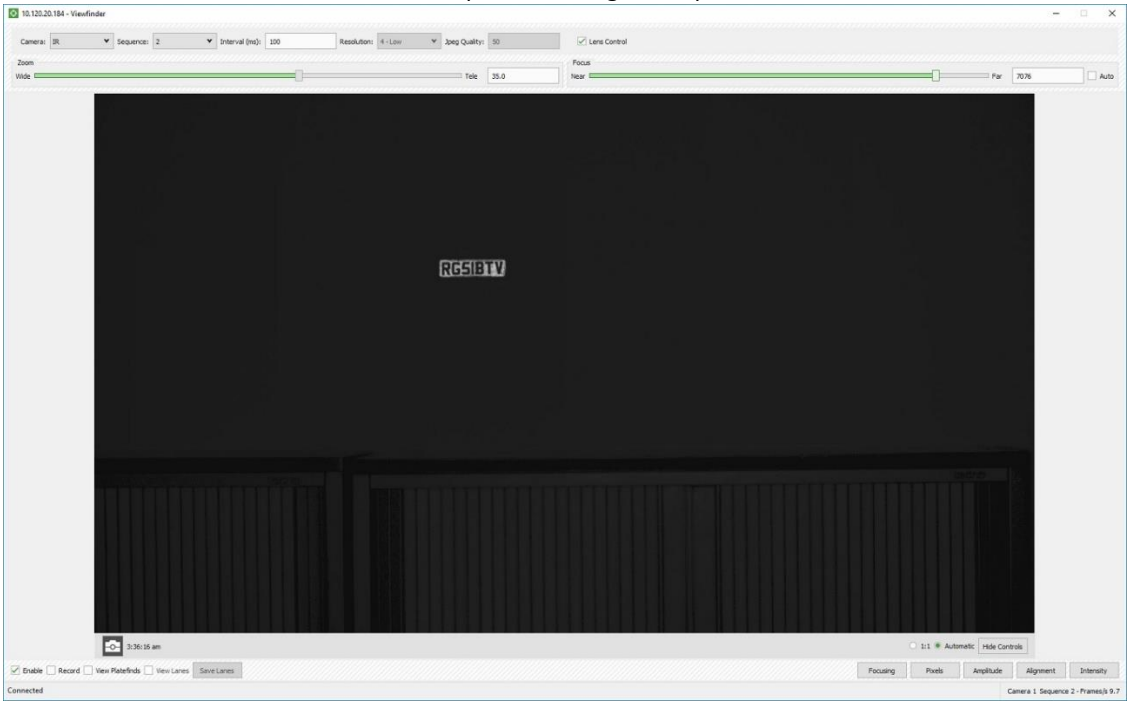
If you have a retro reflective license plate (from an appropriate jurisdiction for your OCR software) that you would like to read, proceed as follows:

1. Place the license plate at a convenient location such that the camera can easily be aimed at it.
2. The plate should be placed at least 4m from the camera.
3. Use the colour channel viewfinder to ensure the plate is nicely placed in the field of view (not too close to any edge). Adjust the zoom (and focus as appropriate) until the plate is between100 and 150 pixels wide in the field of view.
4. Hint: to measure the size of the plate in the field of view, click on the “Pixels” button. If you subsequently click anywhere in the field of view, the x,y coordinates of the mouse pointer will be printed below the image (the red arrow on the image below indicates where the x,y coordinates will be displayed.). The plate width is the difference between the x coordinate representing the right and left edge of the plate

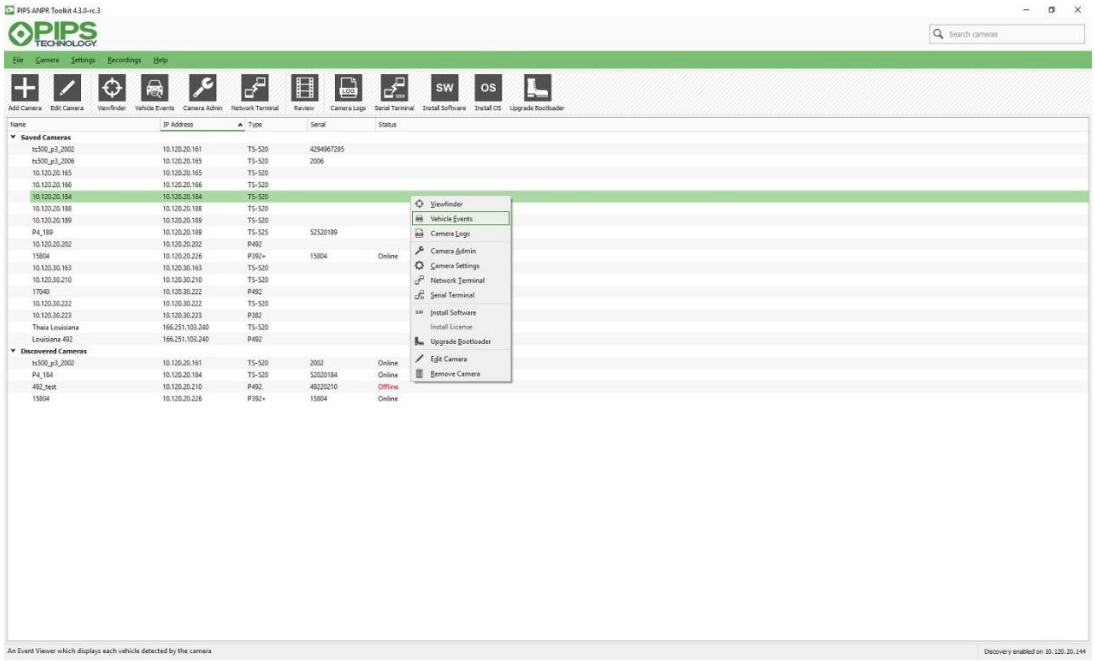
(the right edge x coordinate will be the greater value).



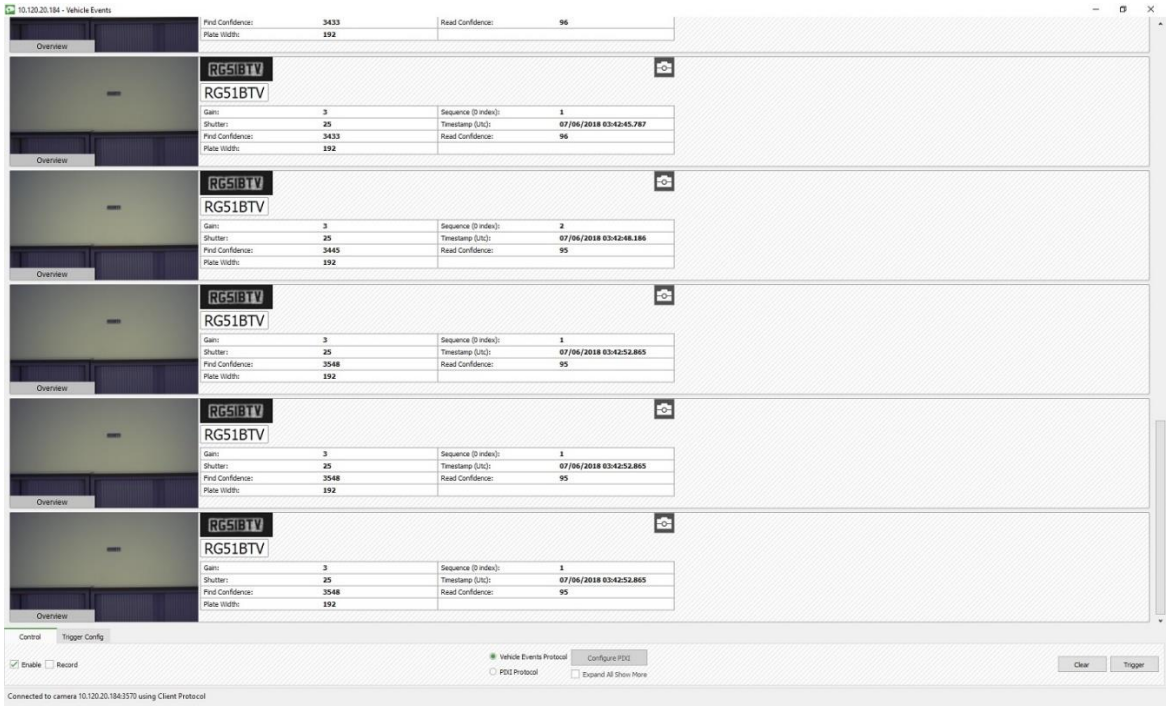
5. Open a new viewfinder window and select the IR camera from the dropdown at the top left.
6. Tick the “Lens Control” and copy the zoom and focus settings from the colour channel to the IR channel. (Note the focus differs between IR and colour but using the value from the colour will get you in the ballpark).
7. Refine the focus of the IR camera until the plate lettering is sharp.



8. The camera should now be reading the plate. To view the plate reads, select the camera entry in the “Saved Cameras” list, right click and select “Vehicle Events”



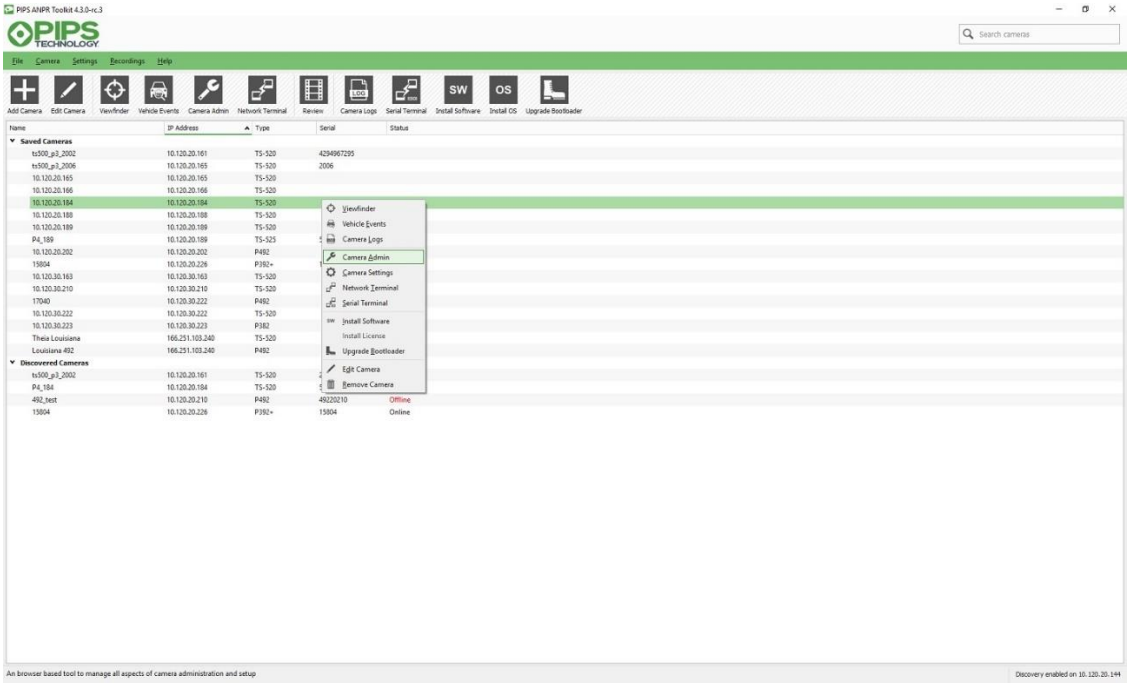
9. The event viewer will be displayed. The plate will be read repeatedly. The default event viewer will display the read plate text, other metadata, plate patch image and the associated colour image. The display will scroll as repeated reads continue to come in. Note: it is possible to disable the reading repeat. It is enabled by default as it is useful during camera familiarisation and installation.



Webmin Web Interface

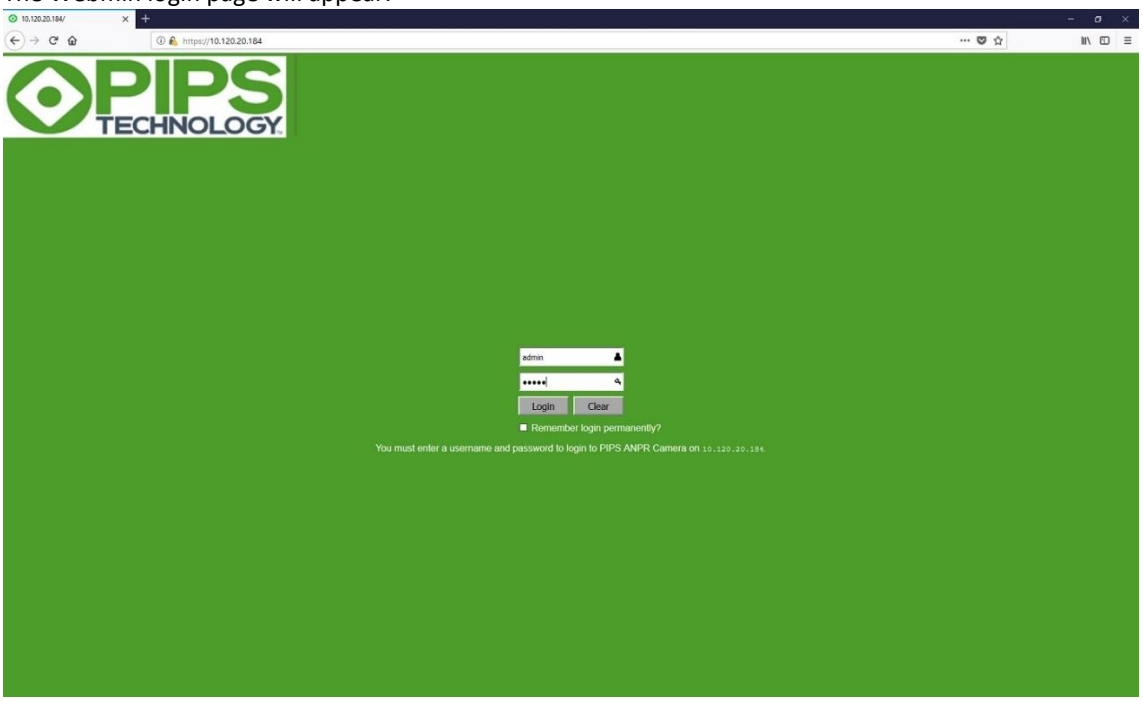
The P500 supports the Webmin web interface.

To access the web interface from Toolkit, select a saved camera, right click and select “Camera Admin”.

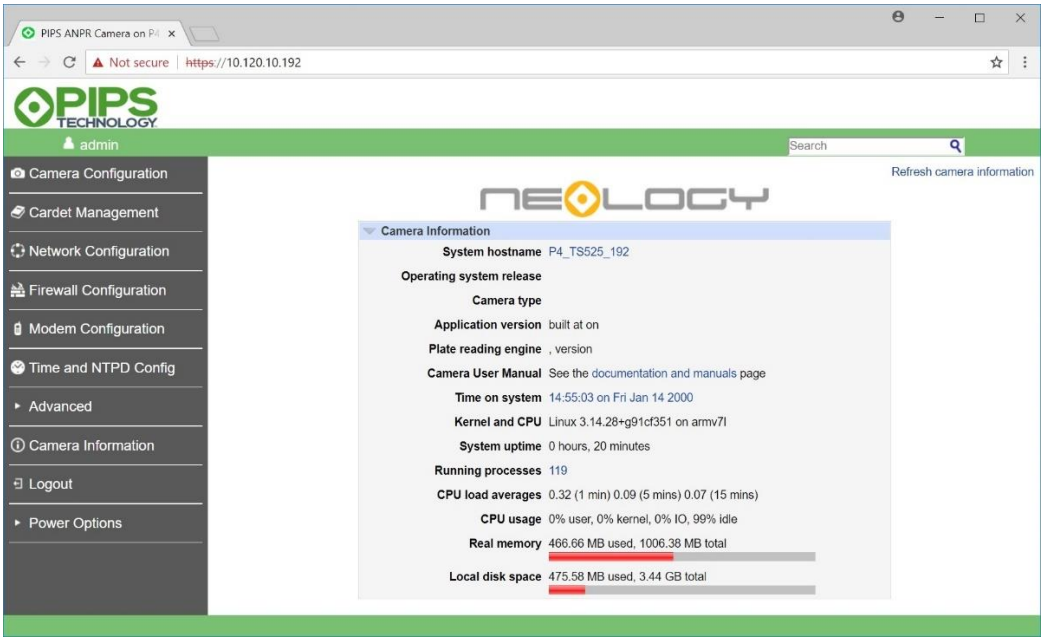


Alternatively open your browser and type in the URL **https://10.120.20.184/** replacing 10.120.20.184 what what the IP address that is assigned to the camera and displayed in Toolkit.

The Webmin login page will appear:



And once logged in it lands on the Camera Information page:



Note the links down the left hand side – including the link to Camera Information which is also the default landing page.

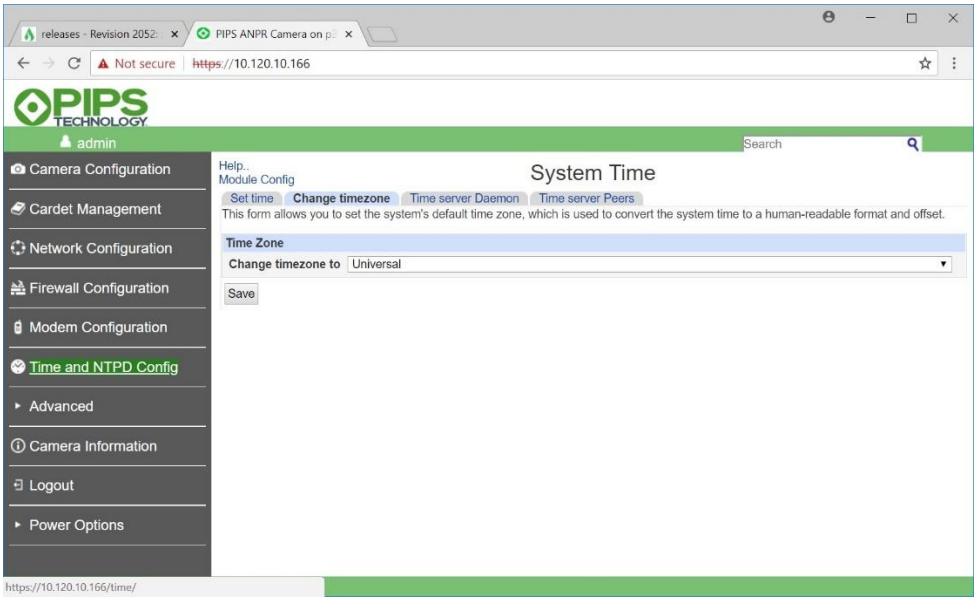
Feel free to click on the other links to see where they take you, just be a little careful not to unintentionally change a setting.

Note that Webmin documentation can be found online. At the time of writing, the documentation is available here: http://doxfer.webmin.com/Webmin/Main_Page.

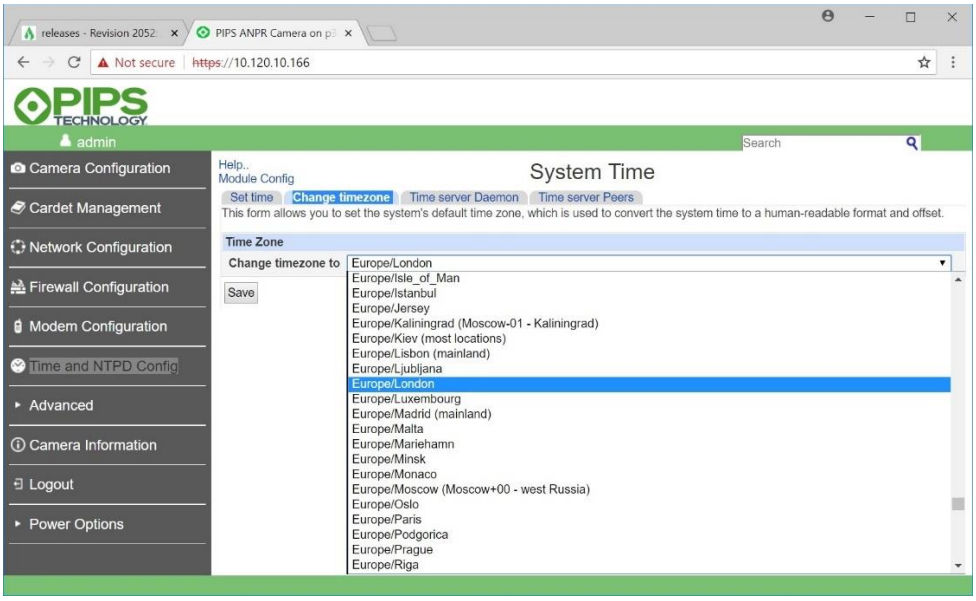
Camera Time

Setting the Time-zone

In order to set the time-zone, connect with Webmin and click on “Time and NTPD Config” and then on the “Change timezone” tab as in the figure below:



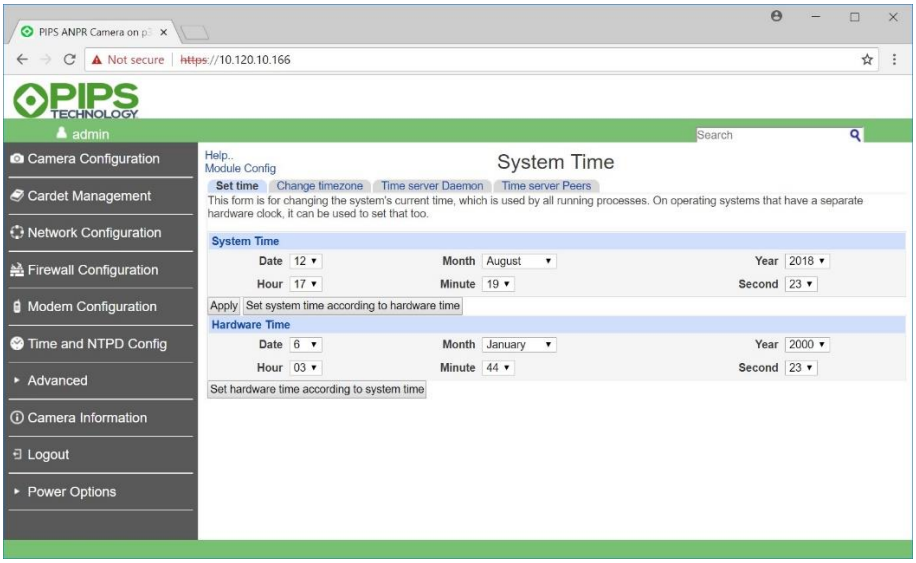
Then use the dropdown to select your time-zone.



