County of San Diego

JOHN M. PELLEGRINO
DIRECTOR

DEPARTMENT OF PURCHASING AND CONTRACTING
5560 OVERLAND AVENUE, SUITE 270, SAN DIEGO, CALIFORNIA 92123-1204
Phone (858) 505-6367 Fax (858) 715-6452

ALLEN R. HUNSBERGER
ASSISTANT DIRECTOR

December 14, 2020

NOTICE OF REJECTION OF ALL BIDS

LICENSE PLATE READER – (RFB 10493)

The County of San Diego is rejecting all bid submittals for RFB 10493 and will be issuing a new bid on BuyNet under RFB 10684. Per RFB 10493, Section B - Instructions for Completing and Submitting Bid and Pre-Award Survey Requirements; C – Evaluation and Award, # 5 states "5. The County reserves the right to reject any or all bids and to accept or reject any item(s) thereon or waive any informality in the bid." The County of San Diego is exercising this right and is rejecting all bids.

For questions regarding this notification, please contact Assistant Procurement Specialist Punnita Dinmuong at: punnita.dinmuong@sdcounty.ca.gov.

Punnita Dinmuong

Punnita Dinmuong, Assistant Procurement Specialist
Department of Purchasing and Contracting

SOLICITATION:	10493	OPENING DATE:	Thursday, November 5, 2020
PROJECT:	License Plate Reader		

BIDDER	BASIS OF AWARD
FLOCK SAFETY	$108,500.00 Non-Responsive Revised Date: 11/13/2020
MOTOROLA SOLUTIONS	$130,015.00
NEOLOGY	$290,760.00
PORTABLE COMPUTER SYSTEMS	$183,725.02
REKOR	$153,922.00
UTILITY ASSOCIATES	$287,880.00

Date: 11/5/2020 Bid Officer: Diane Padilla Bid Clerk:

This Notice of Intent to Award / Abstract ONLY indicates the APPARENT low bidder. Conditions that may displace an apparent low bidder include, but are not limited to: math errors, conditioning of bid, mistake in bid, failing pre-award Survey, and the bid being non responsive.

SOLICITATION:	10493	OPENING DATE:	Thursday, November 5, 2020
PROJECT:	License Plate Reader		

BIDDER	BASIS OF AWARD
FLOCK SAFETY	$108,500.00
MOTOROLA SOLUTIONS	$130,015.00
NEOLOGY	$290,760.00
PORTABLE COMPUTER SYSTEMS	$183,725.02
REKOR	$153,922.00
UTILITY ASSOCIATES	$287,880.00

Date: 11/5/2020 Bid Officer: Diane Padilla Bid Clerk:

This Notice of Intent to Award / Abstract ONLY indicates the APPARENT low bidder. Conditions that may displace an apparent low bidder include, but are not limited to: math errors, conditioning of bid, mistake in bid, failing pre-award Survey, and the bid being non responsive.

Bids Received

County of San Diego

JOHN M. PELLEGRINO
DIRECTOR

DEPARTMENT OF PURCHASING AND CONTRACTING
5560 OVERLAND AVENUE, SUITE 270, SAN DIEGO, CALIFORNIA92123-1204
Phone (858) 505-6367 Fax (858) 715-6452

ALLEN R. HUNSBERGER
ASSISTANT DIRECTOR

October 22, 2020

COUNTY OF SAN DIEGO - REQUEST FOR BIDS (RFB # 10493)
SHERIFF'S DEPARTMENT
LICENSE PLATE READERS

The County of San Diego (County) has a requirement for License Plate Readers per the Statement of Work herein.

The contract term is anticipated to be an initial (base) period of one (1) year with two (2) one-year option renewals.

RFB CONTENT
This RFB package includes the following:
Transmittal Letter to Release the RFB # 10493

Section A – Cover Page (PC 600 Form) **(Submit with the bid)**
Representations and Certifications Form **(Submit with the bid)**
Indemnification Agreement **(Submit with the bid)**

Section B – Instructions for Completing and Submitting Bid and Pre-Award Survey Requirements

Section C – Sample Contract
Exhibit A – Statement of Work
Exhibit B – Insurance Requirements
Exhibit C – Pricing Schedule (Submit with the bid)
Exhibit D – Federal Grant Requirements

BID SPECIAL INSTRUCTIONS
The County will be temporarily changing procurement processes due to the social distancing and other requirements put in place in response to the COVID-19 virus. This RFB is posted on the BuyNet site with a solicitation type of RFP, to allow for the submission of electronic bids though BuyNet. Bids submittals by electronic upload through BuyNet will be accepted for this RFB; this is in addition to the currently available option of mail delivery. Bids will not be accepted by personal delivery. Bid openings will be conducted through a video feed using the WebEx platform instead of in person attendance. A link to the virtual WebEx meeting will be posted prior to the bid opening. Additional COVID-19 procurement information is available at: https://www.sandiegocounty.gov/content/sdc/purchasing/COVID-19_Updates.html

BID DUE DATE
Submit to the County of San Diego, Department of Purchasing and Contracting at **5560 Overland Avenue, Suite 270, San Diego, CA 92123-1204** in a sealed envelope or package clearly marked on the exterior with "RFB # **10493**" and the name and address of the Offeror prior to **11:00 AM, Local Time on November 5, 2020.**

Bids will be publicly opened at that time with the following link: https://sdcountyca.webex.com/sdcountyca/j.php?MTID=ma3b5b7182847ca8efa33e72cb2de989a

Late submission cannot be considered unless there was mishandling on the part of the County of San Diego purchasing staff. Submittals must be received at the Purchasing and Contracting front counter by the identified date and time. If utilizing a courier service or USPS, be advised that all courier service deliveries, including USPS, may be delivered to

COUNTY OF SAN DIEGO - REQUEST FOR BIDS (RFB # 10493)
SHERIFF'S DEPARTMENT
LICENSE PLATE READERS
SECTION A: COVER PAGE (P&C 600 FORM)

COUNTY OF SAN DIEGO
SECTION A-P&C 600 FORM
This is not an order

Issued: October 22, 2020

MAIL OR DELIVER TO:
COUNTY OF SAN DIEGO, RFB NO. 10493
DEPARTMENT OF PURCHASING & CONTRACTING
5560 OVERLAND AVE., SUITE 270
SAN DIEGO, CA 92123

AWARD WILL BE MADE TO THE LOWEST RESPONSIVE, RESPONSIBLE BIDDER BASED ON
[ ] ALL OR NONE
[ ] EACH LOT
[X] TOTAL PRICE
[ ] OTHER (SEE PRICING SCHEDULE)

UNSPSC commodity code: **461716.0000**

FOR INFORMATION, PLEASE CONTACT:
PUNNITA DINMUONG, ASSISTANT PROCUREMENT SPECIALIST
PUNNITA.DINMUONG@SDCOUNTY.CA.GOV

BID OPENING DATE: NOVEMBER 5, 2020
BIDS MUST BE RECEIVED AT THE ABOVE ADDRESS PRIOR TO 11:00 A.M. ON DATE OF BID OPENING.

PLEASE STATE YOUR LOWEST PRICE F.O.B. DESTINATION AND BRAND NAME OR TRADE NAME IF APPLICABLE.
(Please use typewriter or black ink)
YOUR ENVELOPE MUST INCLUDE RFB NO. 10493

DESCRIPTION

THE COUNTY OF SAN DIEGO (COUNTY), SHERIFF'S DEPARTMENT HAS A REQUIREMENT FOR LICENSE PLATE READERS IN ACCORDANCE WITH THE TERMS & CONDITIONS AND THE STATEMENT OF WORK REFLECTED HEREIN.

INITIAL TERM: DATE OF AWARD – OCTOBER 31, 2021
1ST OPTION YEAR: NOVEMBER 1, 2021 – OCTOBER 31 2022
2ND OPTION YEAR: NOVEMBER 1, 2022 – OCTOBER 31, 2023

PRICING SUBMITTED IS TO REMAIN FIRM FIXED FOR THE TERM PERIOD IDENTIFIED ABOVE. ALL ITEMS WITHIN EACH TERM PERIOD MUST BE PRICED TO BE CONSIDERED RESPONSIVE. AWARD WILL BE MADE TO THE LOWEST RESPONSIVE, RESPONSIBLE OFFEROR BASED ON THE TOTAL PRICE. OFFEROR WHO SUBMITS THE LOW BID WILL BE DEEMED RESPONSIBLE BASED ON THE RESULTS OF THE PRE-AWARD SURVEY.

ARE YOU ABLE TO COMPLY WITH ALL ITEMS SPECIFIED WITHIN THE SCOPE OF WORK? YES X OR __ NO

BIDDER ACKNOWLEDGES ADDENDUM NO. 1 | | 2 | | 3 | | 4 | | 5 | |

SUBJECT TO ACCEPTANCE WITHIN **90** DAYS

NAME AND ADDRESS OF BIDDER
Flock Safety
STREET, CITY, STATE, ZIP
1170 Howell Mill Rd NW Unit 210
Atlanta, GA 30318
TELEPHONE: NUMBER (949 901 - 1781
FAX TELEPHONE: ( )

E-MAIL: Alex@FlockSafety.com

PAYMENT TERMS NET **30** DAYS OR % DAY

NAME AND TITLE OF PERSON AUTHORIZED TO SIGN OFFER:

11/5/20
SIGNATURE OFFEROR DATE

PRINTED NAME: Alex Cotravesse

PRINTED TITLE: VP of Sales

NOTIFICATION OF AWARD

ACCEPTANCE AS TO ITEM(S) NUMBERED:

(VC NO.)

(THIS SECTION FOR COUNTY USE ONLY)
COUNTY OF SAN DIEGO
BY: _____ DATE: _____
JOHN M. PELLEGRINO, DIRECTOR
DEPT OF PURCHASING & CONTRACTING

TOTAL AMOUNT
P&C 600 Form

AWARD NO.

NAME AND TITLE OF CONTRACTING OFFICER

County of San Diego
Department of Purchasing and Contracting

REPRESENTATIONS AND CERTIFICATIONS

The following representations and certifications are to be completed, signed and returned with the offer (the term "offer" includes a bid, proposal, quote, statement of qualifications, or any other submission to provide goods and/or services).

1. BUSINESS TYPE

X For-profit ☐ Non-profit ☐ Government

2. INTERLOCKING DIRECTORATE

In accordance with Board of Supervisors Policy A-79, if Offeror is a non-profit and will be subcontracting with a related for-profit entity where an interlocking directorate, management or ownership relationship exists, Offeror must list all such entity(ies) on an attached separate sheet, and authorization must be sought from Board of Supervisors. If Offeror is a non-profit and does not submit such a list, Offeror certifies it has not entered into a subcontract relationship with a related for-profit entity.

List Attached? Yes ☐

3. BUSINESS REPRESENTATION

Offeror represents as a part of this offer the following information regarding the ownership, operation, and control of its business:

3.1. Are you a local business with a physical address within the County of San Diego? ☐ Yes x No

3.2. Are you certified by the State of California as a:

☐ Disabled Veteran Business Enterprise(DVBE)
Certification #: _____

☐ Small Business Enterprise (SBE)
Certification #: _____

3.3. Are you certified by the U.S. Dept Of Veterans' Affairs as:

☐ Veteran Owned Small Business (VOSB)
Certification # _____

☐ Service Disabled Veteran Owned Small Business (SDVOSB)
Certification # _____

3.4. Estimated percentage of work in this offer to be performed or fulfilled locally (within the geographic boundaries of the County of San Diego):100%

4. DEBARMENT, SUSPENSION, AND RELATED MATTERS

4.1. Offeror certifies to the best of its knowledge that neither it nor any of its officers:

4.1.1. Are presently debarred, suspended, declared ineligible, or voluntarily excluded from covered transactions by any state, local, or federal department or agency.

4.1.2. Have within a three (3) year period preceding this agreement been convicted of or had a civil judgment rendered against them for commission of fraud or criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or contract under a public transaction; violation of federal or state antitrust statutes; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;

4.2. Except as allowed for in Section 4.2.5, Offeror hereby certifies to the best of its knowledge that neither it nor any of its officers:

4.2.1 Are presently indicted for or otherwise criminally or civilly charged by a government entity (federal, state, or local) with the commission of any of the offenses enumerated in paragraph 4.1.2 of this certification;

4.2.2 Have within a three (3) year period preceding this agreement had one or more public transactions (federal, state or local) terminated for cause or default;

4.2.3 Are presently the target or subject of any investigation, accusation or charges by any federal, state or local agency or law enforcement, licensing, certification, ethics, or compliance body;

4.2.4 Are proposed for debarment by any state, local, or federal department or agency.

4.2.5 If Offeror is unable to certify Sections 4.2.1, 4.2.2, 4.2.3, or 4.2.4, it certifies that it has disclosed and attached to this Representations and Certifications the reason(s) it cannot do so. The disclosure must include the Section(s), specific relevant facts including dates, contracts, individuals involved, status of actions, and any other relevant information that prevent it from making the requested certification(s). The County reserves the right to disqualify an Offeror based upon information disclosed.

Disclosure Attached? Yes ☐

5. RELATED WORK

Offeror certifies to the best of its knowledge that, other than as disclosed in an attached separate sheet, it and its proposed subcontractors, agents, and consultants have not previously contracted with the County to perform work on or related to this project (e.g. preparing related studies or recommendations, components of the statement of work, or plans and specifications).

Disclosure Attached? Yes ☐

6. CURRENT COST OR PRICING

Offeror certifies to the best of its knowledge that cost and/or pricing data submitted with this offer, or specifically identified by reference if actual submission of the data is impracticable, are accurate, complete, and current as of the date signed below.

7. INDEPENDENT PRICING

Offeror certifies that in relation to this offer:

7.1. The prices in this offer have been arrived at independently, without consultation, communication, or agreement, for the purpose of restricting competition, as to any matter relating to such prices with other offerors, with any competitors, or with any County employee(s) or consultant(s) involved in this or related procurements;

7.2. Unless otherwise required by law, the prices that have been quoted in this offer have not been knowingly disclosed by the Offeror and will not knowingly be disclosed by the Offeror prior to opening, in the case of a bid, or prior to award, in the case of a proposal, directly or indirectly to any other Offeror or to any competitor or with any County employee(s) or consultant(s) involved in this or related procurements; and

7.3. No attempt has been made or will be made by the Offeror to induce any other person or firm to submit or not to submit an offer for the purpose of restricting competition.

8. ADDITIONAL DISCLOSURES

Offeror shall report in writing to the County Department of Purchasing and Contracting within five business days of discovering or having any reason to suspect any change in status as certified in the preceding paragraphs. Upon County's request, Offeror shall provide additional information supporting Offeror's Representations and Certifications. Offeror's obligations under this Section 8 shall continue until Offeror is no longer under consideration for award of a contract, or until termination or expiration of any resulting contract(s).

CERTIFICATION

The information furnished in Paragraphs 1 through 8 and in the accompanying offer is certified to be factual and correct as of the date submitted and this certification is made under penalty of perjury under the laws of the State of California.

Name: Alex Letourneau Signature: _____

Title: VP of Sales Date: 11/5/20

Company/Organization: Flock Safety

SUBMIT THIS FORM AS DIRECTED IN THE REQUEST FOR SOLICITATION DOCUMENTS OR WITH THE OFFER

COUNTY OF SAN DIEGO

NONDISCLOSURE INDEMNIFICATION AGREEMENT

IF OFFEROR SUBMITS EXHIBIT CONFIDENTIAL/PROPRIETARY, THE FOLLOWING NONDISCLOSURE INDEMNIFICATION AGREEMENT MUST BE COMPLETED, SIGNED AND RETURNED WITH THE OFFER

This indemnification agreement ("Agreement") is made and entered into by and between the County of San Diego ("County") and Offeror Company/Organization Name: Flock Safety ("Offeror") with reference to the following facts: _____

WHEREAS the County may receive a request for disclosure of Offeror's submission under the California Public Records Act, Government Code Section 6250, et seq.; and

WHEREAS, Offeror has included in its submission an exhibit entitled "*EXHIBIT – CONFIDENTIAL/PROPRIETARY*" containing records that Offeror has determined to constitute trade secrets or other proprietary information exempt from disclosure under the California Public Records Act; and

WHEREAS the County requires defense and indemnity from Offeror for the County's ongoing non-disclosure of Offeror's *EXHIBIT-CONFIDENTIAL/PROPRIETARY*;

NOW, THEREFORE, for good and valuable consideration and the mutual promises contained herein, the parties agree to the following:

1. The above recitals are incorporated herein by this reference.

2. Except as otherwise provided herein, the County will not release Offeror's *EXHIBIT-CONFIDENTIAL/PROPRIETARY* based on Offeror's representation that the records contained therein are proprietary and exempt from disclosure under the California Public Records Act and/or are trade secrets as that term is defined in Government Code Section 6250, et seq. Notwithstanding the foregoing, however, the County may release Offeror's *EXHIBIT-CONFIDENTIAL/PROPRIETARY* in the event of any of the following:
   a. Offeror fails to comply with the terms and conditions of this Agreement; or
   b. Offeror provides the County with written notice that some or all of the records may be released; or
   c. A court of competent jurisdiction orders the County to release the records and the County has exhausted or waived its appeal rights.

3. To the fullest extent allowed by law, the County shall not be liable for, and Offeror shall defend and indemnify County and its Board of Supervisors, officers, directors, employees and agents of County (collectively "County Parties"), against any and all claims, demands, liability, judgments, awards, fines, mechanics' liens or other liens, labor disputes, losses, damages, expenses, charges or costs of any kind or character, including attorneys' fees (whether incurred by County attorneys or attorneys employed by County) and court costs (hereinafter collectively referred to as "Claims"), related to Offeror's *EXHIBIT-CONFIDENTIAL/PROPRIETARY.*

4. Offeror waives any and all claims in law or equity and hereby releases the County Parties from any and all claims, deductibles, self-insured retentions, demands, liability, judgments, awards, fines, mechanics' liens or other liens, labor disputes, losses, damages, expenses, charges or costs of any kind or character, including attorneys' fees and court costs, which arise out of or are in any way connected to Offeror's *EXHIBIT-CONFIDENTIAL/PROPRIETARY.*

TO BE COMPLETED BY AN AUTHORIZED REPRESENTATIVE OF THE OFFEROR	
Offeror Company/Organization Name:	Flock Safety
Authorized Representative Name:	Alex Lastravesse
Authorized Representative Title:	VP of Sales
Signature:	Date: 11/5/20

1. BACKGROUND INFORMATION

1.1. The San Diego County (County) has a requirement for the purchase of Automatic License Plate Reader (LPR) camera systems.

2. SPECIFICATIONS

2.1. SECURITY

2.1.1. Must be compliant with California Senate Bill 34 (SB34). Flock Response: YES - Flock Safety is compliant with SB34 including the necessary auditing and security protocols around accessing the LPR System.

2.1.2. Single Sign-On (SSO) implementation options. Flock Response: YES - Flock Safety is able to support an number of SSO options including Active Directory, Okta, ADFS, Azure AD, and Google G Suite.

2.1.2.1. Security Assertion Markup Language (SAML) 2.0 compliance. Flock Response: YES – Flock Safety is compliant with SAML 2.0

2.1.2.2. Other SSO methods, such as Active Directory and Office 365. Flock Response YES – Flock Safety can support Active Directory and Azure AD (aka Office 365).

2.1.3. User and Entity Based Behavioral Analytics (UEBA) Flock Response: YES – Flock Safety uses UEBA based methods for detective anomalous behavior for security reasons.

2.1.4. Distributed Denial of Service (DDoS) protection Flock Response: YES – Flock Safety services have DDoS protection

2.1.5. Data sanitization and anti-malware prevention. Minimizing attack vectors throughout the LPR solution using a multi-layered approach Flock Response: YES – Flock Safety leverages a number of methods to ensure that all data and services are secure.

2.1.5.1. Anti-malware scanning and threat prevention with up to date signatures Flock Response: YES – Flock Safety completes anti-malware scanning and ensures up to date signatures

2.1.5.2. Alerts and notifications Flock Response: YES – Flock Safety has implemented alerting via a number of methods to ensure active response to any potential threats.

2.1.5.3. Input sanitization: All data coming into the system from users or application programming interfaces (API's) Flock Response: YES – Flock Safety ensures users and API based inputs are sanitized and meet the data structure/type criteria for the purpose.

2.1.5.4. White list of file types for attaching/uploading for all purposes Flock Response: YES – Flock Safety accepts a select list of file types for use across the system and requires strict adherence to the schema and data types.

2.1.5.5. File Contents Disarm and Reconstruction (CDR) Flock Response: YES – Flock Safety pre parses all files to ensure they meet the necessary schema and does not contain anything malicious.

2.1.6. Disaster Recovery

2.1.6.1. Data protection, backup, and recovery strategy Flock Response: YES – Flock Safety leverages a multi datacenter approach for both standard AWS services as well as AWS Gov Cloud instances. Backups are constantly being created and the system can be recovered from these backups.

2.1.6.2. Disaster recovery liability in case of catastrophic event YES – Flock Safety leverages a multi datacenter approach for both standard AWS services as well as AWS Gov Cloud instances. Backups are constantly being created and the system can be recovered from these backups.

2.1.6.3. California Consumer Privacy Act (CCPA) compliance YES – Flock Safety complies with the CCPA.

2.1.7. Contractor shall provide a secure, database encrypted and web-based system that provides real-time access to uploaded data. Flock Response: YES - All Flock Safety footage is uploaded to AWS with all CJIS stored in AWS Gov Cloud. Flock uses KMS based encryption for storing of all data in AWS and all data is encrypted on camera and in-transit.

2.1.8. Contractor shall allow authorized users access to LPR data in a number of LPR-specific dashboards. Flock Response: YES – Flock Safety provides a number of tools and dashboards that allow authorized users to access LPR data.

2.1.9. Dashboard will show LPR vehicle scans in an easy to read graphical format. Flock Response: YES – Flock Safety provides graph based analytics for individual license plates as well as for bulk data analysis of traffic patterns across all Flock Safety cameras.

2.1.11. LPR dashboard will show vehicle location, images captured and provide the ability to search using the license plate. Flock Response: YES - Flock Safety provided detailed information about the location, time, and vehicle captured to go along with the license plate. Flock Safety provides a powerful search experience for searching by License Plate number but also by vehicle characteristics, such as vehicle color, make, type, as well as, license plate type (i.e. paper plates) and the absence of a license plate.

2.1.12. Contractor shall provide an option to purge data at specified intervals or dates Flock Response: YES – Flock Safety purges all data at the end of the rolling retention period (start being 30 days). This occurs each evening for data that has expired that day.

2.1.12.1. Will have a notification process to assure compliance YES – Flock Safety can provide notification of purging of data

2.1.12.1.1. Provide notification of purge date. YES – Flock Safety can provide notification of purging of data including purge date

2.1.12.1.2. Provide confirmation and notification that specified data was purged. YES – Flock Safety can provide notification of purge completion.

2.1.13. Data uploaded will only be shared at the discretion of an administrator designated by the San Diego County Sheriff's Department. Flock Response: YES - The Sheriff's Department will determine who can assess the Flock System.

2.2. LPR CAMERAS

2.7.1

Contractor shall have LPR systems capable of being installed on a fixed object (i.e. light pole), marked patrol vehicles, covert vehicles and speed trailers. Flock Response: YES - Flock is a fixed LPR solution, which can be mounted on any virtually any Pole. Flock cameras can also be mounted on existing speed trailers provided by the SDCSD. Flock partners with Axon for providing an interconnected mobile LPR experience with the Flock Safety system.

2. Marked patrol vehicle camera mounting brackets must be compatible with Whelen, Code3, TOMAR, Federal Signal, Arjent S2 light bars. Flock Response: Flock partners with Axon for providing an interconnected mobile LPR experience with the Flock Safety system.

3. Cameras shall be self-illuminating Infrared (IR) for effective license plate image capture in a variety of weather and lighting conditions. Flock Response: YES – Flock Safety leverages IR for capturing plates during all weather and light conditions. Even when using IR, Flock Safety captures a full picture of the vehicle that is used to determine make, type, etc. During the day no IR is used and full color images of the vehicle are available.

4. LPR cameras shall be water-resistance with few moving parts that can be damaged. Flock Response: YES – Flock Safety's LPR cameras is sealed to IP66 standard.

5. LPR cameras shall have the ability to automatically capture all variations of California license plates, to include California dealer issued plates (paper plates). Flock Response: YES - Flock Safety's Vehicle Fingerprint technology provides the ability to capture paper plates as well as information on vehicles with no plates and/or covered plates.

6. Cameras shall have a dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle for verification purposes YES - Flock Safety's solution does not require the use of two lenses for capturing a full color image and license plate capture. License plate capture is done off of the full color image, therefore, requiring only one lens for both use cases.

7. Cameras shall be sealed to NEMA 6 (IP67) standards. Flock Response: Flock Safety's camera complies with IP66 standards. IP66 is "dust tight" and protected against heavy seas or powerful jets of water.

8. Dual lens cameras shall be capable of capturing up to 60 frames per second Flock Response: Flock Safety's camera functions with a variable FPS allowing for best capture of images in varying deployment scenarios

9. Cameras shall have the ability to adjust shutter, brightness, and gain settings to ensure a high-quality image regardless of weather or lighting conditions. Flock Response: YES – The Flock Safety camera constanstly calibrates itself including adjusting adjust shutter, brightness, and gain settings to ensure a high-quality image regardless of weather or lighting conditions.

10. The cameras shall be able to have a fixed focal point or target distance from the camera to the vehicle's license plate from 9 ½ feet to 30 feet. Flock Response: YES – The Flock Safety camera works across distances of 8-120 ft.

11. The camera shall be capable of various configurations to capture plates in any of the following modes depending on the configuration:

11.1. An adjacent lane on either side of the vehicle while driving through traffic and/or parking lots. Flock Response: Flock partners with Axon for providing an interconnected mobile LPR experience with the Flock Safety system.

11.2. Traffic in an adjacent lane while parked on the side of the shoulder of a roadway. Flock Response: Flock partners with Axon for providing an interconnected mobile LPR experience with the Flock Safety system.

11.3. Parked vehicles in parking lots. Flock Response: Flock partners with Axon for providing an interconnected mobile LPR experience with the Flock Safety system.

2.3.

2.3.1. Processor shall have a "self-trigger" mode to detect the presence of correctly mounted vehicle license plates in the camera's field of view for image capture from the camera Flock Response: YES – Flock Safety uses Passive Infrared (PIR) to detect motion and in turn triggering the capturing of footage. All footage is full color images which then is run through Flock Safety's Vehicle Fingerprint technology for reading the license plate. This approach allows Flock to capture vehicles without license plates and determine other attributes of the vehicle beyond just the license plate.

2.3.2. Processor's installed in vehicles shall be equipped with an intelligent Power Supply Unit (PSU) that provides for a safe start and shut-down each time the vehicle's ignition is turned on and turned off. Flock Response: Flock partners with Axon for providing an interconnected mobile LPR experience with the Flock Safety system.

2.3.3. Processor controls the power supplied to the cameras and provides video connection points for simplified system wiring. Flock Response: Flock partners with Axon for providing an interconnected mobile LPR experience with the Flock Safety system. Flock Safety's fixed LPR is installed almost exclusively with solar technology, to prevent expensive infrastructure needs.

2.3.4. Processor shall have at least four (4) LPR camera connections and multiple USB ports. Flock Response: Flock partners with Axon for providing an interconnected mobile LPR experience with the Flock Safety system.

