

VLP Processor Installation Guide





© 2021 Motorola Solutions, Inc. All rights reserved

Legal and Support

Intellectual Property and Regulatory Notices

Copyrights

The Motorola Solutions products described in this document may include copyrighted Motorola Solutions computer programs. Laws in the United States and other countries preserve for Motorola Solutions certain exclusive rights for copyrighted computer programs. Accordingly, any copyrighted Motorola Solutions computer programs contained in the Motorola Solutions products described in this document may not be copied or reproduced in any manner without the express written permission of Motorola Solutions.

No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without the prior written permission of Motorola Solutions, Inc.

Trademarks

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

License Rights

The purchase of Motorola Solutions products shall not be deemed to grant either directly or by implication, estoppel or otherwise, any license under the copyrights, patents or patent applications of Motorola Solutions, except for the normal non-exclusive, royalty-free license to use that arises by operation of law in the sale of a product.

Open Source Content

This product may contain Open Source software used under license. Refer to the product installation media for full Open Source Legal Notices and Attribution content.

European Union (EU) and United Kingdom (UK) Waste of Electrical and Electronic Equipment (WEEE) Directive



The European Union's WEEE directive and the UK's WEEE regulation require that products sold into EU countries and the UK must have the crossed-out wheelie bin label on the product (or the package in some cases). As defined by the WEEE directive, this crossed-out wheelie bin label means that customers and end-users in EU and UK countries should not dispose of electronic and electrical equipment or accessories in household waste.

Customers or end-users in EU and UK countries should contact their local equipment supplier representative or service centre for information about the waste collection system in their country.

Disclaimer

Please note that certain features, facilities, and capabilities described in this document may not be applicable to or licensed for use on a specific system, or may be dependent upon the characteristics of a specific mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola Solutions contact for further information.

© 2021 Motorola Solutions, Inc. All Rights Reserved

Contact Us

For inquiries, see https://www.motorolasolutions.com/en_us/support.html > License Plate Recognition (Vigilant) or contact our 24 hours support staff at:

- Tel: 925-398-2079
- Fax: 925-398-2113
- Email: vigilantsupport@motorolasolutions.com

Document History

Version	Description	Date	
MN007808A01-AA	Initial Release	March 2021	
MN007808A01-AB	The following section is added for this release: July 2021		
	Adding Cameras on page 14		
	The following sections are updated for this re- lease:		
	UbuntuHD Control Setup on page 10		
	VPN Configuration on page 20		
	WebUI Setup on page 25		
MN007808A01-AC	The following sections are updated for this re- lease:	December 2021	
	WebUI Setup on page 25		
	TAS for WebUI Setup on page 40		

Read Me First

Notations Used in This Manual

Throughout the text in this publication, you notice the use of **Warning**, **Caution**, and **Notice**. These notations are used to emphasize that safety hazards exist, and the care that must be taken or observed.



WARNING: An operational procedure, practice, or condition, and so on, which may result in injury or death if not carefully observed.



CAUTION: An operational procedure, practice, or condition, and so on, which may result in damage to the equipment if not carefully observed.



NOTE: An operational procedure, practice, or condition, and so on, which is essential to emphasize.

Special Notations

The following special notations are used throughout the text to highlight certain information or items:

Table 1: Special Notations

Example	Description
Menu key or Camera button	Bold words indicate a name of a key, button, or soft menu item.
The display shows Settings Applied.	Typewriter words indicate the MMI strings or messages displayed.
<required id=""></required>	The courier, bold, italic, and angle brackets indi- cate user input.
Setup→Settings→All Settings	Bold words with the arrow in between indicate the navigation structure in the menu items.

Contents

Legal and Support	2
Intellectual Property and Regulatory Notices	2
Contact Us.	3
Document History	
Read Me First	3
List of Figures	7
List of Tables	9
Chapter 1: UbuntuHD Control Setup	10
1.1 UbuntuHD Control Overview	10
1.2 Downloading the UbuntuHD Control Software	11
1.3 Connecting over Ethernet	11
1.4 Connecting to the Wi-Fi Hotspot	13
1.5 Launching UbuntuHD Control	14
1.6 Adding Cameras	14
1.7 Configuring Wi-Fi Hotspot Mode	16
1.8 Connecting the VLP to a Wi-Fi Network	
1.9 Inverting the Camera Feed	18
Chapter 2: VPN Configuration	20
2.1 Downloading the WireGuard VPN Software	20
2.2 Configuring WireGuard in UbuntuHD Control	20
2.3 Configuring WireGuard	
2.4 Testing the VPN Connection	23
Chapter 3: WebUI Setup	
3.1 Logging In to the WebUI	25
3.2 VLP Controls Overview	27
3.2.1 Enabling or Disabling Engine	27
3.2.2 Configuring Zone Settings	
3.2.3 Upgrading Firmware	
3.2.4 Changing Source Type	
3.2.5 Resetting DSP	30
3.2.6 Changing IP	
3.2.7 Configuring Wi-Fi Management	
3.2.8 Configuring a LEARN Connection	32
3.2.9 Getting Log Files	34
3.2.10 Generating Health Information	34

3.2.11 Unlocking License	35
3.3 Camera Controls Overview	35
3.3.1 Resetting Camera	36
3.3.2 Upgrading Firmware	36
3.3.3 Changing Camera IP	37
3.3.4 Unlocking Camera	38
3.3.5 Generating Camera Health Information	38
3.3.6 Getting Camera Log Files	39
Chapter 4: TAS for WebUI Setup	40
4.1 Downloading the TAS Client	40
4.2 Configuring LEARN Connection in WebUI	41
4.3 Configuring the TAS Client	44

List of Figures

Figure 1: UbuntuHD Control Main Window Overview	. 10
Figure 2: Ethernet Properties	. 12
Figure 3: Internet Protocol Version (TCP/IPv4) Properties	13
Figure 4: Wi-Fi IP Address	. 13
Figure 5: VLP Ethernet Adapter IP Address	14
Figure 6: Select Camera	14
Figure 7: Address Resolution Protocol	. 14
Figure 8: Change Source Type	. 15
Figure 9: Select Camera in Change Source Type	15
Figure 10: Wi-Fi Management	. 17
Figure 11: Wi-Fi Management	. 17
Figure 12: Wi-Fi Management-Radio Status	. 18
Figure 13: Select Type of Camera Settings	19
Figure 14: Camera Settings	19
Figure 15: Download Windows Installer	. 20
Figure 16: Connecting to the VLP	. 20
Figure 17: WireGuard Setup	21
Figure 18: WireGuard Public IP Address	21
Figure 19: WireGuard Select Client	22
Figure 20: Add Tunnel	. 22
Figure 21: Create New Tunnel	. 23
Figure 22: Connect WireGuard to VLP VPN	. 23
Figure 23: WebUI Main Page	. 25
Figure 24: LPR Web Control Sign In	. 26
Figure 25: Select Camera	26
Figure 26: VLP Controls	. 27
Figure 27: Enable/Disable Engine	. 27
Figure 28: Zone Setting	. 28
Figure 29: Update Engine	28
Figure 30: Change Source Type	. 29
Figure 31: Reset Confirmation	30
Figure 32: Change IP	. 31
Figure 33: Wi-Fi Management	. 32
Figure 34: VLP LEARN Window	33
Figure 35: Get Log	~ ~
	34