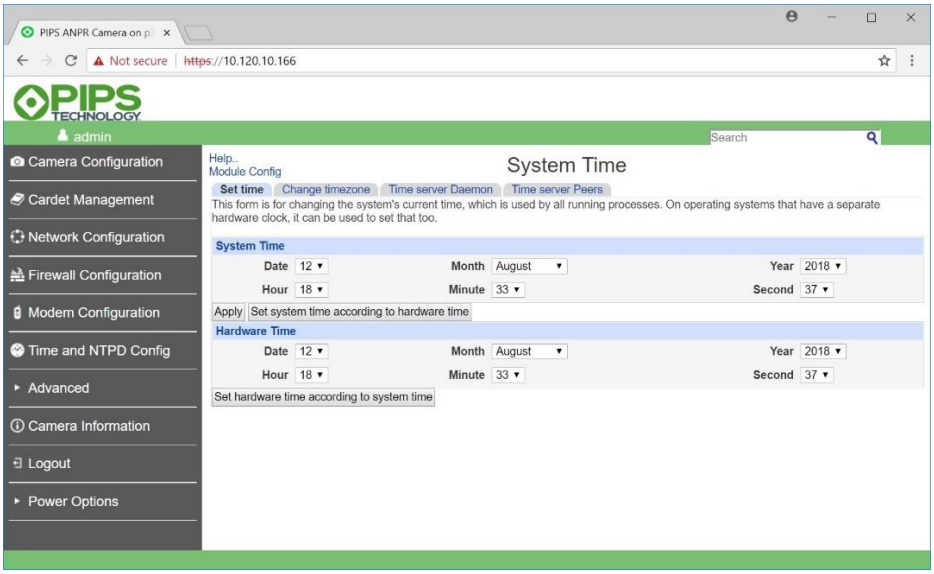
And then press the “Save” button.

Setting the Time

In order to set the time, connect with Webmin and click on “Time and NTPD Config” and then on the “Set time” tab.



Use the dropdowns to set the date and time and then press “Apply”. It is suggested you then press the “Set hardware time according to system time” button for the time to be saved to the Hardware clock. Normally the system time is automatically written to the Hardware clock on shutdown, but the system may not be cleanly shut down – which is why it is advisable to save the system time to the hardware clock after you have set it. The Hardware Time will then match the System Time as below.



Note that the camera hardware clock will allow the camera to maintain time after a power cycle, but it will not be able to do so if the camera has been powered off for an extended period. For this reason, it is recommended to configure NTP as will be described in the next section.

Configuring NTP

The camera clock does not hold it’s time for very long.

It is strongly recommended that NTP is used to maintain accurate time on the cameras. The most typical scenarios are:

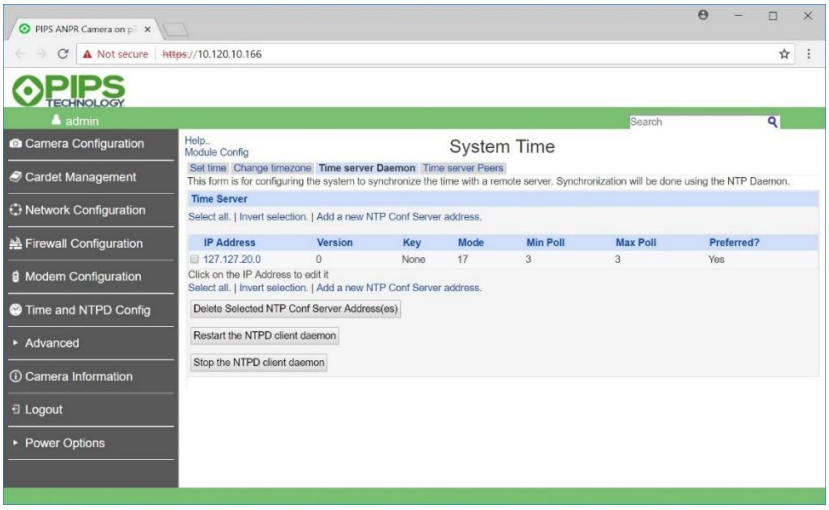
1. Synchronising of the internal GPS. This will only work if the optional GPS unit is fitted and the GPS has achieved synchronisation with sufficient satellites.
2. Synchronising off an NTP server.

The camera can also be configured as a synchronisation source. This makes the most sense if the camera is fitted with a GPS allowing it to act as a stratum-1 NTP time server. Other cameras and back-office systems may then synchronise off this camera.

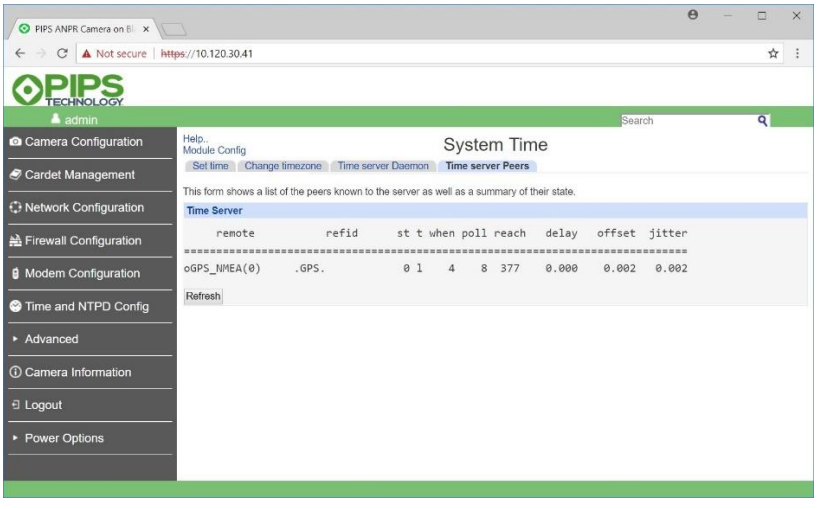
GPS Synchronisation of NTP

The camera is configured by default to synchronise of GPS. However, it won't be able to successfully do this if no GPS is fitted, or the GPS is not seeing sufficient satellites to synchronise.

You can form the presence of the GPS synchronisation source by connecting with Webmin, click on "Time and NTPD Config" and then on the "Time server Daemon" tab. You should see the following screen:



The Time Server IP Address 127.127.20.0 is the GPS clock source and is by default the preferred clock source. In order to see if the NTP time is in fact synchronised, click on the "Time server Peers" tab. The following screen indicates a system where NTP has synchronised properly with GPS:

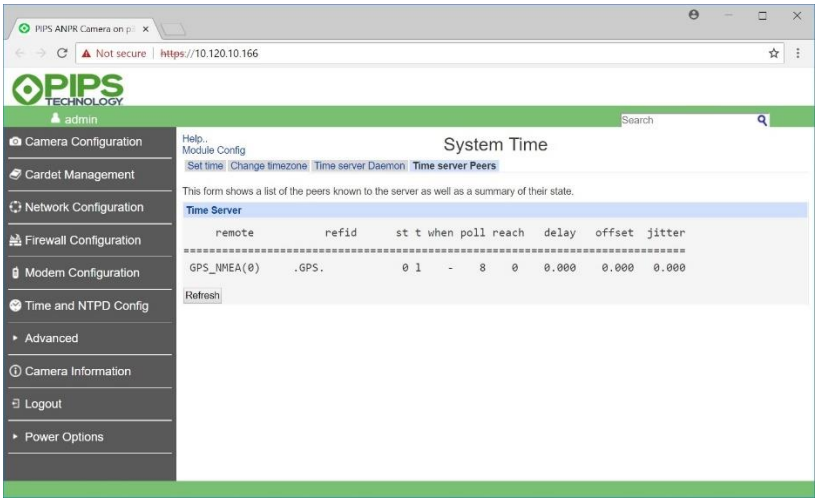


Note on the above screen the tell-tale character 'o' on the left of the "GPS_NMEA(0)" string, specifically: "oGPS_NMEA(0)". This indicates that it is using the GPS as it's time synchronisation source *and* that the Pulse Per

Second (PPS) from the GPS unit is available and being used. The pulse per second is necessary in order to get the best possible accuracy. Note the values of “offset” and “jitter” are in milliseconds, so in the above example we are looking at 2us (0.002ms) for both offset and jitter. This is extremely accurate time. Synchronising off a network based NTP server will not get close to this accuracy. This also allows the camera to provide extremely accurate time to other NTP clients on the network. This could be other cameras or back-office servers.

Note if the system was using a GPS source, but PPS wasn’t available, the tell-tale character on the left of the “GPS_NMEA(0)” would be a ‘*’, specifically: “*GPS_NMEA(0)”. While a ‘*’ is normal for non-local time sources (e.g. external NTP time servers) it is not what is expected when using the cameras own GPS – the presence of a ‘*’ would indicate there is a problem with PPS. This may suggest the GPS unit has not properly synchronised with satellites – or there is some other problem.

The following screen indicates a system where NTP has not managed to synchronise with GPS. This may mean that the camera is not equipped with a GPS – or that the GPS has not been able to synchronise off sufficient satellites.



Specifically, there is no ‘o’ to the left of “GPS_NMEA(0)”.

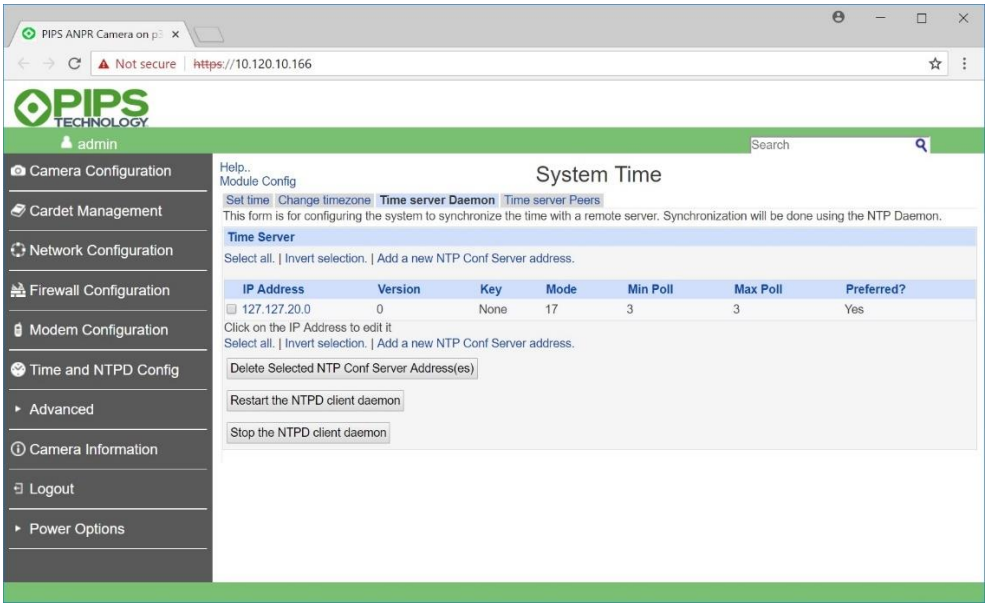
Other indications that all is not well:

- The “when” value is not set. The “when” entry indicates when that synchronisation source was last heard from.
- “reach” is 0. This is an indication of how many of the last polls were successful. The value should reach 377 and stick there – meaning the last 8 polls were successful (it is an 8 bit value reported in octal with a 1 bit shifted in from the left on every successful poll). If the system has recently been configured “reach” may not be 377, but it should be increasing in value over time. If it is decreasing in value (or 0) this suggests the synchronisation source is not providing the time.

If the camera cannot synchronise from GPS, then an alternative NTP source should be configured. This is described in the next section.

Server Synchronisation of NTP

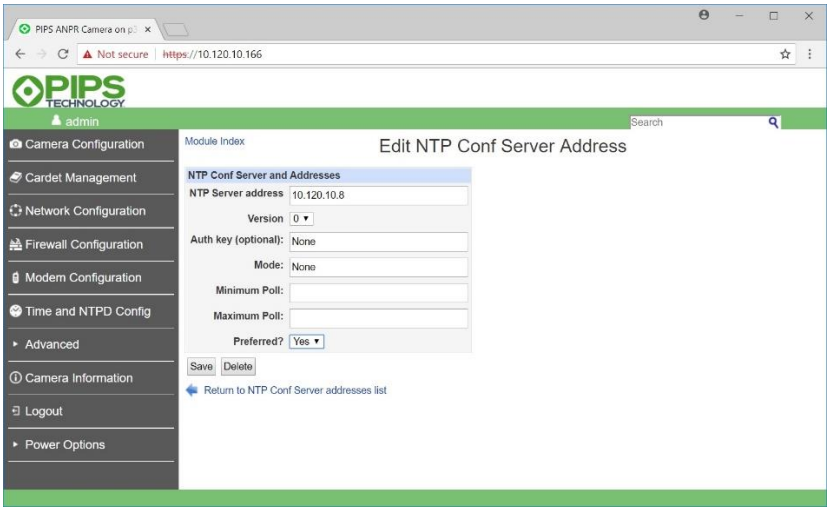
In order to configure NTP to synchronise from a remote server, you will need it’s IP address. To specify an NTP server, connect with Webmin, click on “Time and NTPD Config” and then on the “Time server Daemon” tab. You should see the following screen:



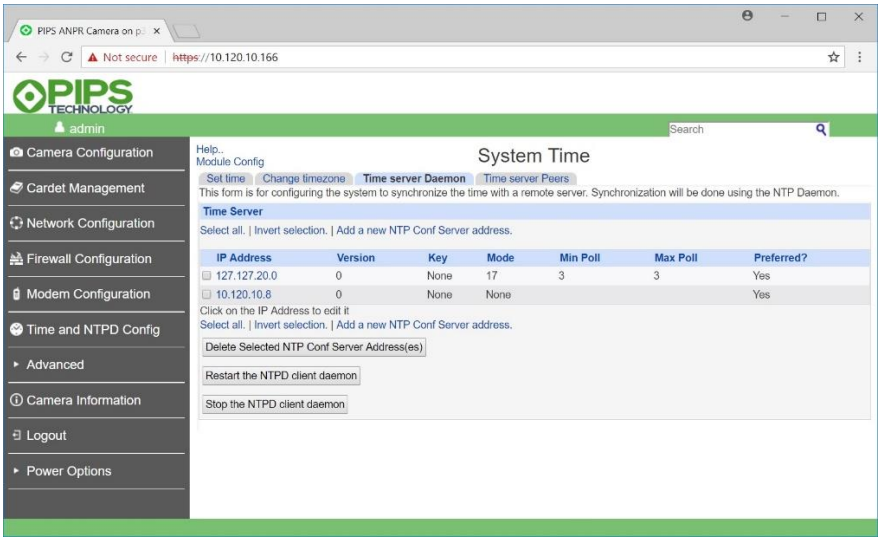
The 127.127.20.0 IP Address represents the camera's internal GPS and is present by default. If your camera is not equipped with a GPS you do *not* need to delete this entry. It can simply be left as is, it won't do any harm.

Even if your GPS is working and your time is synchronised to it, you can still add another (or multiple other) NTP time server(s). These will act as a backup to the GPS – should the GPS fail to provide time for any reason.

To add a network NTP server, click on "Add a new NTP Conf Server address." The following screen will appear:

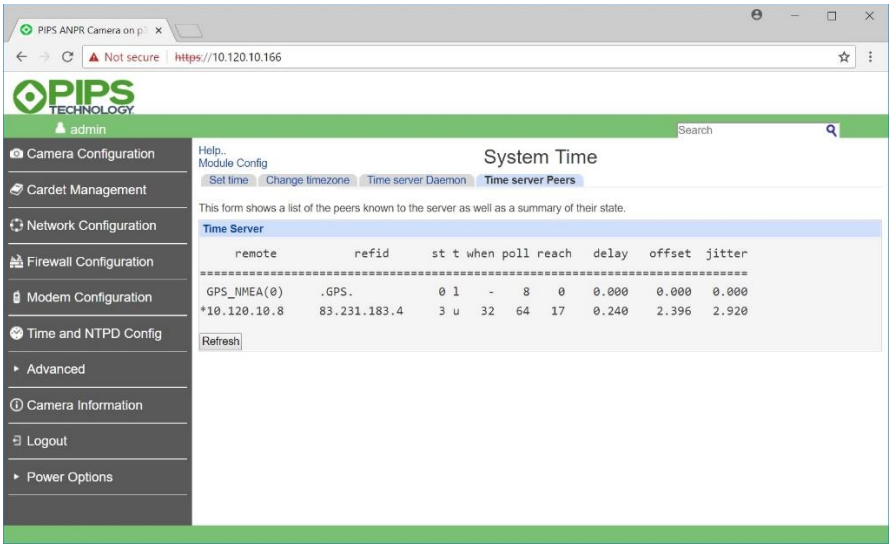


- Type in the "NTP Server address".
- If your GPS is not working, then you can also designate this server as "Preferred". Use the dropdown to select "Yes" for "Preferred". (You could also then deselect your 127.127.20.0 "Preferred" status, although if GPS is not present, the setting is irrelevant.).
- Click "Create". Note, if you are editing an existing NTP server, you will have a "Save" button rather than a "Create" button. After clicking "Create" (or "Save") you will return to the following screen after a few seconds:



Note that there is now an added IP Address. For the NTP daemon to use the added server, click on the “Restart the NTPD client daemon”.

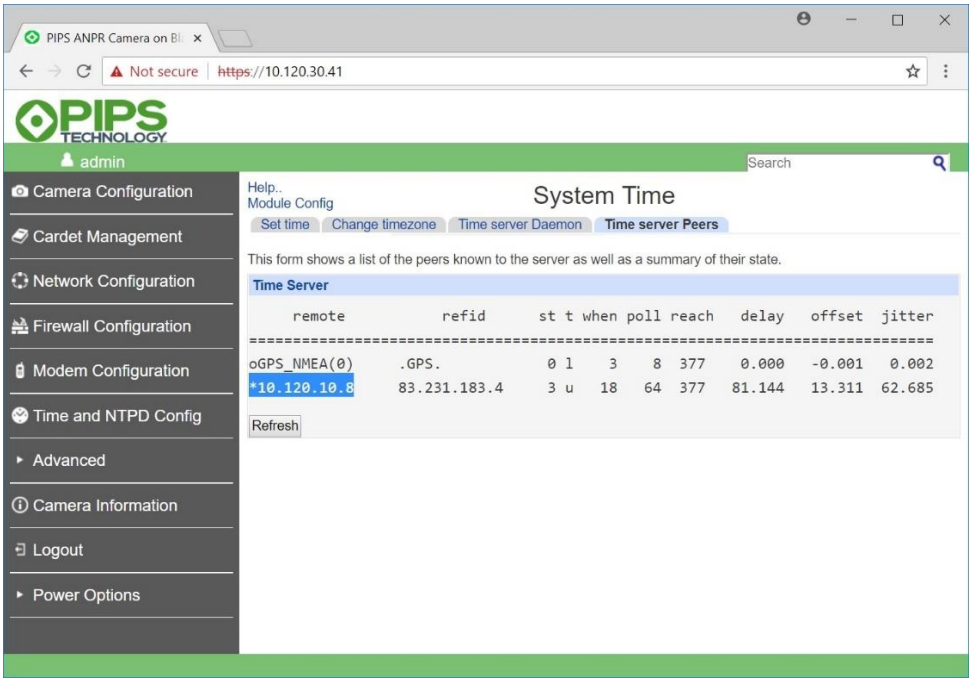
If you then subsequently click on “Time server Peers” you should see something like:



In the case of a network NTP server, the currently selected peer is designated by a ‘*’. Specifically “*10.120.10.8”.

Note also that the “when” and “reach” values are set. The “reach” value should eventually reach 377.

If you are using your internal GPS and a remote NTP Server, you could see something like:



Note both the ‘o’ and ‘*’ tell-tale characters and the “reach” being 377 in each case (meaning the last 8 polls in each case were successful). Note also how much higher the offset and jitter are for the network NTP time server (10.120.10.8) than the GPS. For most practical purposes however, the accuracy provided by a network connected NTP Time server is sufficient.

Security

This section details how to configure and improve security related aspects of the camera, ranging from user accounts and passwords through to the network firewall.

The stock configuration on a newly received P500 camera is tuned primarily for ease of initial configuration whilst also attempting to strike a balance with good security, however some changes are recommended on the part of the user to fully protect the system.

Neology strongly recommends that all its cameras are to be installed on secure private networks; avoid providing access to cameras via insecure public networks including the internet.

If the cameras are not secured both physically and through tightening the system security it is possible for someone to compromise the camera. If they do this, it is possible to gain access to your private network, install custom programs on the camera, and modify camera settings.

Implications of a compromised camera include your confidential and private data being stolen, your network becoming part of a spam or bot net used in hacking, someone could block their license/number plate from being passed onto the back office and thus evading law enforcement agencies or toll agencies.

User Accounts

A stock P500 range camera comes preinstalled with the following user accounts configured for remote access.

User Account	Description
admin	Referred to as the “administrative account”, this user has full access to a standard shell on the camera and can be used to run ad-hoc commands, as well as full configuration access for all aspects of the camera software, network settings, etc.
pshell	This account is a slightly more restricted version of the administrative account with access only to the Platereader Shell. This allows the account to configure the operation of the camera software itself, without having the ability to run ad-hoc Linux commands or directly change other critical aspects of the camera such as network configuration.

These accounts may be used for accessing the camera via both serial/network terminals and the Webmin interface with the same password. Changes to the password are synchronized, and will apply to logins from all of the above listed sources.

Creating Accounts

Additional user accounts can be created via a terminal or the web interface.

Terminal

Connect to the camera via either a serial or network terminal and log in with an existing user that has administrative privileges.

Execute the “invoker adduser” command as shown below to create a new user, replacing “<user>” with the name of the user account to create. Usernames must consist of only alphanumeric characters, underscores, and hyphens. No spaces may be present.

```
CIL50012345678:~$ invoker adduser <user>
```

If the command executes successfully without error, this will display no output. Otherwise if an error occurs due to for example, the user already existing, the command will fail and output the error message.

By default, user accounts created via this command are limited to Platefinder Shell access only. To grant full Bash shell access, the optional “allowBash” parameter may be added after the name:

```
CIL50012345678:~$ invoker adduser <user> allowBash
```

Administrative users can be created by appending the optional “allowAdmin” parameter. This option may be combined freely with the previous “allowBash” option (separate the two by the space) to create administrative accounts with Bash shell access.

```
CIL50012345678:~$ invoker adduser <user> allowAdmin allowBash
```

The user will be created with a locked password by default, preventing password-based logins from taking place. To enable password access to the account, run the “invoker passwd” command replacing “<user>” with the username.

```
CIL50012345678:~$ invoker passwd <user>
Changing password for <user>
New password:
Retype password:
Password for <user> changed by root
```

SSH key-based authentication may also be configured as described in the Key-Based Authentication section.