2.3.5. Vehicle mounted processors shall meet the environmental conditions associated with being mounted in a trunk. Flock Response: Flock partners with Axon for providing an interconnected mobile LPR experience with the Flock Safety system.

2.4. <u>LPR SOFTWARE</u>

2.4.1. Application software shall be capable of running on a Windows based mobile computer. Flock Response: YES - Flock is 100% cloud based, and only requires access to the internet to function.

2.4.2. There shall be no Java programming or Java derivatives. Flock Response: YES – Flock Safety does not leverage Java or any Java derivates.

2.4.3. LPR system shall have real time alerting and the ability to program custom hotlist. Flock Response: YES – Flock Safety provides real time hotlist alerting from the CA SVS, NCIC, and custom hotlists. Custom hotlists can be configured by user, role, and even shared with other jurisdictions leveraging Flock Safety. Custom hotlists can be uploaded into the Flock Safety system via csv.

2.4.4. There shall be a secure login and password function on the LPR software; The user's access shall be controlled by an administrator designated by the San Diego County Sheriff's Department. Flock Response: YES – Flock Safety provides secure login functionality including MFA. All access is controlled by the administrator at the San Diego County Sheriff's Department.

2.4.4.1. API capable of integrating user defined active directory Flock Response: YES – Flock Safety has an API capable of integrating user defined active directories.

2.4.5. The software shall provide live, simultaneous display of all the following data:

2.4.5.1. The IR license plate image Flock Response: YES – Flock Safety provides an image of the license plate which is cropped from the full color image.

2.4.5.2. The license plate interpretation or system read. Flock Response: YES – Flock Safety leverages machine learning to provide a read of the license plate.

2.4.5.3. A corresponding color overview of the vehicle displaying the captured IR license plate. Flock Response: YES – Flock Safety provides a full color image of the vehicle as well as information about the vehicle via Flock's Vehicle Fingerprint technology. Additional info includes, color, make, type, plate type, and more

2.4.5.4. The date and time stamp. Flock Response: YES – Flock Safety provides the time and date stamp for all footage.

2.4.5.5. Identification of the camera capturing the image. Flock Response: YES – Flock Safety provides the information about the camera that captured the footage.

2.4.6. Software shall capture GPS coordinates for every recorded license reads Flock Response: YES – Flock Safety captures the GPS coordinates of the camera that captured all license plate reads.

2.4.7. Software shall have the ability to GPS stamp all the reads. Flock Response: YES – Flock Safety has the ability to GPS stamp all license plate reads.

2.4.8. Software will give a unique audible and visible alert when a wanted license plate is discovered. Flock Response: YES – Flock Safety provides both and audible and visible alerts when a wanted license plate is discovered. Additionally, Flock Safety can provide SMS and email based alerts.

2.4.9. The Alert Screen remains displayed until acknowledged by the user, and, while displayed, the system continues to process license plate data in the background. Flock Response: YES – All alerts continue to be displayed until acknowledged by the user, additionally additional reads will continue to be processed and alerted on in the background.

1. DEMONSTRATION OR SAMPLE

1.1. County reserves the right to request an on-site demonstration of the LPR camera system being bid or a sample be sent to determine if it meets the requirements stated. All specifications listed in the General Requirements shall be confirmed. All travel, demonstration supplies and/or shipping expenses shall be at the contractor's expense. Flock Response: Understood – Flock Safety is happy to provide on-site demonstration of the Flock LPR system.

2. INSTALLATION

2.1. Contractor shall provide the option to purchase systems as a "kit" that includes all hardware, wiring and software for standard installations. Flock Response: YES - Flock pricing includes all required hardware components to install the camera and associated solar panel (if needed). Based on locations selected by the Sheriff's department, the appropriate installation hardware will be included.

2.2. Contractor shall provide installation and warranty repair options on vehicles within San Diego County. Flock Response: Flock partners with Axon for providing an interconnected mobile LPR experience with the Flock Safety system.

2.3. Contractor shall provide a technician or representative to visit customer site for system start-up, configuration and commissioning of LPR system. Flock Response: YES – Flock Safety will complete all installation and maintenance as part of the purchase of the Flock Safety solution. This includes start-up, configuration, and commissioning, all which is minimal with the Flock Safety solution.

3. CUSTOMER SUPPORT

3.1.The Contractor shall provide technical advice and sales support within 72 business hours. Flock Response: YES – Flock Safety can provide technical and sales support in less than 72 hours.

6. TRAINING

6.1. The County reserves the right to request up to eight (8) hours of training at a San Diego County Sheriff's Department facility within 30 days of delivery at no additional charge. This is in addition to the requirement set forth in 4.3. Flock Response: Understood – Flock Safety is happy to provide as much training as is needed to support the San Diego County Sheriff's Department.

7. DELIVERY REQUIREMENTS

7.1. Delivery address:

San Diego County Sheriff's Department
Attn: Ivy Scites - Grants Unit
9621 Ridgehaven Court
San Diego, CA 92123

8. INVOICE

8.1. Invoices shall be sent to:

San Diego County Sheriff's Department
Attn: Ivy Scites - Grants Unit
9621 Ridgehaven Court
San Diego, CA 92123

8.2. Only new products shall be accepted. An LPR system that has been used in any way, refurbished, reconditioned, or gray market is unacceptable and will be rejected and returned. Flock Response: Understood

8.3. The County shall be given credit for damaged and returned items within five (5) business days. Flock Response: Understood

8.4. There shall be no restocking fees or other charges for returns of damaged or incorrect items. Flock Response: Understood

8.5. Deviations to the terms, conditions and/or specifications shall be conspicuously noted in writing by the respondent. Flock Response: Understood

9. LEAD TIME

9.1. Department requested deliver lead time: 60 days. Flock Response: Understood

BASE YEAR
DATE OF AWARD – OCTOBER 31, 2021

DESCRIPTION	MFG & MODEL	ESTIMATED QUANTITY	UNIT PRICE	TOTAL
Mobile LPR 1 camera system, dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle	Flock's Falcon-Annual Subscription	4	$2500	$10000
Portable LPR 1 camera system, dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle	Flock's Falcon-Annual Subscription	10	$2500	$25000
LPR Camera Mounting Brackets for Light Bar	Flock's Falcon does not mount on Vehicles	4	$0	$0
LPR Mounting for Portable system	Mounting Solution included	10	$0	$0
LPR Processor	Included	14	$0	$0
Modem	LTE chip and data included	14	$0	$0
LPR Software	Included with unlimited licenses	14	$0	$0
LPR Speed Trailer complete package	Flock Falcon-to be mounted on existing trailer-Not a new trailer	1	$0	$0
Start-up, configuration, and commissioning of LPR Systems at Sheriff's facility to include all expenses such as travel	Included	14	$0	$0
Installation	One time installation cost per camera	14	$250	$3500
Covert Installation in vehicle	N/A	1	$0	$0
Installation "Kit", Includes all hardware, wiring and software for "do it yourself" standard installations (on poles & trailers)	Included in subscription-Flock will provide required hardware for solution of choice (trailer or Pole) Solar or wired.	14	$0	$0
Training	Included	8	$0	$0
Shipping	Included		$0	$0
			BASE YEAR SUBTOTAL:	$38500

**Quantities are estimates only and not guaranteed

OPTION YEAR 1
NOVEMBER 1, 2021 – OCTOBER 31, 2022

DESCRIPTION	MFG & MODEL	ESTIMATED QUANTITY	UNIT PRICE	TOTAL
Mobile LPR 1 camera system, dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle	Flock Falcon Camera-Annual Subscription	4	$2500	$10000
Portable LPR 1 camera system, dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle	Flock Falcon Camera-Annual subscription	10	$2500	$25000
LPR Camera Mounting Brackets for Light Bar		4	$0	$0
LPR Mounting for Portable system		10	$0	$0
LPR Processor		14	$0	$0
Modem		14	$0	$0
LPR Software		14	$0	$0
LPR Speed Trailer complete package		1	$0	$0
Start-up, configuration and commissioning of LPR Systems at Sheriff's facility to include all expenses such as travel		14	$0	$0
Installation		14	$0	$0
Covert Installation		1	$0	$0
Installation "Kit", Includes all hardware, wiring and software for do it yourself standard installations (on poles & trailers)		5	$0	$0
Training per hour	As Needed/included	8	$0	$0
Shipping				$0
			OPTION YEAR 1 SUBTOTAL:	$35000

**Quantities are estimates only and not guaranteed

OPTION YEAR 2
NOVEMBER 1, 2022 – OCTOBER 31, 2023

DESCRIPTION	MFG & MODEL	ESTIMATED QUANTITY	UNIT PRICE	TOTAL
Mobile LPR 1 camera system, dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle	Flock Falcon Camera- Annual subscription	4	$2500	$10000
Portable LPR 1 camera system, dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle	Flock Falcon Camera- Annual Subscription	10	$2500	$25000
LPR Camera Mounting Brackets for Light Bar		4	$0	$0
LPR Mounting for Portable system		10	$0	$0
LPR Processor			$0	$0
Modem		14	$0	$0
LPR Software		14	$0	$0
LPR Speed Trailer complete package		14 1	$0	$0
Start-up, configuration and commissioning of LPR Systems at Sheriff's facility to include all expenses such as travel		14	$0	$0
Installation			$0	$0
Covert Installation		14	$0	$0
Installation "Kit", Includes all hardware, wiring and software for do it yourself standard installations (on poles & trailers)		14	$	$0
Training per hour	As needed/included		$0	$0
Shipping		14	$0	$0
			OPTION YEAR 2 SUBTOTAL:	$35000

**Quantities are estimates only and not guaranteed

GRAND TOTAL (BASIS OF AWARD) :	$ 108,500

PRICING

1. Enter unit prices for each line item, Base Term Period, 1st Option Period, and 2nd Option Period tabs for each line item on the appropriate tab.
2. These worksheets have built-in formulas that will calculate the extended prices for each line item and each term period. The aggregate total for each term period will be automatically transferred to the Grand Total (Extended Price) where your total will be calculated.
3. The worksheets are locked/protected. The format and the contents of the worksheets should not be tampered with or altered in any way.
4. Bids must meet specifications provided.
5. All items must be priced to be considered responsive.

2. GENERAL REQUIREMENTS

1. A specifications sheet with pictures and operations manual for the product shall be submitted with the bid. Flock Response: Included with our information packet.

COMPANY: Flock Safety

REPRESENTATIVE NAME: Jesse Mund

REPRESENTATIVE EMAIL: Jesse.mund@flocksafety.com

REPRESENTATIVE PHONE: 713-899-6379

TAXABLE YEAR

CALIFORNIA FORM

2020 Withholding Exemption Certificate 590

The payee completes this form and submits it to the withholding agent. The withholding agent keeps this form with their records.

Withholding Agent Information

Name

Payee Information

Name

Flock Group inc dba Flock Safety

☑ SSN or ITIN ☐ FEIN ☐ CA Corp no. ☐ CA SOS file no.

820594875

Address (apt./ste., room, PO box, or PMB no.)

1170 Howell Mill Rd NW UNIT 210

City (If you have a foreign address, see instructions.)

Atlanta

State: GA

ZIP code: 30318

Exemption Reason

Check only one box.

By checking the appropriate box below, the payee certifies the reason for the exemption from the California income tax withholding requirements on payment(s) made to the entity or individual.

☐ **Individuals — Certification of Residency:**
I am a resident of California and I reside at the address shown above. If I become a nonresident at any time, I will promptly notify the withholding agent. See instructions for General Information D, Definitions.

☑ **Corporations:**
The corporation has a permanent place of business in California at the address shown above or is qualified through the California Secretary of State (SOS) to do business in California. The corporation will file a California tax return. If this corporation ceases to have a permanent place of business in California or ceases to do any of the above, I will promptly notify the withholding agent. See instructions for General Information D, Definitions.

☐ **Partnerships or Limited Liability Companies (LLCs):**
The partnership or LLC has a permanent place of business in California at the address shown above or is registered with the California SOS, and is subject to the laws of California. The partnership or LLC will file a California tax return. If the partnership or LLC ceases to do any of the above, I will promptly inform the withholding agent. For withholding purposes, a limited liability partnership (LLP) is treated like any other partnership.

☐ **Tax-Exempt Entities:**
The entity is exempt from tax under California Revenue and Taxation Code (R&TC) Section 23701 _____ (insert letter) or Internal Revenue Code Section 501(c) _____ (insert number). If this entity ceases to be exempt from tax, I will promptly notify the withholding agent. Individuals cannot be tax-exempt entities.

☐ **Insurance Companies, Individual Retirement Arrangements (IRAs), or Qualified Pension/Profit-Sharing Plans:**
The entity is an insurance company, IRA, or a federally qualified pension or profit-sharing plan.

☐ **California Trusts:**
At least one trustee and one noncontingent beneficiary of the above-named trust is a California resident. The trust will file a California fiduciary tax return. If the trustee or noncontingent beneficiary becomes a nonresident at any time, I will promptly notify the withholding agent.

☐ **Estates — Certification of Residency of Deceased Person:**
I am the executor of the above-named person's estate or trust. The decedent was a California resident at the time of death. The estate will file a California fiduciary tax return.

☐ **Nonmilitary Spouse of a Military Servicemember:**
I am a nonmilitary spouse of a military servicemember and I meet the Military Spouse Residency Relief Act (MSRRA) requirements. See instructions for General Information E, MSRRA.

CERTIFICATE OF PAYEE: Payee must complete and sign below.

To learn about your privacy rights, how we may use your information, and the consequences for not providing the requested information, go to **ftb.ca.gov/forms** and search for **1131**. To request this notice by mail, call 800.852.5711.

Under penalties of perjury, I declare that I have examined the information on this form, including accompanying schedules and statements, and to the best of my knowledge and belief, it is true, correct, and complete. I further declare under penalties of perjury that if the facts upon which this form are based change, I will promptly notify the withholding agent.

Type or print payee's name and title: Jonathan Love, Head of Finance

Telephone: (415) 623-6313

Payee's signature ▶ _____

Date: 11/4/2020

Form **W-9**
(Rev. October 2018)
Department of the Treasury
Internal Revenue Service

Request for Taxpayer Identification Number and Certification

► **Go to *www.irs.gov/FormW9* for instructions and the latest information.**

Give Form to the requester. Do not send to the IRS.

Print or type. See **Specific Instructions** on page 3.

1 Name (as shown on your income tax return). Name is required on this line; do not leave this line blank.
Flock Group Inc

2 Business name/disregarded entity name, if different from above
Flock Safety

3 Check appropriate box for federal tax classification of the person whose name is entered on line 1. Check only **one** of the following seven boxes.

☐ Individual/sole proprietor or single-member LLC ☑ C Corporation ☐ S Corporation ☐ Partnership ☐ Trust/estate

☐ Limited liability company. Enter the tax classification (C=C corporation, S=S corporation, P=Partnership) ► _____

Note: Check the appropriate box in the line above for the tax classification of the single-member owner. Do not check LLC if the LLC is classified as a single-member LLC that is disregarded from the owner unless the owner of the LLC is another LLC that is **not** disregarded from the owner for U.S. federal tax purposes. Otherwise, a single-member LLC that is disregarded from the owner should check the appropriate box for the tax classification of its owner.

☐ Other (see instructions) ►

4 Exemptions (codes apply only to certain entities, not individuals; see instructions on page 3):

Exempt payee code (if any) _____

Exemption from FATCA reporting code (if any) _____

(Applies to accounts maintained outside the U.S.)

5 Address (number, street, and apt. or suite no.) See instructions.
1170 Howell Mill Rd NW Suite 210

Requester's name and address (optional)

6 City, state, and ZIP code
Atlanta, Georgia, 30318

7 List account number(s) here (optional)

Part I Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. The TIN provided must match the name given on line 1 to avoid backup withholding. For individuals, this is generally your social security number (SSN). However, for a resident alien, sole proprietor, or disregarded entity, see the instructions for Part I, later. For other entities, it is your employer identification number (EIN). If you do not have a number, see *How to get a TIN,* later.

Note: If the account is in more than one name, see the instructions for line 1. Also see *What Name and Number To Give the Requester* for guidelines on whose number to enter.

Social security number
			–			–				

or

Employer identification number
8	2	–	0	5	9	4	8	7	5

Part II Certification

Under penalties of perjury, I certify that:

1. The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me); and
2. I am not subject to backup withholding because: (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding; and
3. I am a U.S. citizen or other U.S. person (defined below); and
4. The FATCA code(s) entered on this form (if any) indicating that I am exempt from FATCA reporting is correct.

Certification instructions. You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and generally, payments other than interest and dividends, you are not required to sign the certification, but you must provide your correct TIN. See the instructions for Part II, later.

Sign Here **Signature of U.S. person** ►  **Date** ► 2/12/2020

General Instructions

Section references are to the Internal Revenue Code unless otherwise noted.

Future developments. For the latest information about developments related to Form W-9 and its instructions, such as legislation enacted after they were published, go to *www.irs.gov/FormW9.*

Purpose of Form

An individual or entity (Form W-9 requester) who is required to file an information return with the IRS must obtain your correct taxpayer identification number (TIN) which may be your social security number (SSN), individual taxpayer identification number (ITIN), adoption taxpayer identification number (ATIN), or employer identification number (EIN), to report on an information return the amount paid to you, or other amount reportable on an information return. Examples of information returns include, but are not limited to, the following.

- Form 1099-INT (interest earned or paid)
- Form 1099-DIV (dividends, including those from stocks or mutual funds)
- Form 1099-MISC (various types of income, prizes, awards, or gross proceeds)
- Form 1099-B (stock or mutual fund sales and certain other transactions by brokers)
- Form 1099-S (proceeds from real estate transactions)
- Form 1099-K (merchant card and third party network transactions)
- Form 1098 (home mortgage interest), 1098-E (student loan interest), 1098-T (tuition)
- Form 1099-C (canceled debt)
- Form 1099-A (acquisition or abandonment of secured property)

Use Form W-9 only if you are a U.S. person (including a resident alien), to provide your correct TIN.

If you do not return Form W-9 to the requester with a TIN, you might be subject to backup withholding. See What is backup withholding, *later.*

flock safety

flocksafety.com
866.831.5326

Your partner in fighting crime

RFP RESPONSE-SAN DIEGO COUNTY SHERIFF



Hi RFP Committee,

When we started Flock Safety in 2017, we were just concerned citizens trying to use our talents in electrical engineering and software development to help our neighborhoods stop property crime. Since that time, we've heard from Chiefs of Police, Command Staff, City Councils, and other Concerned Neighbors like us from all across the country. There is a growing desire to work together to eliminate crime and I believe that with the right technology, hard-working officers, and community engagement we can make a serious dent in the crime in your jurisdiction.

Why? Because it's happening today in 1000+ cities across the country. We're seeing lower crime rates, kidnapping victims returned to their families unharmed, millions of dollars in recovered stolen vehicles, a renewed energy among detectives and patrol officers, and most importantly, communities that support their local law enforcement because they are safer than ever before.

We want to continue that success with you and your community, so that you can:

- Use the latest, most advanced technology to capture better evidence
- Build tighter partnerships between law enforcement and the communities you serve
- Have a local team of Flock Safety reps dedicated to working with you and serving you

Together, we can change the fabric of our country. We look forward to hearing from you and hope you will join the "flock"!

Thank you,



Garrett Langley
Founder and CEO

Protecting your jurisdiction is of the utmost importance. Thank you for considering Flock Safety's technology system as part of your comprehensive strategy to protect your city, citizens, and officers. We are more than just a camera company - we are a crime-fighting technology company with a mission to eliminate non-violent crime in the United States.

What makes Flock Safety's technology different



YOUR DEDICATED TEAM

You have a team of Flock Safety representatives dedicated to your account's success. You already know your local Law Enforcement rep, but you also have a Market Manager who ensures your cameras are in good working order, a Community Engagment team that sells LPRs to neighborhoods and small businesses in your city, and a PR team that can help with all your media requests.



CONSTANT INNOVATION

In 2018, we had one product - the Falcon ALPR. Every 3 months we've launch a new flagship product including the Sparrow ALPR, Vehicle Fingerprint™ technology, the TALON network, the Wing integration, and much, much more. We partner with you to build the products you need to capture evidence, gain insights from that evidence, and then deliver that evidence to the right person at the right time.



PUBLIC & PRIVATE PARTNERSHIPS

Thousands of communities use privately funded Flock Safety cameras throughout the country, which provide a huge benefit to local law enforcement as they can have access to those cameras without having to pay for them.



SIMPLE & AFFORDABLE

Our pricing is incredibly straightforward. LPR cameras cost just $2,500 per camera per year, which includes hardware, software, upgrades, unlimited users, and more. Our full suite of products work together to help you stop crime.

flock safety

Meet your dedicated team:



JESSE MUND
LAW ENFORCEMENT
TERRITORY MANAGER

The jurisdiction's main point of contact on new products and services.



PAUL PARK
COMMUNITY SAFETY
TERRITORY REP

Your community's point of contact on new products and services (HOAs, Neighborhood Watch groups, small businesses, etc.).



HECTOR SOLIMAN -VALDEZ
MARKET MANAGER
SOUTHERN CALIFORNIA

The Southern California regional leader who ensures customer satisfaction.



WILL WARREN
ONBOARDING
SPECIALIST

Your guide to optimal camera placement, installation, permitting, and camera maintenance.



MEG HEUSEL
COMMUNITY ENGAGEMENT
TEAM LEAD

Hosts meetings with you and your commnity (think: neighborhood watch meetings, crime prevention, etc.).



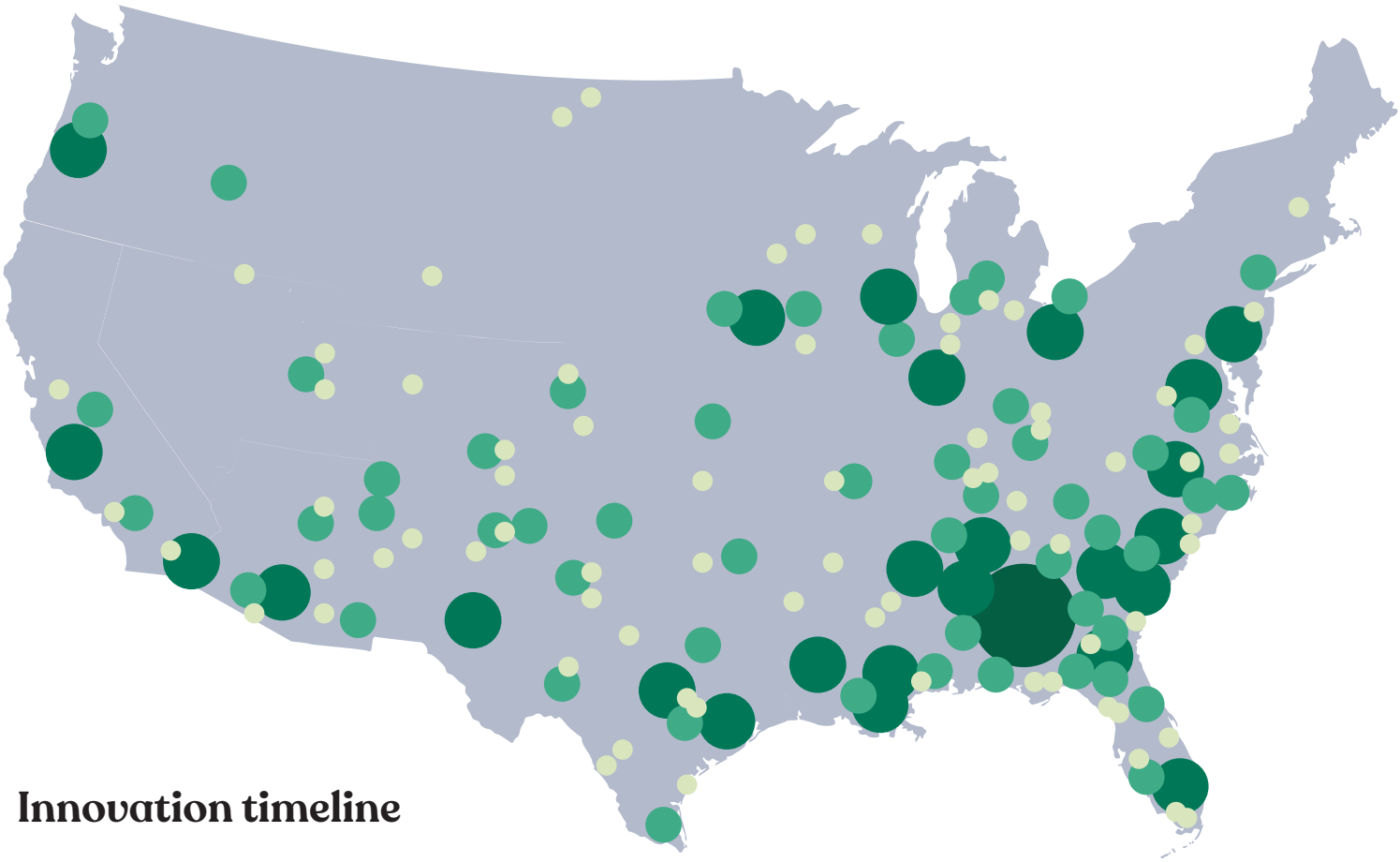
JOSH MILLER
PR MANAGER

Provides proactive and positive media relations with your jurisdiction, your community, and local media.

500
Police departments

1000+
US cities

120
Stolen vehicle reads/hr



Innovation timeline



2017
NEIGHBORHOOD ALPR

2018
VEHICLE FINGERPRINT™ TECHNOLOGY

2019
FALCON POLICE ALPR

2020
TALON & WING

Flock Safety's pace of innovation is unmatched in the industry. We launch new flagship products and features on a regular cadence.

Flock Safety Falcon™ Fixed ALPR

Unrivaled accuracy

Our cameras deliver 1.3 times the plate reads of traditional LPR cameras, and capture state details, temporary tags, and details on no-plate vehicles.

Install anywhere

Leverage solar or wired electric for power, so cameras can go anywhere you need.



Fast and easy

Use a Google-like search from your computer or phone to access footage from our secure cloud, identifying vehicles in seconds.

Affordable for all

$2,500 per camera annually includes maintenance, cloud storage, and software updates. One-time installation fee of $250.

Worry-free maintenance

We install, service, and continuously upgrade your cameras at no additional cost.



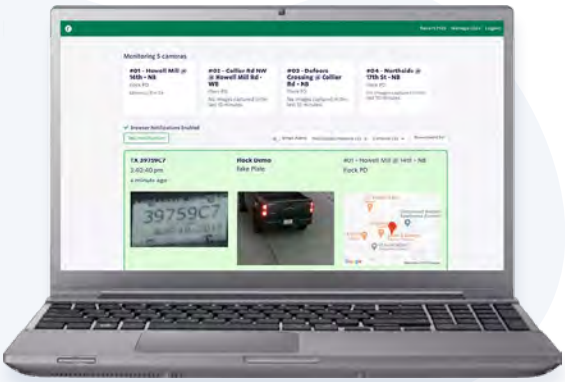
Products and services

Flock Safety Automatic License Plate Reading (ALPR) cameras do not just identify the plate seen, but all the objects within the frame. Even if the vehicle does not have a tag, the image can be captured for review.

The user interface is a simple search with unlimited user licenses. Within the software component, law enforcement can receive hotlist alerts and create custom alerts for plates under your investigation.

SOFTWARE USER INTERFACE

Included at no additional cost with unlimited user licenses. Receive alerts to help detect crime and search footage to access evidence — with any internet-connected device (based on user credentials that are easily managed/approved by admin).