Figure 37: License	35
Figure 38: ReaperHD Controls Tab	35
Figure 39: Reaper HD Camera Controls	35
Figure 40: L5F Controls Tab	35
Figure 41: L5F Camera Controls	36
Figure 42: Reset Camera	36
Figure 43: Upgrade Firmware ReaperHD	37
Figure 44: Change IP	. 37
Figure 45: Unlock Camera	38
Figure 46: Camera Health Information	39
Figure 47: Vigilant PlateSearch User Profile	41
Figure 48: VLP PlateSearch Window	42
Figure 49: TAS Center Setting	. 43
Figure 50: Add TAS User	. 43
Figure 51: TAS User Permission	43
Figure 52: TAS Server	44
Figure 53: Add Source	45
Figure 54: Connect to TAS Server	. 45
Figure 55: TAS Alert	46
Figure 56: Stored Alerts	46

List of Tables

Table 1: Special Notations	4
Table 2: Change Source Type Fields Description	16
Table 3: Change Source Type Fields Description	29
Table 4: Change IP Interface Information	31
Table 5: VLP LEARN Field Description	
Table 6: Change IP Fields Description	
Table 7: TAS Server Fields Descriprion	44

Chapter 1

UbuntuHD Control Setup

1.1 UbuntuHD Control Overview

UbuntuHD Control (also known as MiniControlCenter) is a Windows app for controlling, configuring, and troubleshooting VLP camera systems with Motorola Solutions' ReaperHD ,L5F, or L5M LPR cameras. UbuntuHD Control can also be used with third party ONVIF compatible IP LPR cameras.



NOTE: L5Q standalone cameras do not use a VLP and are not compatible with VLP based camera systems. For L5Q cameras, see L5Q Provisioning Leaflet and the L5Q Installation Guide.

Figure 1: UbuntuHD Control Main Window Overview



To use it, you need to have the following:

- An Ethernet or Wi-Fi enabled 64-bit Windows 10 PC.
- The UbuntuHD Control software.
- · An assembled and powered VLP based camera system.
- One Ethernet cable.
- A ReaperHD, L5F, L5M, or other ONVIF compatible IP camera.

There are three ways to connect the UbuntuHD Control software to a VLP:

- Ethernet cable.
- Wi-Fi hotspot.
- Over the Internet through a VPN.

To configure a VPN connection for the VLP, refer to the VPN Configuration on page 20 section.

1.2 **Downloading the UbuntuHD Control Software**

Procedure:

1 Download the UbuntuHD Control software from the following link: https://get.vaasfiles.com/ VLPMCC



NOTE: The UbuntuHD Control software is also included in the CarDetector Mobile and CarDetector Fixed software packages.

1.3 Connecting over Ethernet

Procedure:

1 Connect a Windows PC to the LAN 1 port on the VLP with an Ethernet cable.



NOTE: The LAN 2 Ethernet port on the VLP is configured for DHCP and can be used to connect the VLP to a DHCP/Internet enabled router. When using this configuration, connect the Windows PC to the router instead and use the IP address assigned to the VLP by the router to connect to UbuntuHD Control.

- 2 Configure the IP Address of the Windows PC in network settings:
 - a Open the Windows Control Panel and click Network and Internet→Network and Sharing CenterChange Adapter Settings.
 - **b** Right-click the **Ethernet** adapter and click **Properties**.

Figure 2: Ethernet Properties

Ethernet	Properties	\times
Networking	Authentication Sharing	
Connect usi	ing:	
🚅 Intel(R) Ethemet Connection (4) I219-V	
	Configure	
This connect	ction uses the following items:	-
	ent for Microsoft Networks	^
File	e and Printer Sharing for Microsoft Networks	
v 🚽 🖉	niper Network Service	
	ernet Protocol Version 4 (TCP/IPv4)	
🗌 🛄 🔔 Mi	crosoft Network Adapter Multiplexor Protocol	
✓ <u>_</u> Mi	crosott LLDP Protocol Driver	~
Mi	II Uninstall Properties	`
Insta Descriptio Transmis wide area across di	Il Uninstall Properties International Action Properties Internation Internatinternatinteree Internation Internation Internation	×
Insta Descriptio Transmis wide area across di	Il Uninstall Properties Il Uninstall Properties In sion Control Protocol/Internet Protocol. The default a network protocol that provides communication iverse interconnected networks.	×

- c Double-click Internet Protocol Version (TCP/IPv4) and select the Use the following IP address radio button.
- **d** Enter the following IP address information:
 - IP address: 192.168.5.99
 - Subnet mask: 255.255.255.0

Internet Protocol Version 4 (TCP/IPv4)	Properties ×
General	
You can get IP settings assigned autor this capability. Otherwise, you need to for the appropriate IP settings.	natically if your network supports ask your network administrator
Obtain an IP address automatical	ly
• Use the following IP address:	
IP address:	192.168.5.99
Subnet mask:	255.255.255.0
Default gateway:	
Obtain DNS server address auton	natically
• Use the following DNS server add	resses:
Preferred DNS server:	
Alternate DNS server:	
Validate settings upon exit	Advanced
	OK Cancel

e To save, click OK.

1.4

Connecting to the Wi-Fi Hotspot

Most VLP Units come equipped with a built in Wi-Fi adapter broadcasting a hidden Wi-Fi Access Point. This AP can be used to connect to a VLP with the default SSID and Password (Key) when an Ethernet connection is not available.

Procedure:

- 1 From the Windows system tray, click Wi-Fi→Wi-Fi name Hidden Network→Connect.
- 2 In the Enter the name (SSID) for the network text field, enter the default VLP SSID: VLP-COMMS.
- 3 Enter the VLP's default Wi-FI key: 7tM&L1G!b. Or, enter the key generated from step step 6 and click Next.
- 4 Open the UbuntuHD Control software.
- **5** In the IP address field at the top of the window, enter the default IP of the VLP's Wi-Fi adapter: 10.42.0.1. Select a connected camera, and then click **Connect**.

Figure 4: Wi-Fi IP Address

IP Address	10.42.0.1	Camera 3	•	Connect
------------	-----------	----------	---	---------

The video streams from the selected camera appears.