Web Interface

Access the web interface as documented in the “Webmin Web Interface” section. Expand the “Advanced” header within the left sidebar and click the “Users and Groups” link to open the following page.

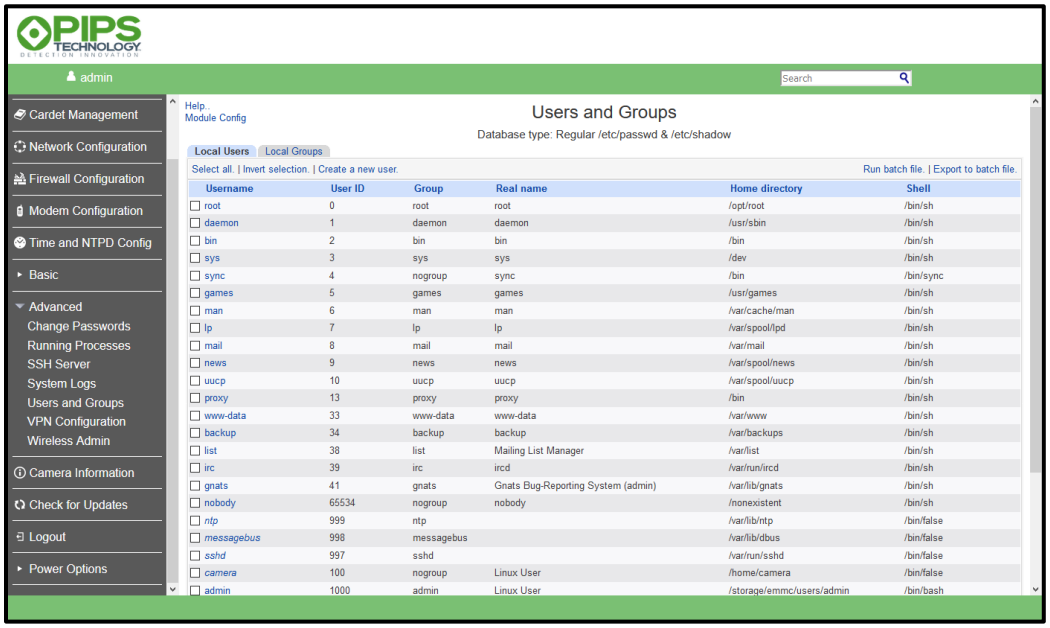


Figure 1 Users and Groups Page

At the top and bottom of the table is a link labelled “Create a new user.”. Clicking that will open the user creation page.

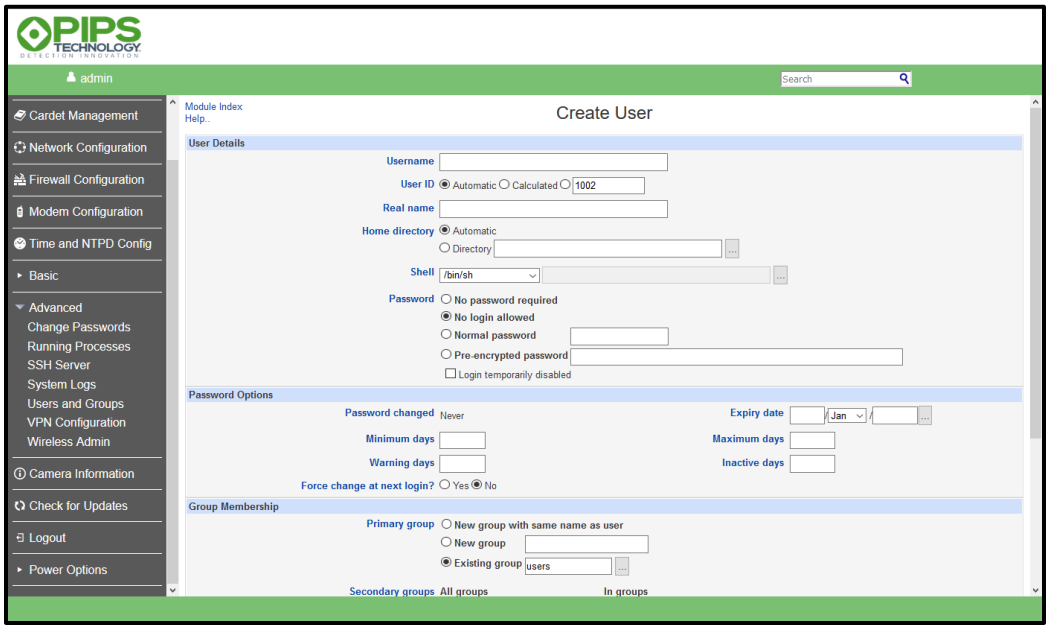


Figure 2 Create User Page

The most important options from this page are listed below.

Field	Description
Username	The name of the user to create.
Home Directory	The directory where the user's personal data will be stored. This should be set to /storage/emmc/<username>
Shell	The default terminal shell for the user. The following options are of interest: • /bin/bash will use a standard Bash shell upon terminal login. Recommended if the user requires terminal access. • /bin/false will disallow shell access entirely. • /opt/camera/pshell will restrict the user to the Platereader Shell only.
Password	Password to assign the user. The default is to create an account that disallows all password-based logins, but if required a password may be set by selecting the "Normal Password" option and entering it here. It is not recommended to select the "No password required" option.
Primary Group	The primary group to assign the user. This may be a new group named the same as the user, or the default of assigning them to a common "users" group.
Secondary Groups	This field contains two lists; the left displays all the groups installed on the system, and the right is the list of groups to assign. Selecting a group from the left list and clicking the "->" button will place the group in the right list, and vice versa for the "<-" button. In terms of useful groups, the following are documented: • admin: Members of this group may run the "/opt/camera/invoker" utility which is used to perform operations that require administrator privileges. • storage: Members of this group are granted write access to the storage devices on the camera mounted under /storage.

After filling in fields as appropriate, click "Create" to create the user account.

Deleting Accounts

Accounts may be deleted from the terminal. Log in via either a serial or network terminal as an administrative user and run the “invoker deluser” command replacing “<user>” with the name of the user account to be deleted.

```
CIL50012345678:~$ invoker deluser <user>
```

Warning

Deleting administrative or system users may render the camera inaccessible, requiring that the camera have a clean OS reinstallation performed.

Default Passwords

The default password associated with both accounts is inherently insecure. The choice of password is to ease initial setup of the cameras but is **strongly recommended** to be changed as soon as possible.

When you first receive your P500 camera, both users will be preinstalled with the user accounts listed above. The passwords will be communicated to you separately.

Changing Passwords

User passwords can be changed via a terminal or the web interface.

Terminal

Connect to the camera via either a serial or network terminal and log in with an existing user that has administrative privileges.

Execute the “invoker passwd” command as shown below to change a user password, replacing “<user>” with the name of the user. The command will prompt for the new password twice before replacing it.

```
CIL50012345678:~$ invoker passwd <user>
Changing password for <user>
New password:
Retype password:
Password for <user> changed by root
```

To lock an account from password-based authentication entirely, the “invoker passwd lock” command can be used instead. This will prevent the user from logging into the system with anything except SSH key-based authentication as described in the Key-Based Authentication section below.

```
CIL50012345678:~$ invoker passwd lock <user>
Password for <user> changed by root
```

Warning

Locking the password to an administrative account **may lock you out of the system** if you have not set up an alternative administrative user. This situation can be recovered via a clean OS reinstallation of the camera.

Web Interface

Access the web interface as documented in the “Webmin Web Interface” section. Expand the “Advanced” header within the left sidebar and click the “Change Passwords” link to open the following page.

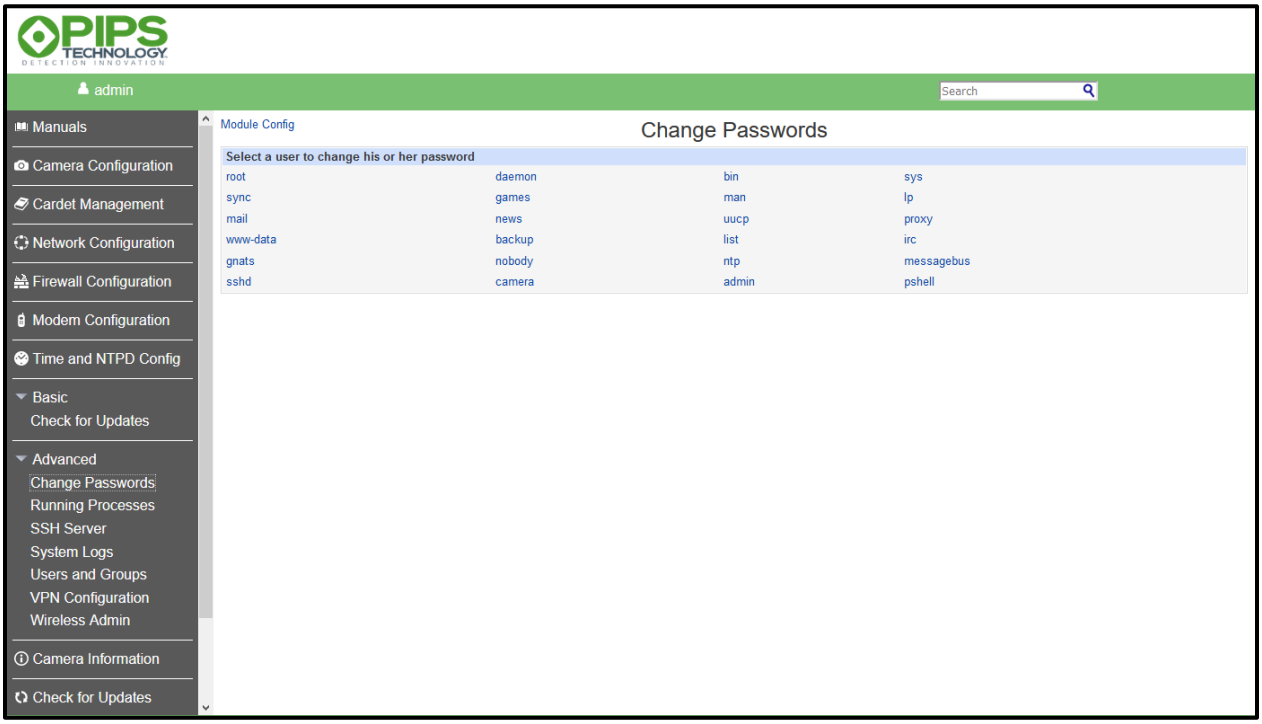


Figure 3 Change Passwords Page

Select the user account to be configured (typically “admin” or “pshell”) and the change password page will open.

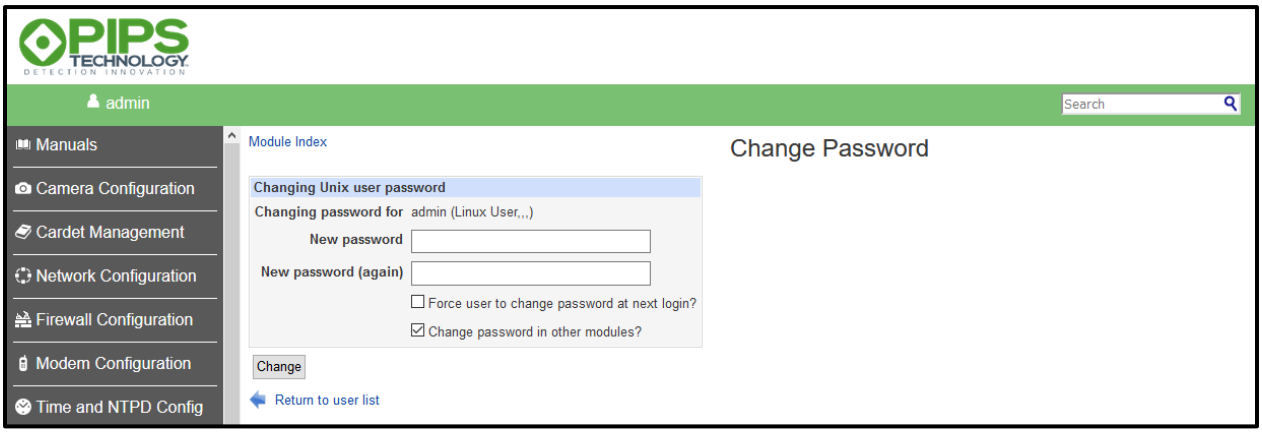


Figure 4 Change User Password Page

Enter your new password for this account and click “Change”. The password will be immediately applied, but any existing login sessions will not be terminated. Do not select the “Force user to change password” check box, as this functionality is not currently available.

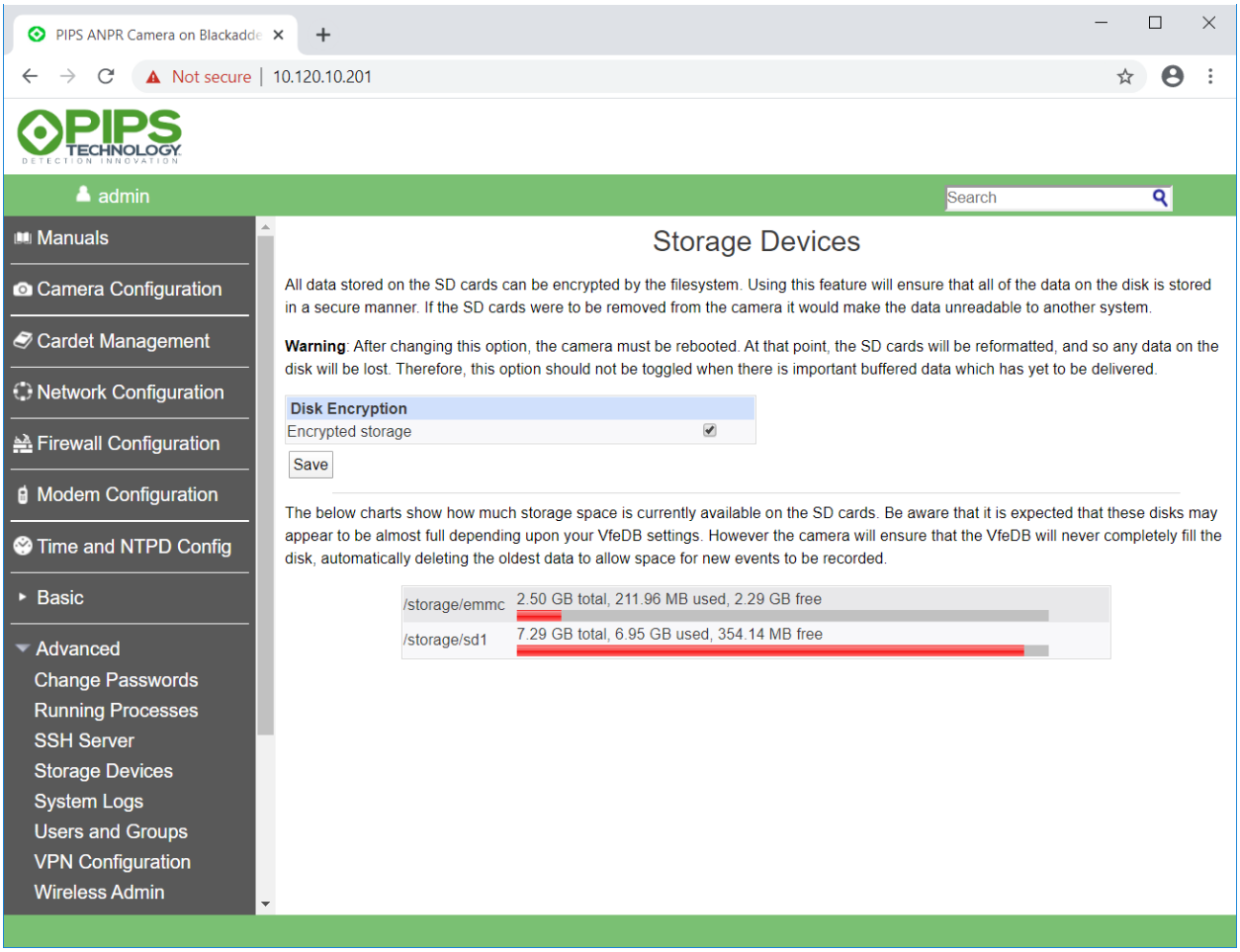
Root Account

The root account is by default disabled and cannot be logged in. This is for security reasons, as the root user has total control of the system and is frequently the target of attacks on any Linux system.

Disk Encryption

The removable SD cards that are used to store the event data can be set to use encrypted disks. This will make the data secure such that if the disks are removed from the camera, no data can be retrieved from them.

Enabling this option on an already installed camera will cause the camera to format the disks upon next reboot so will lose any data that is currently buffered, so it is recommended this is done either at first installation, or at a time when the camera is known not to have important buffered data.



OpenSSH

The camera provides network shell access via the SSH protocol and is fully compatible with compliant SSH client implementations such as PuTTY and the OpenSSH client.

Key-Based Authentication

Use of key-based authentication is strongly recommended where possible as this greatly increases the security of user accounts if combined with disabling password-based authentication.

To generate an SSH key under windows, PuTTY is assumed to be installed by the user complete with its "PuTTY Key Generator" application. Launching that application will display the following screen.

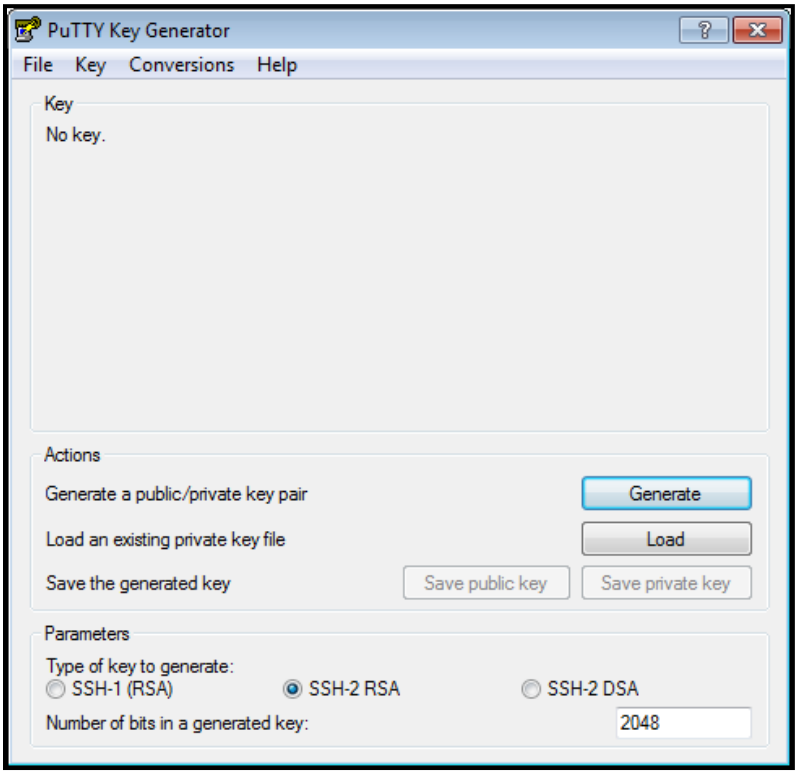


Figure 5 PuTTY Key Generator Window

Press the "Generate" button to begin generation of a new private/public key pair. Once generated, save the private key (via "Save Private Key") and copy the contents of the "Public key" box near the top of the window to your clipboard.

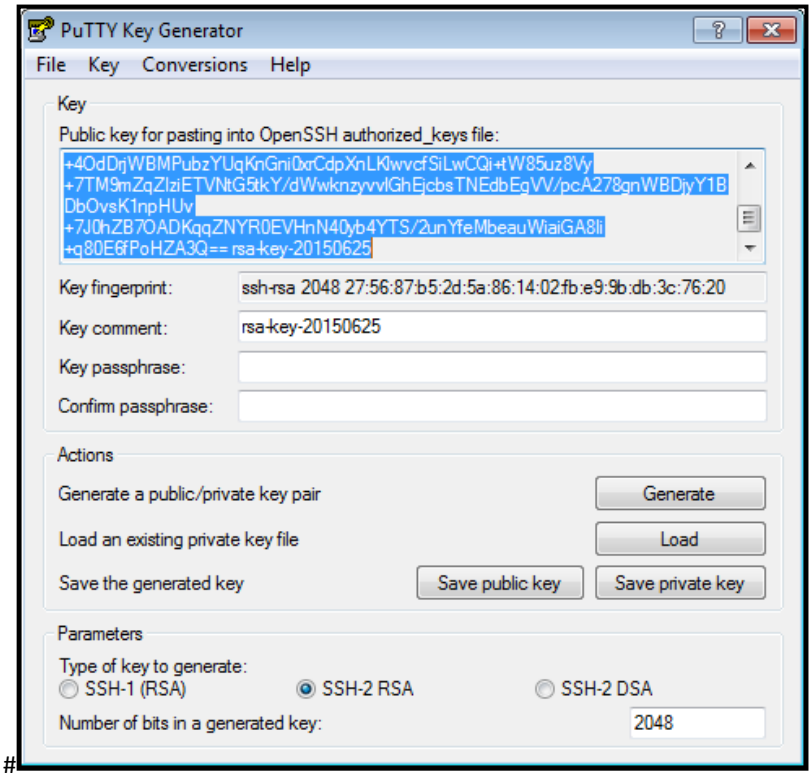


Figure 6 PuTTY Key Generation Example

Connect to the camera via a terminal and log in with an administrative account.

Run the “nano” command with the name of a non-existent file that we’ll use for installing the key. For full usage instructions on “nano”, see **Error! Reference source not found.**.

```
CIL50012345678:~$ nano key.pub
```

Figure 7 Nano Text Editor (Blank)

Paste the contents of the key by either right-clicking the black background of the window, or Ctrl+Right-Click and click “Paste” and save the file via Ctrl+O (exiting with Ctrl+X).