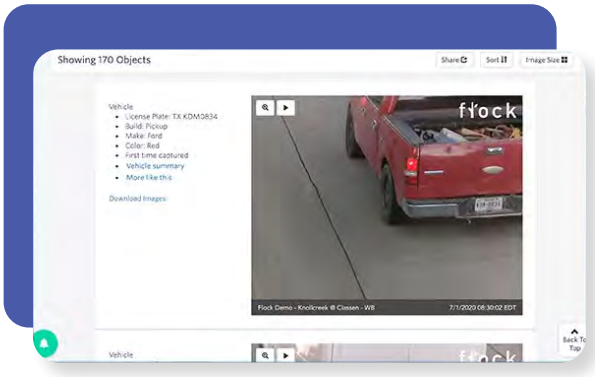


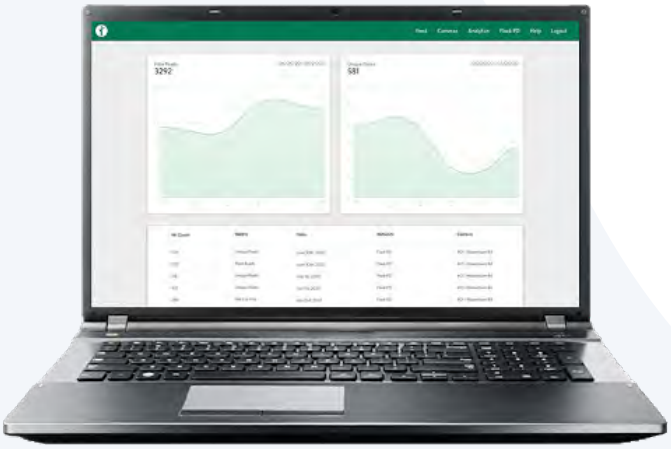
Patrol and Dispatch

- Connected to the California SVS & CJIS compliant
- 1 Hot List tool designed for MDTs and 1 Hot List tool designed for running in Dispatch
- State detection and picture to ensure accurate alerts
- Create and save custom alerts for any vehicles (including non-license plate searches)
- Filter notifications by reason codes (exclude stolen plates, include stolen vehicles, etc.)
- Audible and visual via email and SMS to users
- Receive hot list alerts from privately owned cameras in your jurisdiction

Access Evidence

- Filter search by specific camera location
- Capture vehicles regardless of plate type (paper, no plate, etc.)
- Search results with vehicle summary in multiple formats
- Filter by Vehicle Fingerprint™
  - Date and time
  - Vehicle Characteristics
    - Plate (partial/full)
    - Plate Type (in state, out of state, temporary tag)
    - Build & Color
    - Resident status
    - Location/Date/Time





Insights

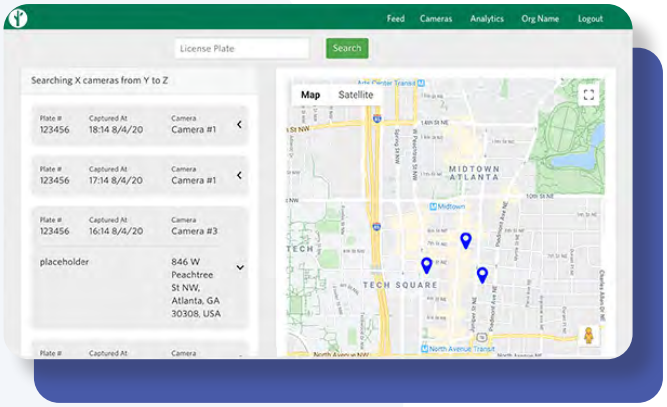
Give city council an ROI report

- Discover crime and traffic patterns
- Prioritize changes by greatest impact
- Change your community for the better

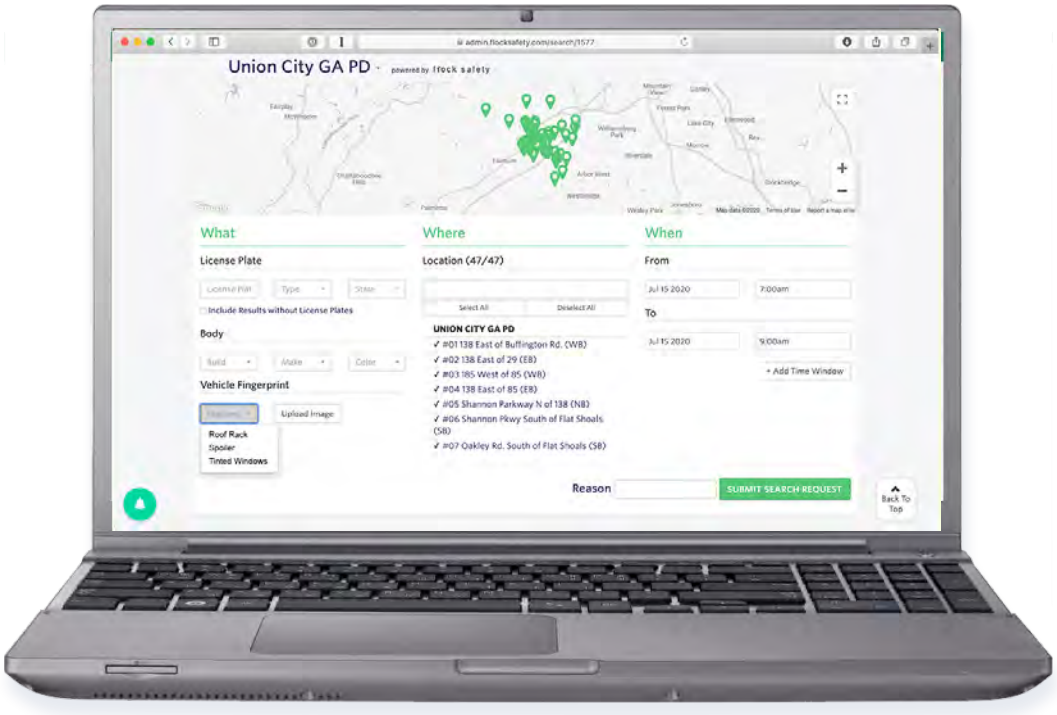
Advanced Search

Search plates across your jurisdiction

- **Multiple times** - Get a full view of all vehicle activity in your network
- **Multiple cameras** - See every location where your suspect traveled
- **Convoy analysis** - Find suspect vehicle groups



Vehicle Fingerprint™ technology



Our PATENTED vehicle recognition software delivers much more than just the license plate.

- **Vehicle type search** - Find vehicles by easily sorting on the type of vehicle in question:
  - Sedan, Coupe, Convertible, Wagon, Hatchback
  - SUV, Crossover
  - Work Van, Minivan
  - Pickup, Semi-Truck
  - Bus
  - Motorcycle
  - Golf Cart
  - Trailer

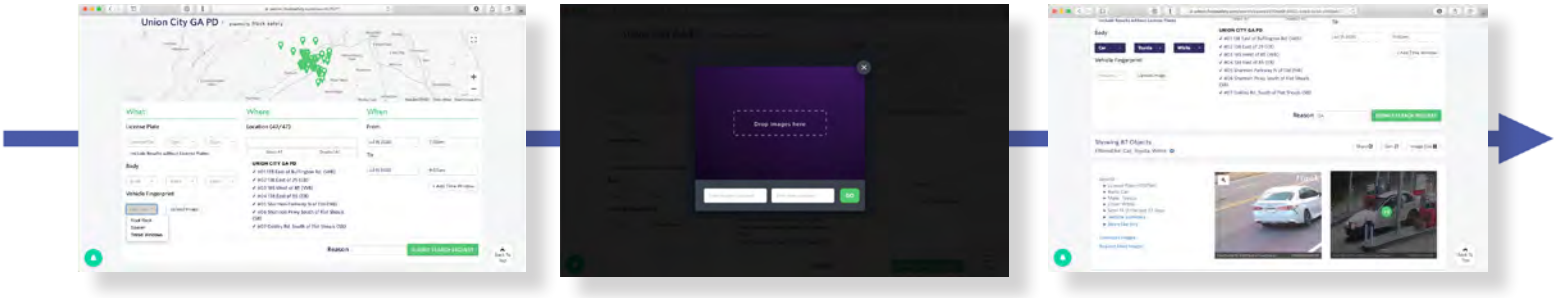
- **Vehicle feature search -** Search any unique details (think: roof rack, spoiler, trailer hitch), you can find similar vehicles across your entire network

Our team of machine learning engineers is releasing new features of our Vehicle Fingerprint software every week. Stay tuned as we continue to develop this further.

Coming in 2021

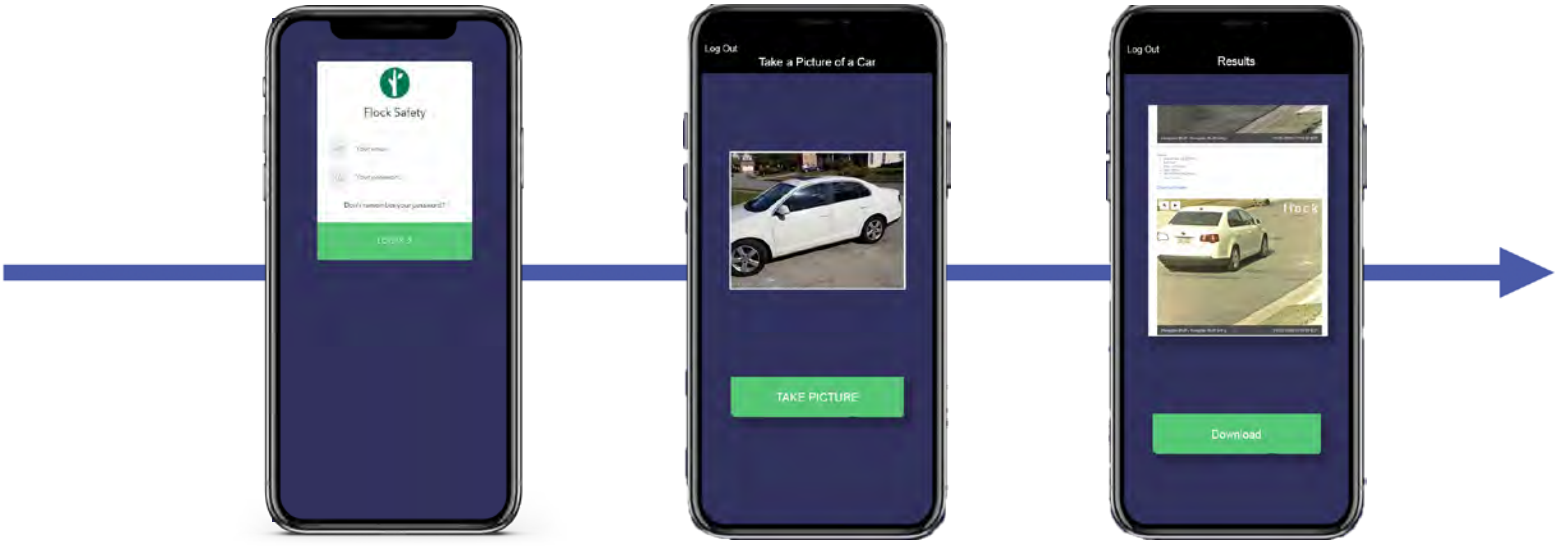
Reverse Image Search

Do you have a picture of the suspect vehicle? Upload that image of the suspect vehicle into your admin portal to find similar vehicles, license plates, and all identifying features of the vehicle.



Foot Patrol App

Does your officer need to indentify a suspect vehicle? Snap a picture of that car with a dedicated application, and find the search results related to that car. Download and unlock your investigation.



talon

Total Analytics Law Officer's Network

> **“Flock Safety works on an interconnected system, allowing us to view footage from other jurisdictions. That's a huge advantage”**
>
> Chief Paul Irwin
> Pell City Police Department

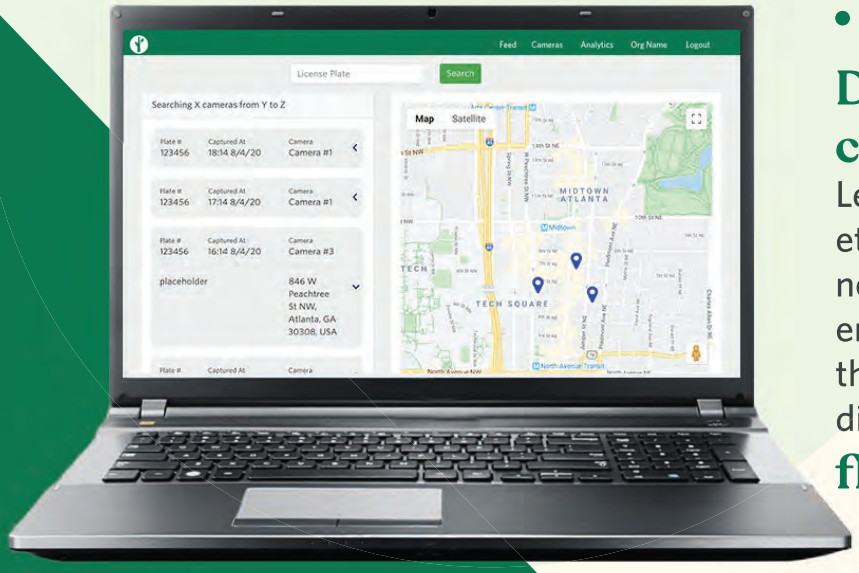
The TALON - the Total Analytics Law Officer's Network, from Flock Safety is the only ethically-designed local and national network of ALPRs for law enforcement officers. Don’t waste your entire budget on mismatched data. Get FREE access to 500M vehicle reads each month, so you can gather the evidence you need to close more cases.

Solve more cases with a larger network of footage

How often do your detectives run into this situation, “I have the plate, now I just need to find the car”? The TALON allows you and your department to search all cameras, all time. Whether you opt-in to share state-wide or nationally, the FREE access to the Flock Safety network of publicly-owned LPRs helps law enforcement solve more cases to help eliminate non-violent crime.

Access crime and traffic patterns intelligence

Many factors impact the safety of your city/county. From reckless drivers to stolen vehicles casing neighborhoods and businesses for their next target. The analytics reporting, Insights, not only detects these factors, but also allows you to analyze the events that are most important to help solve crime.



Discover more to solve crime in your Community

Learn how the only ethically-designed local and national network of ALPRs for law enforcement officers can give you the analytics you need to make a difference.

flocksafety.com/TALON

flock safety

wing

The Wing™ integration



Transform your cameras into cameras that see like a detective.

The Flock Safety Wing integration is for law enforcement agencies who want to transform existing cameras into cameras that see like a detective. Unlike buying new hardware, you can upgrade your existing cameras with the power of Flock Safety's Vehicle Fingerprint™ technology.

Detectives are key to solving crime

They see things differently, pick up on clues, and identify leads. They might notice that a suspect vehicle had a roof rack, tinted windows, a trailer hitch, bumper stickers, step boards, aftermarket wheels, etc. Those details can unlock an investigation and solve crime.

Cities already have 100s or 1000s of cameras

For years, cameras have promised a safer future. But who has the resources to scroll through hours and hours of footage? Even if you do have time, how can you be sure that you'll catch all the unique features of a suspect vehicle? When every second matters, you need to find the single frame that gives an investigator a lead.

Learn how your agency can take advantage of the Wing integration.

flocksafety.com/WING

flock safety

Solve more crime by putting Flock Safety software on your IP cameras.



Day Footage



Night Footage

Filter hours of footage to find actionable evidence

Leverage Flock Safety's patented Vehicle Fingerprint technology on your 3rd party camera and use machine vision to find your suspect vehicle. Think:

- Vehicle make, type, color
- License plate (full, partial, missing)
- Temporary tags and state of plate



Let's get started today. Transform your cameras into cameras that see like a detective.

flock safety

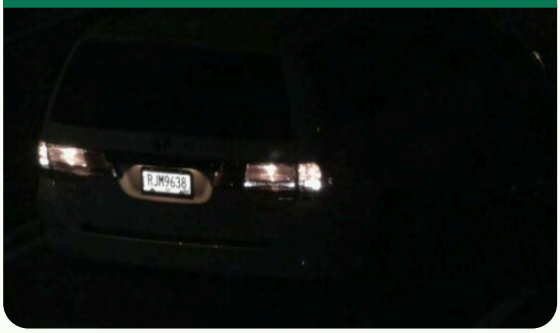
flocksafety.com/WING

Day or Night, Plate or No Plate. Crystal clear footage you need.

DAY TIME FOOTAGE



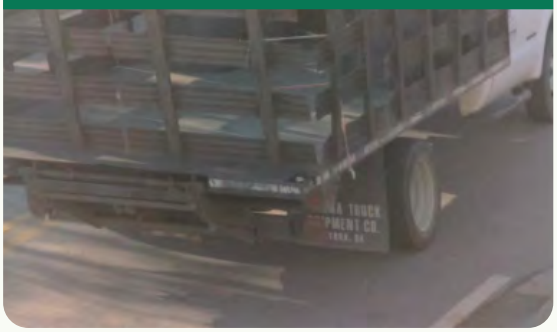
NIGHT TIME FOOTAGE



TEMPORARY PLATE



NO PLATE

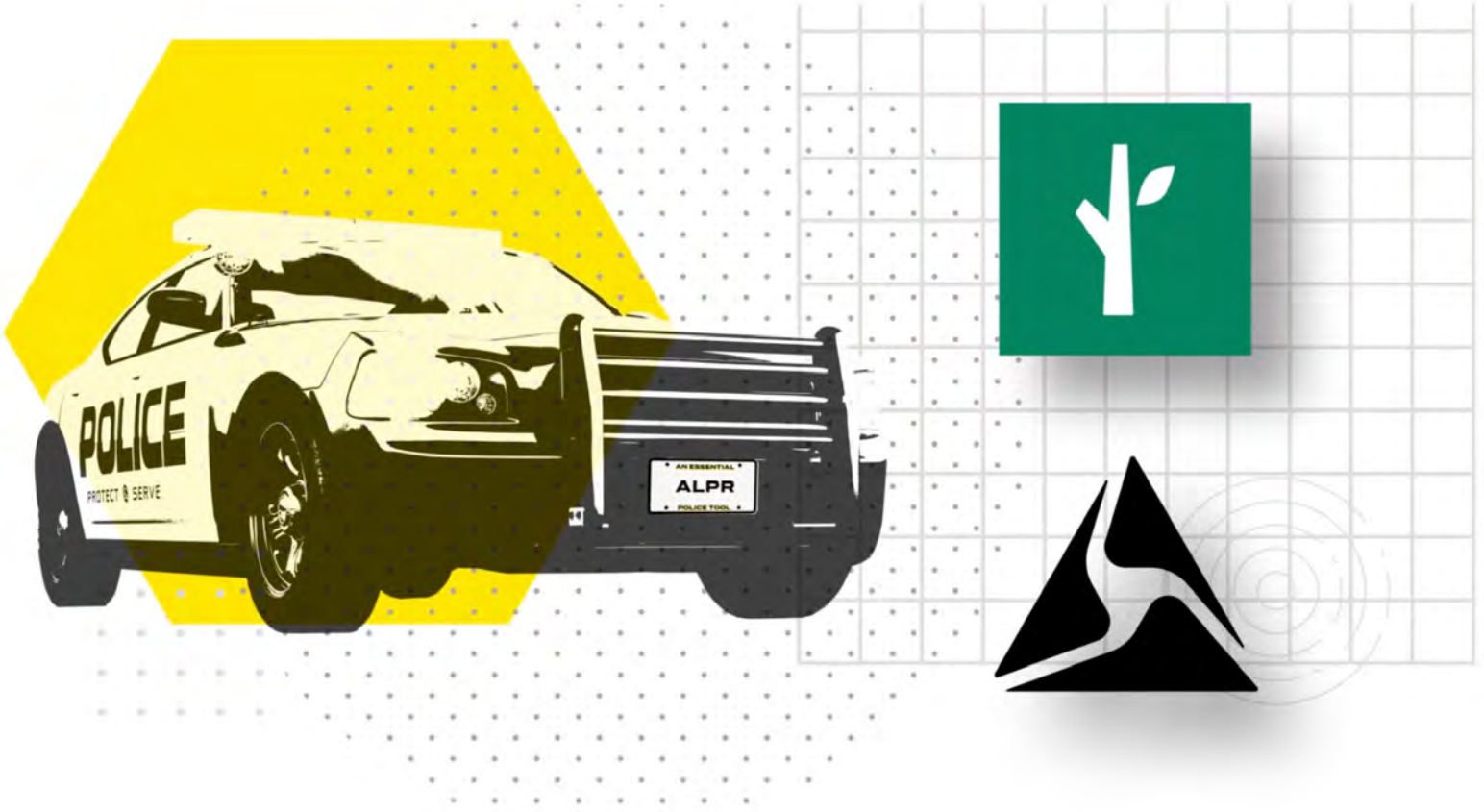


COVERED PLATE



TWO LANES OF TRAFFIC





Axon Fleet 3 + Flock Safety = the best in class mobile + fixed ALPR solution

Flock Safety and Axon have partnered to bring the most affordable, ethically designed, and smartest total ALPR solution to law enforcement across America. Axon Fleet 3 mobile ALPR will be integrated into the Flock Safety System allowing law enforcement to use Flock's Vehicle Fingerprint Technology across both mobile and fixed ALPR reads. This will create an unmatched city-wide ALPR network designed to not only capture license plate numbers, but to capture objective vehicle evidence to help law enforcement solve more crime.

Flock Safety is the only ALPR solution integrated with Evidence.com

Flock Safety has become the first ALPR solution to natively integrate with Evidence.com allowing users to seamlessly manage evidence through a single platform. Users can move vehicle evidence from the Flock system to Evidence.com with the click of a button. This integration went live in October 2020 and is being used by 100's of agencies across the country. This integration is just the start of Flock and Axon's commitment to providing smarter, easier, more affordable, and more intuitive tools to law enforcement across the country.

Summary

Police departments need a scalable solution to increase clearance rates and deter crime. The Flock Safety camera sees like a detective to make actionable evidence available when needed that is easily searchable by vehicle type, make, model, color, timeframe, or plate details. We deliver this detail through AI and Machine Learning technology that scans each image for distinguishing features, instead of traditional metal plates. This means we can also detect vehicles with no plates, temporary plates, dirty/covered plates, and even get accurate state detection.

30% ▲

Our solution **captures 30% more plates** than our leading competitor, according to a side-by-side study done by LASD in 2019, largely due to using AI and Machine Learning to analyze the entire vehicle profile, instead of legacy Infrared based technology.

34% ▼

In April 2019, Marietta Police Department released a study that shows they experienced a **34% reduction in calls for service** by targeting crime hot spots throughout the city with Flock Safety cameras.

60% ▼

In October 2019, Cobb County Police Department released a study based on their installation of 13 Flock Safety cameras in March. Over the six month period, Cobb police reported a **60% reduction in overall crime** by focusing on the beat with the highest

Company Overview

Flock Safety's mission is to eliminate non-violent crime. This is possible with city-wide coverage of automatic license plate readers (ALPRs) for both public safety organizations and private citizens. When a crime occurs, Flock Safety cameras deliver the actionable evidence you need to make an arrest.

Our company is headquartered in Atlanta, Georgia. Flock Safety camera systems are live in over 1,000 cities in 38 states and over 500 police departments. With an average of 120 Hot List notifications sent an hour with jurisdictions throughout the U.S., our team is helping agencies solve and prevent crime every minute.

Customer Results

Police departments need a scalable solution to increase clearance rates and deter crime. The Flock Safety camera sees like a detective to make actionable evidence available when needed that is easily searchable by vehicle type, make, model, color, timeframe, or plate details. We deliver this detail through AI and Machine Learning technology that scans each image for distinguishing features, instead of traditional metal plates. This means we can also detect vehicles with no plates, temporary plates, dirty/covered plates, and even get accurate state detection.



JERSEY VILLAGE, TEXAS

A camera on every street to create a virtual gate

Within one week, Flock Safety cameras notified officers of two vehicles on the NCIC Hot List. During the seizure of one of the vehicles, a wanted murderer in the state of Louisiana was arrested. Both vehicles were returned to their owners.

- Location: Houston suburb
- Flock Cameras: 50+
- Residents: 8,000
- Installation: Two months from purchase

MARIETTA, GEORGIA

34% reduction in calls for service in targeted hotspots

Cameras within the city led to the arrest of a suspect who allegedly brutally attacked a woman. Officers were able to locate and arrest the suspect using Flock cameras after weeks of the suspect being on-the-run.

- Location: Atlanta suburb, in Cobb County, Georgia
- Flock Cameras: 70 and growing within the county (30 police and 40 private cameras)
- Residents: 65,000 in Marietta
- Installation: Two months from purchase for first hotspot created





COBB COUNTY, GEORGIA

Containment strategy in highest crime beat of the county

Cobb County Police Department utilized 35 Flock cameras in 2 containment zones in their highest crime beats to reduce crime by over 60%.

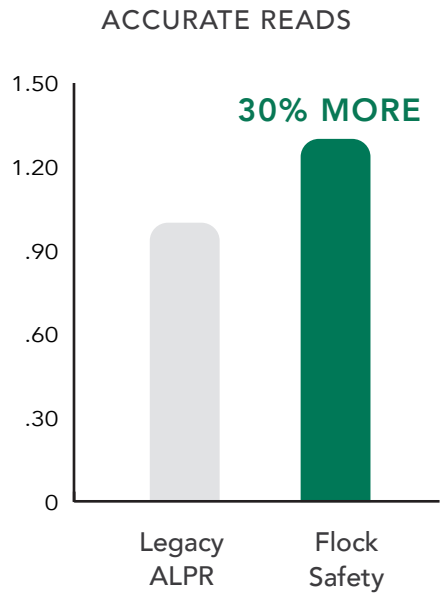
- Location: Cobb County, GA is just outside of Atlanta
- Flock Cameras: 35 for PD, over 100 including private sector cameras
- Residents: 750,000 in Cobb County
- Installation: Phased approach
- Contact: Deputy Chief Stuart Vanhoozer at **stuart.vanhoozer@cobbcounty.org** or (404) 375-1926

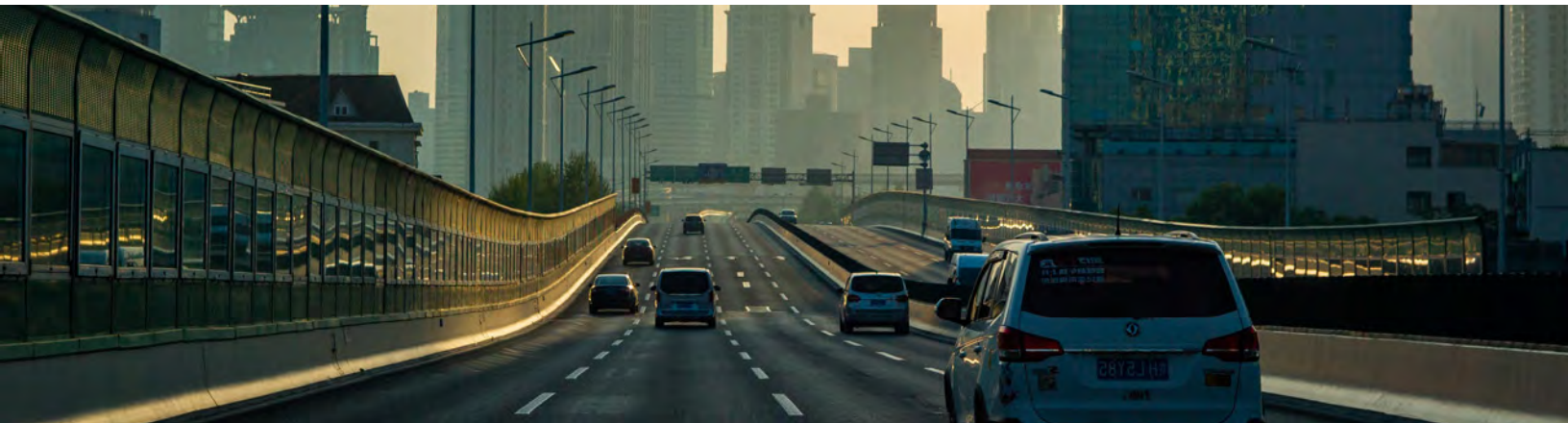
LOS ANGELES, CALIFORNIA

Sheriff's Department performs detection accuracy test

Los Angeles Sheriff's Department performed a head-to-head test of the Flock Safety camera versus a legacy ALPR solution.