1.5 Launching UbuntuHD Control

Procedure:

- 1 On the Windows PC, open the UbuntuHD Control software zip file and extract the contents into a new folder.
- 2 Double-click the UbuntuHDControl.exe file to launch the software.
- 3 In the IP address field at the top of the window, enter the default IP address for the VLP's LAN 1 Ethernet adapter: 192.168.5.150.



NOTE: If using the LAN 2 Port with DHCP, use the IP address assigned to the VLP instead.

Figure 5: VLP Ethernet Adapter IP Address



4 Select a connected camera and click Connect.

The video streams from the selected camera will appear.

1.6 Adding Cameras

When and where to use: To configure ReaperHD, L5F and L5M cameras connected to a VLP system, configure the cameras with the Change Source Type menu.

Procedure:

1 Select the camera to be added with the camera drop-down menu and click Connect.

Figure 6: Select Camera

IP Address	192.168.5.150	Camera 1	•	Connect	
	,				

2 To view the IP addresses of devices connected to the VLP, select the **ARP** (Address Resolution Protocol) button.

Figure 7: Address Resolution Protocol

Console Logs	>
== Output of: ip neighbour === 192.168.3.053 dev emp380 lladdr f4:4d:30:6d:72:c7 STALE 192.168.3.103 dev bro TNCOMPLETE 192.168.3.235 dev bro FAILED 192.168.7.203 dev bro PS0 lladdr f6:c3:35f2:c80:1fd REACHABLE 192.168.7.300 dev bro PS0 lladdr f6:c3:35f2:c80:1fd REACHABLE 192.168.7.100 dev bro PAILED 192.168.7.208 dev emp380 lladdr 60:361:26:0e:56:a4 STALE 192.168.7.1 dev emp380 lladdr 80:d6:193/27:92 STALE 192.168.7.1 dev emp380 lladdr 80:d6:193/27:92 STALE 192.168.3.101 dev bro lladdr 00:04:40:c84-42:16 REACHABLE 192.168.3.101 dev bro lladdr 00:04:40:c84-42:16 REACHABLE	
	Reboot Close



NOTE: By default, ReaperHD, L5F, and L5M cameras have an IP address assigned as 192.168.3.101 - 192.168.3.104.

- **3** Look for the devices with IP addresses of the form 192.168.3.1XX with the **REACHABLE** state. These are cameras connected to the PoE ports on the VLP.
- 4 Select Change Source Type.

Figure 8: Change Source Type

Controls			
Enable Engine Disable Engine	Change Source Type	LEARN	Clear File Statistic
Get Eclipse Setting File	Reset DSP	GetLog	Set Profile
Set Eclipse Setting File	Change IP	Set time zone	Unlock
Zone Settings	Realtime Log	Resize Overview Image	Enable Aiming Tool
Development Mode	TAS Center Settings	Get Health Infomation	Check Realtime Status
Hardware Status	WIFI Management	Health Monitor Setting	Setting Send Email Alert
ReaperXD Settings	Wireguard Setup	Auto Upgrade Settings	Web Page
GSM Status/Control	ARP	FTP Upload	L5F/L5M Settings
RHD Settings			

- 5 Check the **Enable** check box.
- 6 Select the camera type from the **Source Type** drop-down menu.

Figure 9: Select Camera in Change Source Type

Camera Name	(for LEARN Uploading)		
Video Source C	Configuration		
Source Type:	✓ Enable L5F camera	3	1 cc
Address: Port:	192.168.3.101 80		Video Server ReaperHD camera
UserName: Password:			HTTP Stream ReaperXD camera ReaperSD Camera
In/Out:	Front car is in	- -	Local Video Folder ONVIF Camera WatchGuard4RE System
Video:			

- 7 Enter the IP address of the camera into the Address field.
- 8 Select Save Change.

The video streams from the camera should now appear in the main window.

9 Repeat this process for the other cameras in the system with their respective IP addresses from the **ARP** window.

For ReaperHD, L5F L5M cameras, only the **Address** and **Source Type** fields need to be configured. The other fields can be left blank. For reference, see the following table for descriptions of the other fields.

Field	Description
Camera Name	The identifier that the camera will be referred to as in LEARN. (Used only as a label. Does not determine the selected camera.)
Source Type	This drop-down is used to select the camera or stream type for the video feed.
Address	The IP Address to connect to for the currently selected camera.
Port	The port associated with the camera or stream. Default is the HTTP port 80. Other commonly used ports are: RTSP: 554 and HTTPS: 443 for other camera types.
Username/Password	Login credentials for the selected camera can be entered here if required. ReaperHD and L5F/L5M cameras do not require credentials by default.
In/Out	Designates this camera in PlateSearch as monitoring the entrance or exit of a location.
Profile	Specify a desired camera profile name here if needed. By default, this can be left blank.
Video	Fill in this field if using a video server.

Table 2: Change Source Type Fields Description

1.7 Configuring Wi-Fi Hotspot Mode

The VLP's Wi-Fi Access Point can be configured to change the default SSID and password.

When and where to use: To connect to the VLP using the default SSID and password, see Connecting to the Wi-Fi Hotspot on page 13.



NOTE: Some early VLP versions do not have built-in Wi-Fi capability. These VLP units will not broadcast a hidden Wi-Fi network and will not show the 'VLP-COMMS' SSID entry in the Wi-Fi management window. Such systems will need a CradlePoint router to provide a Wi-Fi Access Point. For consistency, setup the AP on the CradlePoint router using the same default settings as the VLP: (SSID: VLP-COMMS, Key: 7tM&L1G!b).

Procedure:

1 From the Controls section, click Wi-Fi Management.

Figure 10: Wi-Fi Management

Enable Engine Disable Engine	Change Source Type	LEARN	Clear File Statistic
Get Eclipse Setting File	Reset DSP	GetLog	Set Profile
Set Eclipse Setting File	Change IP	Set time zone	Unlock
Zone Settings	Realtime Log	Resize Overview Image	Enable Aiming Tool
Development Mode	TAS Center Settings	Get Health Infomation	Check Realtime Statu
Hardware Status	WIFI Management	Health Monitor Setting	Setting Send Email Ale
ReaperXD Settings	Wireguard Setup	Auto Upgrade Settings	Web Page
GSM Status/Control	ARP	FTP Upload	L5F/L5M Settings
RHD Settings			

- 2 To change the SSID or Wi-Fi password , double-click the VLP-COMMS entry in the Radio Status box and click OK to disconnect the hotspot.
- 3 Enter a new SSID and Wi-Fi Key (password) if desired.
- 4 Copy the text in the **Key** field.
- **5** To randomly generate a secure key, click the **Randomize** button.
- 6 In the **Wi-Fi Management** window, copy the randomized characters from the **Key** text box as reference.

NOTE: The Wi-Fi hotspot SSID and password can be changed from this window.