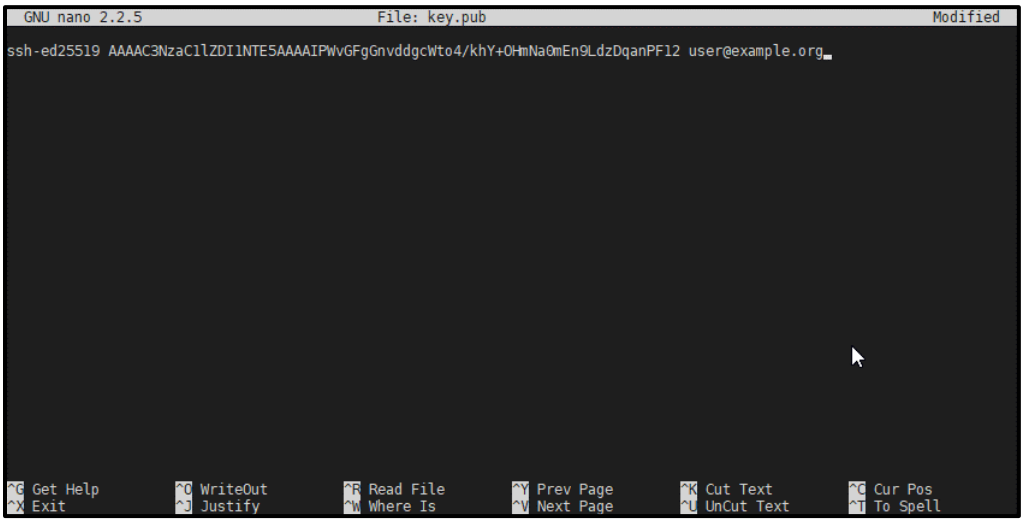


Figure 8 Nano Text Editor with SSH Key

Once exited, you’ll be returned to the shell. Run the “invoker addkey” command replacing “<user>” with the name of the user to install this key for, and <file> with the name of the file created with nano.

```
CIL50012345678:~$ invoker addkey <user> <file>
```

If using the commands outlined above, replace “<file>” with “key.pub”.

```
CIL50012345678:~$ invoker addkey <user> key.pub
```

Password Authentication

By default, password authentication is allowed for SSH. If key-based authentication is configured for all users, this may be disabled via Webmin.

Access the web interface as documented in the “Webmin Web Interface” section, expand the “Advanced” header in the left sidebar and click “SSH Server”. On the page that opens, click “Authentication”.

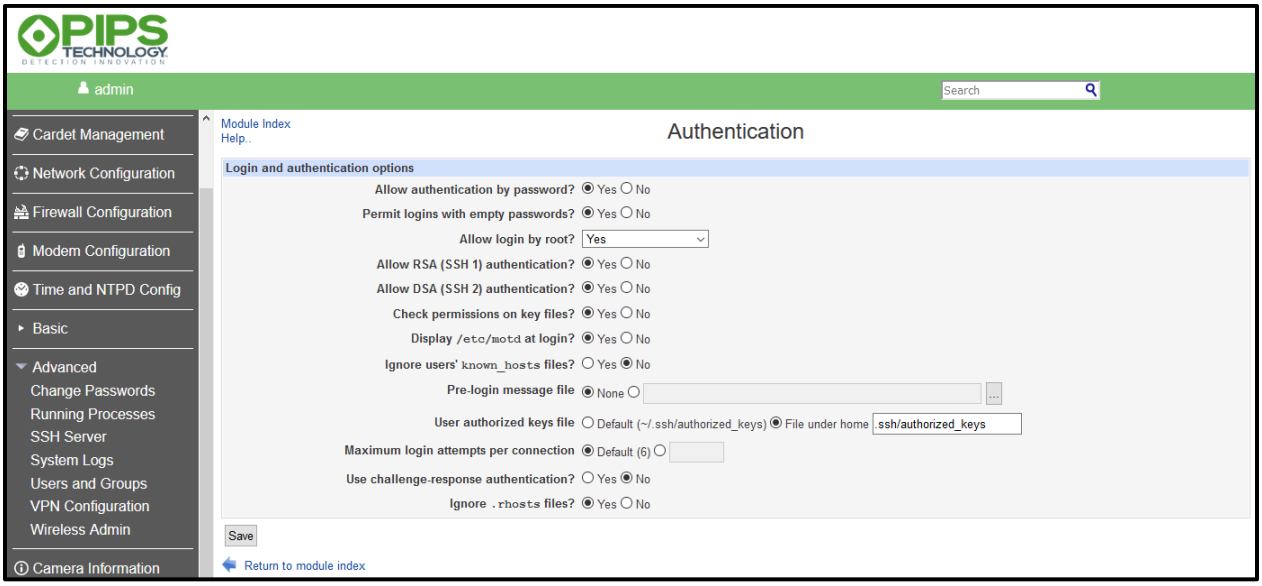


Figure 9 OpenSSH Authentication Configuration Page

Set the “Allow authentication by password?” field to “No” and click “Save” to persist the change, followed by clicking the “Apply Changes” button on the main OpenSSH server configuration page. This setting will apply to all user accounts.

Root Logins

Root logins are enabled by default for SSH; however, the stock configuration of the camera does not set a root user password, and no authorized SSH keys are installed, and therefore root access via SSH is by default not possible.

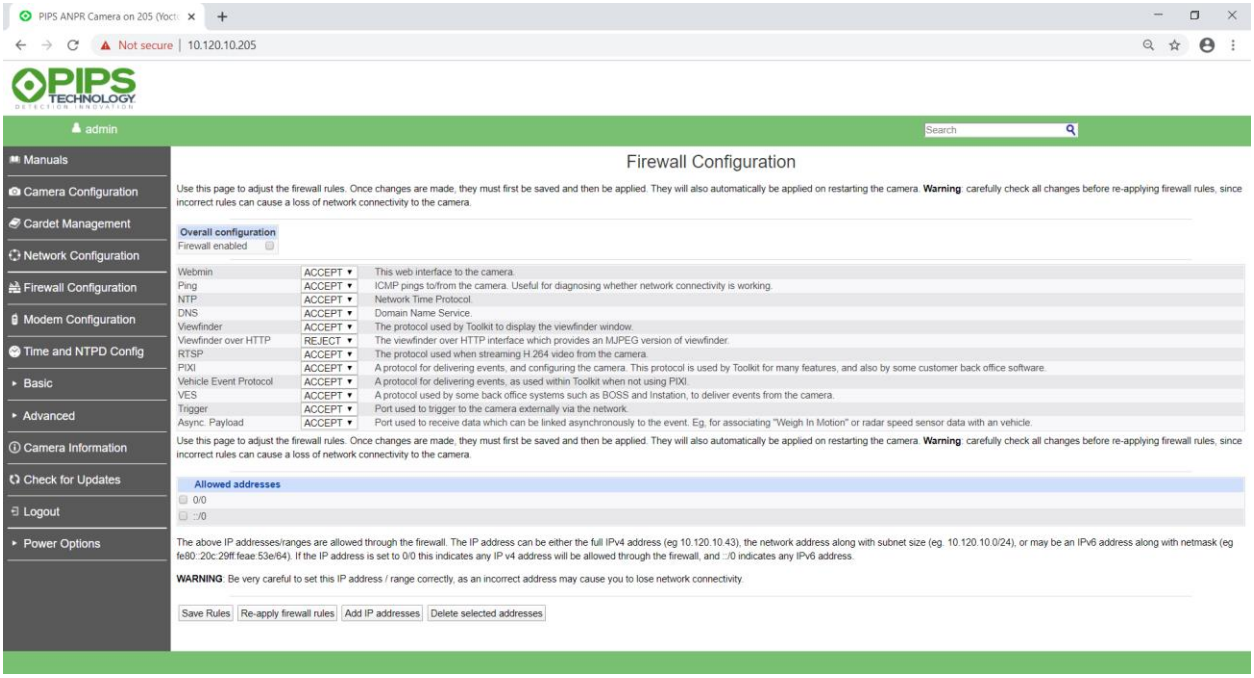
If a password or SSH key are added to the root user, it will become possible to access via SSH. If this is not desired, the steps described in the “SSH” section can be followed to configure the OpenSSH server.

Set the “Allow login by root?” option to “No” to disable root logins via SSH, or “Only with RSA auth” to require key-based authentication (not password-based) for root logins via SSH.

Firewall

The camera is configured to block everything except that which is explicitly allowed. If you wish to change the defaults, connect via Webmin and navigate to the Firewall page by clicking on “Firewall Configuration” on the left.

The following screen will be displayed:



The various protocols or services can be allowed/disallowed by selecting ACCEPT (to allow) or REJECT (to disallow) and then clicking on “Save Rules”, and then finally “Reapply firewall rules” once all changes are complete. Note also “Firewall enabled” should be ticked (as above).

Conversely – a quick way to get rid of all the rules is to untick “Firewall enabled” and click “Save Rules” and then “Re-apply firewall rules”. This should really only be used temporarily. In general, you should only enable that which is necessary. The default configuration is a good start.

How you choose to configure the Firewall also depends on the cameras situation on the internet. If the cameras are already on a private network (behind another Firewall) the configuration may not need to be as strict.

It is not recommended that a camera is ever situated on the open internet. If it is, every possible security precaution should be taken.

The “allowed addresses” section allows configuration of whitelisted IP addresses or address ranges. It is recommended that the camera is restricted to only be accessible from known IP addresses, however care must be taken when setting these addresses as the camera could be made unreachable over the network with incorrect settings.

To add an allowed address, click “Add IP addresses” and then enter an IP address or address range in terms of a network address. For example, add 123.123.123.0/24 to allow all addresses in the range 123.123.123.*, or 192.168.0.0/16 to allow all 192.168.* addresses.

To remove address ranges, select the checkboxes next to the address ranges, and then select the “delete addresses” button. If all addresses are removed, the default “any” addresses of 0/0 and ::/0 are automatically re-

added, however it is recommended that these “Any” addresses should be removed once specific whitelisted IP addresses have been added.

Regarding the protocols:

- Webmin should be set to ACCEPT unless you are happy to do some configuration via the command line.
- Ping is usefully set to ACCEPT in order to verify network connectivity with the camera.
- NTP – set this to ACCEPT if you want your camera to be able to act as an NTP Time server (server time to other cameras or back-office systems).
  NB: It does not need to be set to ACCEPT for the camera to synchronise it’s time off an external NTP server.
- DNS – in general this may be left as REJECT unless you wish the camera to act as a DNS server.
- Viewfinder – will need to be set to ACCEPT if you wish to use the Toolkit Viewfinder. You may choose to do this to configure the camera, and then set to REJECT once configured.
- Viewfinder over HTTP – set to ACCEPT if you wish to use the MJPEG stream over HTTP.
- RTSP – set this to ACCEPT if you want to use the H264 Video Stream.
- PIXI – set this to ACCEPT if you are using the PIXI protocol. This may be via Toolkit (for extra functionality) or a back-office system that implements the PIXI protocol to configure and retrieve events from the camera.
- Vehicle Event Protocol – set this to ACCEPT if you want to view plate read events and images from Toolkit. Note PIXI is another alternative to be able to view plate read events and images via Toolkit – and provides more features and flexibility than the Vehicle Event Protocol.
- VES – Enable this if you wish to use the VES Lite protocol. The VES Lite protocol is a subset of the VES protocol (which is deprecated). The VES Lite protocol provides sufficient functionality to work with BOSS servers.
- Trigger – the camera can be triggered via an incoming TCP connection (3820). Set this to ACCEPT to be able to do this. Otherwise leave it as REJECT as this port has no other function.
- Async. Payload – The camera can accept packets of asynchronous data via a TCP Connection (Port 3821). This data may be subsequently associated with plate read – typically based on time proximity, but other criteria may be used to associate. This feature may be used to associate Weigh In Motion (WIM) or Radar Speed gun data with license plate reads. If you wish to use this feature, select ACCEPT.

Physical Security

- Physical security is very important for the security of the camera. An unauthorised user can gain access to the camera via the serial port, it is strongly recommended to ensure that the cable which has the serial, ethernet and power going to the camera is terminated in a secured housing to prevent unauthorised tampering.

Command Line Tools

Most people will prefer to use Toolkit and/or Webmin rather than typing commands into a shell. However a quick introduction to the command line interface is provided in this section.

Conventions

We use several typographic conventions in this manual to describe things including interaction with a computer terminal.

Commands to be typed in are described as follows:

- **command**
  The name of the command.
- {required_argument}
  A required argument to the command is within curly brackets {}.
- [optional_arument]
  An optional argument to the command is within square brackets [].
- [*replace_me*]
  Text which should be replaced by you to indicate, for example, the file to be worked on is written in *italics*.

These can be combined, for example

ls [-l] [*directory*]
describes part of how to use the ls command in Linux.

Some text needs to be typed in exactly as given:
type this in exactly

If we provide a representative response from the system
```
it will print out like this, or at least something similar
```

SSH

Secure Shell (or SSH) Secure Shell or SSH is a secure networking protocol which can be used for many things, but here we will use it to provide a shell on the camera. It is running on the standard port, 22.

Some operating systems (e.g. Linux) have an ssh client built in which can be invoked by typing ssh from the command line. Briefly:

ssh [*user@*] {*hostname*}

Windows does not have an SSH client, so for Windows we recommend PuTTY although any ssh client capable of SSH2 should work.

The Toolkit installation includes PuTTY and it is possible to launch PuTTY from Toolkit and this is what will be described here.

Assuming you have a saved camera (see the Quick Start section or the Toolkit Manual regarding how to create a “Saved Camera”), select the camera, right click and select

Once you have logged in you have the network working correctly and you can configure and use the camera.

You are logged into a Linux shell, and can use many normal Linux commands to navigate. A brief set of useful commands and arguments are given here.

- **ls** [-l] [*directory*]
  get a directory listing, similar to dir under DOS
- **pwd** display the current working directory
- **cd** {*directory*} change directory to given directory. Use .. to go up one directory
- **nano** {*filename*} edit a file using the Nano text editor. See Appendix G, Nano - text editor [152] for more details.
- **cat** {*filename*} quickly show a file.
- **less** {*filename*} display a file, so you can scroll up and down.

This is only a very brief list. Further information is available on the web.

Note: Linux Manual pages are not installed on the camera.

Serial Terminal

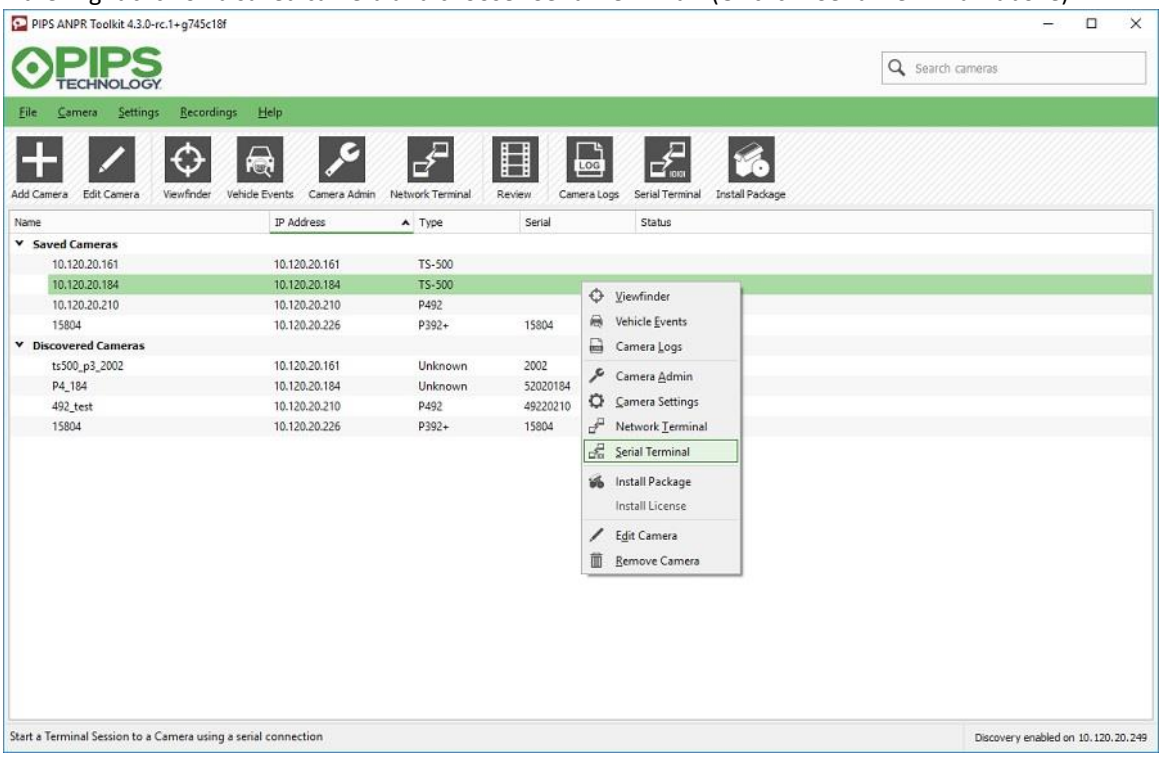
It is possible to communicate with the camera via a serial cable and login via a serial terminal. This is not normally necessary, but may be so when:

1. If you cannot connect via the network for some reason for example when configuring the network for the first time (although there are other ways to do this, see: Network Connection to the Camera.)
2. To debug or resolve problems where the camera is not booting, or not booting fully.
3. To install a new operating system

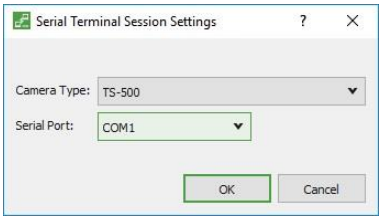
The serial connection to the camera is RS232. Many modern PCs and laptops no longer have RS232 serial connections and therefor a serial to USB adapter will be needed.

On windows serial interfaces are identified via a “com port” number, e.g. com1, com2, com3 etc.

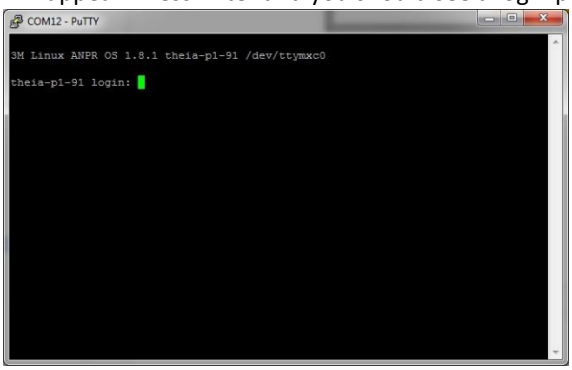
A serial terminal will also be necessary. The recommended option is PuTTY and this may be launched from Toolkit. Either right click on a saved camera and choose “Serial Terminal” (Or click “Serial Terminal” above).



The following will be displayed:



Ensure that the P500 camera is selected and the correct Serial Port and then click OK. A blank PuTTY serial terminal will appear. Press Enter and you should see a login prompt.



Logging in will bring you to the bash shell where you will be able to perform configuration tasks such as network configuration. You will also be able to access the platereader shell (pshell) as described here: The pshell.

The PuTTY serial terminal does not have to be launched from Toolkit and it is also not the only Serial Terminal available. One advantage of launching it from Toolkit is that provided you select the correct camera type it will correctly configure the PuTTY terminal for you.

If you launch PuTTY standalone (or use other terminal software), you will need to know the serial terminal settings which are as follows:

- Speed (baud): 115200 bits per second
- Data bits: 8
- Stop bits: 1
- Parity: None
- Flow Control: None

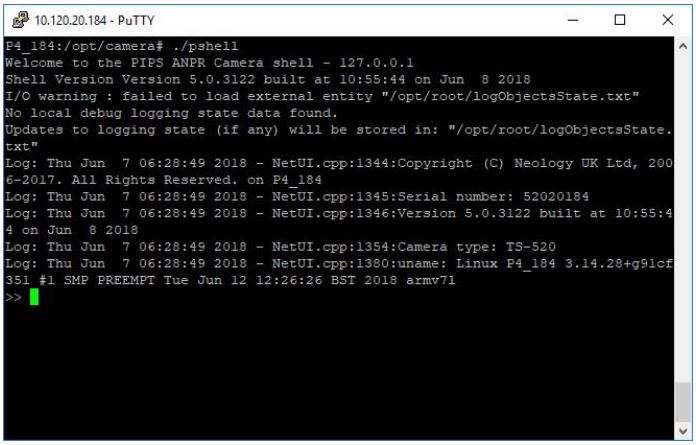
The pshell

The camera has its own shell for interacting with the ALPR camera application.

This is the Platereader Shell (or pshell).

The shell is an alternative way to access and control the camera's parameters. If you have an admin password you can start it whilst at the Linux bash prompt (either via SSH or on the console serial port) by typing:

```
/opt/camera/pshell
```



You can ignore the “I/O warning : failed to load external entity "/opt/root/logObjectsState.txt"

No local debug logging state data found.” The file mentioned is where any enabled logging settings are stored. If no logging has been previously enabled, this file will not exist.

The double chevrons >> are the prompt where you may type commands.

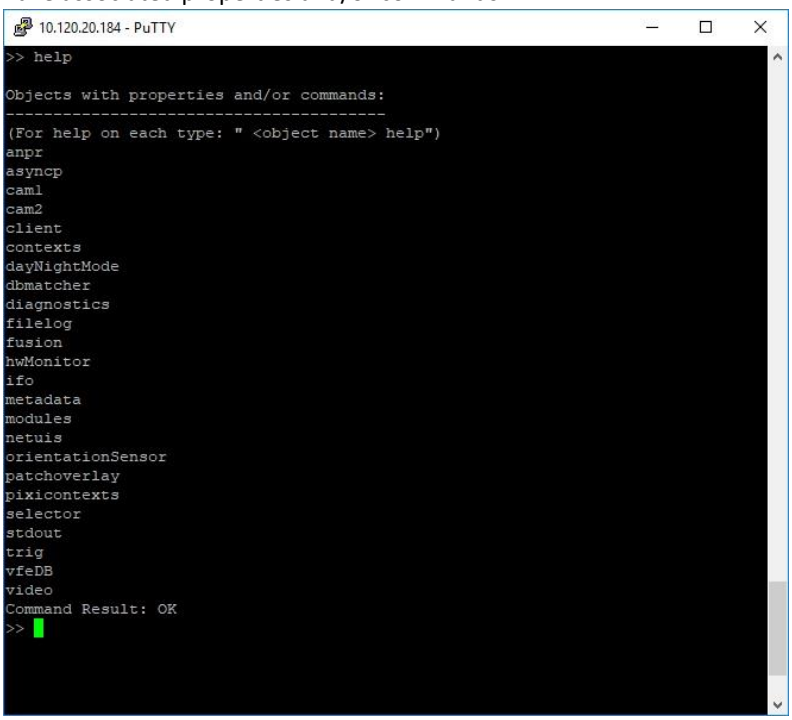
The model of the pshell commands is one of objects, where each object may have properties (that can be set or queried) and/or commands that may be executed for that object.

Objects can be nested, and the sub-object's name is separated by a space from the parent.

help

You can see a list of objects by typing help with no arguments, and see properties and commands of each object by giving the object name as an argument.