- The results showed that the Flock Safety camera captures 30% more vehicle images and provides more accurate reads than traditional cameras triggered by infrared technology.
- Conducted in limited lighting from 2:00 AM to 8:00 AM, and from 11:00 PM to 6:00 AM.
- Causes for missed vehicles and/or misread plates were associated with the amount of reflectivity of the plate (older/dirtier tags, and dealer provided paper plates).





CAMERA SPECIFICATIONS

Design
Dimensions: 8.75" x 3"
Weight: 3 lbs
IP65 Waterproof

Power
14Ah Battery
30W Solar Panel (14" x 21")
AC Power (5 ft. range)

Data
16GB local storage, ~2 weeks

Image
5MP Image Sensor

Motion
Passive Infrared Motion Detection

Connectivity
Embedded Cellular LTE Connection
Cellular service provider depends on area

Production
Designed & manufactured in the U.S.

Night Vision
850nm Custom IR Array

Cloud Storage
30 days storage (Amazon Web Services)
Accessible via secure website
Images can be downloaded and stored by department

CAMERA PERFORMANCE

Traffic
NCIC and Custom Alert Notifications
- Average of 10-15 seconds

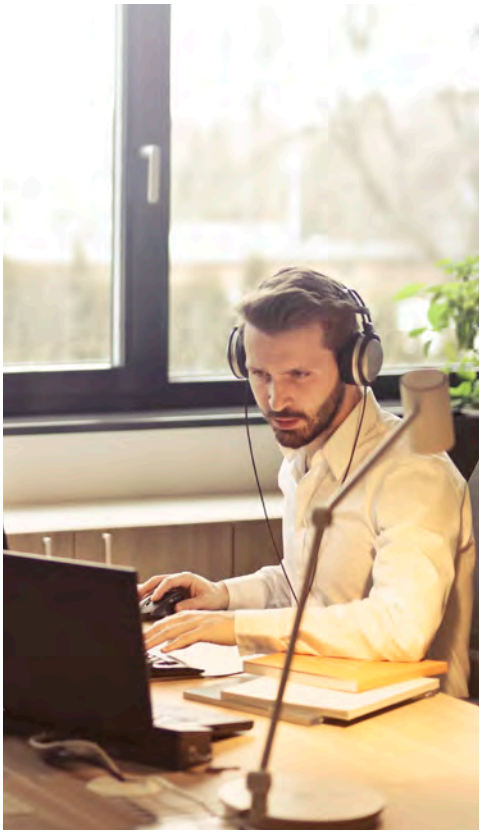
Includes time, location, plate, and vehicle image
Includes state specific alerts based on image

Power Source
100-240 VAC <1 amp
60 W Solar
11-14 Volt

Processing Power
1.4GHz
64-bit quad-core CPU

Image Capture
30-50 ft from vehicles
Up to 2 lanes of traffic per camera
Date and time with camera location
Plate (state, partial, paper, and none)
Vehicle details (Make, type, and color)





Training, Ongoing Support & Timeline

New customers will first get connected with their dedicated Onboarding Specialist who will spearhead the installation project to completion. Once cameras are successfully capturing footage, customers get introduced to their dedicated Market Manager. This person serves as the main point of reference for all things Flock Safety (training, setup questions, etc). In addition, the Flock Safety Support team monitors the **support@flocksafety.com** inbox Monday through Friday, 8:00 AM to 5:00 PM EST.

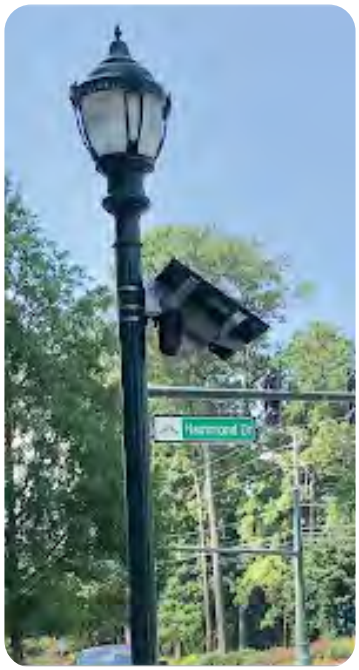
SAFETY-AS-A-SERVICE

- Regular software updates at no additional cost
- Camera maintenance is included in the subscription
- Unlimited users for hotlist integration and alerts, and camera footage search

INSTALLATION & CAMERA LOCATIONS

The average installation is to 6-8 weeks. Camera locations and installation timing is coordinated by the Flock Safety Customer Support team.

City intersection
Solar & existing pole



Entrance to Hotel
Solar & Flock 14 foot pole



City Foot Traffic Street
Electric & existing pole



Install Process Guide

TERMS, CONDITIONS, & SERVICE LEVEL AGREEMENT INFORMATION

For the complete list of Terms & Service, please visit **https://www.flocksafety.com/legal**.

WARRANTY

- All Flock products are under warranty for the duration of the Customer's contract.
- Flock cameras have built-in alarms to alert us if a camera is not performing at optimal standards. In the event of a camera performance issues, maintenance teams will be deployed at no additional cost.
- In the event the Flock camera is physically damaged or stolen, the first camera replacement will be made by Flock at not additional cost. A reassessment of camera location will be made at that time to deter further issues.
- In the unlikely case that an additional replacement camera is needed, you can learn about the process here: https://www.flocksafety.com/reinstall-fee-schedule
- Flock reserves the right to refuse or delay replacement or its choice of remedy for a Defect until after it has inspected and tested the affected Unit; provided that such inspection and test shall occur within 72 hours after the Agency notifies the Flock of defect.

Product Installation Guide

Thank you for installing our license plate reading camera in this local community. With your help, criminal activity in this neighborhood will be reduced and police will be provided with actionable evidence.

Table of Contents

Before You Begin……..……..……...2

Conducting a Site Survey..……..……..……3

Installation of a Flock pole..……..……..……4

Mounting a Camera……...……..X

New Pole……..……...……..……..X

Existing Pole……...……...X

Setting up and aiming the camera..……...……...……..X

Troubleshooting……..……..X

Examples……...……...……..…X

Before You Begin

iPhone:

* Go to https://apps.apple.com/us/app/testflight/id899247664
  - Download the TestFlight app via the iOS App Store

* Go to https://testflight.apple.com/join/VaycxuHW
  - Download the Flock Field App through the TestFlight app

Android:

* Go to: https://play.google.com/store/apps/details?id=com.flockaftershock

  - Download the Flock Field App from the Google Play store.

Both:

* Download the SunPosition (Android) or lumos (iOS) app on your phone via the App Store. Use the Sun Path feature while standing at final pole location to find ideal solar panel position for maximum direct sunlight.



Flock Field App



SunPosition



Lumos

Check everything is in the box



Hose Clamp



8 ft. Aluminum Pole



Pole-Camera Mount



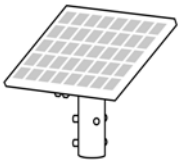
Flock Camera



Flock Sign



Return Shipping Label



Solar Panel w/ Screws and Cables

Required Tools



Post Hole Digger/Shovel



Smartphone (WiFi + Camera)



Ladder (10 ft.)



Quikrete Fast Setting Concrete. 1 per 8ft and 2 per 14ft pole (Red Bag)



Ability to Transport 8/14 ft. pole



Driver with 5/16" & 13mm sockets



Zip ties



Water - 1 gal per bag of concrete



Level

Conducting a Site Survey

1. Use the provided Deployment Plan to locate the recommended pole location
2. Look for a location approximately 4 feet from the edge of the road which has a clear view of license plates in the intended direction of aim.
   a. Ensure that there are no trees or building obstructing sunlight from the position
   b. Ensure that there are no street signs in the line of sight of the camera.
3. Check the location with the Lumos or SunPosition app and take multiple screenshots showing the sun from 10am-6pm
4. Place flag in surveyed location which should typically be 2-4' from edge of road unless deployment shows otherwise.
   a. Mark a circle around the flag using white spray paint
   b. Mark the street with a line of spray paint
5. Take three pictures
   a. Standing at the flag showing the camera's point of view
   b. 5 feet from the flag with the street in view
   c. 20 feet from the flag showing the location field of view
6. Open the Flock App
   a. Select "Site Survey"
   b. Choose the Camera number and location being installed. Select "continue"
   c. Fill out the required information fields and update all pictures and screenshots and select "Submit"

1.





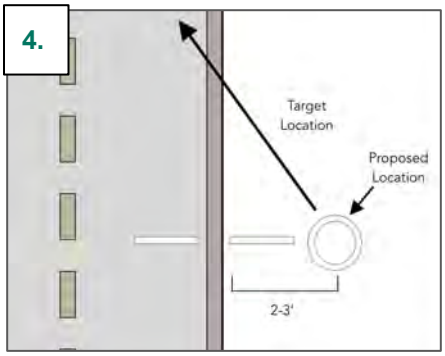
2.



3.

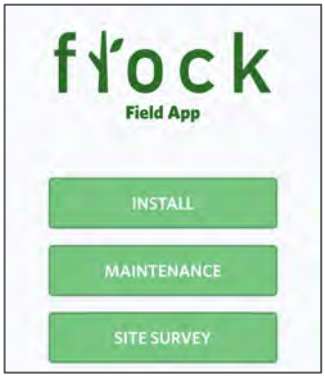


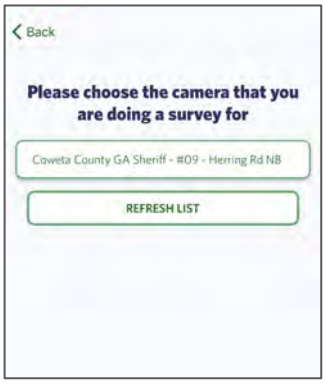
4.

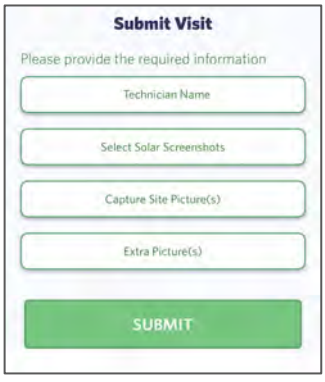


5.









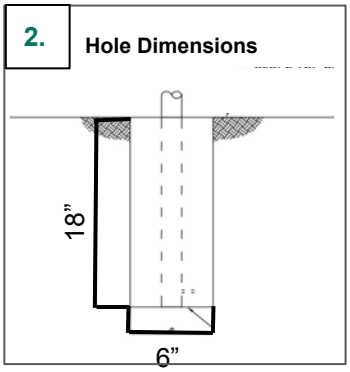
Installation of a Flock Pole

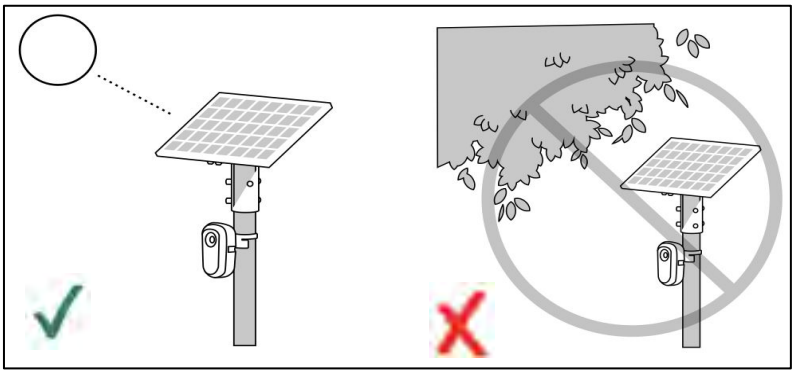
1. Locate the designated installation location denoted by a white “Flock” flag
   a. Select a final location optimizing (1) a clear line of sight to the sun, (2) clear line of sight to the road, and (3) avoiding marked underground utility lines.
   b. Text Flock for approval at (470) 270-5592 if the final location differs from location provided by >5 feet.
2. Use a shovel or post hole digger to dig a foundation hole at the determined final installation location.
   a. 8 ft Poles - **6” diameter x 18”** deep hole
   b. 14 ft. poles - **8” diameter x 24”** deep hole
3. Place pole vertically into the center of the hole (longer section if two piece 14 ft. pole)
   a. Alternate pouring ¼ bag of Quikrete (red bag) quick setting concrete followed by ¼ gallon of water until hole is completely filled.
   b. 1 bag for 8ft and 2 bag for 14ft poles
4. Use a level from two sides of the pole to ensure it is plumb
   a. This should be done repeatedly throughout the installation process as the concrete is still wet
   b. Allow concrete to set for ~10-15 min before proceeding
5. Prepare Solar panel by attaching batteries if needed for this location (see next page)
6. Loosen solar panel fastening bolts with 13mm socket and slide the panel over the pole
7. Use Lumos or SunPosition to verify the solar panel is aligned in a direction which maximizes direct sunlight
8. Tighten 13mm solar panel fastening bolts
9. Place the hose clamp over the pole no more than 12 inches below the base of the solar panel.
   a. Secure the camera mount to the pole facing the intended direction of the camera using a 5/16” socket

1.



2.





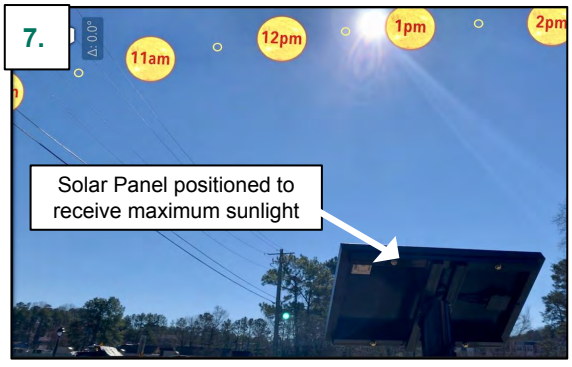
3.



3.



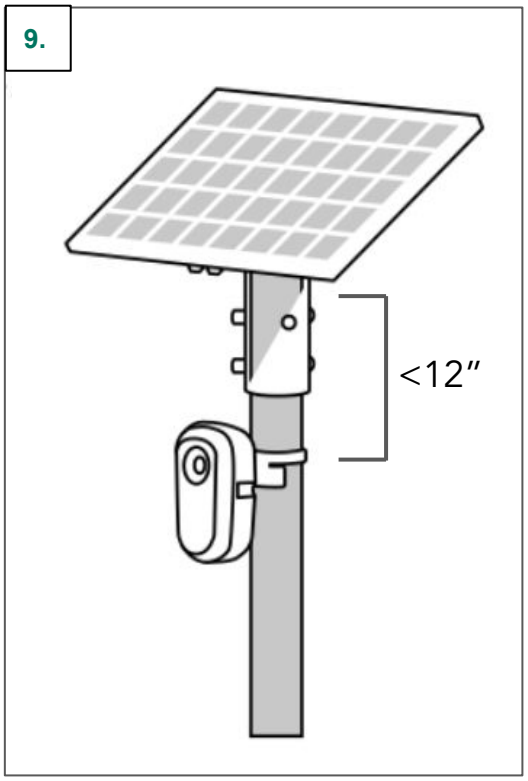
7.



8.

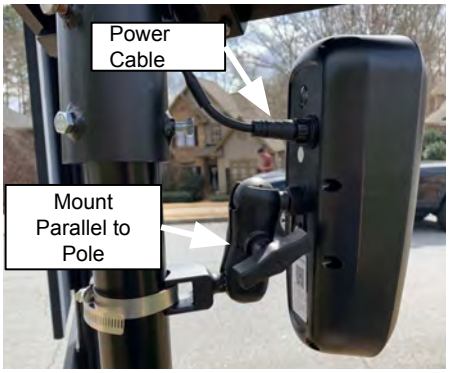


9.

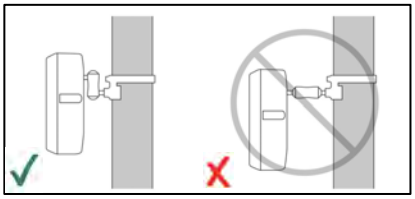


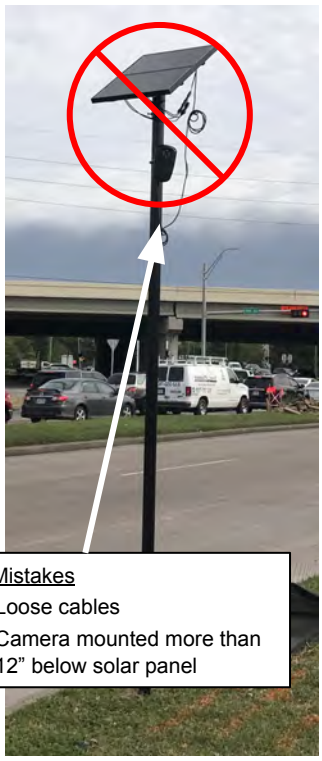
Mounting the Camera - Flock Pole

1. Loosen the provided ball mount clamp and position camera mount parallel to pole with camera facing towards the target location and tighten clamp.
2. Connect the solar panel power cables to the back of the camera and tighten firmly
3. Secure all loose cables to the pole using the provided zip ties









Common Mistakes
- Loose cables
- Camera mounted more than 12" below solar panel

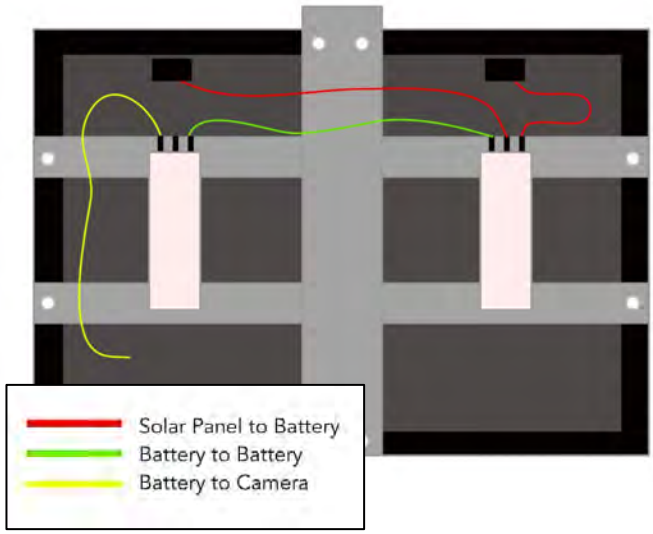
Connecting to an External Battery

1. Use the provided screws to connect the battery pack(s) to the back of the solar panel
2. Using the provided power cable(s) connect the solar panels to a battery pack.
   * For a single battery pack, connect both panels to the same battery
3. Use the connect one connect a battery pack to the camera.
4. If two battery packs are used, connect the packs together.



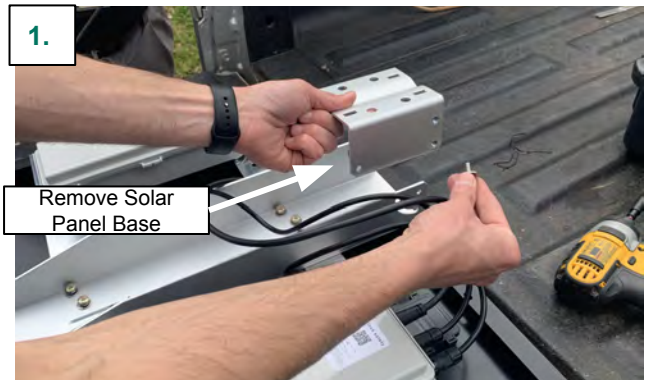
Note: Cables can be plugged into any port on the battery

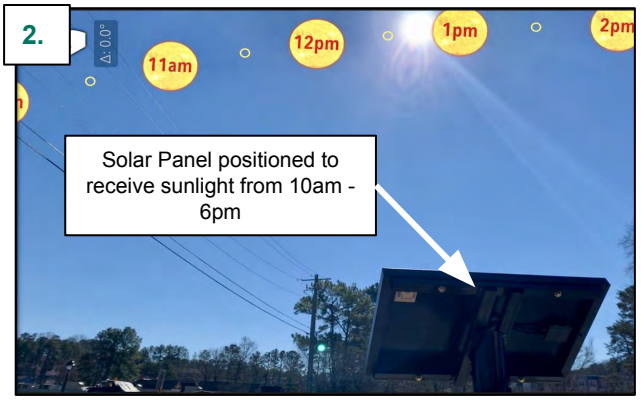


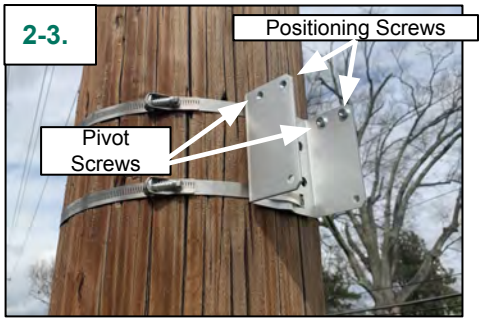


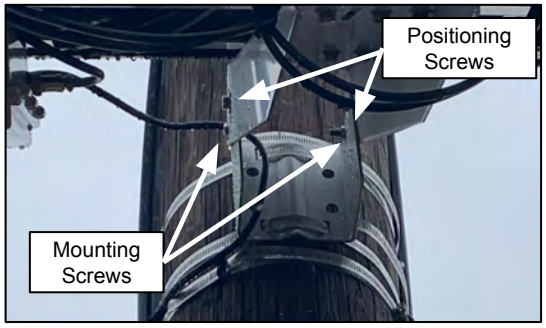
Mounting the Camera - Existing Pole

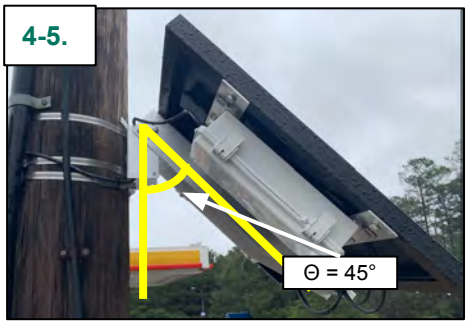
1. Remove the Solar panel base from the rest of the panel by removing the two pivot screws and two positioning screws
2. Use Lumos or SunPosition to determine direction which maximizes direct sunlight throughout the day for the solar panel
3. Place the provided hose clamp over the pole 12 ft. from the ground
    a. Secure the solar panel base to the pole by tightening the two hose clamps with a 5/16” socket
4. Using the mounting screws, secure the solar panel to its base
5. Place the two positioning screws into the base and tighten so that the panel is angled at 45 °
6. To mount the Camera, place the ball mount appx. 12” below the solar panel
7. Tighten the hose clamp with a 5/16” socket to secure the base of the ball mount to the pole.
8. Loosen the provided ball mount clamp and position camera mount parallel to pole with camera facing towards the target location and tighten clamp
9. Connect the solar panel power cables to the back of the camera and tighten firmly
10. Secure all loose cables to the pole using the provided zip ties.
11. Trim excess hose clamp using wire cutters

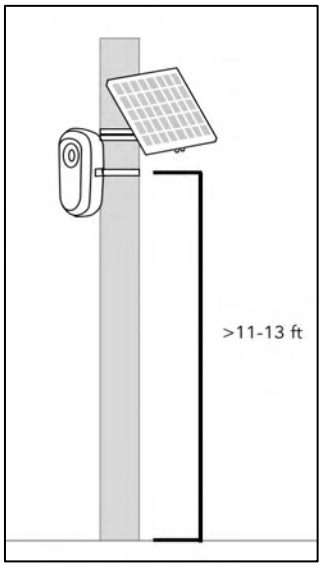


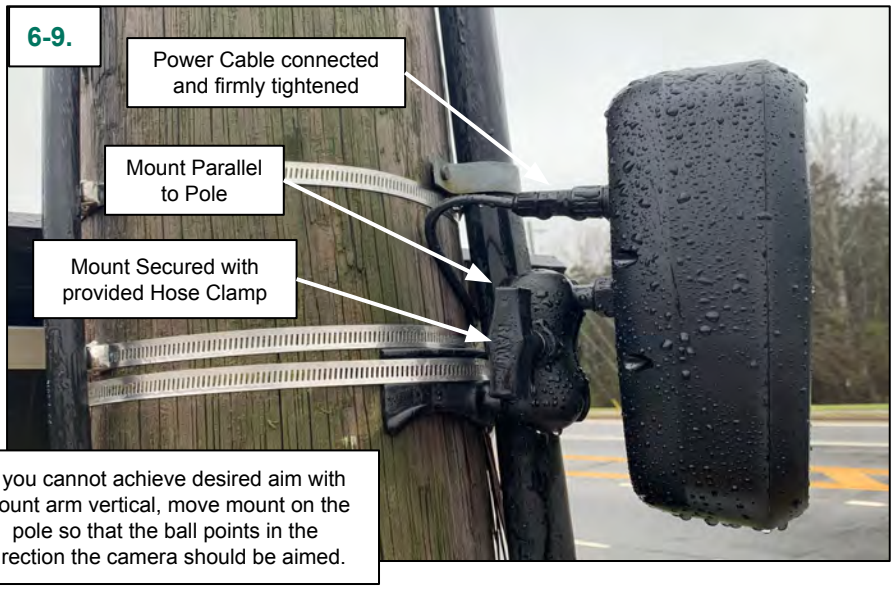








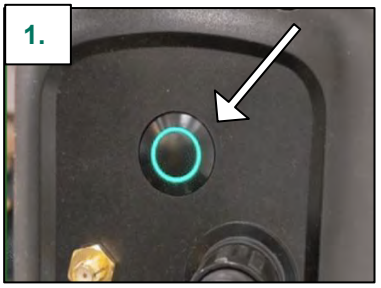


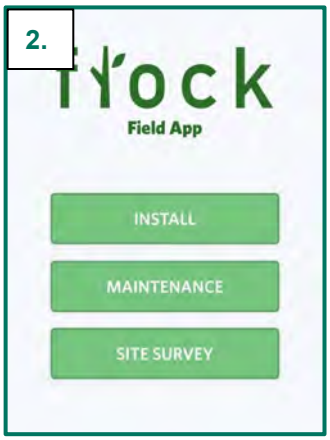


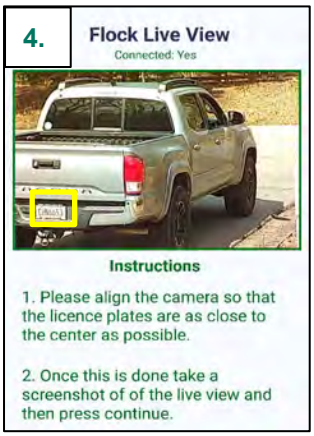
Setting up the Camera

1. Proceed with setup when Infrared LEDs surrounding the camera lens begin flashing (~2+ min after powering on camera).
2. Open up the Flock Field App
   a. Follow prompts: Install -> Solar Install -> Continue
3. Scan the QR code on the back of the camera. If the code will not scan, enter serial number manually.
4. Proceed with LiveView on car ~45 ft. down the street. In most cases you should be able to see most of the vehicle especially the license plate. Take screenshots of LiveView to upload later.
   a. License plate should be easily read and as vehicle passes camera should move across the diagonal of the field of camera view.
   b. See examples of acceptable views the “Examples Page"
5. Upload screenshots from solar evaluation.
6. Text Flock at (470) 279-5592 so they can confirm the camera status and start monitoring the camera.
7. Take pictures of installed camera on pole and view from camera and panel.
8. Submit all pictures through Flock app to complete installation. Press ‘Continue’ in upper right corner and press submit on final screen.
   a. Confirm upload successful.
   b. If not, text Flock
9. Fully tighten camera mount once the final angle has been confirmed via Flock app.
10. If included in the provided materials, hang the provided Flock Safety sign.
11. Return Extra Materials
    a. Repack the materials in the original packaging. Use tape to re-tape switch with “O” side taped down
    b. Drop any extra materials off at UPS store to mail back to Flock Safety with provided shipping label.