Figure 11: Wi-Fi Management

adio Sta (Double	tus	conect)		Refresh	WIFI Devices
In Use	SSID	Signal	Security	BSSID	
*	VLP-COMMS	0 V	VPA1 W	1C:BF:CE:1A:83:3E	
lotspot M	1ode				
SSID	VLP-COMMS	Enat	ole (Dou	uble click on status to Disable)	

- 7 To enable the Wi-Fi hotspot click **Enable**.
- 8 To change the SSID or password, double-click the VLP-COMMS" entry in the **Radio Status** box and click **OK** to disconnect the hotspot.
- 9 Enter the new SSID or password and click Enable.

1.8

Connecting the VLP to a Wi-Fi Network

Instead of operating in hotspot mode, the VLP can also be configured to join another Wi-Fi network to provide it with Internet access.

Procedure:

1 In the **Wi-Fi Management** window, double-click the **VLP-COMMS** entry in the **Radio Status** section.

Figure 12: Wi-Fi Management-Radio Status

0010 0- 0 0- 0	
n Use SSID Sig ∠ Security	BSSID
CH56 100 WPA2	80:DA:13:1C:EC:21
CT56 100 WPA2	80:DA:13:10:24:F1
chipo 99 WPA2	00004133072003
suasys 0J WPA2	44-10-12-04-DE-RE
tspot mode	

- 2 To disable the Wi-Fi hotspot, on the resulting confirmation window, click OK.
- 3 To display a list of available Wi-Fi hotspots, click Refresh.
- 4 To connect to a Wi-Fi network, double-click on the desired entry.
- 5 Enter the password for the Wi-Fi network and click OK.

^{1.9} Inverting the Camera Feed

When and where to use: If the mounting configuration requires the camera to be installed upside down, the video feed can be inverted.

Procedure:

- 1 Select the correct camera.
- 2 Perform one of the following actions:
 - For ReaperHD cameras, select RHD Settings.
 - For L5F/L5M cameras, select L5F/L5M Settings.

Figure 13: Select Type of Camera Settings

ntrols				
Enable Engine	Disable Engine	Change Source Type	LEARN	Clear File Statistic
Get Eclipse	Setting File	Reset DSP	GetLog	Set Profile
Set Eclipse :	Setting File	Change IP	Set time zone	Unlock
Zone S	ettings	Realtime Log	Resize Overview Image	Enable Aiming Tool
Developm	ent Mode	TAS Center Settings	Get Health Infomation	Check Realtime Status
Hardware	e Status	WIFI Management	Health Monitor Setting	Setting Send Email Aler
ReaperXD	Settings	Wireguard Setup	Auto Upgrade Settings	Web Page
GSM Statu	is/Control	ARP	FTP Upload	L5F/L5M Settings
RHD Se	ettings			

3 Select Rotate View 180.

Figure 14: Camera Settings

ReaperHD Camera Controls		×
Capture Video Reset Camera	Change Camera IP	Unlock Camera
Upgrade FW ReaperHD	Get Camera Version	GetLog Camera
RTSP Stream Settings	Get Health Camera	Sensor Settings
Development Mode]	Rotate View 180
L5F Camera Controls		×
Capture Video Reset Camera	Change Camera IP	Unlock Camera
Upgrade FW L5F/L5M	Get Camera Version	GetLog Camera
Image Rotate 180	Get Health Camera	Sensor Settings
Development Mode	Ī	

Chapter 2

VPN Configuration

VLP systems can be configured to connect to a Virtual Private Network (VPN) with the UbuntuHD Control software to enable remote access over the Internet.

2.1

Downloading the WireGuard VPN Software

WireGuard is a lightweight VPN client software used to connect to the VLP over a VPN connection from a remote Windows PC.

Procedure:

- 1 Open a web browser and connect to the WireGuard website at https://www.wireguard.com/ install/.
- 2 Click the Download Windows Installer link.

Figure 15: Download Windows Installer





NOTE: Using WireGuard with other Operating Systems to connect to a VLP is possible but not currently supported.

3 To run the WireGuard installer, double-click on the installer file.

The WireGuard application will open automatically when the installation is complete.

2.2 Configuring WireGuard in UbuntuHD Control

Procedure:

1 Open UbuntuHD Control→Enter an IP address→Camera→Connect to connect to the VLP.



Figure 16: Connecting to the VLP

IP Address	192.168.5.150	Camera 3	•	Connect

2 Click the WireGuard Setup button.

Figure 17: WireGuard Setup

Enable Engine Disable Engine	Change Source Type	LEARN	Clear File Statistic
Get Edipse Setting File	Reset DSP	GetLog	Set Profile
Set Eclipse Setting File	Change IP	Set time zone	Unlock
Zone Settings	Realtime Log	Resize Overview Image	Enable Aiming Tool
Development Mode	TAS Center Settings	Get Health Infomation	Check Realtime Status
Hardware Status	WIFI Management	Health Monitor Setting	Setting Send Email Ale
ReaperXD Settings	Wireguard Setup	Auto Upgrade Settings	Web Page
GSM Status/Control	ARP	FTP Upload	L5F/L5M Settings
RHD Settings			

3 In the **WireGuard Setup** window, select the Public IP address of the VLP and click **Enable**. Figure 18: WireGuard Public IP Address

Wireguard Setup		>
Status: Public IP Address:	Inactive. Enable 192.168.5.150	e
Configuration Files		Del

4 In the Select Client drop down menu, select the client being configured and click Get.

Figure 19: WireGuard Select Client

Wireguard Setup		>	×
Service			_
Stat	is: Active.		
Public IP Addre	s:	- Disable	
Configuration Files			7
Select client	lient1	Get Del	
PrivateKey=cCVy8uj ListenPort=51820 Address= 10.0.0.2/j [Peer] PublicKey=vdYR8Hik Endpoint=192, 168,5 AllowedIPs=10.0.0,	AkI5X3SOzvWObMTlUIexhps) 24 2UVEEWHL +J6M6YuEAnJpGH . 150:51820 I/32	XgSVlCVoulT3c= laNtjO2Z7syy2Y=	

5 Highlight the text that appears in the lower portion of the window and copy the text with Ctrl+C.



NOTE: You can configure up to three VPN clients. For only one client, leave the first default **client1** selected.

2.3 **Configuring WireGuard**

Procedure:

- 1 Open the WireGuard window.
- 2 Click the down-arrow next to Add Tunnel at the bottom of the window and click Add Empty Tunnel.

Figure 20: Add Tunnel

🕹 Add Tunnel 👻 🗙				
_	Import tunnel(s) from file Ctrl+O			
	Add empty tunnel Ctrl+N			

- 3 In the **Create new tunnel** window that opens, enter a name for the tunnel connection in the **Name** field.
- 4 Delete the existing text in the lower text window and press **Ctrl+V** to paste the text copied earlier from the WireGuard Setup window.
- 5 Click Save.