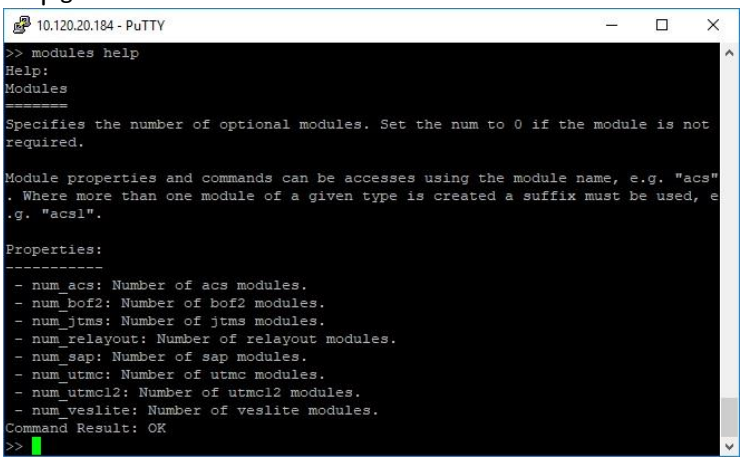
The image below shows the result of typing help with no parameter. Note the list of objects, each of which will have associated properties and/or commands.



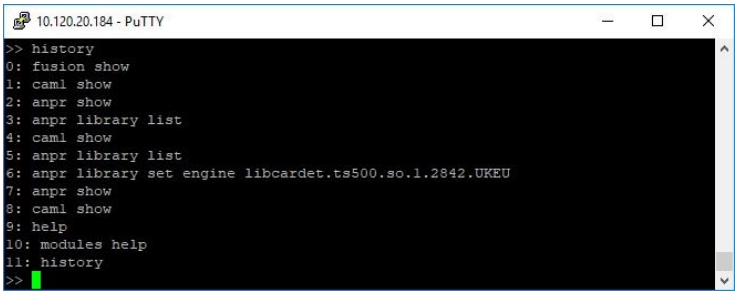
To get help on a specific object/subobject:

{*object name*} [*subobject name*] **help**

The image below shows the more detailed help on one of the objects – specifically "modules". Typing modules help gives:



History



Display a numbered list of old commands you have typed in. To execute a command from the history type: !{*number*}

It is also possible to use the up and down arrow keys to scroll through the history, press Enter to re-execute the currently displayed command.

quit

Leave the shell.

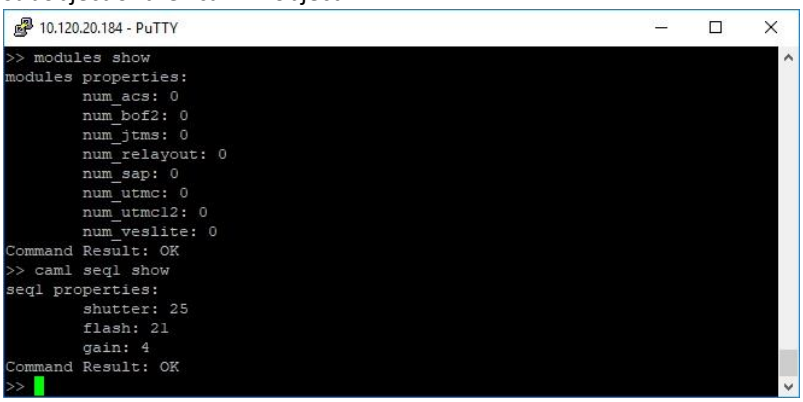
Object Properties

As previously stated the objects in the system may have associated properties.

To display all the properties and current values for an object:

{*object name*} [*subobject name*] **show**

The image below shows the result of two show commands, the first show modules to show the values of the "modules" object properties. The second, cam1 seq1 show shows the value of the properties of the "seq1" subobject of the "cam1" object.



To get the individual value of a property:

{*object name*} [*subobject name*] **get** {*property name*}

For example, to check whether ACS is enabled, we get the "enabled" property as in the image below. (Reminder: To get help regarding supported properties and commands of an object it is {*object name*} [*subobject name*] **help**

so for ACS it is: acs help.)

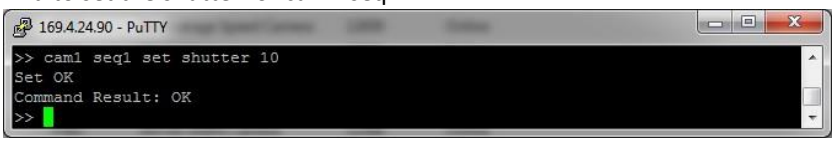
Or the specific property of a subobject – in this case "cam1" is the object, "seq1" is the subobject and "shutter" is the property:

To set a property:

{*object name*} [*subobject name*] **set** {*property name*} {value}

For example, to enable ACS:

And to set the shutter for cam1 seq1:

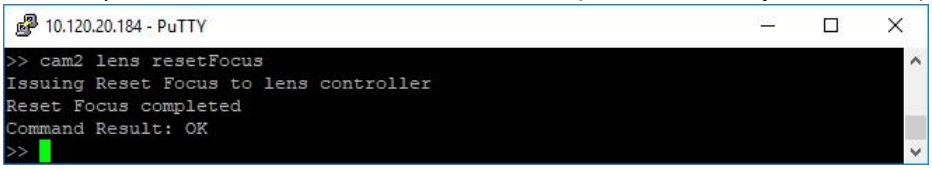


Object Commands

Some objects also have commands that can be executed. The general form for executing a command is:

{*object name*} [*subobject name*] {*command*} [*command args*]

For example, to reset the focus of the "cam2" "lens" ("lens" is a subobject of "cam2"):



Network Configuration

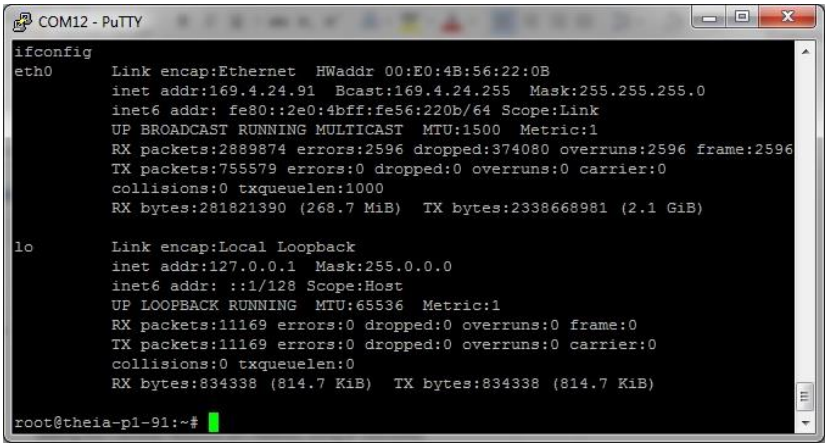
It is possible to perform basic ethernet network configuration using the IP Discovery feature in Toolkit. This is described here: Setting the Cameras Network (IP) Address using IP Discovery.

If for some reason you cannot use IP discovery to perform initial network configuration, it is possible to do it without network access, via a serial terminal.

Basic Network Configuration via Terminal

This is possible using either a serial terminal or network terminal. A possible scenario is initial configuration where your PC is unable to connect to the camera via the network in which case a serial terminal may be used.

To view the current network interfaces and associated IP addresses, type **ifconfig**.



The interface of interest is the Ethernet interface “eth0”. (The “lo” interface is the loopback interface and unlikely to require any configuration).

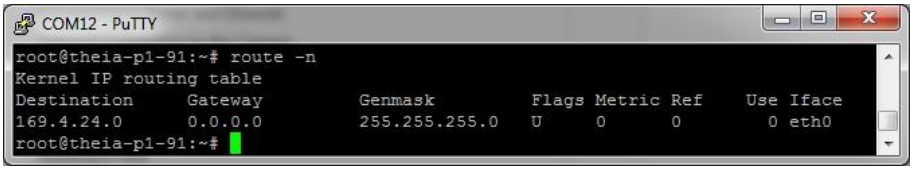
To set the IP4 address and netmask:

ifconfig eth0 {*ip4 address*} netmask {*netmask*}

The example below shows the command to set the address to 168.4.24.91, netmask 255.255.255.0.

Note the shell prints no message if the command succeeds.

Another setting that may be required is setting the default gateway. To display the current routing table, type **route -n**. (Note the –n option is to disable reverse DNS lookups as we don’t assume DNS is properly configured at this time.).



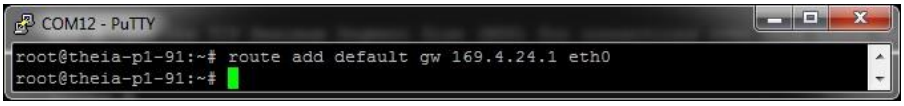
Currently the only entry in the routing table is for the local 169.4.24.0. A gateway is not needed for IP addresses in this range.

Without a gateway, the camera will not be able to communicate with IP addresses outside of the 169.4.24.0 address range. Adding a default gateway will cause traffic to any IP address outside of this range to be routed to the gateway for forwarding.

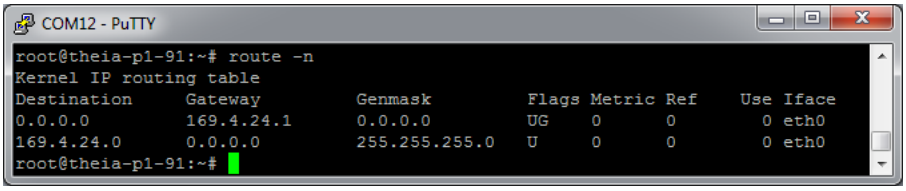
To add a default gateway to the routing table for eth0, the form of the command is:

route add default gw {*gateway IP4 address*} eth0

In the example below the default gateway IP address is 169.4.24.1 is added:



And to confirm it has been added:



At this time the network should be sufficiently configured such that the camera is reachable over the network and the serial terminal is no longer required. While it is possible to continue configuring the network via the command line, it is recommended that further networking or Linux system configuration tasks be performed using:

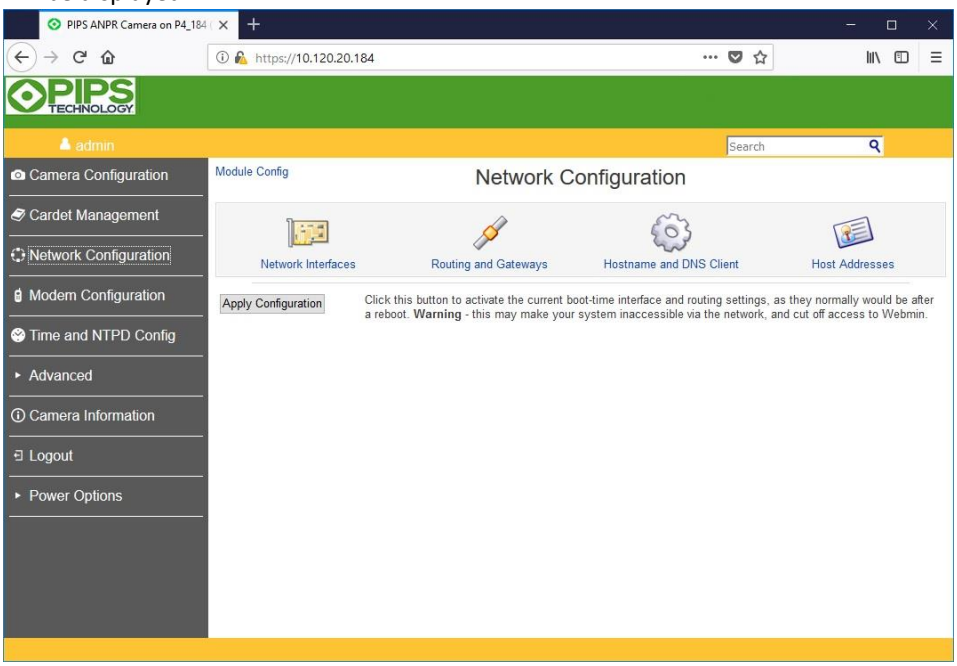
- A web browser to connect to the camera's webmin server
- A Network ssh Terminal (e.g. PuTTY).

Beware however, changing certain settings such as the IP address, netmask or default gateway may cause an existing network connection to be terminated.

Network Configuration with Webmin

Once the camera IP address has been set, you will be able to use Webmin to view and modify network settings. Open Webmin (as described in Webmin Web Interface) and click on "Network Configuration". The following screen

will be displayed:

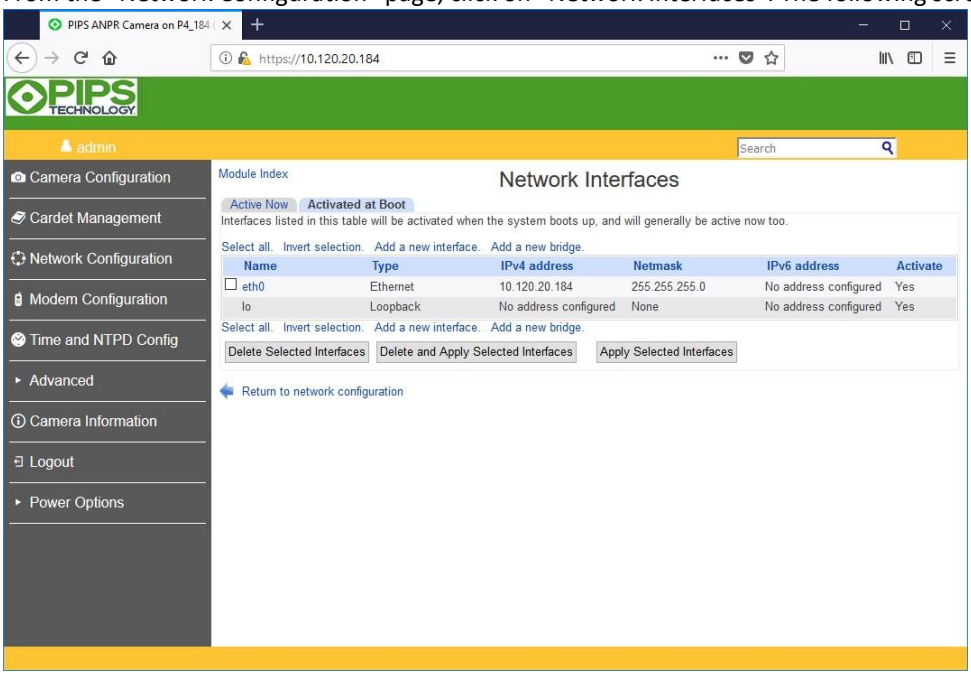


At the time of writing the Network Configuration is documented here: http://doxfer.webmin.com/Webmin/Network_Configuration.

However, we will briefly address the most likely configuration options.

Network Interfaces

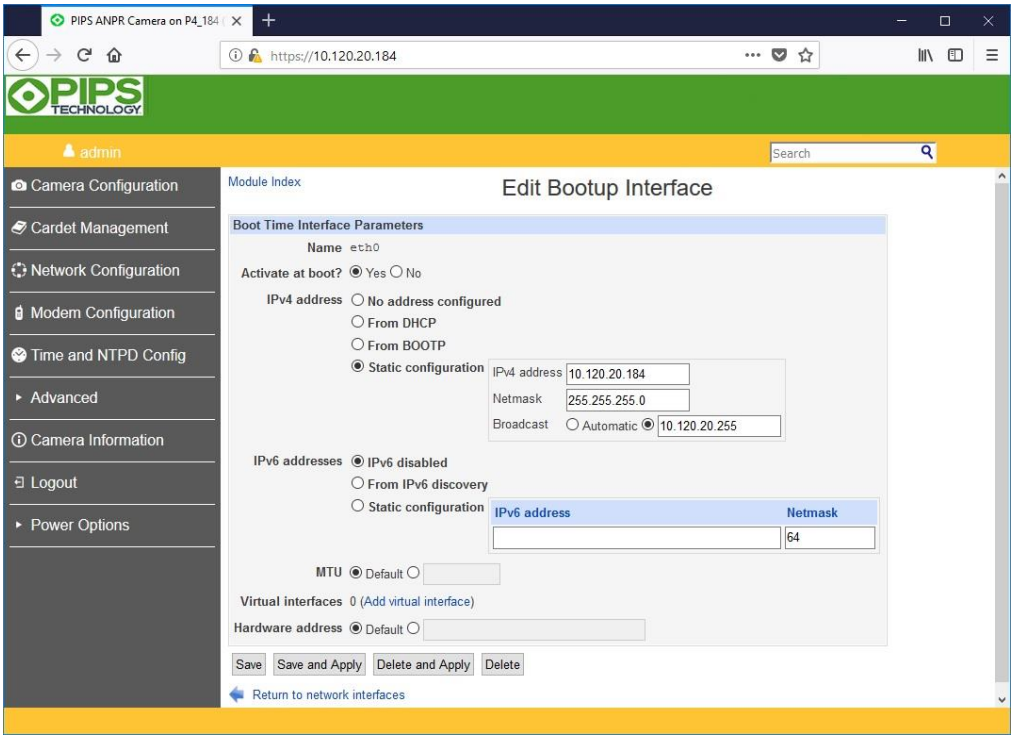
From the "Network Configuration" page, click on "Network Interfaces". The following screen will be displayed:



Normally you would not want to add or delete interfaces. You would also normally only want to modify the interfaces listed on the "Activated at Boot" tab.

To actually view the settings of an interface, click on the interface name.

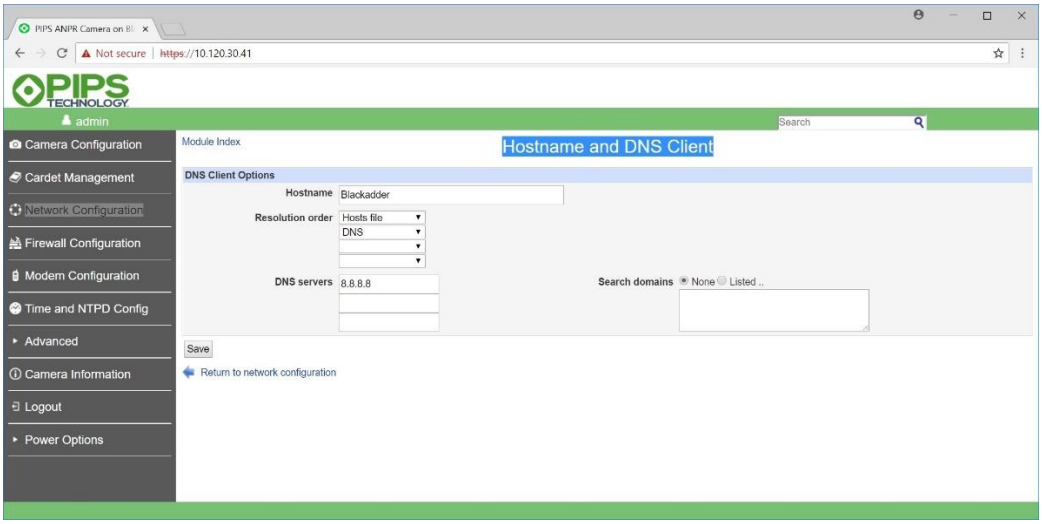
In this case the only selectable interface is the Ethernet interface, “eth0” and clicking on the “eth0” link displays the following:



The only settings you are likely to need to change is the “IPv4 address” “Static Configuration”.

Hostname and DNS Client

To configure the Hostname and/or DNS, click on “Network Configuration” and then on “Hostname and DNS Client”. The following screen will be displayed:



Type in a hostname. If you wish for the camera to use DNS you can also type in the IP address of a DNS server (in this case 8.8.8.8).

Click “Save”.

Wireless Network Configuration

Initial configuration of wi-fi will require that the user first set up networked access to the camera via either ethernet or modem, as documented in their relevant sections.

Wireless Networks

Open Webmin (as described in Webmin Web Interface) and click on “Advanced” and then “Wireless Admin”. Ensure the “Known Networks” tab is selected, and the following screen will be displayed:

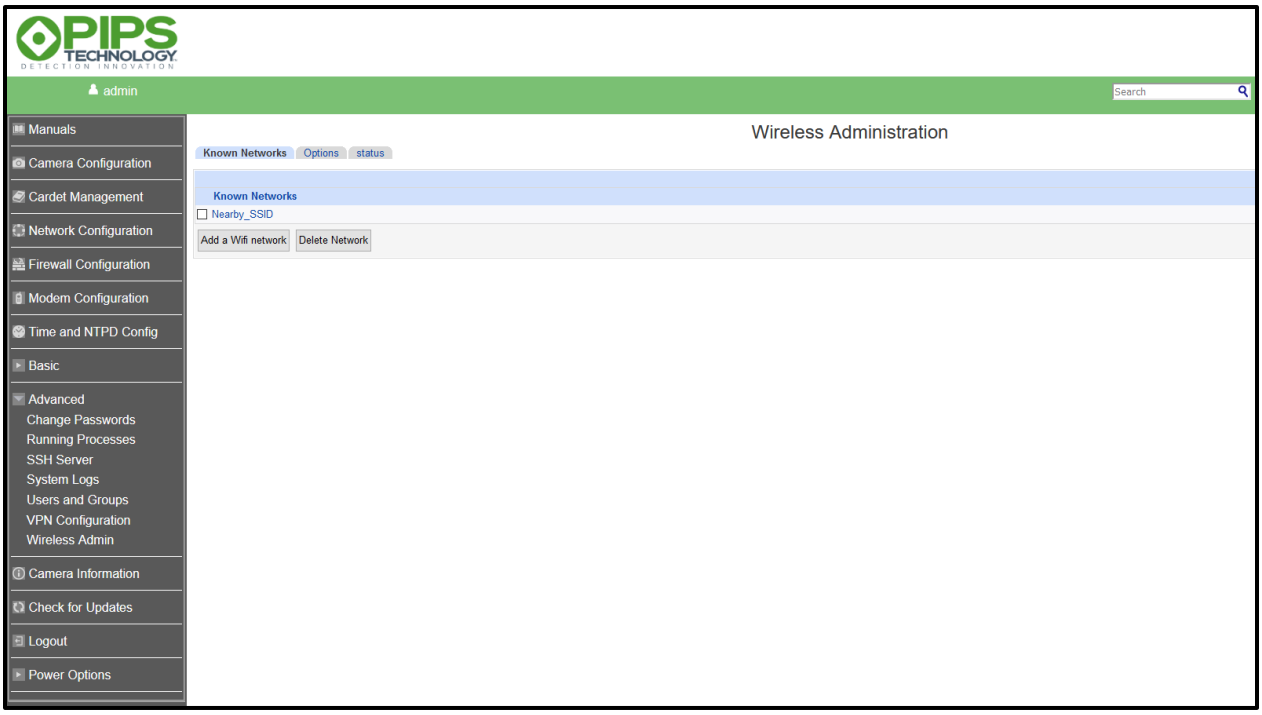


Figure 10 Wireless Configuration - Known Networks Page

This page lists the configured networks on the camera. Each configured network provides a link which, by clicking on its name, will allow you to edit the parameters for that network.