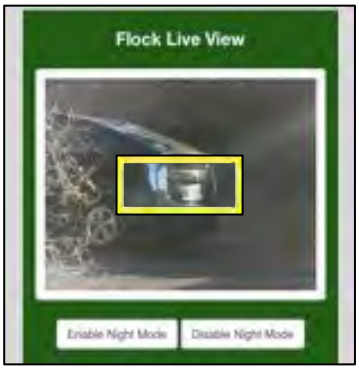


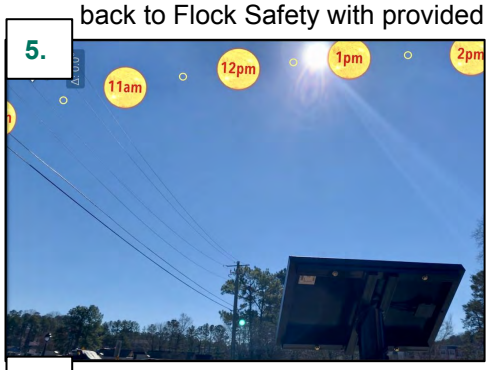


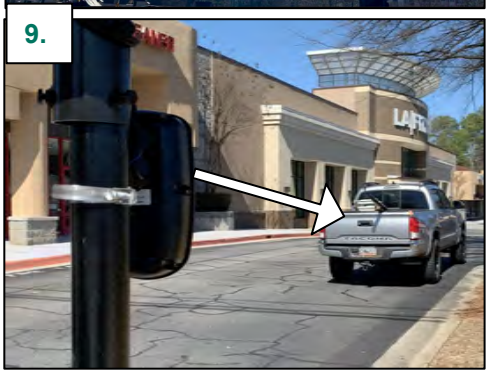


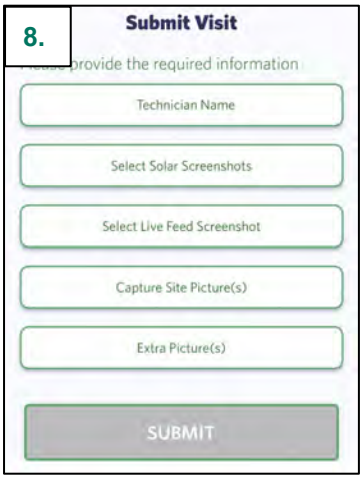








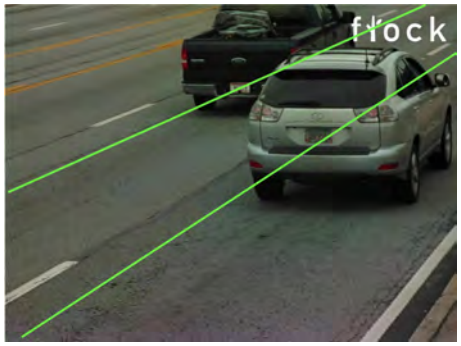




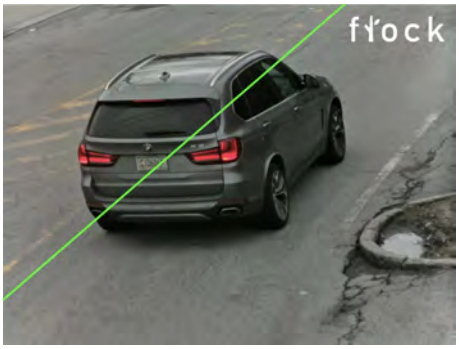


*See Troubleshooting page to if you are having trouble connecting to the camera

Examples



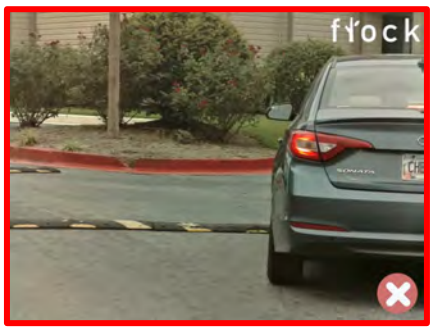
Two-lane road: Path of license plates (green) equidistant from diagonal



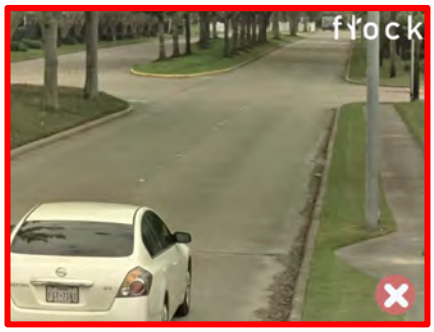
1.5 to 2 car lengths in view, license plate tracks near center of view



Too Low: Aim camera to capture 1 to 1.5 full view car lengths



Split turn: Aim camera to capture centered tag well before the split



Far more than 1.5-2 car lengths are in view. Aimed too far away.



Street Signs should never be in view - they will reflect at night



Street Signs should never be in view - they will reflect at night

Too steep of an angle downward

Troubleshooting

1. Go to your phone's WiFi settings
   a. Select the network named 'Flock-XXXXXX' network and choose to "forget this network
2. Turn camera off ("O" pressed down), wait 2-3 minutes until camera fully stops blinking, turn camera back on. Wait for red IR lights to blink before opening app to begin.

   Note: Flipping camera on and off too quickly/often may cause camera to fail. Patience will save more time.

3. If the application fails after three tries, go to your phone's WiFi network, select the network named 'Flock-XXXXXX' and enter the password "security"
   a. Ensure that your phone does not automatically connect to another network.
   b. Put your phone in 'Airplane' mode and go to flock.cam in your browser.
   c. If connected only to the Flock WiFi network, your phone will begin 'liveview' mode.
   d. The camera will remain in liveview mode for 10-20 minutes or your can fully power down the camera (2-3 minutes) then turn it back on to exit.





Next

Bid

MOTOROLA SOLUTIONS

COUNTY OF SAN DIEGO

SHERIFF'S DEPARTMENT REQUEST FOR BID FOR LICENSE PLATE READERS

RFB # 10493

NOVEMBER 5, 2020



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. © 2020 Motorola Solutions, Inc. All rights reserved.
PS-0000109845

Motorola Solutions, Inc.
500 W Monroe Street, Ste 4400
Chicago, IL 60661-3781
USA

November 5, 2020

Punnita Dinmuong
County of San Diego – San Diego Sheriff's Department
5560 Overland Avenue, Suite 270
San Diego, CA 92123-1204

RE: RFB #10493 – Request for Bids; License Plate Readers

Dear Punnita Dinmuong,

Motorola Solutions, Inc. (Motorola Solutions) is pleased to provide the San Diego Sheriff's Department with this response focused on our industry-leading portfolio of automated license plate recognition products. We have taken great care in providing a detailed and comprehensive response package that consists of all requested sections outlined in RFB #10493.

Motorola Solutions is a global leader in video solutions and system integration with our combined portfolio of Motorola Solutions and Vigilant Solutions branded products and services which are offered in over 125 countries. Our integration experience and successful deployment history with large enterprises and government agencies will allow us to meet the San Diego Sheriff's Department's implementation timeline as referenced in the RFB. As both the manufacturer and integrator of these solutions, Motorola Solutions is in a unique position to leverage our dedicated resources to provide the Sheriff with the necessary support, during, and after system implementation.

This proposal is subject to the is subject to the clarifications and exceptions set forth herein, as well as the enclosed terms and conditions of the existing Enterprise Service Agreement, together with its attachments or a negotiated version thereof. Motorola Solutions will be pleased to address any concerns you may have regarding the proposal and/or the existing agreement.

We appreciate the opportunity to respond to this RFB and for San Diego Sheriff's Department's continued interest in Motorola Solutions' proven system offerings for automated license plate recognition. We value our long-term relationship with you and hope to strengthen it by continuing to work with the department to design and implement the optimal ALPR solution.

Motorola Solutions is pleased to address any questions or clarifications needed in regard to this response. Please direct any inquiries to your Motorola Solutions Regional Sales Manager, Greg Mills, at (858)-287-0067 or greg.mills@motorolasolutions.com.

Sincerely,
MOTOROLA SOLUTIONS, INC.
Greg Mills
Southern California Regional Manager - Vigilant

TABLE OF CONTENTS

Executive Summary 1
1.1 Strategic Vision of San Diego sheriff 1
1.2 The Vigilant Solutions Platform 1
1.3 Law Enforcement Data Sharing and Commercial Data 2
1.4 Proposed Camera Hardware 2
1.5 Law Enforcement Archival Reporting Network (LEARN) 3
1.6 Criminal Justice Information System (CJIS) 3
1.7 Summary 4
1.8 Experience 5
1.9 References 5
1.9.1 Reference 1: Torrance Police Department ALPR Program 5
1.9.2 Reference 2: Los Angeles Sheriff's Department ALPR Program 5
1.9.3 Reference 3: San Bernardino Sheriff's Department ALPR Program 6

Section A

Cover Page, Certifications and Indemnification Agreement A-1
A.1 Cover Page (P&C 600 Form) A-1
A.2 Representations and Certifications Form A-2
A.3 Nondisclosure Indemnification Agreement Form A-3

Section B

Submitting Bid and Pre-Award Survey Requirements B-1
B.1 Completing and Submitting Bid and Pre-Award Survey Requirements B-1

Section C

Sample Contract C-1
C.1 Clarifications and Exceptions C-1
C.2 Supplemental Terms and Conditions C-4
C.3 Exhibit A – Statement of Work C-38
C.4 Exhibit B – Insurance Requirements C-44
C.5 Exhibit C – Pricing Schedule C-49
C.6 Exhibit D – Federal Grant Requirements C-52
C.6.1 Form W-9 ..... C-52

EXECUTIVE SUMMARY

Vigilant Solutions, a wholly owned subsidiary of Motorola Solutions, Inc. is known as an industry leader in Automated License Plate Recognition. Founded in 2005, Vigilant Solutions has successfully partnered with our law enforcement clients to help identify, locate and apprehend security and safety threats by utilizing innovative intelligence solutions proven to help save lives through our innovative LPR hardware, software and investigative tools. Our public safety infrastructure is driven by technology and data that delivers success across the globe.

1.1 STRATEGIC VISION OF SAN DIEGO SHERIFF

Motorola Solutions recognizes that the vision of San Diego Sheriff includes some of the following:

- Provide a state-of-the art LPR system designed to be housed in a secure CJIS compliant hosted environment.
- Provide the State with a cost-effective license plate recognition system that is delivered on time and within budget.
- Provide highly accurate, low profile LPR cameras that capture license plate images in color and infrared.

Motorola Solutions' Vigilant Solutions will not only satisfy all these requirements as described throughout our response, we will also provide the most benefit to the San Diego Sheriff Department its Law Enforcement officers and the communities they serve.

Thousands of vehicle detections alone will not solve crimes; they create more work. That is why we do more than provide detections and the ability to load a hot list. We help with the legwork by providing powerful analytics that make sense of those detections that enables San Diego Sheriff to develop targeted leads that lead to closed cases.

1.2 THE VIGILANT SOLUTIONS PLATFORM

Vigilant Solutions has worked hard to create a network of people, devices and applications for law enforcement by law enforcement and the communities they serve. Every component of the Vigilant Solutions ecosystem works together to deliver a cohesive public safety LPR solution.



1.3 LAW ENFORCEMENT DATA SHARING AND COMMERCIAL DATA

With Vigilant Solutions as your LPR provider, law enforcement agencies have 100% control over their data and whom they share their data with, if they choose to do so. Vigilant Solutions also owns and manages the single largest license plate recognition data sharing initiative that consists of over 11 billion LPR detections and is growing at a rate of over 175 million scans monthly. This data consists largely of commercial data harvested by Vigilant Solutions and made available for law enforcement consumption. This extensive LPR data set provides intangible value from an investigative perspective inside of the LEARN suite of applications. With more than 1,600 agencies and 41,000 active law enforcement users currently utilizing the LEARN platform, partnering with other local law enforcement to share data is extraordinary. The commercial data along with shared law enforcement data is comprised of nearly 20 billion detections nationwide.

Vigilant Solutions' facial recognition module is an intuitive, user-friendly system that includes a highly accurate matching algorithm. The IDP consisting of both commercial data and facial recognition will provide the state's law enforcement with a phenomenal investigative tool.

1.4 PROPOSED CAMERA HARDWARE

Vigilant's Reaper HD camera is a high definition, low profile, dual lens camera that provides high speed image processing of up to 60 images per second (Color and Infrared). Both MSI's fixed and mobile cameras offer several features including CarDetector and TAS alerts. Fixed Camera solutions complement our mobile systems and can be used to create a virtual fence, detect patterns of travel, be used as a crime deterrent and gather data at high volume locations around the city/critical infrastructure even in extreme weather conditions. We provide law enforcement purpose built LPR cameras and solutions.







1.5 LAW ENFORCEMENT ARCHIVAL REPORTING NETWORK (LEARN)

Our **LAW ENFORCEMENT ARCHIVAL REPORTING NETWORK (LEARN)** software platform offers a host of analytic and investigative tools proven to assist law enforcement's efforts in providing safe communities within San Diego Sheriff's jurisdiction. LEARN offers an exclusive application known as Locate Analysis, which is designed to provide a probabilistic assessment of where to most likely locate a suspect vehicle. In addition, LEARN offers an exclusive reporting option in its Stakeout application allowing for multiple points of interest to be defined on a map, with corresponding geo-zones and times/dates, for the location of "common plates" that are seen in more than one of the locations of interest. Coupled with Stakeout is an exclusive query utility known as Associate Analysis. A query on a known plate can be sent for Associate Analysis to identify other vehicles in close proximity to the suspect vehicle. This is very useful in identifying possible associates of a known suspect, or perhaps establishing a pattern of surveillance between a perpetrator and a victim.

1.6 CRIMINAL JUSTICE INFORMATION SYSTEM (CJIS)

Maintaining CJIS compliance is a critical component to any law enforcement solution. Vigilant Solutions' hosted environment is compliant with all relevant requirements set forth in the FBI-CJIS Security Policy. Vigilant Solutions' LPR data is hosted on secure servers in an accessed controlled facility in Virginia.

With redundancy on every level, on-site system administrators and engineers continually monitor the system to ensure that only credentialed law enforcement officers with a valid ORI have access to the data on the hosted server. Vigilant Solutions uses technical controls and mechanisms within its suite of products that facilitate privacy controls on the data and restrict access to only those that are granted access by the agency.

LEA information is not comingled, combined, or shared with any commercial database. ALPR data is the sole property of the submitting agency.

1.7 SUMMARY

1. Vigilant Solutions has worked hard to create a network of people, devices and applications for law enforcement by law enforcement and the communities they serve. Every component of the Vigilant Solutions ecosystem works together to deliver a cohesive public safety ALPR solution.
2. Vigilant is the only ALPR company with an integrated platform of commercial data which is the largest ALPR data repository in the nation. We see 18-22% of all license plates every 30 days, greatly enhancing the ability to generate an investigative lead and alerts from across the country.
3. Vigilant is the industry leader in sharing technologies backed by a commitment to privacy and CJIS standards - granular permissions allow precise management of data access privileges. We are the only platform that offers seamless sharing/receipt of Law Enforcement data nationwide. There are more than 10 Billion Law Enforcement scans available through LE data sharing.
4. Vigilant has world-class OCR capabilities and is the leader in video analytics. We own our own technology - no licensed algorithms.
5. Vigilant has superior data analytics including Stakeout, Make/Model search and Locate Analysis.
6. Law Enforcement Data Sharing and Commercial Data

   San Diego Sheriff is a current customer of Vigilant Solutions and utilizes our shared data platform to successfully develop leads. San Diego Sheriff has partnered with other local law enforcement to share data (nearly every San Diego agency, every Orange County municipal agency, Riverside County Sheriff, San Bernardino Sheriff, all Imperial County agencies). With Vigilant Solutions as your ALPR provider, you will have 100% control over your data and who your agency chooses to share data with.

   Vigilant Solutions also owns and manages the single largest license plate recognition data sharing initiative that consists of over 20 billion ALPR detections and is growing at a rate of over 175 million scans monthly. This data consists largely of commercial data harvested by Vigilant Solutions and made available for law enforcement consumption. This extensive ALPR data set provides intangible value from an investigative perspective inside of the LEARN suite of applications. With more than 1,600 agencies and 41,000 active law enforcement users currently utilizing the LEARN platform.
7. Vigilant Solutions is the only ALPR company that puts the power of mobile device scanning of License Plates directly into the agency's LEARN account. We are the only company with both an HTML5 and APP available to be used for data collection and analytics in a mobile environment.

1.8 EXPERIENCE

A detailed description of the Proposer's experience designing, implementing, training, and supporting similar technology systems in other local governments. Including References from Similar Projects completed within the last five (5) years.

MOTOROLA SOLUTIONS RESPONSE

Vigilant Solutions has installed and serviced, fixed and mobile ALPR assets in communities ranging in size from 2 sworn to 10,000 sworn. Vigilant Solutions has implemented over 15,000 fixed cameras throughout the US. With the ability to seamlessly integrate fixed and mobile assets into our LEARN platform the scans are available within seconds for active alerting and crime analysis. Our LEARN Platform allows for both proactive policing and criminal investigations.

1.9 REFERENCES

References of similar projects are provided below.

1.9.1 Reference 1: Torrance Police Department ALPR Program

Torrance Police Department ALPR Program	
Contact Name	Captain Mark Athan mathan@torrance.gov
Project Description	40 Fixed Cameras, 3 Mobile Units, 1 Covert Unit
Phone	310-415-2178

1.9.2 Reference 2: Los Angeles Sheriff's Department ALPR Program

Los Angeles Sheriff's Department ALPR Program	
Contact Name	Deputy Sam Paul sspaul@lasd.org
Project Description	Many Deployment's Directly with the Sheriff and with Contract Cities, Includes Fixed, Mobile, Trailers, and more.
Phone	323-829-0072

1.9.3 Reference 3: San Bernardino Sheriff's Department ALPR Program

San Bernardino Sheriff's Department ALPR Program	
Contact Name	Jenny Anderson janderson@sbcsd.org
Project Description	Many Deployment's Directly with the Sheriff and with Contract Cities, Includes Fixed, Mobile, Trailers, and more
Phone	909-387-3517

SECTION A

COVER PAGE, CERTIFICATIONS AND INDEMNIFICATION AGREEMENT

A.1 COVER PAGE (P&C 600 FORM)

The Cover page (P&C 600 Form) is provided below.

COUNTY OF SAN DIEGO - REQUEST FOR BIDS (RFB # **10493**)
SHERIFF'S DEPARTMENT
LICENSE PLATE READERS
SECTION A: COVER PAGE (P&C 600 FORM)

COUNTY OF SAN DIEGO
SECTION A-P&C 600 FORM
This is not an order

Issued: October 22, 2020

MAIL OR DELIVER TO:
COUNTY OF SAN DIEGO, RFB NO. 10493
DEPARTMENT OF PURCHASING & CONTRACTING
5560 OVERLAND AVE., SUITE 270
SAN DIEGO, CA 92123

AWARD WILL BE MADE TO THE LOWEST RESPONSIVE, RESPONSIBLE BIDDER BASED ON
[ ] ALL OR NONE
[ ] EACH LOT
[X] TOTAL PRICE
[ ] OTHER (SEE PRICING SCHEDULE)

UNSPSC commodity code**: 461716.0000**

FOR INFORMATION, PLEASE CONTACT:
PUNNITA DINMUONG, ASSISTANT PROCUREMENT SPECIALIST
PUNNITA.DINMUONG@SDCOUNTY.CA.GOV

BID OPENING DATE: NOVEMBER 5, 2020
BIDS MUST BE RECEIVED AT THE ABOVE ADDRESS PRIOR TO 11:00 A.M. ON DATE OF BID OPENING.

PLEASE STATE YOUR LOWEST PRICE F.O.B. DESTINATION AND BRAND NAME OR TRADE NAME IF APPLICABLE.
(Please use typewriter or black ink)
YOUR ENVELOPE MUST INCLUDE RFB NO. 10493

DESCRIPTION

THE COUNTY OF SAN DIEGO (COUNTY), SHERIFF'S DEPARTMENT HAS A REQUIREMENT FOR LICENSE PLATE READERS IN ACCORDANCE WITH THE TERMS & CONDITIONS AND THE STATEMENT OF WORK REFLECTED HEREIN.

INITIAL TERM: DATE OF AWARD – OCTOBER 31, 2021
1ST OPTION YEAR: NOVEMBER 1, 2021 – OCTOBER 31 2022
2ND OPTION YEAR: NOVEMBER 1, 2022 – OCTOBER 31, 2023

PRICING SUBMITTED IS TO REMAIN FIRM FIXED FOR THE TERM PERIOD IDENTIFIED ABOVE. ALL ITEMS WITHIN EACH TERM PERIOD MUST BE PRICED TO BE CONSIDERED RESPONSIVE. AWARD WILL BE MADE TO THE LOWEST RESPONSIVE, RESPONSIBLE OFFEROR BASED ON THE TOTAL PRICE. OFFEROR WHO SUBMITS THE LOW BID WILL BE DEEMED RESPONSIBLE BASED ON THE RESULTS OF THE PRE-AWARD SURVEY.

ARE YOU ABLE TO COMPLY WITH ALL ITEMS SPECIFIED WITHIN THE SCOPE OF WORK? YES__OR__NO

BIDDER ACKNOWLEDGES ADDENDUM NO. 1 [X] 2 [X] 3 [ ] 4 [ ] 5 [ ]

SUBJECT TO ACCEPTANCE WITHIN **90** DAYS

PAYMENT TERMS NET **30** DAYS OR % DAY

Motorola Solutions Inc. 10680 Treena Street,
San Diego, CA, 92131

NAME AND TITLE OF PERSON AUTHORIZED TO SIGN OFFER:
Jerry Burch, MGR Sales

SIGNATURE November 5, 2020

TELEPHONE: NUMBER (971) 219-8970
FAX TELEPHONE: (N/A)
E-MAIL: jburch@motorolasolutions.com

PRINTED NAME: Jerry Burch
PRINTED TITLE: Area Sales Manager

NOTIFICATION OF AWARDS

ACCEPTANCE AS TO ITEM(S) NUMBERED:

(VC NO.)

COUNTY OF SAN DIEGO
BY: _____ DATE: _____ JOHN M. PELLEGRINO, DIRECTOR
DEPT OF PURCHASING & CONTRACTING

TOTAL AMOUNT AWARD NO. NAME AND TITLE OF CONTRACTING OFFICER

A.2 REPRESENTATIONS AND CERTIFICATIONS FORM

The Representations and Certifications Form is provided below.

County of San Diego
Department of Purchasing and Contracting

REPRESENTATIONS AND CERTIFICATIONS

The following representations and certifications are to be completed, signed and returned with the offer (the term "offer" includes a bid, proposal, quote, statement of qualifications, or any other submission to provide goods and/or services).

1. BUSINESS TYPE

■ For-profit ☐ Non-profit ☐ Government

2. INTERLOCKING DIRECTORATE

In accordance with Board of Supervisors Policy A-79, if Offeror is a non-profit and will be subcontracting with a related for-profit entity where an interlocking directorate, management or ownership relationship exists, Offeror must list all such entity(ies) on an attached separate sheet, and authorization must be sought from Board of Supervisors. If Offeror is a non-profit and does not submit such a list, Offeror certifies it has not entered into a subcontract relationship with a related for-profit entity.

List Attached? Yes ☐

3. BUSINESS REPRESENTATION

Offeror represents as a part of this offer the following information regarding the ownership, operation, and control of its business:

3.1. Are you a local business with a physical address within the County of San Diego? ☐ Yes ☐ No

3.2. Are you certified by the State of California as a:

☐ Disabled Veteran Business Enterprise(DVBE)
Certification #: _____

☐ Small Business Enterprise (SBE)
Certification #: _____

3.3. Are you certified by the U.S. Dept Of Veterans' Affairs as:

☐ Veteran Owned Small Business (VOSB)
Certification # _____

☐ Service Disabled Veteran Owned Small Business (SDVOSB)
Certification # _____

3.4. Estimated percentage of work in this offer to be performed or fulfilled locally (within the geographic boundaries of the County of San Diego): 100 %

4. DEBARMENT, SUSPENSION, AND RELATED MATTERS

4.1. Offeror certifies to the best of its knowledge that neither it nor any of its officers:

4.1.1. Are presently debarred, suspended, declared ineligible, or voluntarily excluded from covered transactions by any state, local, or federal department or agency.

4.1.2. Have within a three (3) year period preceding this agreement been convicted of or had a civil judgment rendered against them for commission of fraud or criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or contract under a public transaction; violation of federal or state antitrust statutes; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;

4.2. Except as allowed for in Section 4.2.5, Offeror hereby certifies to the best of its knowledge that neither it nor any of its officers:

4.2.1 Are presently indicted for or otherwise criminally or civilly charged by a government entity (federal, state, or local) with the commission of any of the offenses enumerated in paragraph 4.1.2 of this certification;

4.2.2 Have within a three (3) year period preceding this agreement had one or more public transactions (federal, state or local) terminated for cause or default;

4.2.3 Are presently the target or subject of any investigation, accusation or charges by any federal, state or local agency or law enforcement, licensing, certification, ethics, or compliance body;

4.2.4 Are proposed for debarment by any state, local, or federal department or agency.

4.2.5 If Offeror is unable to certify Sections 4.2.1, 4.2.2, 4.2.3, or 4.2.4, it certifies that it has disclosed and attached to this Representations and Certifications the reason(s) it cannot do so. The disclosure must include the Section(s), specific relevant facts including dates, contracts, individuals involved, status of actions, and any other relevant information that prevent it from making the requested certification(s). The County reserves the right to disqualify an Offeror based upon information disclosed.

Disclosure Attached? Yes ☐

5. RELATED WORK

Offeror certifies to the best of its knowledge that, other than as disclosed in an attached separate sheet, it and its proposed subcontractors, agents, and consultants have not previously contracted with the County to perform work on or related to this project (e.g. preparing related studies or recommendations, components of the statement of work, or plans and specifications).

Disclosure Attached? Yes ☐

6. CURRENT COST OR PRICING

Offeror certifies to the best of its knowledge that cost and/or pricing data submitted with this offer, or specifically identified by reference if actual submission of the data is impracticable, are accurate, complete, and current as of the date signed below.