Figure 21: Create New Tunnel

🔆 Create n	new tunnel	<		
Name:	VPN_Client1]		
Public key:	8+ODDyKX9ue1qe6ewNYwKR0mwgAVlCtcD9s1tZ8Xfw4=			
[Interfac PrivateKe ListenPor Address= [Peer] PublicKey Endpoint: AllowedII	e] ay=cCVy8ujAkI5X3SOzvWObMTlUIexhpsXgSVlCVoulT3c= t=51820 = 10.0.0.2/24 r=vdYR8HilQUVEEWHL+J6M6YuEAnJpGHaNtjO2Z7syy2Y= =192.168.5.150:51820 Ps=10.0.0.1/32			
	Save Cancel			

6 To connect WireGuard to the VLP VPN, click Activate.

Figure 22: Connect WireGuard to VLP VPN

VPN_Client1	Interface: VPN	V_Client1			
	Status:	Active			
	Public key:	8+ODDyKX9ue1qe6ewNYwKR0mwgAVI0	tcD9s1tZ8Xf	w4=	
	Listen port:	51820			
	Addresses:	10.0.2/24			
		Deactivate			
	Peer				
	Public key:	vdYR8HilQUVEEWHL+J6M6YuEAnJpGH	aNtjO2Z7syy	/2Y=	
	Allowed IPs:	10.0.0.1/32			
	Endpoint:	192.168.5.150:51820			

If the connection is successful, the Status will change to Active. A Windows notification window will also appear.

2.4

Testing the VPN Connection

Procedure:

1 In Windows, open a Command Prompt window.

2 Type "ping 10.0.0.1" and press **Enter**.

If the VPN connection to the VLP is active and configured correctly, ping replies from the VLP appears. Type **http://10.0.0.1** into a web browser to access the VLP WebUI from the new tunneled Public IP.



NOTE: If using the client2 or client3 profile in the WireGuard Setup window use 10.0.0.3 and 10.0.0.4 respectively to test on the VPN tunnel connections.

WebUI Setup

The VLP WebUI is a web-based version of the UbuntuHD Control Windows software. It runs directly on the VLP and can be accessed by any computer that has a web browser and a LAN or Internet connection without the need to download and run the UbuntuHD Control software.

This section describes some of the more common tools and configuration options available for WebUI setup.

Figure 23: WebUI Main Page



3.1 Logging In to the WebUI

Prerequisites: Connecting to a remote VLP requires an active VPN connection. Refer to VPN Configuration on page 20 for instructions on connecting to a remote VLP unit. Refer to UbuntuHD Control Setup for instructions on connecting to the VLP over a local LAN connection.

Procedure:

- 1 Open a web browser window and enter the IP address of the VLP into the address bar.
- 2 Enter the following default WebUI login credentials:
 - Username: VLP5200
 - Password: Moto4ever!

Figure 24: LPR Web Control Sign In

LPR Web Control Sign In User Name		
Password		
Remember my username		
Sign in		

3 Select the desired camera and click Connect.

Figure 25: Select Camera

Select camera	a before con	ne
Camera 4 🔺	Connect	
Camera 1	n	
Camera 2		
Camera 3		
Camera 4		
Camera 5		
Camera 6		

hafe . ect

If the selected camera is connected, the IR and Color video feeds will appear.

3.2 VLP Controls Overview

This section contains configuration and diagnostic tools for the VLP unit.

Figure 26: VLP Controls



3.2.1 Enabling or Disabling Engine

Procedure:

1 To start or stop the Optical Character Recognition engine (license plate detection) on the VLP while troubleshooting or testing, use the **Enable/Disable Engine** buttons.

Figure 27: Enable/Disable Engine



3.2.2 Configuring Zone Settings

Capture zones allow you to mask off sections of the camera stream that should not be captured and highlight areas that are more likely to have license plates in them.

Procedure:

1 To create capture zones for the IR and Color camera streams, use the **Zone Settings** menu.

6

NOTE: License plate detection will only occur inside the capture zone border.

Figure 28: Zone Setting



- 2 To start a capture zone border line, click on a camera feed.
- 3 Click on another point on the camera feed to complete each border line.
- 4 Continue clicking to form the border of the capture zone.
- 5 After creating at least two lines, click the starting point to complete the capture zone.

3.2.3 Upgrading Firmware

Procedure:

- 1 Download the latest VLP firmware from: https://sites.google.com/motorolasolutions.com/vaassoftware.
- 2 To install a new firmware version onto the VLP, use the Update Engine menu.



NOTE: Only use valid firmware files received from Motorola Solutions or vaasfiles.com to update firmware.

Figure 29: Update Engine

Choose F	ile No file chosen
Update	Close

- 3 Click the Browse button locate the file and click Update to install the Firmware.
- **4** Wait for the Firmware Install process to complete before closing the browser window. When complete, the VLP will restart.



NOTE: Do not interrupt power or turn the VLP off during the firmware update!

3.2.4 Changing Source Type

Procedure:

To configure the connection and login information for the camera currently selected at the top of the WebUI main window, use the **Change Source Type** menu.

Figure 30: Change Source Type

amera Name (for LEA	R Uploading)	
Camera 4		
/ideo Source	Configuration	
Enable	-	
ource type		
L5F camera		•
ddress		
192.168.3.104		
Port		
80		
Isername		
assword		
n/Out		
Front Car Is In		•
Profile		
/ideo		

Following are the description for each field:

Table 3: Change Source Type Fields Description

Field	Description
Camera Name	The identifier that the camera will be referred to as in LEARN.
Source Type	This drop-down is used to select the camera or stream type for the video feed.
Address	The IP Address to connect to for the current- ly selected camera. By default for ReaperHD cameras, the number in last octet corre- sponds with the camera number selected in the WebUI main window (192.168.3.101 108)
Port	The port associated with the camera or stream. Default is the HTTP port 80. Other commonly used ports are: RTSP: 554 and HTTPS: 443 for other camera types.
Username/Password	Login credentials for the selected camera can be entered here if required. ReaperHD and L5F/L5M cameras do not require cre- dentials by default.

Field	Description
In/Out	Designates this camera in PlateSearch as monitoring the entrance or exit of a location.
Profile	Specify a desired camera profile name here if needed. By default, this can be left blank.
Video	Fill in this field if using a video server.

3.2.5 Resetting DSP

Procedure:

- 1 To perform a hardware reboot of the VLP, use the **Reset DSP** button.
- 2 Click Yes in the confirmation window and the VLP will reset.



NOTE: The WebUI will disconnect until the VLP resets. Refresh the browser window if the WebUI does not load.

Figure 31: Reset Confirmation

Confirm

Are you sure you want to reset?