Ticking the box next to a network and clicking the “Delete Network” button will delete all selected networks.

Adding or Editing a Network

Navigate to the “Wireless Admin” page and select the “Known Networks” tab.

To add a network, click the “Add a Wifi network” button. If you wish to edit an existing network, click its name from the provided list.

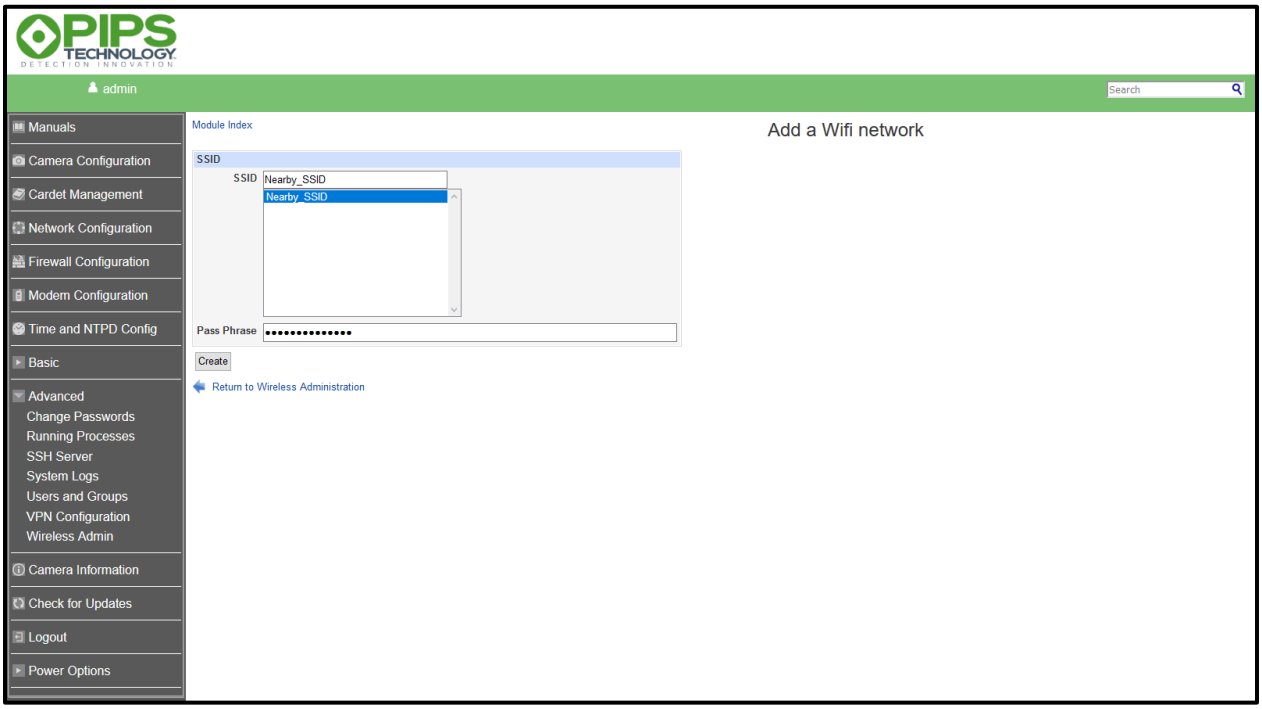


Figure 11 Wireless Configuration - Add Wi-fi Network Page

The displayed page has the following fields, which must both be supplied to configure an SSID.

Field	Description
SSID	The name of the wireless network to connect to. The name may be provided by selecting from the list of discovered networks, or typing in a name manually to the text field.
Pass Phrase	The password for the wireless network. The camera does not support connecting to open (password-less) networks.

Table 1 Wireless Configuration - SSID Configuration Fields

Once configured, click “Create” or “Save” and you will be returned to the Known Networks page.

Wireless Options

The “Options” tab on the “Wireless Admin” page will display the following screen:

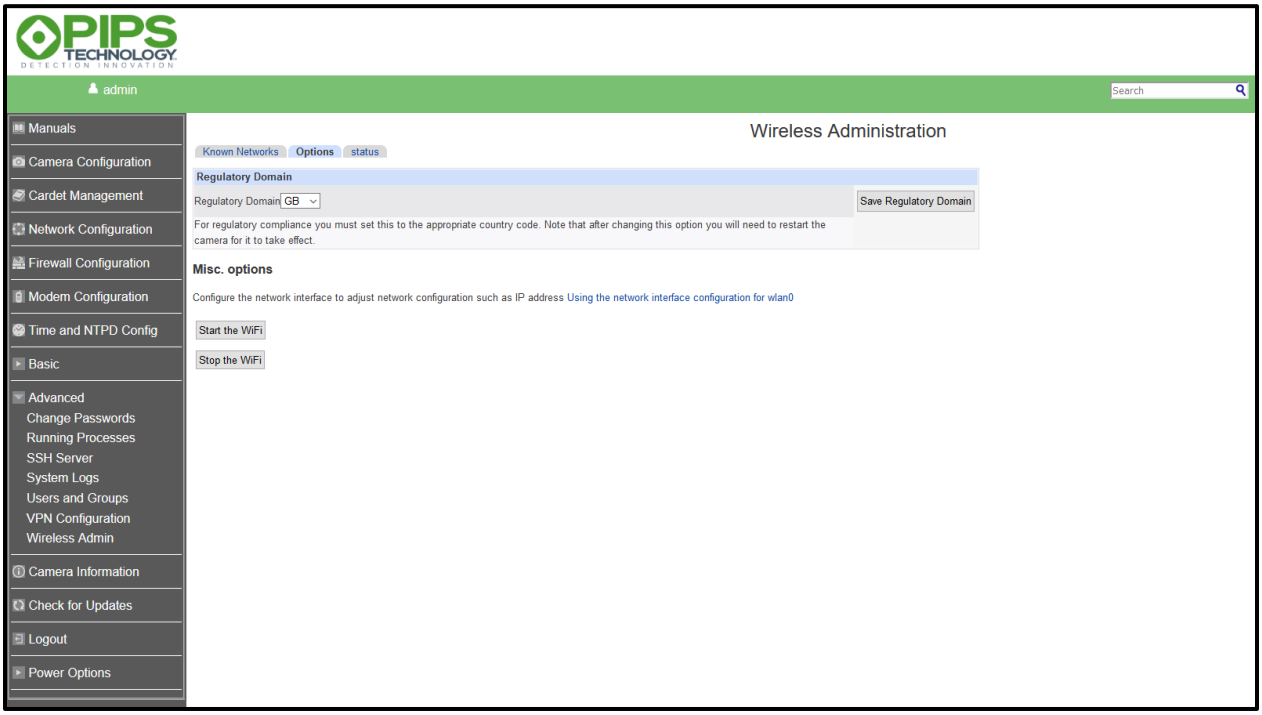


Figure 12 Wireless Configuration – Options Page

This page provides a way to configure the regulatory domain for the wireless connection, which must be set to the appropriate country code that the camera is being used in. Additionally, tools are provided for starting/stopping the wireless network.

Regulatory Domain

The regulatory domain must be set to an appropriate country code for which the camera is operating in to ensure regulatory compliance.

Select an appropriate country code from the “Regulatory Domain” dropdown and click the “Save Regulatory Domain” button. Note that after changing this setting, you must restart the camera to apply the changes.

IP Address and Routing Configuration

The IP addressing mechanism (static IP, DHCP, and routing preferences) uses the same page as described in the Network Interfaces section of the document, for which the page will list a “wlan0” network representing the interface used by wireless connections. A link to this page is provided under the “Misc. Options” header.

Starting and Stopping the Wireless Network

Navigate to the “Wireless Admin” page and click the “Options” tab. The buttons at the bottom of the page (“Start the Wifi” and “Stop the Wifi”) may be used to start and stop wireless network connectivity, respectively.

Wireless Status

The “Status” tab on the “Wireless Admin” page will display the following screen:

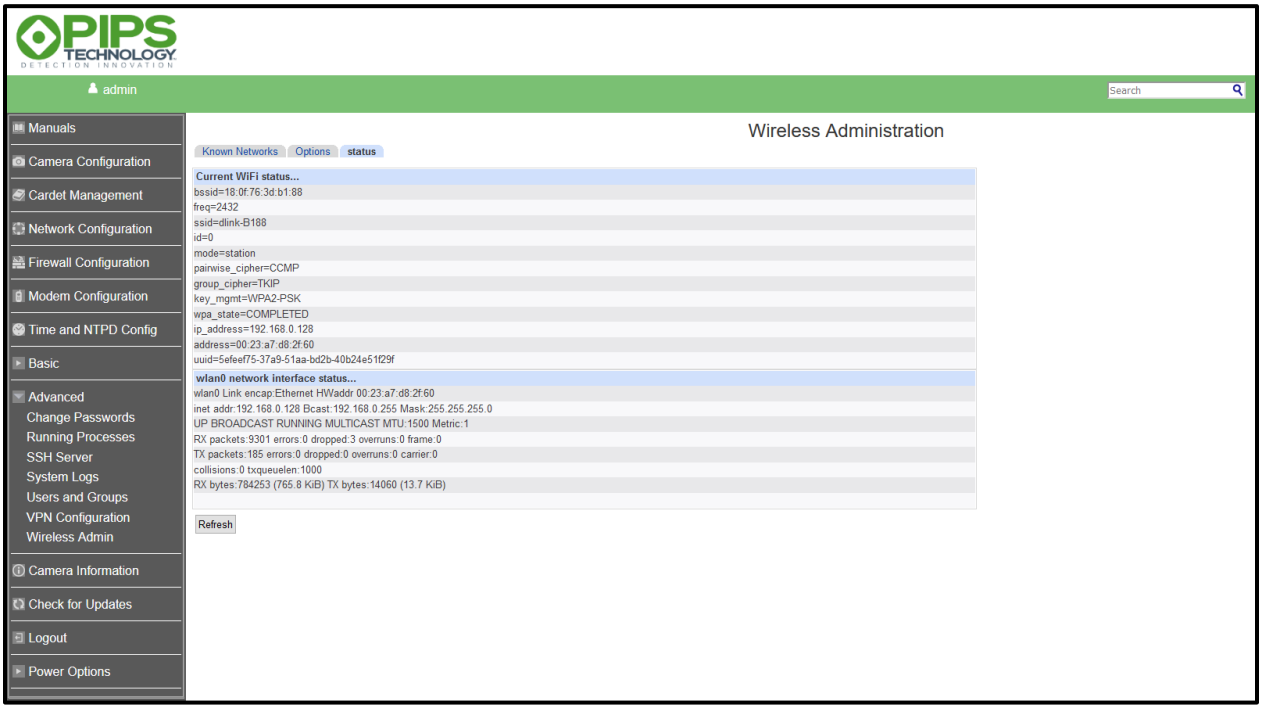


Figure 13 Wireless Configuration - Status Page

This page can be used to diagnose the wireless connection and assist in determining if it has been configured correctly and is able to connect to a remote access point.

Particularly useful fields are outlined below:

Field	Description
SSID	The SSID of the network that is used by the current connection.
WPA State	The state of the WPA authentication process. This will be “COMPLETED” if a connection has been successfully established, and authentication was successful.
IP Address	The local IP address of the wireless interface on the camera.
UP	The keyword UP will be in the output of the wlan0 network interface status, as shown on the 3rd line in the screenshot if the network interface is currently deemed up. This will be omitted if the interface is currently down.
TX / RX packets	The number of packets sent / received, and the number of errors / dropped packets can be useful in confirming network connectivity is good.

Table 2 Wireless Configuration - Status Fields

Modem Configuration

Initial configuration of the modem will require that the user first set up networked access to the camera via either ethernet or wireless, as documented in their relevant sections.

Open Webmin (as described in Webmin Web Interface) and click on “Modem Configuration”. The following screen will be displayed:

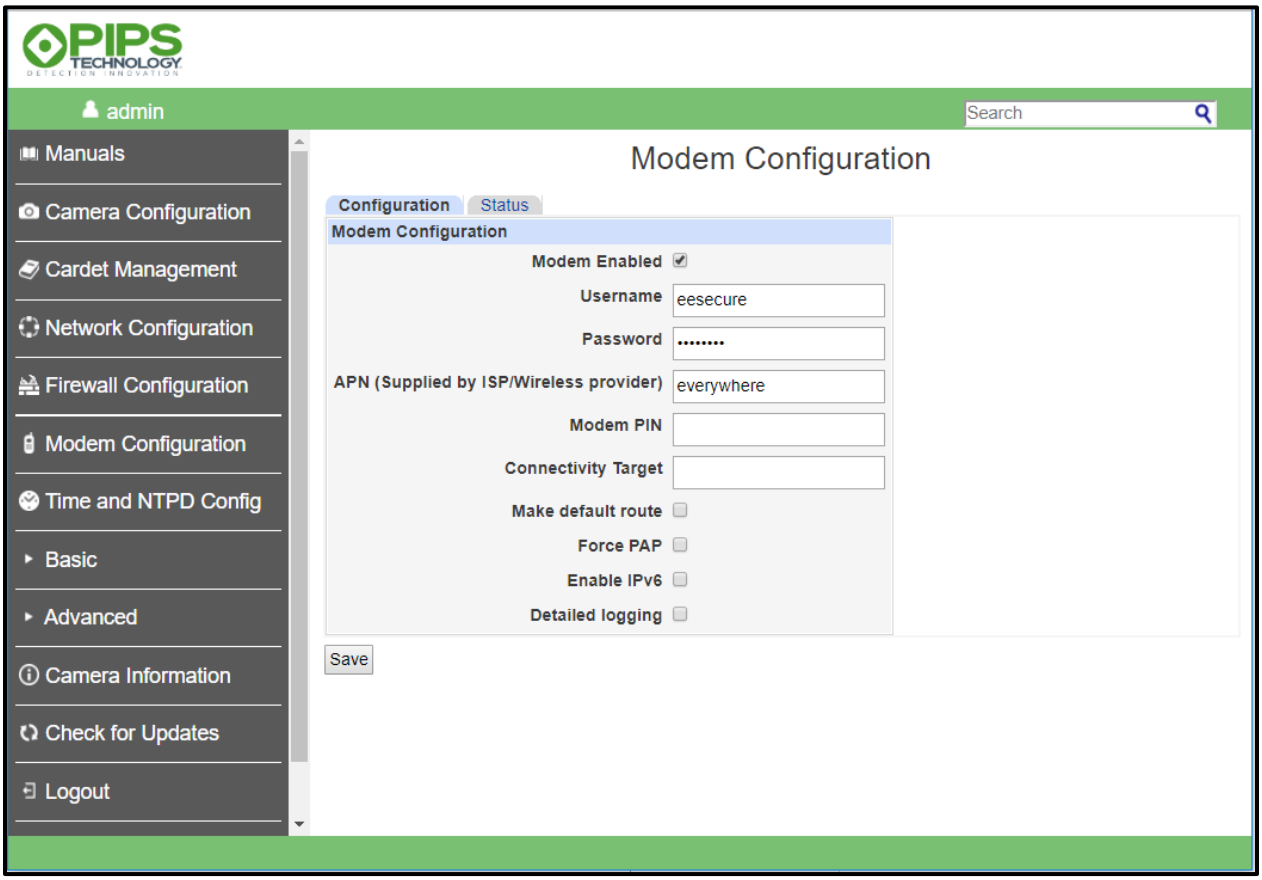


Figure 14 Modem Configuration Page

A description of each of the fields can be found below.

Field	Description
Modem Enabled	If checked, enables the modem.
Username	The username to use when connecting to the wireless provider.
Password	The password to use when connecting to the wireless provider.
APN	The access point name provided by the wireless provider.
Modem PIN	Some SIMs are supplied with a PIN which must be entered to unlock the SIM. If your SIM does not require a PIN, leave this blank.
Connectivity Target	An optional IP address to ping upon establishing the modem connection. If the target cannot be reached, the camera will assume that the modem connection is non-functional.
Make Default Route	If checked, the network established by the modem upon a successful connection will become the default route for all traffic on the camera. If the user is intending upon using the modem as the primary network access method for the camera, checking this box is recommended.

Force PAP	Forces the use of PAP for authentication on the network, instead of CHAP. This option is not recommended.
Enable IPv6	Allows the camera to attempt to obtain an IPv6 IP address in addition to the IPv4 address normally used.
Detailed Logging	If checked, more verbose logging messages will be stored on the camera in the file /var/log/modem-monitor.log. This can be used to diagnose issues.

Table 3 Modem Configuration Fields

Initial configuration of the modem should check the "Modem Enabled" box and enter any required username, password, and APN values. It is not recommended to check "Make Default Route" until the user has verified the modem can initially connect, as changes to the default route may impact the accessibility of the camera via other network methods.

The "Status" tab at the top of the page can be clicked to display information on the current state of the modem as a table of fields presenting all known information about the state of the modem and the connection, if one has been established. Some example fields are documented below.

Field	Description
Status	The status of the modem. This will be "disabled" if the modem has not been explicitly enabled on the configuration page, otherwise it will indicate the state of the connection. A successful and working connection will display "up" in this field.
Sim Card ID	The ID of the SIM card. If this displays an erroneous value, it may indicate that no SIM card is present in the camera.
Number	The mobile number associated with the SIM.
Access Band Technology	This reports the technology being used to connect to the network – and can be used to distinguish between 3G / 4G connections.
Signal Strength Status	The signal strength of the connection to the wireless provider. A poor signal strength may lead to connectivity issues. Note that this is only updated when the modem connects onto the network.
Remote IP	The remote IP address of the network that the camera has connected to.
Local IP	The local IP address of the network interface established on the camera.

Table 4 Modem Status Fields

VPN Configuration

The camera supports both Point-to-Point Tunnelling Protocol (PPTP) and Internet Protocol Security (IPsec) VPN connections. Instructions for configuring these can be found in the following sections.

PPTP Configuration

Configuration of the PPTP VPN will require that the user first set up networked access to the camera.

Open Webmin (as described in Webmin Web Interface) and click on “Advanced”, and then “VPN Configuration”. The following screen will be displayed:

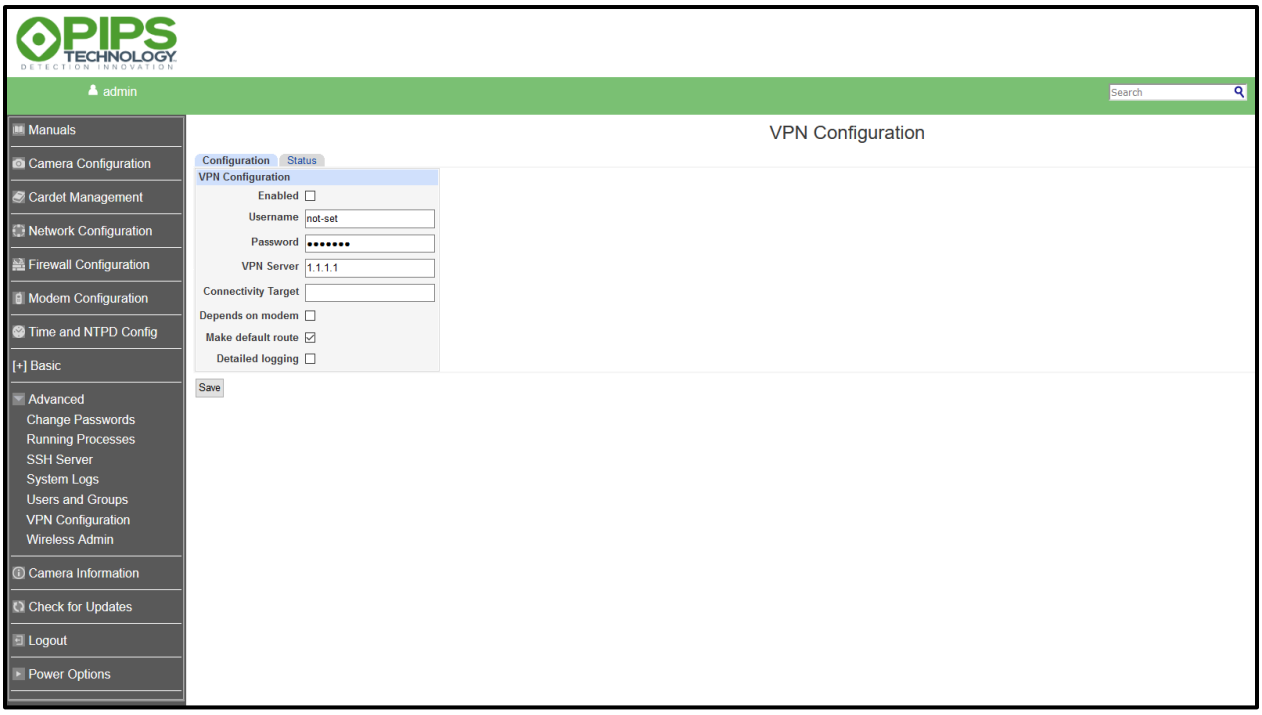


Figure 15 VPN Configuration Page

A description of each of the fields can be found below.

Field	Description
Enabled	If checked, enable the use of the PPTP VPN.
Username	The username to use when authenticating with the VPN server.
Password	The password to use when authentication with the VPN server.
VPN Server	The IP address of the remote server to connect to.
Connectivity Target	An optional IP address to ping when the VPN connection is established. If the target cannot be reached, the camera will assume that the VPN connection is non-functional.
Depends on Modem	If checked, the camera will first configure the modem prior to establishing a VPN connection. This should be checked if, for example, the modem is intended to be the primary network access method on the camera.
Make Default Route	If checked, the connection established by the VPN will be marked as the default route for all traffic to/from the camera.
Detailed Logging	If checked, more verbose logging messages will be stored on the camera in the file /var/log/vpn-monitor.log. This can be used to assist in diagnosing issues.

Table 5 VPN Configuration Fields

Initial configuration of the PPTP VPN should check the “Enabled” box and enter valid values for the “Username”, “Password”, and “VPN Server” fields. It is not recommended to enable the “Make Default Route” option on initial configuration, as changes to the default route may impact the accessibility of the camera via other network methods.