7. INDEPENDENT PRICING

Offeror certifies that in relation to this offer:

7.1. The prices in this offer have been arrived at independently, without consultation, communication, or agreement, for the purpose of restricting competition, as to any matter relating to such prices with other offerors, with any competitors, or with any County employee(s) or consultant(s) involved in this or related procurements;

7.2. Unless otherwise required by law, the prices that have been quoted in this offer have not been knowingly disclosed by the Offeror and will not knowingly be disclosed by the Offeror prior to opening, in the case of a bid, or prior to award, in the case of a proposal, directly or indirectly to any other Offeror or to any competitor or with any County employee(s) or consultant(s) involved in this or related procurements; and

7.3. No attempt has been made or will be made by the Offeror to induce any other person or firm to submit or not to submit an offer for the purpose of restricting competition.

8. ADDITIONAL DISCLOSURES

Offeror shall report in writing to the County Department of Purchasing and Contracting within five business days of discovering or having any reason to suspect any change in status as certified in the preceding paragraphs. Upon County's request, Offeror shall provide additional information supporting Offeror's Representations and Certifications. Offeror's obligations under this Section 8 shall continue until Offeror is no longer under consideration for award of a contract, or until termination or expiration of any resulting contract(s).

CERTIFICATION

The information furnished in Paragraphs 1 through 8 and in the accompanying offer is certified to be factual and correct as of the date submitted and this certification is made under penalty of perjury under the laws of the State of California.

Name: Jerry Burch Signature: Jerry Burch

Title: Area Sales Manager Date: November 5, 2020

Company/Organization: Motorola Solutions, Inc.

SUBMIT THIS FORM AS DIRECTED IN THE REQUEST FOR SOLICITATION DOCUMENTS OR WITH THE OFFER

A.3 NONDISCLOSURE INDEMNIFICATION AGREEMENT FORM

The Nondisclosure Indemnification Agreement is provided below.

COUNTY OF SAN DIEGO

NONDISCLOSURE INDEMNIFICATION AGREEMENT

IF OFFEROR SUBMITS EXHIBIT CONFIDENTIAL/PROPRIETARY, THE FOLLOWING NONDISCLOSURE INDEMNIFICATION AGREEMENT MUST BE COMPLETED, SIGNED AND RETURNED WITH THE OFFER

This indemnification agreement ("Agreement") is made and entered into by and between the County of San Diego ("County") and Offeror Company/Organization Name: Motorola Solutions, Inc. ("Offeror") with reference to the following facts: _____

WHEREAS the County may receive a request for disclosure of Offeror's submission under the California Public Records Act, Government Code Section 6250, et seq.; and

WHEREAS, Offeror has included in its submission an exhibit entitled "*EXHIBIT – CONFIDENTIAL/PROPRIETARY*" containing records that Offeror has determined to constitute trade secrets or other proprietary information exempt from disclosure under the California Public Records Act; and

WHEREAS the County requires defense and indemnity from Offeror for the County's ongoing non-disclosure of Offeror's *EXHIBIT-CONFIDENTIAL/PROPRIETARY*;

NOW, THEREFORE, for good and valuable consideration and the mutual promises contained herein, the parties agree to the following:

1. The above recitals are incorporated herein by this reference.
2. Except as otherwise provided herein, the County will not release Offeror's *EXHIBIT-CONFIDENTIAL/PROPRIETARY* based on Offeror's representation that the records contained therein are proprietary and exempt from disclosure under the California Public Records Act and/or are trade secrets as that term is defined in Government Code Section 6250, et seq. Notwithstanding the foregoing, however, the County may release Offeror's *EXHIBIT-CONFIDENTIAL/PROPRIETARY* in the event of any of the following:
   a. Offeror fails to comply with the terms and conditions of this Agreement; or
   b. Offeror provides the County with written notice that some or all of the records may be released; or
   c. A court of competent jurisdiction orders the County to release the records and the County has exhausted or waived its appeal rights.
3. To the fullest extent allowed by law, the County shall not be liable for, and Offeror shall defend and indemnify County and its Board of Supervisors, officers, directors, employees and agents of County (collectively "County Parties"), against any and all claims, demands, liability, judgments, awards, fines, mechanics' liens or other liens, labor disputes, losses, damages, expenses, charges or costs of any kind or character, including attorneys' fees (whether incurred by County attorneys or attorneys employed by County) and court costs (hereinafter collectively referred to as "Claims"), related to Offeror's *EXHIBIT-CONFIDENTIAL/PROPRIETARY.*
4. Offeror waives any and all claims in law or equity and hereby releases the County Parties from any and all claims, deductibles, self-insured retentions, demands, liability, judgments, awards, fines, mechanics' liens or other liens, labor disputes, losses, damages, expenses, charges or costs of any kind or character, including attorneys' fees and court costs, which arise out of or are in any way connected to Offeror's *EXHIBIT-CONFIDENTIAL/PROPRIETARY*.

TO BE COMPLETED BY AN AUTHORIZED REPRESENTATIVE OF THE OFFEROR	
Offeror Company/Organization Name:	Motorola Solutions, Inc.
Authorized Representative Name:	Jerry Burch
Authorized Representative Title:	Area Sales Manager
Signature: 	Date: November 5, 2020

SECTION B

SUBMITTING BID AND PRE-AWARD SURVEY REQUIREMENTS

B.1 COMPLETING AND SUBMITTING BID AND PRE-AWARD SURVEY REQUIREMENTS

RFB Section B. The County reserves the right to perform a pre-award survey of the bidder to determine capability to perform, including but not limited to insurability, staffing, equipment, experience, references, past performance, financial stability, certification, and the submission of documentation as requested in the Pre-Award Survey (Section B, Paragraph C7). The determination of the County as to the bidder's prospective ability to perform the contract shall be conclusive.

MOTOROLA SOLUTIONS RESPONSE

Understood.

RFB # C7. The County will conduct a pre-award survey of the apparent low bidder. This survey will be used to determine the bidders' capacity to perform under this contract. Items that will be considered will include the contractor's licenses, insurability, staffing, facilities, equipment, supplies, current financial statements, references, and performance history.

MOTOROLA SOLUTIONS RESPONSE

Understood.

Use or disclosure of this proposal is subject to the restrictions on the cover page.

SECTION C

SAMPLE CONTRACT

C.1 CLARIFICATIONS AND EXCEPTIONS

RFB Section C.9

MOTOROLA SOLUTIONS RESPONSE

Comply with Clarification: Motorola complies with the clarification that in the event its response is the only one received for this RFP, Motorola's negotiations would be limited to listed price only and not profit margin. If awarded, Motorola would provide the County with Commercial Off the Shelf license plate solution, a commercial item available to its customers. As a publicly traded corporation, Motorola will not disclose its internal cost or pricing information.

RFB # 21. Indemnity.

MOTOROLA SOLUTIONS RESPONSE

Comply with Clarification: Motorola agrees to the concept of indemnity as outlined in the County's agreement and proposes the following edits:

County shall not be liable for, and Vendor shall defend and indemnify County and the employees and agents of County collectively, "County Parties") against any and all claims, demands, liability, judgments, awards, fines, mechanics' liens or other liens, labor disputes, losses, damages, expenses, changes or costs of any kind or character, including attorneys' fees and court costs (hereinafter collectively referred to as "Claims"), related to or arising out of this purchase order for personal injury, death and direct damage to tangible property, and arising ~~either~~ directly ~~or indirectly~~ from any act, error, omission or negligence of Vendor or its contractors, licensees, agents, servants, or employees while performing their duties under this agreement, ~~including Claims caused by the concurrent negligent act, error or omission of County Parties~~. However, Vendor shall have no obligation to defend or indemnify County Parties against Claims (I) to the extent they arise from the active concurrent negligence of County Parties, or (ii) caused by the sole negligence or willful misconduct of County Parties. County will give Vendor prompt, written notice of any claim or suit. County will cooperate with Vendor in its defense or settlement of the claim or suit. This Section sets forth the full extent of Vendor's general indemnification of County from liabilities that are in any way related to Vendor's performance under this agreement.

RFB # 25.2 Cost or pricing data.

MOTOROLA SOLUTIONS RESPONSE

Comply with Clarification: Motorola's proposed pricing enclosed in its response to this RFP is based on discounts against its list pricing. Therefore, while Motorola acknowledges the County's right to audit certain Motorola books and records to verify Motorola's performance on the contract, it requests the following clarification to the language outlined herein:

If the Contractor submitted cost or pricing data in connection with the pricing of this contract or any change or modification thereto, unless such pricing was based on adequate price competition, established catalog or market prices of commercial items sold in substantial quantities of the general public, or prices set by law or regulation, the Contracting Officer or his representatives who are employees of the County or its agent shall have the right to examine all directly pertinent books, records, documents and other data of the Contractor related to the negotiation pricing or performance of such contract, change or modification, for the purpose of evaluating the accuracy, completeness and currency of the cost or pricing data submitted. For the avoidance of doubt, 'cost or pricing data' as contemplated in this section means Contractor's published pricing provided to County. In no circumstances will Contractor be required to create or maintain documents not kept in the ordinary course of Contractor's business operations, nor will Contractor be required to disclose any information, including but not limited to product cost data, which it considers confidential or proprietary to Contractor.

RFB # 29. Insurance.

MOTOROLA SOLUTIONS RESPONSE

Comply with Clarification: Motorola will comply with the County's insurance requirements with the clarifications included on the attached redlined RFP Section C Exhibit B.

RFB # 44. Subcontractor for work or services.

MOTOROLA SOLUTIONS RESPONSE

Comply: Motorola proposes to utilize the services of a subcontractor as identified it its proposal for the mobile installation.

RFB # 52.2. Subcontracting Requirements.

MOTOROLA SOLUTIONS RESPONSE

Comply with Clarification: Motorola will utilize the services of a Subcontractor for mobile installation subject to its subcontract agreement with the Subcontractor. Motorola will flow through, to the extent permitted, the Subcontractor requirements described herein. Motorola asserts and clarifies its subcontract agreement is its proprietary and confidential information that is not released externally and not subject to Director approval.

Motorola is not engaging the services of an equipment rental firm as defined in this section and if awarded the opportunity, proposes removing the equipment rental firm requirements as not applicable to Motorola's scope of work under the agreement.

RFB Exhibit D Federal Grant Requirements.
RFB # D.

MOTOROLA SOLUTIONS RESPONSE

Comply with Clarification: If selected for award, Motorola would be providing a commercial item available to its customers. Motorola therefore considers the requirements rights to inventions as described in this section are not applicable.

RFB # H.

MOTOROLA SOLUTIONS RESPONSE

Exception. Motorola asserts it does not perform under Cost Accounting Standards ("CAS") covered contracts; (ii) does not accept contracts where cost or pricing data is required to be provided; (iii) does not need to have and maintain an estimating system such as described in DFARS 252.215-7002; (iv) does not generate labor hour estimates from an estimating system; (v) does not provide cost information; and (vi) does not calculate or submit cost-based indirect or labor rates so it cannot agree to be bound by the Uniform Administration Requirements of 2 CFR Part 200. Additionally, Motorola cannot agree to terms and conditions imposed by any federal agency without the ability to review such terms and conditions to ensure compliance so we respectfully request deletion of this clause.

In addition to its clarifications and exceptions, Motorola includes the attached supplemental contract terms (Section C.2) as part of its proposal and anticipates incorporation of these terms in the final contract to be negotiated between the parties. These terms provide the contractual provisions required for software licensing, camera license keys, and the use of LEARN.

C.2 SUPPLEMENTAL TERMS AND CONDITIONS

Please see the attached Motorola Enterprise Service Agreement (ESA) and Equipment Purchase Addendum.

Enterprise Service Agreement (ESA)

This Enterprise Service Agreement (the "Agreement") is made and entered into as of this_____ Day of _____, 202_ by and between Motorola Solutions, Inc. ("Motorola"), a Delaware corporation, and County of San Diego , a law enforcement agency (LEA) or other governmental agency, having its principal place of business at 5560 Overland Avenue, Suite 270, San Diego, CA 92123 ("Customer").

WHEREAS, Motorola designs, develops, licenses and services advanced video analysis software technologies for the law enforcement and security markets;

WHEREAS, Motorola provides access to license plate data as a value-added component of the Vigilant law enforcement package of license plate recognition equipment and software;

WHEREAS, Customer will separately purchase License Plate Recognition (LPR) hardware components from Motorola for use with the Software Products (as defined below);

WHEREAS, Customer desires to license from and receive service for the Software Products provided by Motorola;

WHEREAS, Customer may elect to purchase LPR hardware components, professional or subscription services in addition to the license and service for the Software Products and related services. Any such services will be governed by the terms in the applicable Addendum containing terms specific to such service. Such Addenda will be labeled with the name of the service being purchased;

THEREFORE, In consideration of the mutual covenants contained herein this Agreement, Customer and Motorola hereby agree as follows:

I. Definitions:

"Addendum (Addenda)" is the title of the document(s) containing a specific set of terms and conditions applicable to a particular service or other offering beyond the Software Products contemplated in the Enterprise Service Agreement. The terms in the Addendum are applicable only to the specific service or offering described therein.

"Booking Images" refers to both LEA Booking Images and Commercial Booking Images.

“CJIS Security Policy” means the FBI CJIS Security Policy document as published by the FBI CJIS Information Security Officer.
“CLK” or **“Camera License Key”** means an electronic key that will permit each license of Motorola’s CarDetector brand LPR software or FaceAlert brand facial recognition software (one CLK per camera) to be used with other Motorola approved and licensed LPR hardware components (i.e., cameras and other hardware components provided by Motorola) and Software Products. CLKs shall be not issuable and if issued in error shall be removed and immediately rendered null and void for cameras and other hardware components that are not Motorola-authorized cameras and other hardware.

“Commercial Booking Images” refers to images collected by commercial sources and available on LEARN with a paid subscription.

“Commercial LPR Data” refers to LPR data collected by private sources and available on LEARN with a separately paid subscription.

“Criminal Justice Information Services Division” or “CJIS” means the FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and to qualified law enforcement, criminal justice,
civilian, academic, employment, and licensing agencies.

“Effective Date” means sixty (60) days subsequent to the date set forth in the first paragraph of this Agreement.

“Enterprise License” means a non-exclusive, non-transferable license to install and operate the Software Products, on applicable media provided by Vigilant. This Enterprise Service Agreement allows Customer to install the Software Products on such devices, in accordance with the selected Service Package(s), and allow benefits of all rights granted hereunder this Agreement.

“LEA Booking Images” refers to images collected by LEAs and available on the Software Service for use by other LEAs. LEA Booking Images are freely available to LEAs at no cost and are governed by the contributing LEA’s policies.

“LEA LPR Data” refers to LPR data collected by LEAs and available on LEARN for use by other LEAs. LEA LPR Data is freely available to LEAs at no cost and is governed by the contributing LEA’s retention policy.

“Service Fee” means the amount due from Customer prior to the renewal of this Agreement as consideration for the continued use of the Software Products and Service Package benefits according to Section VIII of this Agreement.

"Service Package" means the Customer designated service option(s) which defines the extent of use of the Software Products, in conjunction with any service and/or benefits therein granted as rights hereunder this Agreement.

"Service Period" has the meaning set forth in Section III (A) of this Agreement.
"Software Products" means Motorola's Law Enforcement & Security suite of Software Products including CarDetector, Law Enforcement Archival & Reporting Network (LEARN), PlateSearch, Mobile Companion for Smartphones, Target Alert Service (TAS) server/client alerting package, FaceSearch, FaceAlert, and other software applications considered by Motorola to be applicable for the benefit of law enforcement and security practices. Software Products shall only be permitted to function on approved Motorola cameras and other hardware components provided by Motorola. Software Products shall not be permitted to operate on third-party provided or not Motorola-authorized hardware components, and if found to be operating on third-party provided hardware components Software Products shall be promptly removed by Customer.

"Technical Support Agents" means Customer's staff person specified in the Contact Information Worksheet of this Agreement responsible for administering the Software Products and acting as Customer's Software Products support contact.

"User License" means a non-exclusive, non-transferable license to install and operate theLPR Software Products, on applicable media, limited to a single licensee.

"Users" refers to individuals who are agents and/or sworn officers of the Customer and who are authorized by the Customer to access LEARN on behalf of Customer through login credentials provided by Customer.

II. Enterprise License Grant; Duplication and Distribution Rights:

Subject to the terms and conditions of this Agreement, Motorola hereby grants Customer an Enterprise License to the Software Products for the Term provided in Section III below. Except as expressly permitted by this Agreement, Customer or any third party acting on behalf of Customer shall not copy, modify, distribute, loan, lease, resell, sublicense or otherwise transfer any right in the Software Products. Except as expressly permitted by this Agreement, no other rights are granted by implication, estoppels or otherwise. Customer shall not eliminate, bypass, or in any way alter the copyright screen (also known as the "splash" screen) that may appear when Software Products are first started on any computer. Any use or redistribution of Software Products in a manner not explicitly stated in this Agreement, or not agreed to in writing by Motorola, is strictly prohibited.

III. Term; Termination.

A. Term. The initial term of this Agreement is for one (1) year beginning on the Effective Date (the "Initial Term"), unless earlier terminated as provided herein. Sixty (60)

days prior to the expiration of the Initial Term and each subsequent Service Period, Motorola will provide Customer with an invoice for the Service Fee due for the subsequent twelve (12) month period (each such period, a "Service Period"). This Agreement and the Enterprise License granted under this Agreement will be extended for a Service Period upon Customer's payment of that Service Period's Service Fee, which is due 30 days prior to the expiration of the Initial Term or the existing Service Period, as the case may be. Pursuant to Section XIII below, Customer may also pay in advance for more than one Service Period.

B. Customer Termination. Customer may terminate this Agreement at any time by notifying Motorola of the termination in writing thirty (30) days prior to the termination date and deleting all copies of the Software Products. If Customer terminates this Agreement prior to the end of the Initial Term, Motorola will not refund or prorate any license fees, nor will it reduce or waive any license fees still owed to Motorola by Customer. Upon termination of the Enterprise License, Customer shall immediately cease any further use of Software Products. Customer may also terminate this agreement by not paying an invoice for a subsequent year's Service Fee within sixty (60) days of invoice issue date.

C. Motorola Termination. Motorola has the right to terminate this Agreement by providing thirty (30) days written notice to Customer. If Motorola's termination notice is based on an alleged breach by Customer, then Customer shall have thirty (30) days from the date of its receipt of Motorola's notice of termination, which shall set forth in detail Customer's purported breach of this Agreement, to cure the alleged breach. If within thirty (30) days of written notice of violation from Motorola Customer has not reasonably cured the described breach of this Agreement, Customer shall immediately discontinue all use of Software Products and certify to Motorola that it has returned or destroyed all copies of Software Products in its possession or control. If Motorola terminates this Agreement prior to the end of a Service Period for breach, no refund for any unused Service Fees will be provided. If Motorola terminates this Agreement prior to the end of a Service Period for no reason, and not based on Customer's failure to cure the breach of a material term or condition of this Agreement, Motorola shall refund to Customer an amount calculated by multiplying the total amount of Service Fees paid by Customer for the then-current Service Period by the percentage resulting from dividing the number of days remaining in the then-current Service Period, by 365.

IV. Warranty and Disclaimer; Infringement Protection; Use of Software Products Interface.

A. Warranty and Disclaimer. Motorola warrants that the Software Products will be free from all Significant Defects (as defined below) during the term of this Agreement (the "Warranty Period"). "Significant Defect" means a defect in a Software Product that impedes the primary function of the Vigilant Software Product. This warranty does not include products not manufactured by Motorola. Motorola will repair or replace any Software Product with a Significant Defect during the Warranty Period; *provided, however*, if Motorola cannot substantially correct a Significant Defect in a commercially reasonable manner, Customer may terminate this Agreement and Motorola shall refund to Customer an amount

calculated by multiplying the total amount of Service Fees paid by Customer for the then-current Service Period by the percentage resulting from dividing the number of days remaining in the then-current Service Period, by 365. The foregoing remedies are Customer's exclusive remedy for defects in the LPR Software Product. Motorola shall not be responsible for labor charges for removal or reinstallation of defective software, charges for transportation, shipping or handling loss, unless such charges are due to Motorola's gross negligence or intentional misconduct. **MOTOROLA DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL MOTOROLA BE LIABLE FOR ANY DAMAGES WHATSOEVER ARISING OUT OF THE USE OF, OR INABILITY TO USE, THE SOFTWARE PRODUCTS.**

B. Infringement Protection. If an infringement claim is made against Customer by a third-party in a court of competent jurisdiction regarding Customer's use of any of the Software Products, Motorola shall indemnify Customer, and assume all legal responsibility and costs to contest any such claim. If Customer's use of any portion of the Software Products or documentation provided to Customer by Motorola in connection with the Software Products is enjoined by a court of competent jurisdiction, Motorola shall do one of the following at its option and expense within sixty (60) days of such enjoinment: (1) Procure for Customer the right to use such infringing portion; (2) replace such infringing portion with a non-infringing portion providing equivalent functionality; or (3) modify the infringing portion so as to eliminate the infringement while providing equivalent functionality.

C. Use of Software Products Interface. Under certain circumstances, it may be dangerous to operate a moving vehicle while attempting to operate a touch screen or laptop screen and any of their applications. It is agreed by Customer that Customer's users will be instructed to only utilize the interface to the Software Products at times when it is safe to do so. Motorola is not liable for any accident caused by a result of distraction such as from viewing the screen while operating a moving vehicle.

V. Software Support, Warranty and Maintenance.

Customer will receive technical support by submitting a support ticket to Motorola's company support website or by sending an email to Motorola's support team. Updates, patches and bug fixes of the Software Products will be made available to Customer at no additional charge, although charges may be assessed if the Software Product is requested to be delivered on physical media. Motorola will provide Software Products support to Customer's Technical Support Agents through e-mail, fax and telephone.

VI. Camera License Keys (CLKs).

Customer is entitled to use of the Software Products during the term of this Agreement to set up and install the Software Products on an unlimited number of media centers within Customer's agency in accordance with selected Service Options. As Customer installs additional units of the Software Products and connects them to LPR cameras, Customer is

required to obtain a Camera License Key (CLK) for each camera installed and considered in active service. A CLK can be obtained by Customer by going to Motorola's company support website and completing the online request form to Motorola technical support staff. Within two (2) business days of Customer's application for a CLK, Customer's Technical Support Agent will receive the requested CLK that is set to expire on the last day of the Initial Term or the then-current Service Period, as the case may be.

VII. Ownership of Software.

A. Ownership of Software Products. The Software Products are copyrighted by Motorola and remain the property of Motorola. The license granted under this Agreement is not a sale of the Software Products or any copy. Customer owns the physical media on which the Software Products are installed, but Motorola retains title and ownership of the Software Products and all other materials included as part of the Software Products.

B. Rights in Software Products. Motorola represents and warrants that: (1) it has title to the Software Products and the authority to grant license to use the Software Products; (2) it has the corporate power and authority and the legal right to grant the licenses contemplated by this Agreement; and (3) it has not and will not enter into agreements and will not take or fail to take action that causes its legal right or ability to grant such licenses to be restricted.

VIII. Data Sharing, Access and Security.

If Customer is a generator as well as a consumer of LPR Data, Customer at its option may share its LEA LPR Data with similarly situated LEAs who contract with Motorola to access LEARN (for example, LEAs who share LEA LPR Data with other LEAs). Motorola will not share any LEA LPR Data generated by the Customer without the permission of the Customer.

Motorola has implemented procedures to allow for adherence to the FBI CJIS Security Policy. The hosting facility utilizes access control technologies that meet or exceed CJIS requirements. In addition, Motorola has installed and configured network intrusion prevention appliances, as well as ensured that the configuration of the Microsoft environment adhere to the Windows Server Security Guide.

IX. Ownership and use of Data.

Motorola retains all title and rights to Commercial LPR Data and all Commercial Booking Images. Users shall not utilize Commercial LPR Data or Commercial Booking Images on the behalf of other local, state or Federal LEAs. Customer retains all rights to LEA LPR Data and LEA Booking Images generated by the Customer. Should Customer terminate agreement with Motorola, a copy of all LEA LPR Data and LEA Booking Images generated by the Customer will be created and provided to the Customer.
After the copy is created, all LEA LPR Data and LEA Booking Images generated by the Customer will be deleted from LEARN at the written request of an authorized representative of the Customer or per the Customer's designated retention policy, whichever occurs first. Commercial LPR Data, Commercial Booking Images, LEA LPR Data and LEA Booking Images should be used by the Customer for law enforcement purposes only.

X. Loss of Data, Irregularities and Recovery.

Motorola places imperative priority on supporting and maintaining data center integrity. Using redundant disk arrays, there is a virtual guarantee that any hard disk failure will not result in the corruption or loss of the valuable LPR data that is essential to the LEARN system and clients.

XI. Data Retention and Redundancy.

LEA LPR Data and LEA Booking Images are governed by the contributing LEA's retention policy. LEA LPR Data that reaches its expiration date will be deleted from LEARN. Motorola's use of redundant power sources, fiber connectivity and disk arrays ensure no less than 99% uptime of the LEARN LPR database server system.

XII. Account Access.

A. Eligibility. Customer shall only authorize individuals who satisfy the eligibility requirements of "Users" to access LEARN. Motorola in its sole discretion may deny access to LEARN to any individual based on such person's failure to satisfy such eligibility requirements. User logins are restricted to agents and sworn officers of the Customer. No User logins may be provided to agents or officers of other local, state, or Federal LEAs without the express written consent of Motorola.

B. Security. Customer shall be responsible for assigning an Agency Manager who in turn will be responsible for assigning to each of Customer's Users a username and password (one per user account). A limited number of User accounts is provided. Customer will cause the Users to maintain username and password credentials confidential and will prevent use of such username and password credentials by any unauthorized person(s). Customer shall notify Motorola immediately if Customer believes the password of any of its Users has, or may have, been obtained or used by any unauthorized person(s). In addition, Customer must notify Motorola immediately if Customer becomes aware of any other breach or attempted breach of the security of any of its Users' accounts.

C. CJIS Requirements. Customer certifies that its LEARN users shall comply with the CJIS requirements outlined in Exhibit B.

XIII. Service Package, Fees and Payment Provisions.

A. Service Package. This Enterprise License Agreement is based on one (1) of the three (3) following Service Package Options. Please select one (1) Service Package below:

☐ Service Package - Basic LPR Service Package:

- Vigilant Managed/Hosted LPR server LEARN Account
- Access to all Vigilant Software including all upgrades and updates
- Unlimited user licensing for the following applications:
  - LEARN, CarDetector and TAS

☐ Service Package - Option # 1 – Standard LPR Service Package:

- All Basic Service Package benefits
- Unlimited use of CarDetector – Mobile Hit Hunter (CDMS-MHH)
- Unlimited use of Vigilant's LPR Mobile Companion smartphone application

☐ Service Package - Option # 2 – 'Intelligence-Led Policing (ILP)' Service Package:

- All Service Package Option # 1 benefits
- Mobile LPR hardware up to level of Tier (see Exhibit A)
- Use of Vigilant Facial Recognition technologies up to level of Tier
  - FaceSearch Account
  - FaceSearch Mobile Companion
  - Templates up to limit for FaceSearch Account (details in Exhibit A)
- Tiered based on size of department (Tier 1A up to 50 sworn officers Tier 1 up to 100 sworn officers, Tier 2 up to 200 sworn officers, Tier 3 up to 500 sworn officers, Tier 4 up to 1,000 sworn officers, Tier 5 up to 1,500 sworn officers, Tier 6 up to 2,000 sworn officers)
- States, Federal Agencies, and Departments with greater than 2,000 sworn fall under a, "Custom" Tier which will be defined in the Annual Service Fee Schedule if applicable.