3 Upon reboot, click Connect to reconnect to the VLP.

3.2.6 Changing IP

Procedure:

To modify the IP addresses of the VLP's two network adapters, use the Change IP button.

By Default,

- eno1 is the adapter for the LAN 1 Ethernet port (192.158.5.150).
- br0 is the adapter for the LAN 3-10 PoE ports (192.168.3.200).
- The Wi-Fi adapter's IP address is 10.42.0.1.

By default, ReaperHD cameras connected to the VLP's PoE ports are on the <192.168.3.xxx> subnet.

Figure 32: Change IP

	Interface information
eno1	Орнср
br0	Static
wg0	Ip Address
	192.168.5.150
	Subnet mask
	255.255.255.0
	Default gateway
	Preferred DNS Server
	Alternate DNS Server
	Write to board Close

Table 4: Change IP Interface Information

Field	Description
IP Address	The desired IP address for the currently se- lected adapter.
Subnet Mask	Subnet mask for the entered IP address.
Default Gateway	By default, this field can be left blank.
Preferred DNS Server	By default, this field can be left blank.
Alternate DNS Server	By default, this field can be left blank.

3.2.7

Configuring Wi-Fi Management

Use the Wi-Fi Management window to configure the Wi-Fi adapter of the VLP. The VLP can be configured as a Wi-Fi hotspot to connect to for remote access, or it can connect to other Wi-Fi hotspots for Internet or network access.

Procedure:

1 To connect to a Wi-Fi network, double-click on an entry in the Radio Status list and enter a password if required.

The Radio Status list shows available Wi-Fi hotspots to connect to.

The Wi-Fi Devices list shows any devices connected to the hotspot of the VLP.

Figure 33: Wi-Fi Management

Radio Status				
In Use	SSID	Signal	Security	BSSID
	sbasys	85	WPA2	D8:50:E6:59:1A:F0
	SBG8300-1C21	72	WPA2	84:BB:69:68:20:55
	SBG8300Guest-1C21	69	WPA2	86:88:69:68:20:25
	whiterabbit	65	WPA2	44:10:12:0A:DE:BE
	Nacho hifi	62	WPA2	F4:C1:14:B6:05:08
	DIRECT-7C-HP OfficeJet 3830	62	WPA2	C4:65:16:5C:FE:7D
	housewifi_EXT	59	WPA1 WPA2	CC:32:E5:A8:26:8C
	Hotel 1 California	59	WPA2	A8:70:5D:9D:51:B3
	NETGEAR19	55	WPA2	08:36:C9:8A:82:A1
	NETGEAR28	55	WPA2	94:A6:7E:7E:CC:27
	Master-Guest	55	WPA2	9E:C9:EB:EE:90:55
	housewifi	49	WPA1 WPA2	66:32:B1:FB:1A:89
Double cli	ick on entry to connect/disconect			
Internet Mode				
SSID				
VI P.COM	4S			
Key				Disable
7tM8L1G/t)			
				Randomize
Close				

- 2 To create a hotspot, enter a desired name for it into the SSID box and click **Enable**.
- 3 To create a password for the hotspot, enter the password into the Key box or click **Randomize**.

3.2.8 Configuring a LEARN Connection

Use the LEARN window to configure the VLP to upload LPR detections to LEARN.

Procedure:

- 1 If you have a LEARN .ini file, click Get File to select and install it.
- 2 To check if detections made by this system are recognized by Agency Hot Lists, toggle on Enable Hot List.



NOTE: When configuring users in LEARN, make sure all are configured before downloading the .ini file. Use only one .ini file per site. Only one user account per site is needed regardless of how many cameras are connected.

- 3 Enter your LEARN credentials.
- 4 Click the **Test Connect** button to test the connection to the LEARN server.

Figure 34: VLP LEARN Window

Jpload to LEARN
Enable Server Address
https://learn-nvls.com/learn
SSL Version
SSLV23 ·
Username
justin.bull@motorolasolutions.com
Password
Agency
MSI Technical Writing
System
Test System
Num Buffer
0
Enable Learn Mill Comera
Shald CPS Configuration (Not for V/I D)
Longtidue
-121.768049
Latidue
37685994
nable Hotlist
Enable
Time check hotlist
100
Enable check plate 2
Enable Separate Image To VBD
Enable Separate Image To Amazon S3
Upload Data for YMS India
Test connect Get file Save Change Close

Table 5: VLP LEARN Field Description

Fields	Description
Server Address	Enter the LEARN server address here. The default is https://learn-nvls.com/learn.
SSL Version	Default is SSL V23.
Username/Password	Enter your LEARN credentials here.
Agency	Enter your LEARN Agency here.
System	Enter the system name that this VLP is known by in LEARN.
Num Buffer	The number of records to store before up- loading. Default is 100.
Enable LEARN Multi-Camera	Check this box if there is more than one camera being used with this VLP.
Enable Hot list	Click this switch to enable checking detec- tions against any present hot lists from the selected agency in the Agency field.
	NOTE: To enable Hot List, Up- load to LEARN must first be ena- bled.
Time check Hot list	Time until the next hot list synchronization in seconds. Default is 10000.
Enable Check Plate 2	Check this box to enable checking hot lists against secondary LPR images.

3.2.9 Getting Log Files

Procedure:

To generate and download a log file for the VLP containing diagnostic information, click the **Get Log** button.

Figure 35: Get Log



A .rar file will automatically be downloaded to your browser's download folder. Log files are useful for diagnostic purposes and are sometimes requested by Motorola Solutions support for troubleshooting.

3.2.10 Generating Health Information

Procedure:

To open the **Health Information** window and view various statistics about the current configuration of the VLP, use the **Get Health Information** button.

Useful fields include IP Address, Firmware Version, GPS Coordinates, License Status, and LEARN Connection Status.

Figure 36: Health Information

Health information	
	IP Configuration:
	Current IP address: 192.168.5.150
	Subnet Mask: 255.255.255.0
	Gateway: 0.0.0.0
	DNS Setting: 0.0.0.0
	Hardware information:
	Serial Number: S2190620221
	MachineID: 1D5674278583C913878B2A3FB4D06518
	Operating System Information:
	Kernel Name: Linux
	Kernel Release: 5.4.0-58-generic
	Hostname: vlp
	Operating System: GNU/Linux
	Machine Hardware: x86_64
	Firmware version: 4.1.195.1 (202111111500)
	Engine Profile: ()
	License status: Licensed
	Learn Account Information:
	Server address: https://learn-nvls.com/learn
	Username: justin.bull@motorolasolutions.com
	Agency: MSI Technical Writing
	System: Test System
	Buffer used: 0% of 0.080 GB
	Location's timezone: GMT+07:00
	Hotlist: 0
	Ruby Engine:
	GBase Version: 1.0.20000101010100000
	Date lime:
	Current time: 2021/11/20 08:01:49
	GMT time: 2021/11/20 01:01:49
	Time zone: Asia/Bangkok (+07, +0700)
	Uptime: 02:01:59
	GPS CODFUINATES:
	Latitude: 0.00000000000
	Total plate in learn queue: A
	Total HIT in learn queue: 0
	Scans unload status:
	Joans uproau Status:
	Number of times the samera heated in its lifetime: 22
	Number of times the camera booted in its iffetime: 23

3.2.11 Unlocking License

The Unlock button allows you to upload a license file to the VLP and unlock it for use.