Clicking the “Status” tab will display the following screen:

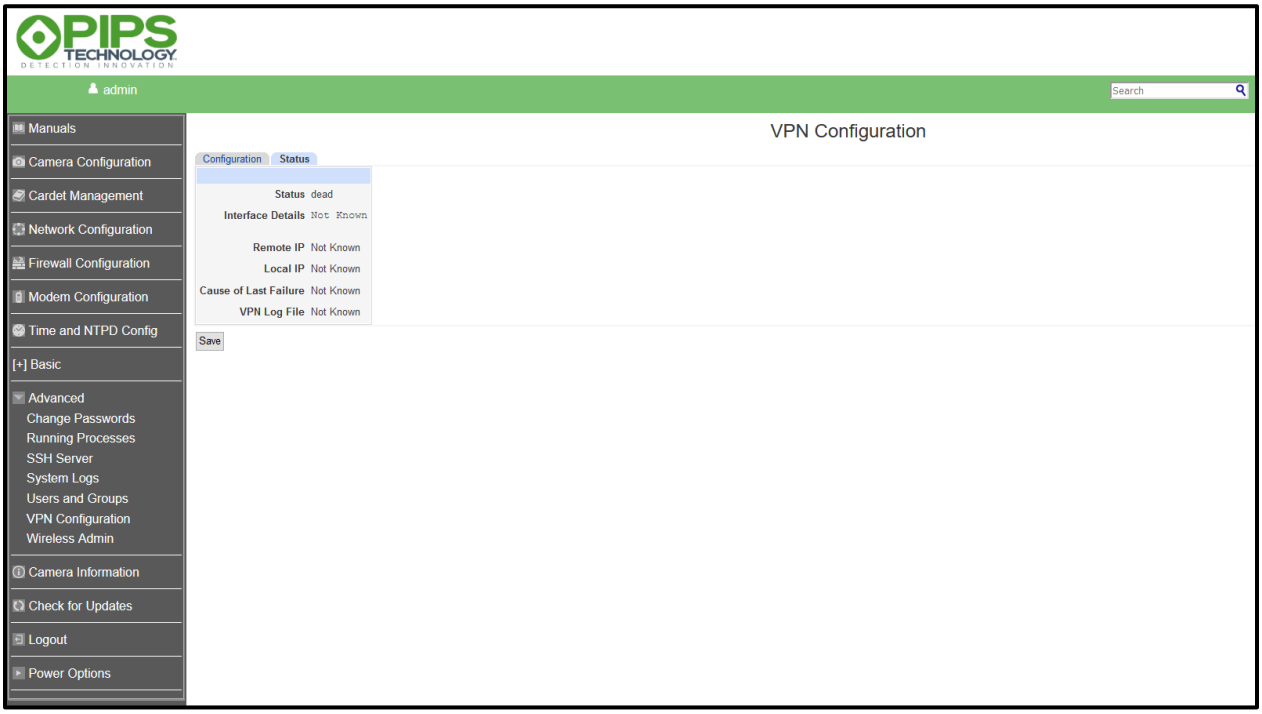


Figure 16 VPN Status Page

This page displays information on the current state of the PPTP VPN as a table of fields presenting all known information about the state of the connection, if one has been established. The fields shown are documented below.

Field	Description
Status	The status of the VPN connection. This will be “dead” if the VPN is disabled, or not able to connect, or “up” if the connection has been established.
Interface Details	Details of the local network interface used on the camera to represent the VPN connection.
Remote IP	The remote IP of the VPN server.
Local IP	The local IP of the VPN network interface on the camera.
Cause of Last Failure	An error message indicating the reason why the VPN connection may not have successfully established.

Table 6 VPN Status Fields

IPsec Configuration

The camera implements IPsec support. Configuring IPsec is not yet possible through the web interface present on the camera, and due to the complexity of the settings involved it is strongly recommended that users wishing to enable this feature should contact the Neology UK technical support team.

Delivery Modules

There are several mechanisms on the camera for the network delivery of license plate read metadata and images. Some of these are legacy. Most of these mechanisms can be used concurrently with the others. In some cases, multiple instances of one mechanism may also be used.

ACS

ACS stands for Access Control System. This is a legacy name and it is by no means restricted to “Access Control”. It is a general-purpose delivery mechanism.

The key distinguishing feature of ACS is that it is a **file** transfer mechanism. Specifically, it delivers image and data files to the back-office system.

The back-office system needs to be running appropriate software in order to accept this file delivery. If your back-office system is running Windows, Filezilla Server is a good choice. There are other possibilities including, of course, on Linux.

ACS can deliver via:

- FTP
- SFTP
- SCP
- File (write to local filesystem)

It is a simple network delivery of image and text **files**.

Typically, for each license plate read event, it will deliver:

- one text file containing selected metadata, and
- 2 or 3 image files, specifically the plate-patch image, the colour image and the IR image.
- Other images (such as context images) are also available.

ACS is very flexible as regards the file paths/names and the content/format of the text (metadata) file.

It is designed for production use, and is recommended as a simple way to get started. This simplicity does not mean it is unsuitable for large scale deployments.

You can run multiple instances of ACS. These instances can run alongside other delivery mechanisms, such as PIXI.

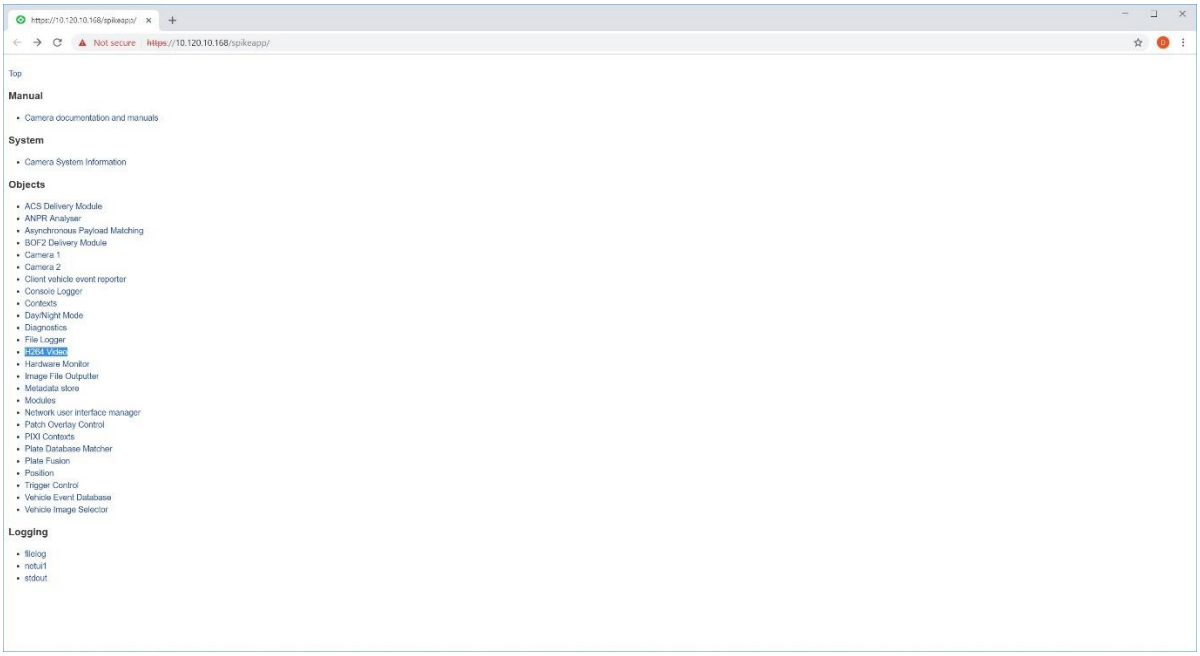
H264 Video

The camera can provide an H264 compressed video stream. The size of the video is limited to 1920x1080 and it is a cropped version of the full image captured. If cropped video is not suitable, consider using the MJPEG stream which can be encoded at the full image dimensions.

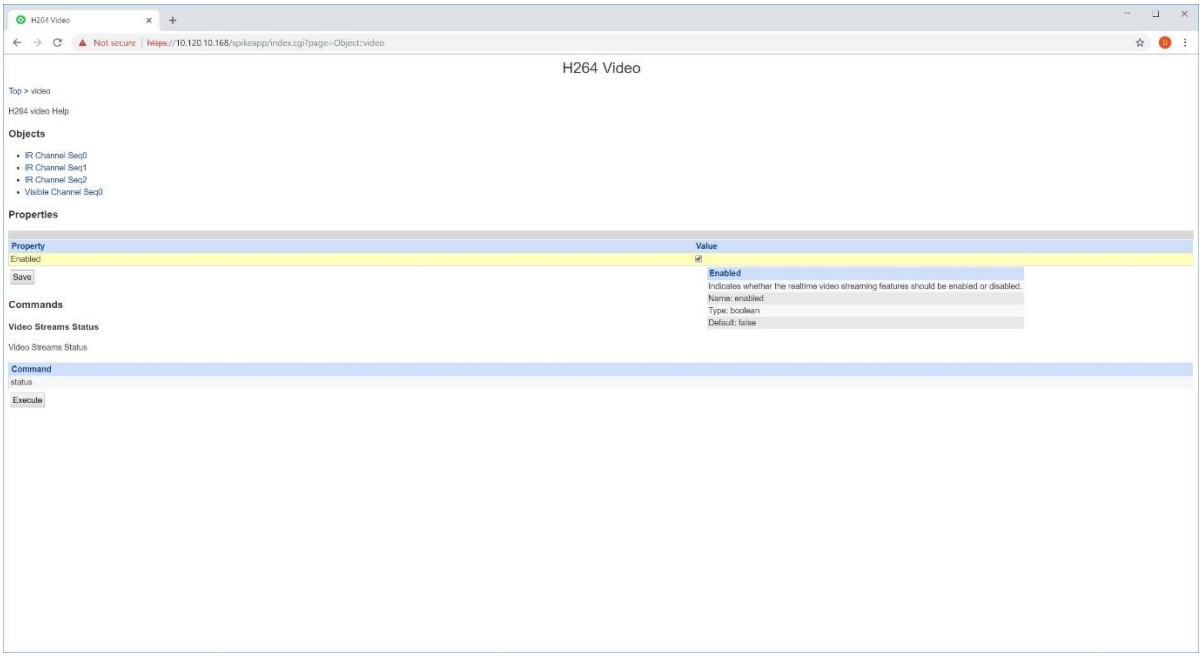
Four different video streams may be retrieved, specifically, the visible sensor stream and each of the 3 exposure sequences from the Infrared stream.

In order to enable the video, the first step is to ensure the firewall is configured to allow RTSP connections. See Firewall and ensure that RTSP is set to ACCEPT.

Next you will need to enable the video streaming facility. In order to do this in Webmin, select “Camera Configuration” on the left-hand side and then select “H264 Video” on the screen that appears – see the image below:

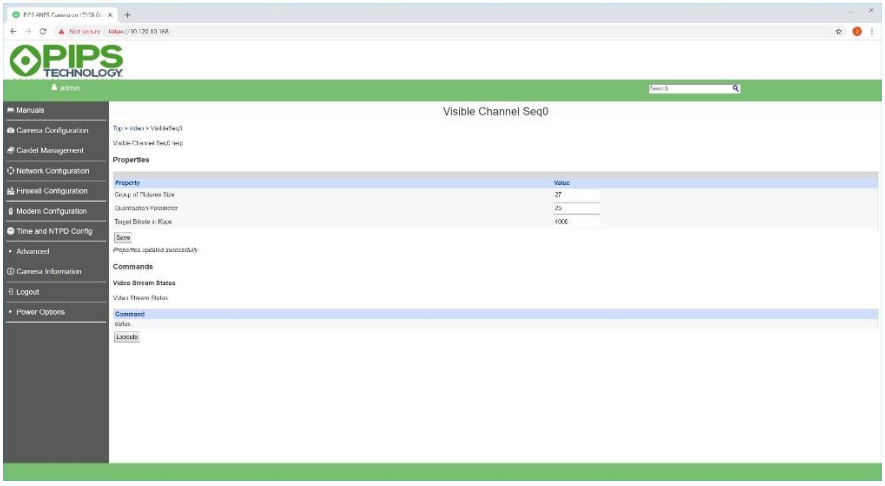


The following screen will be displayed:



Ensure that the “Enabled” is ticked and click on the “Save” button. This will allow you to connect to the RTSP video streams.

It is possible to adjust a few parameters of the available H264 streams. To do this select the stream in question – listed under “Objects” in the image above. For example, if you clicked on “Visible Channel Seq0” the following would be displayed:



Hover over the fields to see the help text. The most likely one you may want to change is “Target Bitrate in Kbps”. In the image above it has been changed from the default 2000 (2Mb/s) to 4000 (4Mb/s).

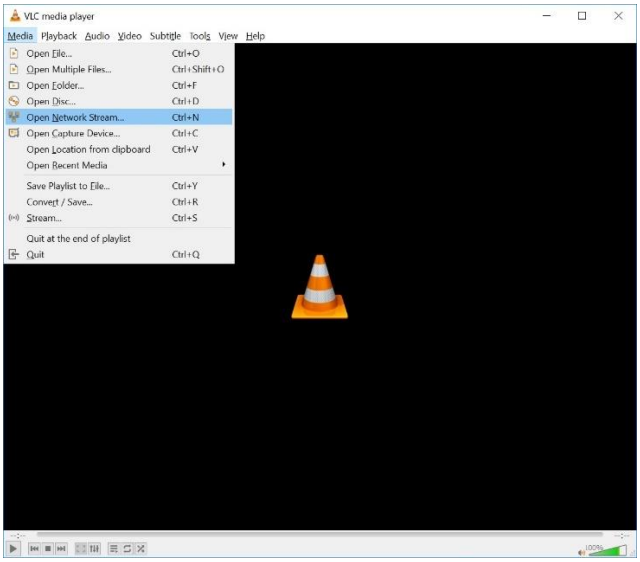
Viewing the H264 Video

To view the streams, you have to use a tool that can connect to RTSP/RTP protocol stream and decode H264 video. We recommend the VLC media player. This is an open source media player available to download. Google should provide you with the appropriate URL.

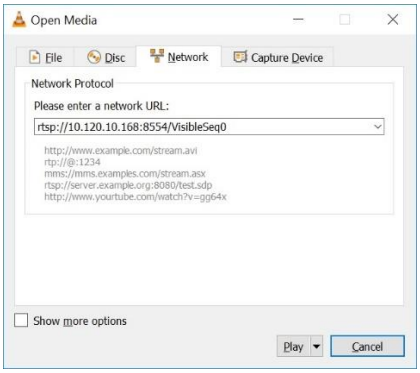
The 4 URLs are:

- rtsp://<IP Address>:8554/VisibleSeq0
- rtsp://<IP Address>:8554/IRSeq0
- rtsp://<IP Address>:8554/IRSeq1
- rtsp://<IP Address>:8554/IRSeq2

Assuming the VLC Media Player, select the “Media” dropdown and then select “Open Network Stream…”.

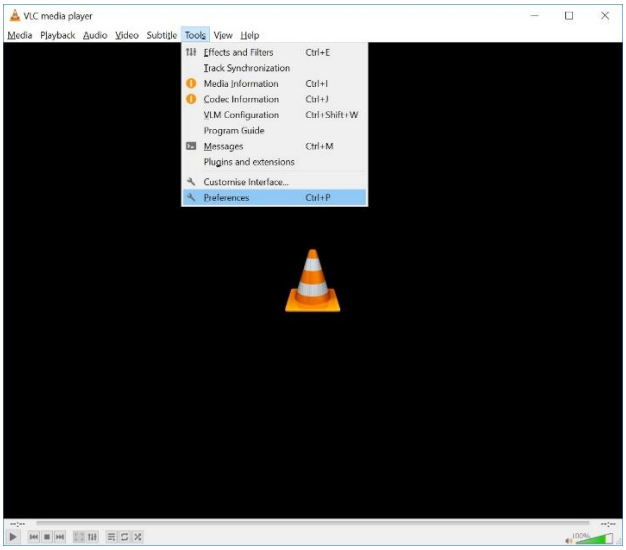


The following dialog will be displayed:

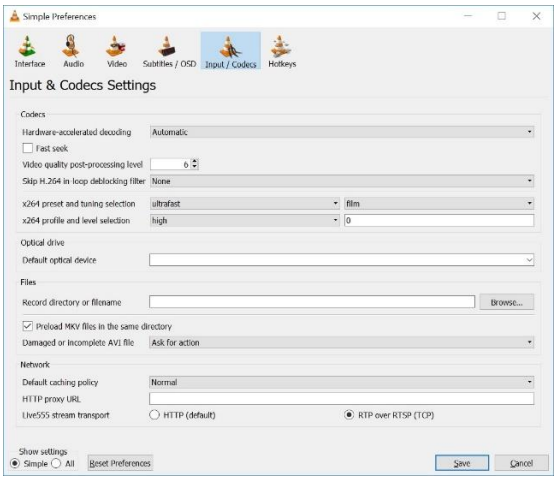


Enter the RTSP URL as per the example above (use the appropriate IP Address for your camera) and press “Play”. The video should appear within a few seconds.

If it does not, and you are not on the same LAN as the camera, it may be that some network firewalling is blocking the RTP (UDP) video packets. It is possible to have the RTP video packets tunnelled over the same TCP connection as the RTSP. In order to do this, select Tools->Preferences as in the image below:



In the Dialog select the “Input/Codecs” tab and ensure “RTP over RTSP (TCP)” is selected and press “Save”.



At which point, go back to “Media->Open Network Stream” and re-attempt the connection.

Developers Reference

This section describes the mechanisms and protocols for interfacing to the camera.

Most mechanisms are for the delivery of plate read metadata and images.

PIXI Protocol

The PIXI interface is the most comprehensive supporting:

- Delivery of images and metadata associated with plate reads. This can be either push or pull.
- Delivery of diagnostics and exceptions
- Delivery of log messages and notifications
- Setting and retrieving configuration settings
- Executing of commands

Unless you have good reason not to, this is the recommended interface to use for OEM back office software developers.

Even if you prefer the camera deliver plate read images and data as **files** (using ACS), PIXI is still useful as it can be used to configure the camera (e.g. configure ACS), monitor diagnostics etc.

Protocol Connection

The PIXI protocol works over a single TCP socket connection. There are two ways to setup this connection:

1. Connect to the camera. The PIXI server listens on TCP port 3382. (Note it may be necessary to unblock this port on the Firewall). This is the default way to connect.
2. Have the camera connect out to you. The camera can be configured to connect out to an IP Address and TCP port number of your choice.

The camera supports multiple PIXI connections (i.e. sessions).

Once the TCP socket connection has been established, PIXI packets may be exchanged. If the connection is idle for 5 minutes, the connection will be closed by the camera. For this reason, if no actual transactions are taking place, heartbeat packets must be periodically exchanged.

PIXI Packet Format

The PIXI packet format encapsulates both XML and binary data.

Note the binary data is not transcoded into text (such as Base64). It is transmitted unmodified.

Binary data is optional.

Name	Bytes	Content
Head	2	1. 0x0000 if there are no binary blobs in this data 2. 0x0001 if there are one or more binary blobs in the data
Length	2	XML Document length in bytes, as 2-byte, big endian value. Maximum length that the camera will accept is 16k. This is only the XML document portion.
Data	As required	Fully formed XML document
Binary Length [Optional]	0 or 4	Length of the binary blob (if marked as present by the header).
Binary Data [Optional]	0 or as required	Zero or more binary blobs. The position and size of the individual may be determined from the XML content.
End	4	0xffffffff

The PIXI link observes the following:

1. Multiple documents can be passed down the same link.

2. The link will stay open for a period, the camera will close it after 5 minutes of inactivity. To prevent this happening, you can send heartbeat message which will be echoed back to you to confirm the camera is alive.
3. Either end can send a message unsolicited.
4. The camera will respond to messages in the order in which the messages were received. This is on a per-connection basis. Multiple connections execute in parallel.
5. The camera will allow a maximum of 10 simultaneous PIXI links.

Software Installation and Upgrades

This section covers the installation and upgrading of camera software via packages supplied by Neology.

Installation of packages is primarily supported via two methods; one option is to use the PIPS ANPR Toolkit application which allows upgrading and clean installation of cameras, or the Webmin interface which provides a simpler approach for managing available upgrades.

Public Download Server

The public download server hosted by Neology contains versioned releases of all our software for each supported camera model. These may be downloaded for use by customers for installation on cameras.

The latest versions of each package can be found here: http://dl.anprlicense.eu/release/public.xml

The file repository (http://dl.anprlicense.eu/release/) itself contains a directory tree of each software package, grouped by supported camera model.

The general hierarchy of each directory is as follows. Please note that differing camera models may use alternative extensions on files, or some files may be omitted entirely.

```
<Camera Model>/
      software/
            app/
                  <Software Version>/
                        app-<version>.sig
                        app-<version>.tar.xz
                        app-<version>.html
            os/
                  <OS Version>/
                        os-package-<version>.tar.xz
```

Camera Application Packages

These packages are contained within the "**P500/software/app**" directory. For P500 software, these consist of three files:

- app-<version>.sig
- app-<version>.tar.xz
- app-<version>.html

The ".html" file is the release note for the software, detailing all the changes in the release. The ".tar.xz" and ".sig" files represent the package contents and signature respectively, and may be downloaded and registered into PIPS ANPR Toolkit as described in the Software Management section.

Camera OS Packages

These packages are contained within the "**P500/software/os**" directory. For P500 software, these consist of a single file with a ".tar.xz" extension.

These packages may be downloaded and registered into PIPS ANPR Toolkit as described in the Software Management section.

PIPS ANPR Toolkit

PIPS ANPR Toolkit provides tools to manage the clean installation of software on cameras, as well as upgrading existing camera software without losing user settings. Where possible, it is strongly recommended to upgrade software in-place and to not perform clean installations unless directed explicitly by our support team.

Usage of PIPS ANPR Toolkit to install software requires that the target camera have, at minimum, a network connection to the system running the PIPS ANPR Toolkit software. The camera does not need to have network connectivity to any external update servers, and so this method may be used on closed networks.

Software Management

Open PIPS ANPR Toolkit and click the “Settings” menu button near the top of the window, then click “Manage Software” in the menu that opens. The following dialog will appear.