B. Service Fee. Payment of each Service Fee entitles Customer to all rights granted under this Agreement, including without limitation, use of the Software Products for the relevant Service Period, replacement of CLKs, and access to the updates and releases of the Software Products and associated equipment driver software to allow the Software Products to remain current and enable the best possible performance. The annual Service

Fee due for a particular Service Period is based on the number of current Motorola issued CLK's at the time of Service Fee invoicing, and which will be used by Customer in the upcoming Service Period. A schedule of annual Service Fees is shown below:

Annual Service Fee Schedule (multiplied by number of CLK's Issued)				
Total # of CLK's under this ESA	0-14 CLK's	15-30 CLK's	31-60 CLK's	Over 60
Basic Service	$525.00	$450.00	$400.00	$275.00
Standard (Option # 1)	$750.00	$640.00	$565.00	$390.00
ILP Subscriber CLK Renewal Fees	$525.00	$450.00	$400.00	$275.00

Intelligence-Led Policing Service Package Annual Fee Schedule		
Tier	Mobile	Fixed
ILP Tier 1B (Option #2)	$ 11,750.00	$ 22,250.00
ILP Tier 1A (Option #2)	$ 15,250.00	$ 25,750.00
ILP Tier 1 (Option #2)	$ 18,750.00	$ 29,250.00
ILP Tier 2 (Option #2)	$ 34,250.00	$ 55,250.00
ILP Tier 3 (Option #2)	$ 55,250.00	$ 86,750.00
ILP Tier 4 (Option #2)	$ 84,750.00	$126,750.00
ILP Tier 5 (Options #2)	$117,495.00	$169,995.00
ILP Tier 6 (Option #2)	$144,995.00	$207,995.00
ILP Tier 7 (Option #2)	$185,000.00	$251,000.00
ILP Tier 8 (Option #2)	$292,500.00	$369,000.00

Payment of the Service Fee is due thirty (30) days prior to the renewal of the then-current Service Period. All Service Fees are exclusive of any sales, use, value-added or other federal, state or local taxes (excluding taxes based on Motorola's net income) and Customer agrees to pay any such tax. Service Fees may increase by no higher than 4% per year for years after the first year of this agreement. For ILP (Option # 2) Tier packages, the Tier amount is due for subsequent periods and Basic Service CLK fees are due for all cameras from previous periods (this is in addition to the Annual Subscription Fee).

Customer and Motorola agree that the number of CLKs issued as of the Effective Date of this Agreement is_____[Insert Quantity]. All future additions of CLKs shall only be those as provided for in the definitions provided above.

C. Advanced Service Fee Payments. Motorola will accept advanced Service Fee payments on a case by
case basis for Customers who wish to lock in the Service Fee rates for subsequent periods at the rates currently in effect, as listed in the table above. If Customer makes advanced Service Fee payments to Motorola, advanced payments to Motorola will be applied in full to each subsequent Service Period's Service Fees until the balance of the credits is reduced to a zero balance. System based advanced credits shall be applied to subsequent Service Fees in the amount that entitles Customer continued operation of the designated camera unit systems for the following Service Period until the credits are reduced to a zero balance.

D. Price Adjustment. Motorola has the right to increase or decrease the annual Service Fee from one Service Period to another; *provided, however*, that in no event will a Service Fee be increased by more than 4% of the prior Service Period's Service Fees. If Motorola intends to adjust the Service Fee for a subsequent Service Period, it must give Customer notice of the proposed increase on or before the date that Motorola invoices Customer for the upcoming Service Period.

XIV. Miscellaneous.

A. Limitation of Liability. IN NO EVENT SHALL MOTOROLA BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL DAMAGES INCLUDING DAMAGES FOR LOSS OF USE, DATA OR PROFIT, ARISING OUT OF OR CONNECTED WITH THE USE OF THE SOFTWARE PRODUCTS, WHETHER BASED ON CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR OTHERWISE, EVEN IF MOTOROLA HAS BEEN ADVISED OF THE POSSIBILITY OF DAMAGES. IN NO EVENT WILL MOTOROLA'S LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT EXCEED THE FEES PAID BY CUSTOMER TO MOTOROLA FOR THE SOFTWARE PRODUCTS LICENSED UNDER THIS AGREEMENT.

B. Confidentiality. Customer acknowledges that Software Products contain valuable and proprietary information of Motorola and Customer will not disassemble, decompile or reverse engineer any Software Products to gain access to confidential information of Motorola.

C. Assignment. Neither Motorola nor Customer is permitted to assign this Agreement without the prior written consent of the other party. Any attempted assignment without written consent is void.

D. Amendment; Choice of Law. No amendment or modification of this Agreement shall be effective unless in writing and signed by authorized representatives of

the parties. This Agreement shall be governed by the laws of the state of Colorado without regard to its conflicts of law.

E. Complete Agreement; Order of Precedence. This Agreement constitutes the final and complete agreement between the parties with respect to the subject matter hereof, and supersedes any prior or contemporaneous agreements, written or oral, with respect to such subject matter. In interpreting this Agreement and resolving any ambiguities: The applicable service Addendum for the services contemplated therein will take precedence over the main body of the Agreement.

F. Relationship. The relationship created hereby is that of contractor and customer and of licensor and Customer. Nothing herein shall be construed to create a partnership, joint venture, or agency relationship between the parties hereto. Neither party shall have any authority to enter into agreements of any kind on behalf of the other and shall have no power or authority to bind or obligate the other in any manner to any third party. The employees or agents of one party shall not be deemed or construed to be the employees or agents of the other party for any purpose whatsoever. Each party hereto represents that it is acting on its own behalf and is not acting as an agent for or on behalf of any third party.

G. No Rights in Third Parties. This agreement is entered into for the sole benefit of Motorola and Customer and their permitted successors, executors, representatives, administrators and assigns. Nothing in this Agreement shall be construed as giving any benefits, rights, remedies or claims to any other person, firm, corporation or other entity, including, without limitation, the general public or any member thereof, or to authorize anyone not a party to this Agreement to maintain a suit for personal injuries, property damage, or any other relief in law or equity in connection with this Agreement.

H. Construction. The headings used in this Agreement are for convenience and ease of reference only, and do not define, limit, augment, or describe the scope, content or intent of this Agreement. Any term referencing time, days or period for performance shall be deemed calendar days and not business days, unless otherwise expressly provided herein.

I. Severability. If any provision of this Agreement shall for any reason be held to be invalid, illegal, unenforceable, or in conflict with any law of a federal, state, or local government having jurisdiction over this Agreement, such provision shall be construed so as to make it enforceable to the greatest extent permitted, such provision shall remain in effect to the greatest extent permitted and the remaining provisions of this Agreement shall remain in full force and effect.

J. Federal Government. Any use, copy or disclosure of Software Products by the U.S. Government is subject to restrictions as set forth in this Agreement and as provided by DFARS 227.7202-1(a) and 227.7202-3(a) (1995), DFARS 252.227-7013(c)(1)(ii) (Oct 1988), FAR 12.212(a)(1995), FAR 52.227-19, or FAR 52.227 (ALT III), as applicable.

K. Right to Audit. Customer, upon thirty (30) days advanced written request to Motorola, shall have the right to investigate, examine, and audit any and all necessary non-financial books, papers, documents, records and personnel that pertain to this Agreement and any other Sub Agreements.

L. Notices; Authorized Representatives; Technical Support Agents. All notices, requests, demands, or other communications required or permitted to be given hereunder must be in writing and must be addressed to the parties at their respective addresses set forth below and shall be deemed to have been duly given when (a) delivered in person; (b) sent by facsimile transmission indicating receipt at the facsimile number where sent; (c) one (1) business day after being deposited with a reputable overnight air courier service; or (d) three (3) business days after being deposited with the United States Postal Service, for delivery by certified or registered mail, postage pre-paid and return receipt requested. All notices and communications regarding default or termination of this Agreement shall be delivered by hand or sent by certified mail, postage pre-paid and return receipt requested. Either party may from time to time change the notice address set forth below by delivering 30 days advance notice to the other party in accordance with this section setting forth the new address and the date on which it will become effective.

Motorola Solutions	**Customer:**
Attn: Sales	_____
500 W Monroe St	Attn: _____
Chicago, IL 60661	Address: _____

M. Authorized Representatives; Technical Support Agents. Customer's Authorized Representatives and its Technical Support Agents are set forth below in the Contact Information Worksheet. Customer's Authorized Representative is responsible for administering this Agreement and Customer's Technical Support Agents are responsible for administering the Software Products and acting as Customer's Software Products support contact. Either party may from time to time change its Authorized Representative, and Customer may from time to time change its Technical Support Agents, in each case, by delivering 30 days advance notice to the other party in accordance with the notice provisions of this Agreement.

N. Facial Recognition Image Integration. Customer may elect, at its sole discretion, to have Motorola enable the ability for the Customer's existing facial recognition

images to be imported into its FaceSearch gallery. This process requires some reformatting of the data for compatibility. The data remains property of the Customer, is maintained according to the retention policy set by the Customer and is shared to other agencies under the rules defined by the Customer. This service is at an additional cost. Motorola uses a third-party service from The Center for Law Enforcement Technology, Training, & Research, Inc. (LETTR) to deliver this service. If the Customer elects to use this service, it acknowledges that The Center for Law Enforcement Technology, Training, & Research, Inc. a non-profit, 501(c)(3) corporation, working under contract with Motorola and acting on behalf of the Customer, will perform the described services for law enforcement information sharing purposes.

IN WITNESS WHEREOF, the parties have executed the Agreement as of the Effective Date.

Company: Motorola Solutions, Inc.

Authorized Agent:

Title:

Date:

_____

Signature:

_____

CustomerOrganization:

_____

Authorized Agent:

_____

Title:

_____

Date:

_____

Signature:

_____

Enterprise Service Agreement
Contact Information Worksheet

Please complete the following contact information for your Software Products Enterprise License program.

Enterprise License Agreement Holder			
Company / Agency Name:			
Company / Agency Type:			
Address:			
Primary Contact			
Name:			
Title:		Phone:	
Email:			
Supervisor Information			
Name:			
Title:		Phone:	
Email:			
Financial Contact (Accounts Payable)			
Name:			
Title:		Phone:	
Email:			
Technical Support Contact # 1			
Name:			
Title:		Phone:	
Email:			
Technical Support Contact # 2			
Name:			
Title:		Phone:	
Email:			

For questions or concerns, please contact Motorola Solutions' sales team:

sales@vigilantsolutions.com

1-925-398-2079

Exhibit A: Option # 2 ILP Tier Package Components

ILP Bundle for Agencies of Up to 25 Sworn Includes: - Agency license for LEARN SaaS - Unlimited access to Commercial LPR data - One (1) 3-Camera Mobile LPR System or Three (3) Fixed Camera Systems - First year of Basic and Standard Service Packages - LEARN-Mobile Companion - Mobile Hit Hunter - Agency license for FaceSearch - Image gallery up to 5,000 images	**ILP Bundle for Agencies of Up to 50 Sworn** Includes: - Agency license for LEARN SaaS - Unlimited access to Commercial LPR data - One (1) 3-Camera Mobile LPR System or Three (3) Fixed Camera Systems - First year of Basic and Standard Service Packages - LEARN-Mobile Companion - Mobile Hit Hunter - Agency license for FaceSearch - Image gallery up to 5,000 images
ILP Bundle for Agencies of 51 to 100 Sworn Includes: - Agency license for LEARN SaaS - Unlimited access to Commercial LPR data - One (1) 3-Camera Mobile LPR System or Three (3) Fixed Camera Systems - First year of Basic and Standard Service Packages - LEARN-Mobile Companion - Mobile Hit Hunter - Agency license for FaceSearch - Image gallery up to 5,000 images	**ILP Bundle for Agencies of 101 to 200 Sworn** Includes: - Agency license for LEARN SaaS - Unlimited access to Commercial LPR data - Two (2) 3-Camera Mobile LPR System or Six (6) Fixed Camera Systems - First year of Basic and Standard Service Packages - LEARN-Mobile Companion - Mobile Hit Hunter - Agency license for FaceSearch - Image gallery up to 20,000 images
ILP Bundle for Agencies of 201 to 500 Sworn Includes: - Agency license for LEARN SaaS - Unlimited access to Commercial LPR data - Three (3) 3-Camera Mobile LPR System or Nine (9) Fixed Camera Systems - First year of Basic and Standard Service Packages - LEARN-Mobile Companion - Mobile Hit Hunter - Agency license for FaceSearch - Image gallery up to 50,000 images	**ILP Bundle for Agencies of 501 to 1,000 Sworn** Includes: - Agency license for LEARN SaaS - Unlimited access to Commercial LPR data - Four (4) 3-Camera Mobile LPR Systems or Twelve (12) Fixed Camera Systems - First year of Basic and Standard Service Packages - LEARN-Mobile Companion - Mobile Hit Hunter - Agency license for FaceSearch - Image gallery up to 75,000 images

ILP Bundle for Agencies of 1,000 to 1,500 Sworn	**ILP Bundle for Agencies of 1,501 to 2,000 Sworn**
Includes: - Agency license for LEARN SaaS - Unlimited access to Commercial LPR data - Five (5) 3-Camera Mobile LPR Systems or Fifteen (15) Fixed Camera Systems - First year of Basic and Standard Service Packages - LEARN-Mobile Companion - Mobile Hit Hunter - Agency license for FaceSearch - Image gallery up to 100,000 images	Includes: - Agency license for LEARN SaaS - Unlimited access to Commercial LPR data - Six (6) 3-Camera Mobile LPR Systems or Eighteen (18) Fixed Camera Systems - First year of Basic and Standard Service Packages - LEARN-Mobile Companion - Mobile Hit Hunter - Agency license for FaceSearch - Image gallery up to 200,000 images

ILP Bundle for Agencies up to 2,500 Sworn	**ILP Bundle for Agencies up to 5,000 Sworn**
Includes: - Agency license for LEARN SaaS - Unlimited access to Commercial LPR data - Seven (7) 3-Camera Mobile LPR Systems or Twenty one (24) Fixed Camera Systems - First year of Basic and Standard Service Packages - LEARN-Mobile Companion - Mobile Hit Hunter - Agency license for FaceSearch - Image gallery up to 250,000 images	Includes: - Agency license for LEARN SaaS - Unlimited access to Commercial LPR data - Eight (8) 3-Camera Mobile LPR Systems or Twenty four (24) Fixed Camera Systems - First year of Basic and Standard Service Packages - LEARN-Mobile Companion - Mobile Hit Hunter - Agency license for FaceSearch - Image gallery up to 500,000 images

Exhibit B: CJIS Requirements

Motorola and the Customer agree on the importance of data security, integrity and system availability and that these security objectives will only be achieved through shared responsibility. Motorola and the Customer agree they will more likely be successful with information security by use of the Motorola supplied technical controls and client Customer use of those controls; in conjunction with agency and personnel policies to protect the systems, data and privacy.

Motorola and the Customer agree that Customer owned and FBI-CJIS supplied data in Motorola systems does not meet the definition of FBI-CJIS provided Criminal Justice Information (CJI). Regardless, Motorola agrees to treat the Customer-supplied information in Motorola systems as CJI. Motorola will strive to meet those technical and administrative controls; ensuring the tools are in place for the proper protection of systems, information and privacy of individuals to the greatest degree possible.

Motorola and the Customer agree that information obtained or incorporated into Motorola systems may be associated with records that are sensitive in nature having, tactical, investigative and Personally Identifiable Information. As such, that information will be treated in accordance with applicable laws, policies and regulations governing protection and privacy of this type of data.

Motorola and the Customer agree that products and services offered by Motorola are merely an investigative tool to aid the client in the course of their duties and that Motorola make no claims that direct actions be initiated based solely upon the information responses or analytical results. Further, Motorola and the Customer agree that the Customer is ultimately responsible for taking the appropriate actions from results, hits, etc. generated by Motorola products and require ongoing training, human evaluation, verifying the accuracy and currency of the information, and appropriate analysis prior to taking any action.
As such, the parties agree to do the following with respect to Software Products, and the obligations contained herein do not apply to any products, software or services supplied by Motorola other than the Software Products

Motorola:

1. Motorola has established the use of FBI-CJIS Security Policy as guidance for implementing technical security controls in an effort to meet or exceed those Policy requirements.
2. Motorola agrees to appoint a CJIS Information Security Officer to act as a conduit to the client Contracting Government Agency, Agency Coordinator, to receive any security policy information and disseminate to the appropriate staff.
3. Motorola agrees to adhere to FBI-CJIS Security Policy Awareness Training and Personnel Screening standards as required by the Customer.
4. Motorola agrees, by default, to classify all client supplied data and information related to client owned infrastructure, information systems or communications systems as “Criminal Justice Data”. All client information will be treated at the highest level of confidentiality by all Motorola staff and authorized partners. Motorola has supporting guidance/policies for staff handling the full life cycle of information in physical or electronic form and has accompanying disciplinary procedures for unauthorized access, misuse or mishandling of that information.

5. Motorola will not engage in data mining, commercial sale, unauthorized access and/or use of any of Customer owned data.
6. Motorola and partners agree to use their formal cyber Incident Response Plan if such event occurs.
7. Motorola agrees to immediately inform Customer of any cyber incident or data breach, to include DDoS, Malware, virus, etc. that may impact or harm client data, systems or operations so proper analysis can be performed and client Incident Response Procedures can be initiated.
8. Motorola will only allow authorized support staff to access the Customer's account or Customer data in support of Customer as permitted by the terms of contracts.
9. Motorola agrees to use training, policy and procedures to ensure support staff use proper handling, processing, storing, and communication protocols for Customer data.
10. Motorola agrees to protect client systems and data by monitoring and auditing staff user activity to ensure that it is only within the purview of system application development, system maintenance or the support roles assigned.
11. Motorola agrees to inform the Customer of any unauthorized, inappropriate use of data or systems.
12. Motorola will design software applications to facilitate FBI-CJIS compliant information handling, processing, storing, and communication of Customer.
13. Motorola will advise Customer when any software application or equipment technical controls are not consistent with meeting FBI-CJIS Policy criteria for analysis and due consideration.
14. Motorola agrees to use the existing Change Management process to sufficiently plan for system or software changes and updates with Rollback Plans.
15. Motorola agrees to provide technical security controls that only permit authorized user access to Customer owned data and Motorola systems as intended by the Customer and data owners.
16. Motorola agrees to meet or exceed the FBI-CJIS Security Policy complex password construction and change rules.
17. Motorola will only provide access to Motorola systems and Customer owned information through Customer managed role-based access and applied sharing rules configured by the Customer.
18. Motorola agrees to provide technical controls with additional levels of user Advanced Authentication in Physically Non-Secure Locations.
19. Motorola agrees to provide compliant FIPS 140-2 Certified 128-bit encryption to Customer owned data during transport and storage ("data at rest") while in the custody and control of Motorola.
20. Motorola agrees to provide firewalls and virus protection to protect networks, storage devices and data.
21. Motorola agrees to execute archival, purges and/or deletion of data as configured by the data owner.
22. Motorola agrees to provide auditing and alerting tools within the software applications so Customer can monitor access and activity of Motorola support staff and Customer

users for unauthorized access, disclosure, alteration or misuse of Customer owned data. (Motorola support staff will only have access when granted by the Customer.)

23. Motorola will only perform direct support remote access to Customer systems/infrastructure when requested, authorized and physically granted access to the applications/systems by the Customer. This activity will be documented by both parties.
24. Motorola creates and retains activity transaction logs to enable auditing by the Customer data owners and Motorola staff.
25. Motorola agrees to provide physical protection for the equipment-storing Customer data along with additional technical controls to protect physical and logical access to systems and data.
26. Motorola agrees to participate in any Information or Technical Security Compliance Audit performed by the Customer, state CJIS System Agency or FBI-CJIS Division.
27. Motorola agrees to perform independent employment background screening for its' staff and participate in additional fingerprint background screening as required by Customer.
28. Motorola agrees that the Customer owns all Customer contributed data to include "hot-lists", scans, user information etc., is only shared as designated by the client and remains the responsibility and property of the Customer.

Customer:

1. Customer agrees to appoint an Agency Coordinator as a central Point of Contact for all FBI-CJIS Security Policy related matters and to assign staff that are familiar with the contents of the FBI-CJIS Security Policy.
2. Customer agrees to have the Agency Coordinator provide timely updates with specific information regarding any new FBI-CJIS, state or local information security policy requirements that may impact Motorola compliance or system/application development and, to facilitate obtaining certifications, training, and fingerprint-based background checks as required.
3. Customer agrees to inform Motorola when any FBI-CJIS Security Awareness Training, personnel background screening or execution of FBI-CJIS Security Addendum Certifications are required.
4. Customer agrees to immediately inform Motorola of any relevant data breach or cyber incident, to include DDoS, Malware, virus, etc. that may impact or harm Motorola systems, operations, business partners and/or other Customers, so proper analysis can be performed, and Incident Response Procedures can be initiated.
5. Customer agrees that they are responsible for the legality and compliance of information recorded, submitted or placed in Motorola systems and use of that data.
6. Customer agrees that they are responsible for proper equipment operation and placement of equipment.
7. Customer agrees that they are responsible for vetting authorized user access to Motorola systems with due consideration of providing potential access to non-Customer information.

8. Customer agrees that responsibility and control of persons granted access to purchased Motorola systems, along with data stored and transmitted via Motorola systems, is that of the Customer.
9. Customer agrees that they have responsibility for all data security, handling and data protection strategies from point of acquisition, during transport and until submission (“Hotlist upload”) into Motorola systems.
10. Customer agrees to reinforce client staff policies and procedures for secure storage and protection of Motorola system passwords.
11. Customer agrees to reinforce client staff policies for creating user accounts with only government domain email addresses. Exceptions will be granted in writing.
12. Customer agrees to reinforce client staff policies for not sharing user accounts.
13. Customer agrees to use Motorola role-based access as designed to foster system security and integrity.
14. Customer agrees that they control, and are responsible for, appropriate use and data storage policies as well as procedures for the data maintained outside the Motorola systems. This includes when any information is disseminated, extracted or exported out of Motorola systems.
15. Customer agrees that they control and are responsible for developing policies, procedures and enforcement for applying deletion/purging and dissemination rules to information within and outside the Motorola systems.
16. Customer agrees that it is their responsibility to ensure data and system protection strategies are accomplished through the tools provided by Motorola for account and user management features along with audit and alert threshold features.
17. Customer agrees to use the “virtual escorting” security tools provided for managing client system remote access and monitor Motorola support staff when authorized to assist the client.
18. Customer agrees that the Motorola designed technical controls and tools will only be effective in conjunction with Customer created policies and procedures that guide user access and appropriate use of the system.
19. Customer agrees that information and services provided through Motorola products do not provide any actionable information, Customer users are responsible for the validity and accuracy of their data and developing procedures to verify information with the record owner and other systems (NCIC) based upon the potential lead generated.

EQUIPMENT SALE ADDENDUM
LPR hardware components

This Addendum is to the Enterprise Service Agreement ("Primary Agreement") and provides additional or different terms and conditions to govern the sale of equipment and related software provided by Motorola. The terms in this Addendum are integral to and incorporated into the Primary Agreement. To the extent there is a conflict between the terms and conditions of the Primary Agreement and the terms and conditions of this Addendum, this Addendum takes precedence, as to the inconsistency only.

1. Exhibits

The Exhibits listed below are incorporated into and made a part of this Addendum. In interpreting this Addendum and resolving any ambiguities, the main body of this Addendum takes precedence over the exhibits and any inconsistency between the exhibits will be resolved in their listed order. Documents included in the proposal and listed below as Exhibits are incorporated by this reference.

Exhibit A Motorola "Software License Agreement"
Exhibit B Equipment List.

2. DEFINITIONS

All capitalized terms not otherwise defined herein shall have the same meaning as defined in the Primary Agreement.

2.1. "Product Price" means the price for the equipment and related Software and installation or related services, excluding applicable sales or similar taxes and freight charges.

2.2. "Effective Date" means that date upon which the last Party executes the Primary Agreement or, the date on which the last Party executes the Addendum, whichever is later.

2.3. "Equipment" means the equipment listed in the Equipment List that Customer purchases from Motorola pursuant to this Addendum.

2.4 "Infringement Claim" means a third party claim alleging that the Equipment manufactured by Motorola or the Motorola Software directly infringes a United States patent or copyright.

2.5. "Motorola Software" means Software that Motorola or its affiliated company owns.

2.6. "Non-Motorola Software" means Software that another party owns.

2.7. "Open Source Software" (also called "freeware" or "shareware") software with either freely obtainable source code, license for modification, or permission for free distribution.

2.8. "Products" mean the Equipment and Software sold by Motorola under this Addendum.

2.9. “Proprietary Rights” means the patents, patent applications, inventions, copyrights, trade secrets, trademarks, trade names, mask works, know-how, ideas and concepts, moral rights, processes, methodologies, tools, techniques, and other intellectual property rights in and to the Equipment and Software, including those created or produced by Motorola under this Addendum and any corrections, bug fixes, enhancements, updates or modifications to or derivative works from the Software whether made by Motorola or another party.

2.10. “Software” means the Motorola Software and Non-Motorola Software in object code format that is furnished with the Equipment.

2.11. “Specifications” means the functionality and performance requirements that are described in the Proposal/Quote or Technical and Implementation Documents (as applicable).

2.12 “Warranty Period” means one (1) year from the date of shipment of the Products.

3. SCOPE AND TERM

3.1. SCOPE OF WORK. Motorola will provide and install (if applicable) the Products, and perform its other contractual responsibilities, all in accordance with this Addendum.

3.2. CHANGE ORDERS. Either Party may request changes within the general scope of this Addendum. Neither Party is obligated to perform requested changes unless both Parties execute a written change order.

3.3. TERM. Unless terminated in accordance with other provisions of the Primary Agreement or extended by mutual agreement of the Parties, the term of this Addendum begins on the Effective Date and continues until the expiration of the Warranty Period or three (3) years from the Effective Date, whichever occurs last.

3.4. ADDITIONAL EQUIPMENT OR SOFTWARE. During the Term of this Addendum, Customer may order additional Equipment or Software if it is then available. Each order must refer to the Primary Agreement and Addendum and must specify the pricing and delivery terms. Notwithstanding any additional or contrary terms in the order, the applicable provisions of this Addendum (except for pricing, delivery, and payment terms) will govern the purchase and sale of the additional Equipment or Software. Payment is due within thirty (30) days after the invoice date, and Motorola will send Customer an invoice as the additional Equipment is shipped or Software is licensed

3.5. MAINTENANCE SERVICE. This Addendum does not cover maintenance or support of the Products except as provided under the warranty. If Customer wishes to purchase maintenance or support, Motorola will provide a separate maintenance and support proposal upon request.

3.6. MOTOROLA SOFTWARE. Any Motorola Software, including subsequent releases, is licensed to Customer solely in accordance with the Software License Agreement.

Customer hereby accepts and agrees to abide by all of the terms and restrictions of the Software License Agreement.