Procedure:

1 To display the machine ID of the VLP, use the **Get** button.

Machine IDs can be provided to Vigilant support to obtain license files.

Figure 37: License

MachinelD		
1D5674278583	Get	
License File Choose File No	file chosen	
Unlock Rer	nove Close	

- 2 To select a license file, click **Browse**.
- 3 Once the license file has been uploaded, click Unlock.

3.3 Camera Controls Overview

Click the **ReaperHD Camera Controls** or **L5F Camera Controls** tab to view configuration and diagnostic tools for connected cameras.

Figure 38: ReaperHD Controls Tab



Figure 39: Reaper HD Camera Controls



Figure 40: L5F Controls Tab



Figure 41: L5F Camera Controls



3.3.1 Resetting Camera

Procedure:

- 1 To reset just the currently selected camera, use the **Reset Camera** button.
- 2 Choose Confirm to reset the camera. Figure 42: Reset Camera

Confirm

Are you sure you want to reset?



3 After receiving a reboot notification, click **Connect** again to reconnect to the camera.

3.3.2 Upgrading Firmware

Procedure:

- 1 Download the latest camera firmware from https://sites.google.com/motorolasolutions.com/vaassoftware.
- 2 To upgrade the selected firmware of the camera, click the **Upgrade Firmware ReaperHD** button.

Figure 43: Upgrade Firmware ReaperHD



NOTE: Only use valid firmware files received from Motorola Solutions Support to update firmware.

3 Select a valid firmware file and click Update.

3.3.3 Changing Camera IP

Procedure:

1 To change the IP address of the selected camera, use the Change Camera IP tool.



NOTE: By default, cameras have DHCP enabled. To view the IP address of the selected camera when DHCP is enabled, use the **Get health camera** button.

Figure 44: Change IP

DHCP		
O Static		
Hostname		
p Address		
		Check IP
Subnet mask		
Default gateway		
DNS Server		

Following are the description for each field:

Table 6: Change IP Fields Description

Field	Description
DHCP/Static	Select Static to specify an IP address. De- fault is Static .
Hostname	A hostname can be specified here. Default is eth0 .
IP Address	Cameras connected to the VLP will always have a LAN address (<192.168.xxx.xxx>). By default for ReaperHD cameras the IP is in the range <192.168.3.101> to <192.168.3.108>.

Field	Description
Subnet Mask	Subnet mask for LAN IP addresses is al- ways <255.255.255.0>.
Default Gateway	By default, this field can be left blank.
DNS Server	By default, this field can be left blank.

3.3.4 Unlocking Camera

This feature allows you to upload a license file to the camera and unlock it for use.

Procedure:

1 To display the machine ID of the camera, use the **Get** button.

Figure 45: Unlock Camera

License status	
MachinelD	
	Get
License File	
Choose File No file chosen	
Unlock Remove Close	



NOTE: Contact Vigilant Support and provide the Machine ID to obtain a license file.

- 2 To select a license file, click Browse.
- 3 Once the license file has been uploaded, click Unlock.

3.3.5 Generating Camera Health Information

Procedure:

To open the **Health Information** window and display statistics specific to the currently connected camera, use the **Get Health Camera** button.

Figure 46: Camera Health Information

```
IP Configuration:
       Current IP address: 192.168.3.103
       Subnet Mask: 255.255.255.0
       Gateway: 192.168.3.254
       DNS Setting: 192.168.3.1
Hardware information:
       Bar Code Number: 40916-50767
       MachineID: 7D88AE982D1BD92A0654F72ABD324B4E
       Current ALS Value: 263
       Camera Revision: 1
Operating System Information:
       Kernel Name: Linux
       Kernel Release: 4.9.79-v7+
       Hostname: raspberrypi
       Operating System: GNU/Linux
       Machine Hardware: armv71
Firmware version: 1.0.060719.1100
License status: Licensed
Current time: 2018/09/28 23:17:13
Uptime: 01:00:15
Number of times the camera booted in its lifetime: 433
```

3.3.6 Getting Camera Log Files

Procedure:

To generate and download a log file for the currently selected camera, click Getlog Camera.

Chapter 4

TAS for WebUI Setup

Target Alert Service (TAS) is an alerting system for Vigilant Solutions camera systems that will check incoming license plate scans against hot lists received from LEARN. An alert is generated in the TAS application when a hot list plate is read by a camera.

4.1

Downloading the TAS Client

Prerequisites: To use TAS, an active PlateSearch user account and a configured camera system are required to connect the VLP to PlateSearch through the WebUI.



NOTE: PlateSearch credentials and System Names are generated by Motorola Solutions support from a processed sales order. Contact your Agency Manager to obtain this information.

Procedure:

- 1 In the PlateSearch portal, log in with your Username and Password.
- 2 Click PlateSearch→My Profile.
- 3 Click on the download icon next to the **Target Alert Service (TAS)** check box and click **Yes** when prompted.



NOTE: The TAS Client software must be installed and running on the computer intended to receive TAS alerts.

Figure 47: Vigilant PlateSearch User Profile

Alert Management		
Email Service	🔘 HTML	🔵 тхт
Receive Historical Hit		
Target Alert Service (TA	s) 💶	
Mobile Companion (MC)	. <u>.</u>	
Single Plate Scanner		
Multi-Plate Scanner		
LEARN Mobile		
Single Plate Scanner		
Mobile Hit Hunter (MHH)		
Filter Alerts:	Configure	
Allow Secondary Plate	Aatching	
Ignore Out-of-State Aler	s Configure	
Geographic Zoning:	Status: In Us	e
State Selection:	County Selection:	
AK 🔶	All	
AL		
AR		
Metropolitan Area:		
Abbeville,LA		A
Aberdeen, SD		
Aberdeen,WA		-

- 4 Ensure that the check box next to **Target Alert Service (TAS)** under Alert Management is checked.
- **5** Check the Agency Name and ensure it matches the supplied information.
- 6 If any of the profile information needs to be updated, click the **Update** button when finished.