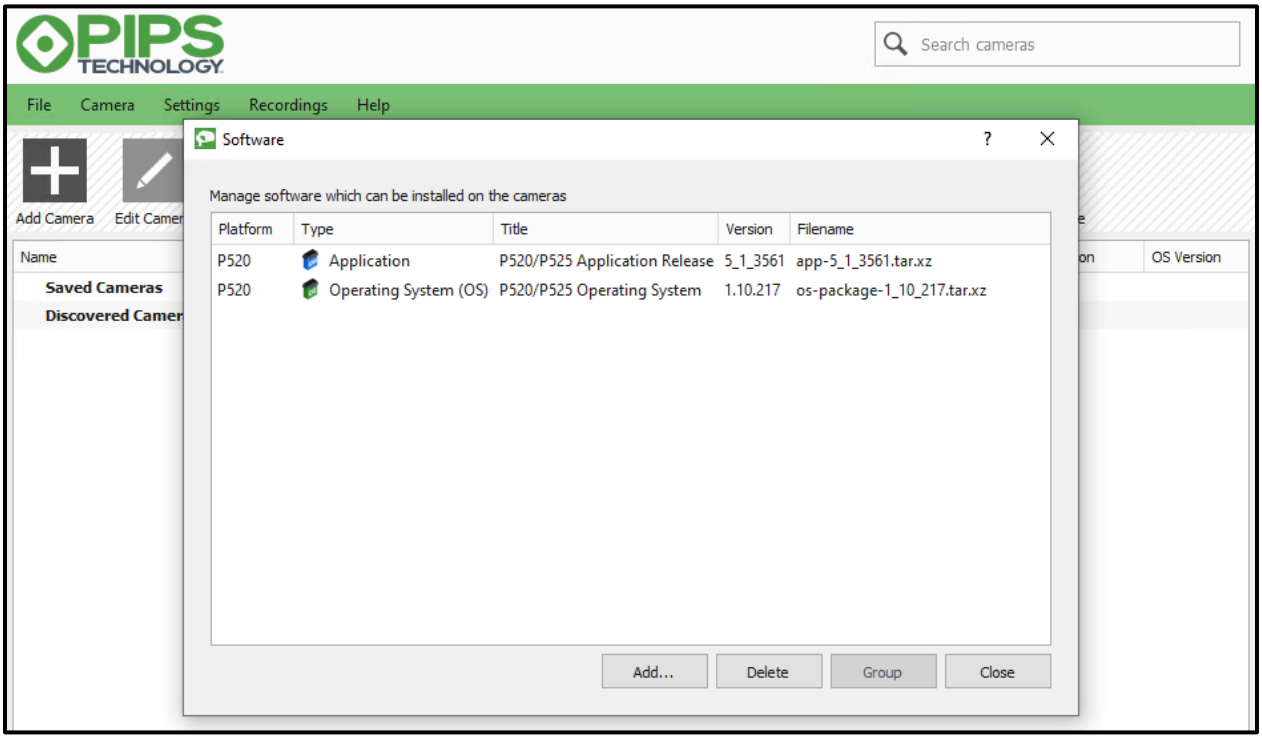


Figure 17 PIPS ANPR Toolkit - Manage Software Dialog

Software may be added to the list by clicking the “Add” button and navigating to/selecting any packages previously downloaded as described in the Public Download Server section.

> **Note**
>
> Camera application packages require that you download both the “.tar.xz” and “.sig” files for a package. Downloading one without the other will prevent successful installation of the software.

OS and Software Upgrades

OS and software upgrades can be performed via usage of the “Install Package” tool present on the toolbar of the main PIPS ANPR Toolkit window. These require a network connection to the camera. Software upgrades will not cause user settings to be wiped upon application.

Click the “Install Package” button on the main window to open the tool as shown below.

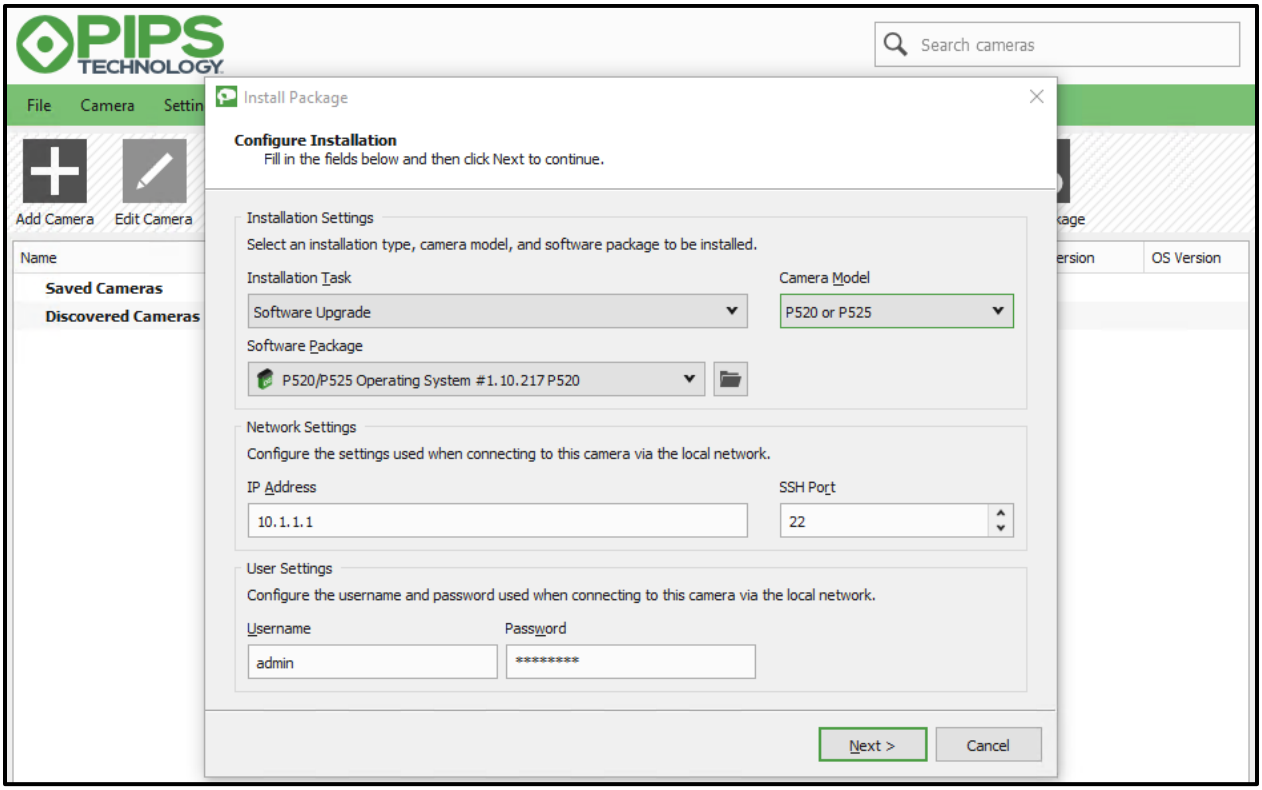


Figure 18 PIPS ANPR Toolkit - Software Upgrade Screen

The fields displayed on this page depend upon the selected values in the Installation Task and Camera Model dropdown; ensure that these are set to “Software Upgrade” and “P520 or P525” respectively.

Select a software package from the dropdown; if no packages are listed, you can click the folder button adjacent to the dropdown to open the Software Management dialog as described in the named section.

Ensure that an IP address is entered for your target camera and fill in the username/password fields with the credentials of an administrative user account if required. These fields will be automatically populated if the tool is opened while having selected a camera from your Saved Cameras list on the main window.

Once all the fields are filled in, click “Next” to begin installation. A progress bar will appear with log output of the installation process displayed below.

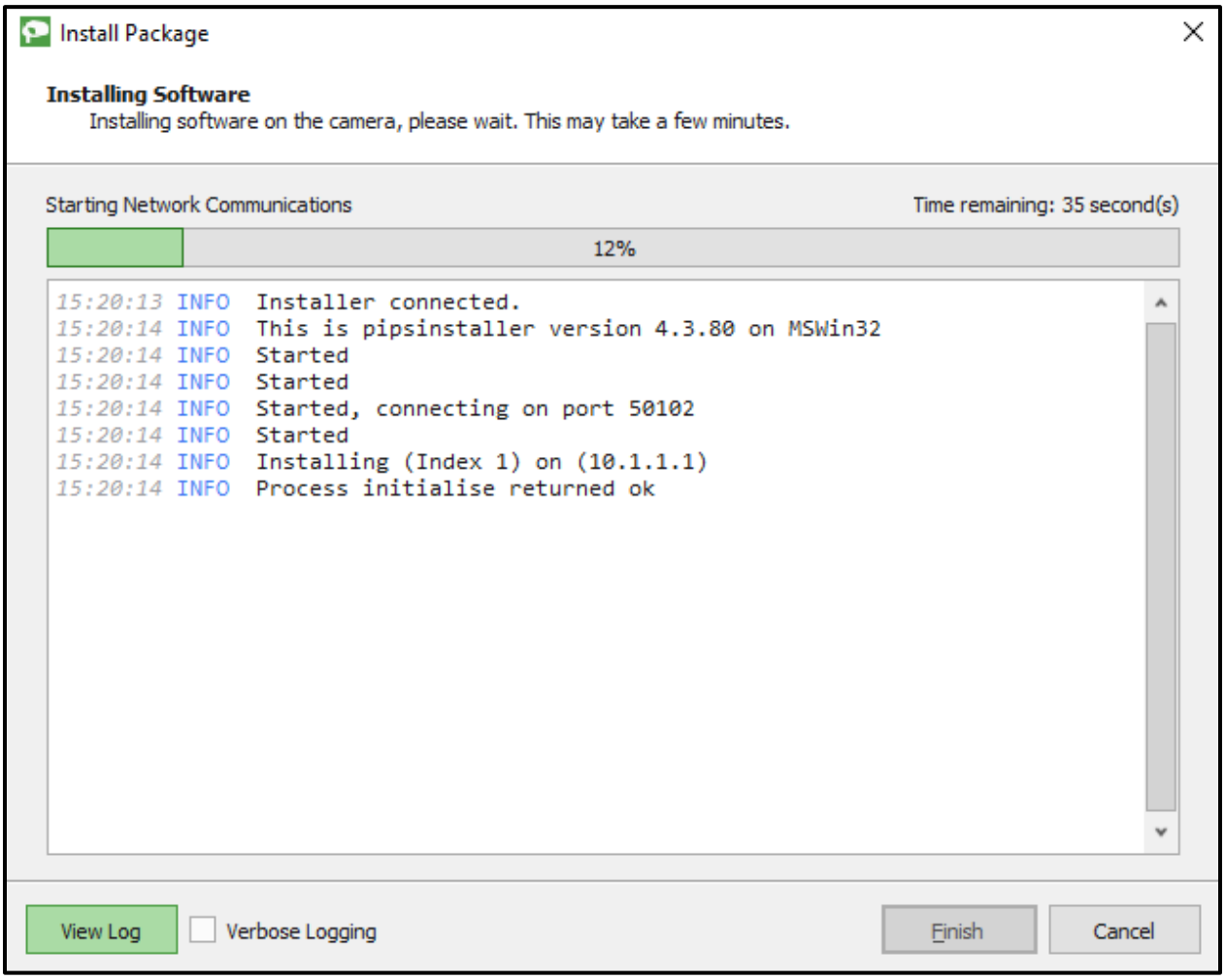


Figure 19 PIPS ANPR Toolkit - Software Installation Progress Screen

Once installation is complete, the camera will be rebooted, and the software upgrade will be in-place. This reboot may take some time depending upon the nature of the upgrade, or the relative age of the software being upgraded from. If any errors occur, they will be listed in the log with a red “ERROR” prefix.

OS Reinstallation

Clean OS reinstallations can be performed via the “Install Package” tool. OS installations require that the camera have both network and RS-232 serial connectivity to the system running PIPS ANPR Toolkit and are best performed on a closed network.

Click the “Install Package” button on the main window to open the tool as shown below.

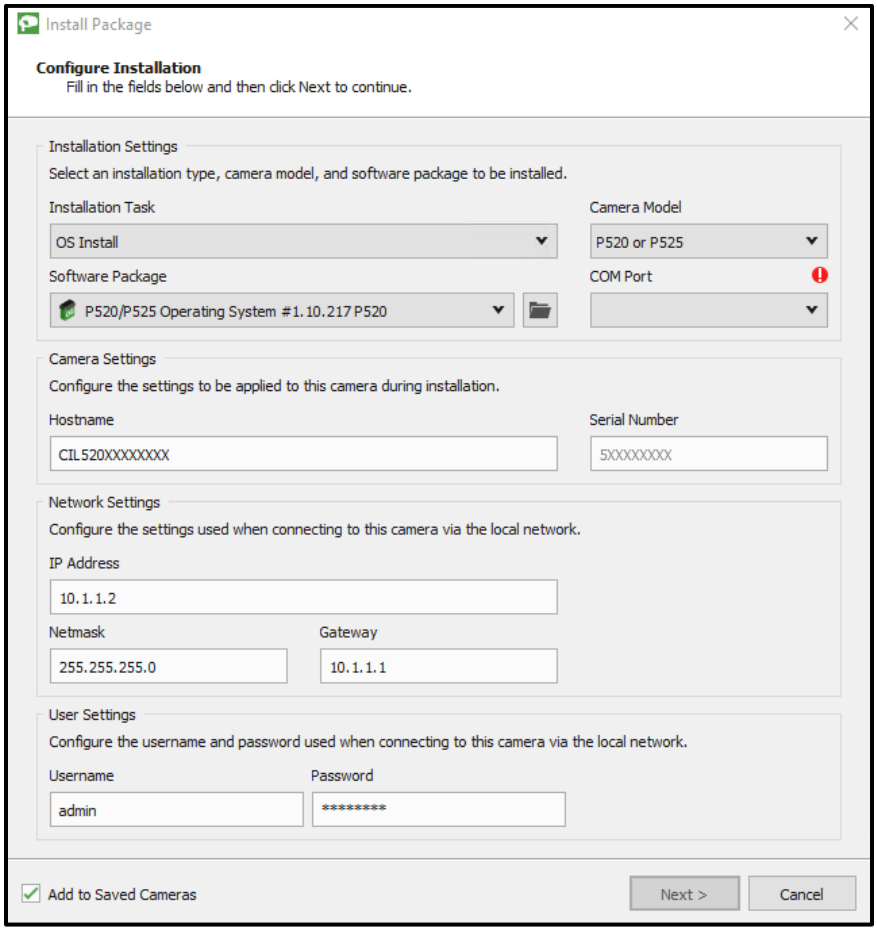


Figure 20 PIPS ANPR Toolkit - OS Install Screen

The fields displayed on this page depend upon the selected values in the Installation Task and Camera Model dropdown; ensure that these are set to “OS Install” and “P520 or P525” respectively.

Select a software package from the dropdown; if no packages are listed, you can click the folder button adjacent to the dropdown to open the Software Management dialog as described in the named section.

Ensure that the COM Port field is configured to the serial port on your system that is connected to the RS-232 serial terminal on the camera. Fill in the hostname field as appropriate, and ensure that the IP address, Netmask, and Gateway fields are appropriate for your network configuration. These settings will be used to configure networking the camera post-installation. Finally, enter a username and password for the default administrative user on the system.

Once all the fields have been supplied, click “Next” to begin the installation process. A progress bar will appear with logging output as described in the OS and Software Upgrades section. Please note that the installation process can take some time to complete.

Webmin

The Webmin interface can be used as an alternative method to check for and apply software upgrades to the camera. This allows the upgrading of both camera software and the operating system.

Clean reinstallations of the operating system are not possible via Webmin. Additionally, the camera must have network access to contact an update server (either hosted locally or, by default, our publicly accessible one).

Check for Updates

Access the web interface as documented in the "**Error! Reference source not found.**" section and click the "Check f or Updates" link in the left sidebar to open the following page.

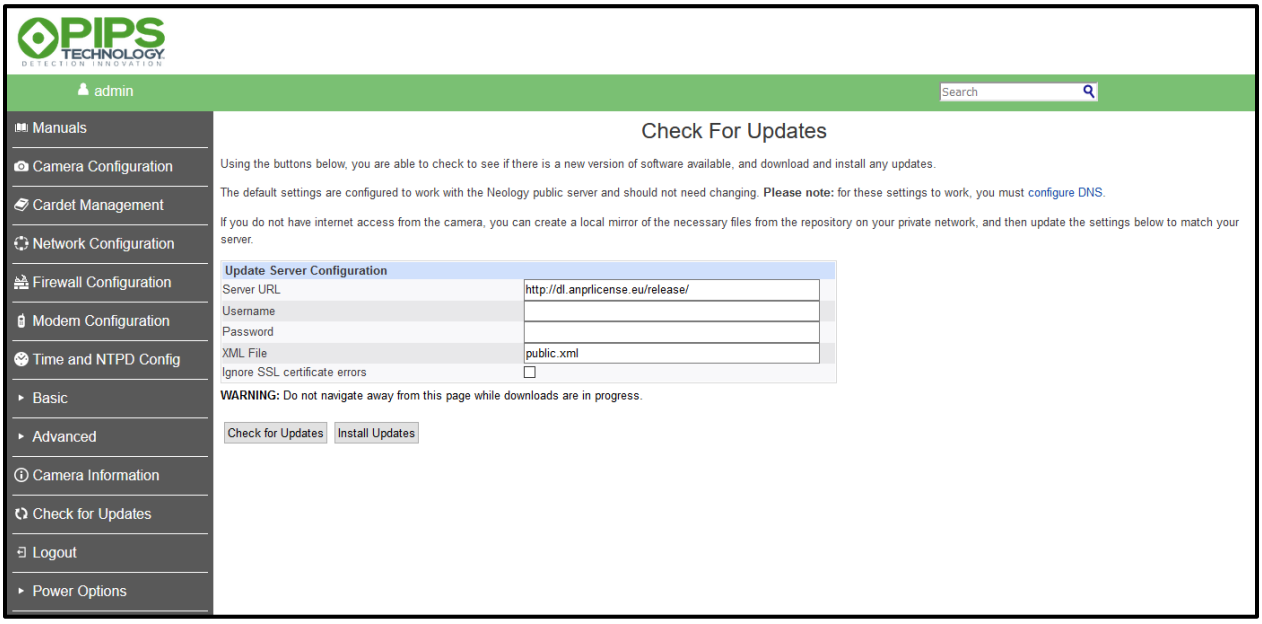


Figure 21 Webmin - Check for Updates Page

The default settings on this page will connect out to the Neology public update server.

> ### Note
>
> If using the Neology public update server, DNS must be configured on the camera. You can click the "configure DNS" link in the description paragraph near the top of the page. Additionally, the camera must have network access to the public server.

Click the "Check for Updates" button to have the system query its own software versions against those available on the server. If an upgrade is available, it will show in a list below the button and you can click the "Install Updates" button to fetch the packages for installation.

Appendix A. Nano text editor

This is a short guide to using nano, the installed text editor on the P500.
Further documentation is available at http://www.nano-editor.org/docs.php

Opening and creating files

Opening and creating files is simple in nano:

nano {*filename*}

You can start typing immediately to insert text, and move around with the cursor keys.

Saving and exiting

To save changes while editing, press Ctrl+O.

To exit nano, type Ctrl+C.

If you ask nano to exit where the file has been modified, it will ask you if you want to save it.
If you don't press N, otherwise press Y.

It will then prompt for a filename (pre filled with the existing filename if there is one). If you wish to overwrite the existing file simply press Enter.

If you change your mind about saving the file, press Ctrl+C when prompted for a filename.

Cutting and pasting

To cut a single line, you use Ctrl+K. To paste it, you simply move the cursor to where you want to paste it and use Ctrl+U.

To move multiple lines, simply cut them with several Ctrl+Ks in a row, move the cursor to the desired location and paste them with a single Ctrl+U. All the previously cut lines reappear at the selected location.

If you need finer selection control, then you have to mark the text. Move the cursor to the beginning of the text you want to cut and initiate the marking with Ctrl+6 (or Alt+A). Now move your cursor to select the text you want to cut noting that the marked text gets highlighted.
If you need to cancel your text marking, simply hit Ctrl+6 again. Press Ctrl+K to cut the marked text. Use Ctrl+U to paste it.

Searching for text

Simply hit Ctrl+W, type in your search string, and press Enter. To search for the same string again, hit Alt+W.

Note: In nano's help texts the Ctrl-key is represented by a caret (^), so Ctrl+W is shown as ^W, and so on. The Alt-key is represented by an M (from "Meta"), so Alt+W is shown as M-W.

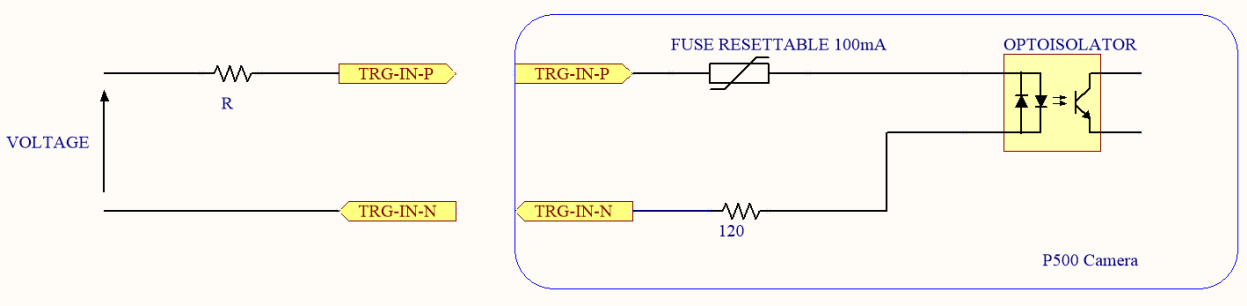
Appendix B. Technical Details

Connectivity

Refer to the Installation Manual for full details of the P500 wiring information.

Trigger Inputs

The P500 camera has support for 2 optically isolated hardware trigger inputs. External current of between 1mA and 25mA must be provided for correct operation. The circuit below shows a possible use case, the value of resistor R needs to be selected to give an appropriate current for the voltage being used. The forward voltage drop of the LED in the opto-coupler is typically 1.25V at 10mA. The table below gives some suggested resistor values for various voltage inputs.



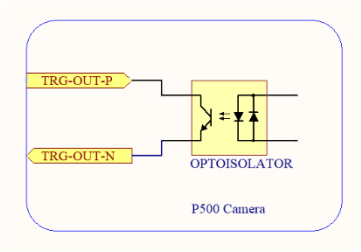
Input Voltage	Suggested Resistor Value	Trigger Current
15V	1.2kΩ	~10mA
18V	1.5kΩ	~10mA
24V	2kΩ	~10mA
48V	4.3kΩ	~10mA

Trigger Outputs

The P500 camera has support for 2 optically isolated phototransistor outputs. When turned on the phototransistor is driven into saturation with a typical collector-emitter voltage drop of 0.2V.

The output ratings are:

Collector-Emitter Voltage	80V
Emitter-Collector Voltage	7V
Collector Current	50mA
Collector Power	150mW



These outputs can be used to provide synchronisation signals for external illuminators. Please contact support if other uses are required.

Relay Output

The P500 relay output has the following ratings:

Nominal Switching Capacity	2A 30V DC, 0.5A 125V AC (resistive load)
Max. Switching Power	60 W (DC), 62.5 VA (AC) (resistive load)
Max. Switching Voltage	220V DC, 125V AC
Max. Switching Current	2A

Appendix C. Contact Information

EMEA

Sales:	sales@pipstechnology.co.uk	Tel: +44 (0) 1256 581134
Customer / Tech support:	support@pipstechnology.co.uk	Tel: +44 (0) 1256 581135
Service Center:	service@pipstechnology.co.uk	Tel: +44 (0) 1513 554313

USA

US Toll Free:	833-PIPS-LPR (747-7577)
Support:	support@pipstechnology.com