4.2 Configuring LEARN Connection in WebUI

Procedure:

1 Open a web browser and connect to the VLP with the WebUI (192.168.5.150) and click **PlateSearch**.

- 2 Check the Enable check boxes under Upload to LEARN and Enable Hotlist.
- **3** Populate the following fields with the respective PlateSearch login credentials and system information.
 - Server Address: https://learn-nvls.com/learn
 - Username
 - Password
 - Agency
 - System
- 4 Click the Test Connect button.

Figure 48: VLP PlateSearch Window

Upload to LEARN
Enable
Server Address
https://learn-nvls.com/learn
SSL Version
SSL V23
Username
justin.bull@motorolasolutions.com
Password
Agency
MSI Technical Writing
System
Test System
Num Buffer
0
Enable Learn Mutti Camera
Shield GPS Configuration (Not for VLP)
Longtidue
-121.768049
Latidue
37.685994
inable Hotlist
Enable
Time check hotlist
100
Enable check plate 2
Enable Separate Image To VBD
Enable Separate Image To Amazon S3
Upload Data for YMS India
Test connect Get file Save Change Close

- 5 Click OK once the The operation completed successfully message appears
- 6 Click Save Change and close the window.
- 7 Click the TAS Center Setting button.



NOTE: An active connection to PlateSearch is required to configure TAS. See Configuring the TAS Client for instructions on configuring a LEARN connection.

8 Check the Enable check box and enter 1234 into the Listen Port field.



9 To manage TAS users, click User→Add User.

Figure 49: TAS Center Setting

	Tas Cent	er Setting					
		inable					
	Listen Po	ort					
	1234						
	User	r					
						OK Cancel	
UseriD	UserName	Status	Force receiver component	Permission by camera	Permission by alert	Actions	
8	Test_User	Active	No	AL	AL	Edit Permissio	ns Delete
Add User	Export template Expo	ert Import	Cancel				

10 Click the Active radio button and create a Username and Password for the TAS user. Click OK. Figure 50: Add TAS User

Edit User			
	Active		
	Username		
	Test_User		
	Force Receiver Comment		
	Password		
	Confirm Password		
		ОК	Cancel

11 After a user has been created, use the **Permissions** button to assign which cameras and hot list types that will send alerts to the configured user.

Figure 51: TAS User Permission

Users							Q
				Perm	issions		
UseriD	UserName	Status	Force receiv	~	All	 AL AL	Actions
8	Test_User	Active	No	2	Camera 1	 Abandoned Vehicle	Edit Permissions Delete
				2	Camera 2	 Amber Alert	
Add User	Export template Export	Import	Cancel	~	Camera 3	 Armed Robbery	
				~	Camera 4	 Assault	
				~	Camera	 Battery Assault	
				~	Camera	 Capias Warrant	
						 Car Jacking	
						 Child Abductor	
						 Deported Felon	
						 Disorderly Conduct	
						 Expired	
						 Felony Theft	I
						 Felony Warrant	
						 Fugitive	
						 Garig Member	
						 🖌 Hit & Run	
						 Law Enforcement Suspect	
						 Mindemeanor	
						 Missing Person	
						 Narcotics	
						Update Cancel	

4.3 Configuring the TAS Client

Procedure:

- 1 To install the TAS software, navigate to the TAS_Installer.msi file.
- 2 Open the software and click Yes.
- **3** Follow the on-screen instructions to install the software. When the installation is complete, the TAS software will open.
- 4 Click the **TAS Server** tab to configure the connection.

Figure 52: TAS Server

TARGET ALERT SER	/ICE			- 0
Preferences TAS Server	Stored Alerts	8 Vehicle Recovery		C Run in Background
Start TAS with computer			Force Pop-Up Priority	
Play Sound file with Alert	Audio Settings		Suppress Duplicate Hits	AIILPR Systems • 3 Im
20 • Number of Records to Store			Save Pop-Up Location	Default Pop-Up Location
Ignore Alerts older than	20 jm		Night Mode Starts	17.00 0 to 06.00 0
Show All Suppress Hits			Night Mode On	
Proxy Settings				
	O Apply	× Cancel		
• TAS	SERVICE IS CURRENTLY: OFF	VERSION 4.0.20200311.1700		

- 5 Click the New button to add a new TAS source.
- 6 In the **TAS server connection** drop-down menu, select **CDFS Server**. Populate the remaining fields and click **Apply**.

Following are the description for each field:

Table 7: TAS Server Fields Descriprion

Field	Description
Name	Create a reference name for the new TAS data source. (Optional).
IP/Hostname	The IP address of the VLP server. Use 192.168.5.150.
Username	The TAS user Username created in step 10.
Password	The TAS user Password created in step 10.
Port	The TAS applications listening port. Use the default of 1234.

Figure 53: Add Source

🕱 TAS			
TARGET ALERT SERVI			x
Preferences	TAS server connection	CDFS Server -	C Run in Background
ST NAME	NAME IPA-DSTNAME USER NAME PASSWORD PORT	V.P. TAS SERVER 1021685150 Berter 	FORCE RECEIVER COMMENT
	Connect	Edit Delete	
• TAS	SERVICE IS CURRENTLY: OFF	VERSION 4.0.20200311.1700	

- 7 Click VLP TAS SERVER→Connect.
- 8 Check to the left of the entry for a check mark indicating that TAS is now connected to the VLP.

Figure 54: Connect to TAS Server

JL IAS					- 0
TARG	ET ALERT SER	VICE			
O Pre	ferences AS Server	Stored Alerta	B Vehicle Recovery		Run in Background
ST	NAME	IP ADDRESS/ URL	USER NAME	PORT	FORCE RECEIVER COMMENT
~	VLP TAS SERVER	192.168.5.150	Barter	1234	No
		Dimment	a News	Delete	
		Disconnect	n Ivew	Unione	
TAS		SERVICE IS CURRENTLY: ON	VERSION 4.0.20200311.1700		

9 TAS alerts will now automatically appear and play a sound when a hotlist license plate is read by the target VLP system. Click the **Save** button to save the alert and view it later.

Figure 55: TAS Alert





NOTE: To generate an alert, a plate must be on a hot list uploaded to (or shared with) the agency of the PlateSearch user being configured. Only agency managers can manage hot lists.

Figure 56: Stored Alerts

TARGET ALERT SERVICE						
	SS PLATE	ALARM	AUTHORIZED	UNAUTHORIZED	MISSING PLATE	DETECTED TIM
4	4PFR572	Vigilant_Test Vigilant_Test				08-06-2020 07:49 PM (UT 08-06-2020 07:44 PM (UT
3	4PFR572 4PFR572	Vigilant_Test Vigilant_Test				08-06-2020 07:33 PM (UT 08-06-2020 07:29 PM (UT
1	4PFR572	Vigilant_Test				08-06-2020 07:26 PM (U
<						>
• TAS		SERVICE IS	CURRENTLY: ON V	ERSION 4.0.20200311.1700		

10 To view the saved alerts, click Stored Alerts tab.