3.7. NON-MOTOROLA SOFTWARE. Any Non-Motorola Software is licensed to Customer in accordance with the standard license, terms, and restrictions of the copyright owner on the Effective Date unless the copyright owner has granted to Motorola the right to sublicense the Non-Motorola Software pursuant to the Software License Agreement, in which case it applies and the copyright owner will have all of Licensor's rights and protections under the Software License Agreement. Motorola makes no representations or warranties of any kind regarding Non-Motorola Software. Non-Motorola Software may include Open Source Software. Upon request by Customer, Motorola will use commercially reasonable efforts to determine whether any Open Source Software will be provided under this Agreement; and if so, identify the Open Source Software and provide to Customer a copy of the applicable standard license (or specify where that license may be found); and provide to Customer a copy of the Open Source Software source code if it is publicly available without charge (although a distribution fee or a charge for related services may be applicable).

3.8 SUBSTITUTIONS. At no additional cost to Customer, Motorola may substitute any Equipment, Software, or services to be provided by Motorola, if the substitute meets or exceeds the Specifications and is of equivalent or better quality to the Customer. Any substitution will be reflected in a change order.

Section 4 ACCEPTANCE, PERFORMANCE SCHEDULE AND DELAYS

4.1 Acceptance of the Products will occur upon delivery to Customer.

4.2 If this Addendum includes the performance of services relating to the Product, the proposal/quote or Statement of Work will describe the performance schedule, or if there is no performance schedule, within a reasonable period of time.

Section 5 CONTRACT PRICE, PAYMENT, AND INVOICING

5.1. PRODUCT PRICE. The Product Price in U.S. dollars is set forth in the Statement of Work and is due and payable as described therein.

5.2. INVOICING AND PAYMENT. Motorola will submit invoices to Customer for Products and for installation or related services when they are performed. Customer will make payments to Motorola within thirty (30) days after the date of each invoice. Customer will make payments when due in the form of a wire transfer, check, or cashier's check from a U.S. financial institution. Overdue invoices will bear simple interest at the maximum allowable rate. For Customer's reference, the Federal Tax Identification Number for Motorola Solutions, Inc. is 36-1115800

5.3 FREIGHT, TITLE, AND RISK OF LOSS. Unless otherwise agreed in writing, title and risk of loss to the Equipment will pass to Customer upon shipment. Notwithstanding, title to Software will not pass to Customer at any time. Motorola will pack and ship all Equipment in accordance with good commercial practices.

SECTION 6 SITES AND SITE CONDITIONS

6.1. ACCESS TO SITES. If Motorola is providing installation or other services, Customer will provide all necessary construction and building permits, licenses, and the like; and access to the work sites or vehicles identified in the Technical and Implementation Documents as reasonably requested by Motorola so that it may perform its contractual duties.

6.2. SITE CONDITIONS. If Motorola is providing installation or other services at Customer's sites, Customer will ensure that these work sites be safe, secure, and in compliance with all applicable industry and OSHA standards.

To the extent applicable and unless the Statement of Work states to the contrary, Customer will ensure that these work sites have adequate: physical space, air conditioning and other environmental conditions; adequate and appropriate electrical power outlets, distribution, equipment and connections; and adequate telephone or other communication lines (including modem access and adequate interfacing networking capabilities), all for the installation, use and maintenance of the Products.

Section 7 REPRESENTATIONS AND WARRANTIES

7.1. EQUIPMENT WARRANTY. During the Warranty Period, Motorola warrants that the Equipment under normal use and service will be free from material defects in materials and workmanship.

7.2. MOTOROLA SOFTWARE WARRANTY. Unless otherwise stated in the Software License Agreement, during the Warranty Period, Motorola warrants the Motorola Software in accordance with the terms of the Software License Agreement and the provisions of this Section that are applicable to the Motorola Software.

7.3. EXCLUSIONS TO EQUIPMENT AND MOTOROLA SOFTWARE WARRANTIES. These warranties do not apply to: (i) defects or damage resulting from: use of the Equipment or Motorola Software in other than its normal, customary, and authorized manner; accident, liquids, neglect, or acts of God; testing, maintenance, disassembly, repair, installation, alteration, modification, or adjustment not provided or authorized in writing by Motorola; Customer's failure to comply with all applicable industry and OSHA standards; (ii) breakage of or damage to antennas unless caused directly by defects in material or workmanship; (iii) Equipment that has had the serial number removed or made illegible; (iv) batteries (because they carry their own separate limited warranty) or consumables; (v) freight costs to ship Equipment to the repair depot; (vi) scratches or other cosmetic damage to Equipment surfaces that does not affect the operation of the Equipment; and (vii) normal or customary wear and tear.

7.4. WARRANTY CLAIMS. To assert a warranty claim, Customer must notify Motorola in writing of the claim before the expiration of the Warranty Period. Upon receipt of this notice, Motorola will investigate the warranty claim. If this investigation confirms a valid warranty claim, Motorola will (at its option and at no additional charge to Customer) repair the defective Equipment or Motorola Software, replace it with the same or equivalent product, or refund the price of the defective Equipment or Motorola Software. That action will be the full extent of Motorola's liability for the warranty claim. If this investigation indicates

the warranty claim is not valid, then Motorola may invoice Customer for responding to the claim on a time and materials basis using Motorola's then current labor rates. Repaired or replaced product is warranted for the balance of the original applicable Warranty Period. All replaced products or parts will become the property of Motorola.

7.5. ORIGINAL END USER IS COVERED. These express limited warranties are extended by Motorola to the original user purchasing the Products for commercial, industrial, or governmental use only, and are not assignable or transferable.

7.6. DISCLAIMER OF OTHER WARRANTIES. THESE WARRANTIES ARE THE COMPLETE WARRANTIES FOR THE EQUIPMENT AND MOTOROLA SOFTWARE PROVIDED UNDER THIS ADDENDUM AND ARE GIVEN IN LIEU OF ALL OTHER WARRANTIES. MOTOROLA DISCLAIMS ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

SECTION 8 INDEMNIFICATION

8.1. RESERVED.

8.2. PATENT AND COPYRIGHT INFRINGEMENT INDEMNIFICATION

8.2.1. Motorola will defend at its expense any suit brought against Customer to the extent it is based on a third-party claim alleging that the Equipment manufactured by Motorola or the Motorola Software ("Motorola Product") directly infringes a United States patent or copyright ("Infringement Claim"). Motorola's duties to defend and indemnify are conditioned upon: Customer promptly notifying Motorola in writing of the Infringement Claim; Motorola having sole control of the defense of the suit and all negotiations for its settlement or compromise; and Customer providing to Motorola cooperation and, if requested by Motorola, reasonable assistance in the defense of the Infringement Claim. In addition to Motorola's obligation to defend, and subject to the same conditions, Motorola will pay all damages finally awarded against Customer by a court of competent jurisdiction for an Infringement Claim or agreed to, in writing, by Motorola in settlement of an Infringement Claim.

8.2.2. If an Infringement Claim occurs, or in Motorola's opinion is likely to occur, Motorola may at its option and expense: (a) procure for Customer the right to continue using the Motorola Product; (b) replace or modify the Motorola Product so that it becomes non-infringing while providing functionally equivalent performance; or (c) accept the return of the Motorola Product and grant Customer a credit for the Motorola Product, less a reasonable charge for depreciation. The depreciation amount will be calculated based upon generally accepted accounting standards.

8.2.3. Motorola will have no duty to defend or indemnify for any Infringement Claim that is based upon: (a) the combination of the Motorola Product with any software, apparatus or device not furnished by Motorola; (b) the use of ancillary equipment or software not furnished by Motorola and that is attached to or used in connection with the Motorola Product; (c) Motorola Product designed or manufactured in accordance with Customer's designs, specifications, guidelines or instructions, if the alleged infringement would not have occurred without such designs, specifications, guidelines or instructions; (d) a modification of the Motorola Product by a party other than Motorola; (e) use of the Motorola Product in a manner for which the Motorola Product was not designed or that is inconsistent with the terms of this Addendum; or (f) the failure by Customer to install an enhancement release to

the Motorola Software that is intended to correct the claimed infringement. In no event will Motorola's liability resulting from its indemnity obligation to Customer extend in any way to royalties payable on a per use basis or the Customer's revenues, or any royalty basis other than a reasonable royalty based upon revenue derived by Motorola from Customer from sales or license of the infringing Motorola Product.

8.2.4. This Section 8.2 provides Customer's sole and exclusive remedies and Motorola's entire liability in the event of an Infringement Claim. Customer has no right to recover and Motorola has no obligation to provide any other or further remedies, whether under another provision of this Addendum or any other legal theory or principle, in connection with an Infringement Claim. In addition, the rights and remedies provided in this Section 8 are subject to and limited by the restrictions set forth in Section 9.

SECTION 9 LIMITATION OF LIABILITY

Except for personal injury, death or damage to tangible property, Motorola's total liability, whether for breach of contract, warranty, negligence, strict liability in tort, indemnification, or otherwise, will be limited to the direct damages recoverable under law, but not to exceed the price of the Equipment, Software, or services with respect to which losses or damages are claimed. ALTHOUGH THE PARTIES ACKNOWLEDGE THE POSSIBILITY OF SUCH LOSSES OR DAMAGES, THEY AGREE THAT MOTOROLA WILL NOT BE LIABLE FOR ANY COMMERCIAL LOSS; INCONVENIENCE; LOSS OF USE, TIME, DATA, GOOD WILL, REVENUES, PROFITS OR SAVINGS; OR OTHER SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES IN ANY WAY RELATED TO OR ARISING FROM THIS ADDENDUM, THE SALE OR USE OF THE EQUIPMENT OR SOFTWARE, OR THE PERFORMANCE OF SERVICES BY MOTOROLA PURSUANT TO THIS ADDENDUM. This limitation of liability provision survives the expiration or termination of the Addendum and applies notwithstanding any contrary provision. No action for contract breach or otherwise relating to the transactions contemplated by this Addendum may be brought more than one (1) year after the accrual of the cause of action, except for money due upon an open account.

Section 10 GENERAL

10.1. TAXES. The Contract Price does not include excise, sales, lease, use, property, or other taxes, assessments or duties, all of which will be paid by Customer except as exempt by law. If Motorola is required to pay any of these taxes, Motorola will send an invoice to Customer and Customer will pay to Motorola the amount of the taxes (including any interest and penalties) within thirty (30) days after the date of the invoice. Customer will be solely responsible for reporting the Equipment for personal property tax purposes, and Motorola will be solely responsible for reporting taxes on its income or net worth.

10.2 MISCELLANEOUS. This addendum may be executed in multiple counterparts, and shall have the same legal force and effect as if the Parties had executed it as a single document. The Parties may sign in writing, or by electronic signature, including by email. An

electronic signature, or a facsimile copy or computer image, such as a PDF or tiff image, of a signature, shall be treated as and shall have the same effect as an original signature. In addition, an electronic signature, a true and correct facsimile copy or computer image of this Addendum shall be treated as and shall have the same effect as an original signed copy of this document.

10.3 AUTHORITY TO EXECUTE ADDENDUM. Each Party represents that it has obtained all necessary approvals, consents and authorizations to enter into this Addendum and to perform its duties under this Addendum; the person executing this Addendum on its behalf has the authority to do so; upon execution and delivery of this Addendum by the Parties, it is a valid and binding contract, enforceable in accordance with its terms; and the execution, delivery, and performance of this Addendum does not violate any bylaw, charter, regulation, law or any other governing authority of the Party.

The Parties hereby enter into this Addendum as of the Effective Date.

Motorola Solutions, Inc.	**Customer**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

EXHIBIT A
MOTOROLA SOFTWARE LICENSE AGREEMENT

This Exhibit A Motorola Software License Agreement ("Agreement") is between Motorola Solutions, Inc., (“Motorola"), and _____ (“Licensee”).

For good and valuable consideration, the parties agree as follows:

Section 1 DEFINITIONS

1.1 “Camera License Key” or “CLK” means an electronic key that will permit each license of Software to be used with license plate recognition (“LPR”) cameras obtained from Motorola. Each LPR camera must have a valid CLK.

1.2 “Designated Products” means products provided by Motorola to Licensee with which or for which the Software and Documentation is licensed for use.

1.3 “Documentation” means product and software documentation that specifies technical and performance features and capabilities, and the user, operation and training manuals for the Software (including all physical or electronic media upon which such information is provided).

1.4 “Open Source Software” means software with either freely obtainable source code, license for modification, or permission for free distribution.

1.5 “Open Source Software License” means the terms or conditions under which the Open Source Software is licensed.

1.6 “Primary Agreement” means the Addendum to which this exhibit is attached.

1.7 “Security Vulnerability” means a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach such that data is compromised, manipulated or stolen or the system damaged.

1.8 “Software” (i) means proprietary software in object code format, and adaptations, translations, de-compilations, disassemblies, emulations, or derivative works of such software; (ii) means any modifications, enhancements, new versions and new releases of the software provided by Motorola; and (iii) may contain one or more items of software owned by a third party supplier. The term "Software" does not include any third party software provided under separate license or third party software not licensable under the terms of this Agreement.

Section 2 SCOPE

Motorola and Licensee enter into this Agreement in connection with Motorola's delivery of certain proprietary software or products containing embedded or pre-loaded proprietary software, or both. This Agreement contains the terms and conditions of the license Motorola is providing to Licensee, and Licensee’s use of the proprietary software and affiliated documentation.

Section 3 GRANT OF LICENSE

3.1. Subject to the provisions of this Agreement and the continued payment of applicable CLK fees, Motorola grants to Licensee during the Term of the Enterprise Software Agreement, a personal, limited, non-transferable (except as permitted in Section 7) and non-exclusive license under Motorola's copyrights and Confidential Information (as defined in the Primary Agreement) embodied in the Software to use the Software, in object code form, and the Documentation solely in connection with Licensee's use of the Designated Products. This Agreement does not grant any rights to source code. Except with prior written approval from Motorola, Licensee may not use the Software on or in connection with any LPR cameras other than the Equipment purchased from Motorola.

3.2. If the Software licensed under this Agreement contains or is derived from Open Source Software, the terms and conditions governing the use of such Open Source Software are in the Open Source Software Licenses of the copyright owner and not this Agreement. If there is a conflict between the terms and conditions of this Agreement and the terms and conditions of the Open Source Software Licenses governing Licensee's use of the Open Source Software, the terms and conditions of the license grant of the applicable Open Source Software Licenses will take precedence over the license grants in this Agreement. If requested by Licensee, Motorola will use commercially reasonable efforts to: (i) determine whether any Open Source Software is provided under this Agreement; and (ii) identify the Open Source Software (or specify where that license may be found).

3.3 TO THE EXTENT, IF ANY, THAT THERE IS A SEPARATE LICENSE AGREEMENT PACKAGED WITH, OR PROVIDED ELECTRONICALLY WITH, A PARTICULAR PRODUCT THAT BECOMES EFFECTIVE ON AN ACT OF ACCEPTANCE BY THE END USER, THEN THAT AGREEMENT SUPERSEDES THIS SOFTWARE LICENSE AGREEMENT AS TO THE END USER OF EACH SUCH PRODUCT.

Section 4 LIMITATIONS ON USE

4.1. Licensee may use the Software only for Licensee's internal business purposes and only in accordance with the Documentation. Any other use of the Software is strictly prohibited. Without limiting the general nature of these restrictions, Licensee will not make the Software available for use by third parties on a "time sharing," "application service provider," or "service bureau" basis or for any other similar commercial rental or sharing arrangement.

4.2. Licensee will not, and will not allow or enable any third party to: (i) reverse engineer, disassemble, peel components, decompile, reprogram or otherwise reduce the Software or any portion to a human perceptible form or otherwise attempt to recreate the source code; (ii) modify, adapt, create derivative works of, or merge the Software; (iii) copy, reproduce, distribute, lend, or lease the Software or Documentation to any third party, grant any sublicense or other rights in the Software or Documentation to any third party, or take any action that would cause the Software or Documentation to be placed in the public domain; (iv) remove, or in any way alter or obscure, any copyright notice or other notice of Motorola's proprietary rights; (v) provide, copy, transmit, disclose, divulge or make the Software or

Documentation available to, or permit the use of the Software by any third party or on any machine except as expressly authorized by this Agreement; or (vi) use, or permit the use of, the Software in a manner that would result in the production of a copy of the Software solely by activating a machine containing the Software. Licensee may make as many copies of the Documentation as it may reasonably require for the internal use of the Software.

4.3. Licensee must obtain a valid CLK for each LPR camera installed and considered in active service during the term of the Enterprise Software Agreement. Payment for the CLK must be received in advance, and will entitle Licensee to use the Software in connection with such camera. Unless otherwise provided in this Agreement, each CLK is good for one year. CLK's shall not be issuable, and if issued in error shall be null and void, for cameras and other hardware components that are not Motorola-approved.

4.4 Licensee will maintain, during the term of this Agreement and for a period of two years thereafter, accurate records relating to this license grant to verify compliance with this Agreement. Motorola or an independent third party ("Auditor") may inspect Licensee's premises, books and records, upon reasonable prior notice to Licensee, during Licensee's normal business hours and subject to Licensee's facility and security regulations. Motorola is responsible for the payment of all expenses and costs of the Auditor. Any information obtained by Motorola and the Auditor will be kept in strict confidence by Motorola and the Auditor and used solely for the purpose of verifying Licensee's compliance with the terms of this Agreement.

Section 5 OWNERSHIP AND TITLE

Motorola, its licensors, and its suppliers retain all of their proprietary rights in any form in and to the Software and Documentation, including, but not limited to, all rights in patents, patent applications, inventions, copyrights, trademarks, trade secrets, trade names, and other proprietary rights in or relating to the Software and Documentation (including any corrections, bug fixes, enhancements, updates, modifications, adaptations, translations, de-compilations, disassemblies, emulations to or derivative works from the Software or Documentation, whether made by Motorola or another party, or any improvements that result from Motorola's processes or, provision of information services). No rights are granted to Licensee under this Agreement by implication, estoppel or otherwise, except for those rights which are expressly granted to Licensee in this Agreement. All intellectual property developed, originated, or prepared by Motorola in connection with providing the Software, Designated Products, Documentation or related services, remains vested exclusively in Motorola, and Licensee will not have any shared development or other intellectual property rights.

Section 6 LIMITED WARRANTY; DISCLAIMER OF WARRANTY

6.1. Unless otherwise stated in the Primary Agreement, the commencement date and the term of the Software warranty will be a period of ninety (90) days from Motorola's shipment of the Software (the "Warranty Period"). If Licensee is not in breach of any of its obligations under this Agreement, Motorola warrants that the unmodified Software, when used properly and in accordance with the Documentation and this Agreement, will be free from a reproducible defect that eliminates the functionality or successful operation of a feature critical to the primary functionality or successful operation of the Software. Whether a defect occurs will be determined by Motorola solely with reference to the Documentation.

Motorola does not warrant that Licensee's use of the Software or the Designated Products will be uninterrupted, error-free, completely free of Security Vulnerabilities, or that the Software or the Designated Products will meet Licensee's particular requirements. Motorola makes no representations or warranties with respect to any third party software included in the Software. Notwithstanding, any warranty provided by a copyright owner in its standard license terms will flow through to Licensee for third party software provided by Motorola.

6.2 Motorola's sole obligation to Licensee and Licensee's exclusive remedy under this warranty is to use reasonable efforts to remedy any material Software defect covered by this warranty. These efforts will involve either replacing the media or attempting to correct significant, demonstrable program or documentation errors or Security Vulnerabilities. If Motorola cannot correct the defect within a reasonable time, then at Motorola's option, Motorola will replace the defective Software with functionally-equivalent Software, license to Licensee substitute Software which will accomplish the same objective, or terminate the license and refund the Licensee's paid license fee.

6.3. Warranty claims are described in the Primary Agreement.

6.4. The express warranties set forth in this Section 6 are in lieu of, and Motorola disclaims, any and all other warranties (express or implied, oral or written) with respect to the Software or Documentation, including, without limitation, any and all implied warranties of condition, title, non-infringement, merchantability, or fitness for a particular purpose or use by Licensee (whether or not Motorola knows, has reason to know, has been advised, or is otherwise aware of any such purpose or use), whether arising by law, by reason of custom or usage of trade, or by course of dealing. In addition, Motorola disclaims any warranty to any person other than Licensee with respect to the Software or Documentation.

Section 7 TRANSFERS

Licensee will not transfer the Software or Documentation to any third party without Motorola's prior written consent. Motorola's consent may be withheld at its discretion and may be conditioned upon transferee paying all applicable license fees and agreeing to be bound by this Agreement.

Section 8 TERM AND TERMINATION

8.1 Licensee's right to use the Software and Documentation will begin when the Primary Agreement is signed by both parties and will continue for the term of the Enterprise Software Agreement, provided that applicable CLK fees are received.
8.2 Within thirty (30) days after termination of this Agreement, Licensee must certify in writing to Motorola that all copies of the Software have been removed or deleted from the Designated Products and that all copies of the Software and Documentation have been returned to Motorola or destroyed by Licensee and are no longer in use by Licensee.

8.3 Licensee acknowledges that Motorola made a considerable investment of resources in the development, marketing, and distribution of the Software and Documentation and that Licensee's breach of this Agreement will result in irreparable harm to Motorola for which monetary damages would be inadequate. If Licensee breaches this Agreement, Motorola may terminate this Agreement and be entitled to all available remedies at law or in equity (including immediate injunctive relief and repossession of all non-embedded Software and

associated Documentation unless Licensee is a Federal agency of the United States Government).

Section 9 COMMERCIAL COMPUTER SOFTWARE

9.1 *This Section 9 only applies to U.S. Government end users.* The Software, Documentation and updates are commercial items as that term is defined at 48 C.F.R. Part 2.101, consisting of "commercial computer software" and "computer software documentation" as such terms are defined in 48 C.F.R. Part 252.227-7014(a)(1) and 48 C.F.R. Part 252.227-7014(a)(5), and used in 48 C.F.R. Part 12.212 and 48 C.F.R. Part 227.7202, as applicable. Consistent with 48 C.F.R. Part 12.212, 48 C.F.R. Part 252.227-7015, 48 C.F.R. Part 227.7202-1 through 227.7202-4, 48 C.F.R. Part 52.227-19, and other relevant sections of the Code of Federal Regulations, as applicable, the Software, Documentation and Updates are distributed and licensed to U.S. Government end users: (i) only as commercial items, and (ii) with only those rights as are granted to all other end users pursuant to the terms and conditions contained herein.

9.2 If Licensee is licensing Software for end use by the United States Government or a United States Government agency, Licensee may transfer such Software license, but only if: (i) Licensee transfers all copies of such Software and Documentation to such United States Government entity or interim transferee, and (ii) Licensee has first obtained from the transferee (if applicable) and ultimate end user an enforceable end user license agreement containing restrictions substantially identical to the ones contained in this Agreement. Except as stated in the foregoing, Licensee and any transferee(s) authorized by this subsection 9.2 may not otherwise use or transfer or make available any Motorola software to any third party nor permit any party to do so.

Section 10 CONFIDENTIALITY

Licensee acknowledges that the Software and Documentation contain Motorola's valuable proprietary and Confidential Information and are Motorola's trade secrets, and that the provisions in the Primary Agreement concerning Confidential Information apply.

Section 11 LIMITATION OF LIABILITY

The Limitation of Liability provision is described in the Equipment Sale Addendum.

Section 13 GENERAL

13.1. COPYRIGHT NOTICES. The existence of a copyright notice on the Software will not be construed as an admission or presumption of publication of the Software or public disclosure of any trade secrets associated with the Software.

13.2. COMPLIANCE WITH LAWS. Licensee acknowledges that the Software is subject to the laws and regulations of the United States and Licensee will comply with all applicable laws and regulations, including export laws and regulations of the United States. Licensee will not, without the prior authorization of Motorola and the appropriate governmental authority of the United States, in any form export or re-export, sell or resell, ship or reship, or divert, through direct or indirect means, any item or technical data or direct or indirect products sold or otherwise furnished to any person within any territory for which the United

States Government or any of its agencies at the time of the action, requires an export license or other governmental approval. Violation of this provision is a material breach of this Agreement.

13.3. ASSIGNMENTS AND SUBCONTRACTING. Motorola may assign its rights or subcontract its obligations under this Agreement, or encumber or sell its rights in any Software, without prior notice to or consent of Licensee.

13.4. GOVERNING LAW. This Agreement is governed by the laws of the United States to the extent that they apply and otherwise by the internal substantive laws of the State to which the Software is shipped if Licensee is a sovereign government entity, or the internal substantive laws of the State of Illinois if Licensee is not a sovereign government entity.

The terms of the U.N. Convention on Contracts for the International Sale of Goods do not apply. In the event that the Uniform Computer Information Transaction Act, any version of this Act, or a substantially similar law (collectively "UCITA") becomes applicable to a party's performance under this Agreement, UCITA does not govern any aspect of this Agreement or any license granted under this Agreement, or any of the parties' rights or obligations under this Agreement. The governing law will be that in effect prior to the applicability of UCITA.

13.5. THIRD PARTY BENEFICIARIES. This Agreement is entered into solely for the benefit of Motorola and Licensee. No third party has the right to make any claim or assert any right under this Agreement, and no third party is deemed a beneficiary of this Agreement. Notwithstanding the foregoing, any licensor or supplier of third party software included in the Software will be a direct and intended third party beneficiary of this Agreement.

13.6. SURVIVAL. Sections 4, 5, 6.4, 7, 8, 9, 10, 11 and 13 survive the termination of this Agreement.

13.7. ORDER OF PRECEDENCE. In the event of inconsistencies between this Exhibit and the Primary Agreement, the parties agree that this Exhibit prevails, only with respect to the specific subject matter of this Exhibit, and not the Primary Agreement or any other exhibit as it applies to any other subject matter.

13.8 SECURITY. Motorola uses reasonable means in the design and writing of its own Software and the acquisition of third party Software to limit Security Vulnerabilities. While no software can be guaranteed to be free from Security Vulnerabilities, if a Security Vulnerability is discovered, Motorola will take the steps set forth in Section 6 of this Agreement.

C.3 EXHIBIT A – STATEMENT OF WORK

MOTOROLA SOLUTIONS RESPONSE

Responses to Exhibit A: Statement of Work are provided in the table below.

Specification	Compliant	Comment
2.1.1 Must be compliant with California Senate Bill 34 (SB34).	Yes	
2.1.2 Single Sign-On (SSO) implementation options	Yes	SAML w/ IDP initiated SAML Assertion
2.1.2.1 Security Assertion Markup Language (SAML) 2.0 compliance	Yes	SAML w/ IDP initiated SAML Assertion
2.1.2.2 Other SSO methods, such as Active Directory and Office 365.	No	
2.1.3 User and Entity Based Behavioral Analytics (UEBA)	Yes	
2.1.4 Distributed Denial of Service (DDoS) protection	Yes	
2.1.5 Data sanitization and anti-malware prevention. Minimizing attack vectors throughout the LPR solution using a multi-layered approach	Yes	
2.1.5.1 Anti-malware scanning and threat prevention with up to date signatures	Yes	
2.1.5.2 Alerts and notifications	Yes	
2.1.5.3 Input sanitization: All data coming into the system from users or application programming interfaces	Yes	
(API's)		
2.1.5.4 White list of file types for attaching/uploading for all purposes	Yes	
2.1.5.5 File Contents Disarm and Reconstruction (CDR)	Yes	
2.1.6 Disaster Recovery	Yes	
2.1.6.1 Data protection, backup, and recovery strategy	Yes	
2.1.6.2 Disaster recovery liability in case of catastrophic event	Yes	
2.1.7 California Consumer Privacy Act (CCPA) compliance	Yes	
2.1.8 Contractor shall provide a secure, database encrypted and web-based system that provides real-time access to uploaded data	Yes	

Use or disclosure of this proposal is subject to the restrictions on the cover page.

Specification	Compliant	Comment
2.1.9 Contractor shall allow authorized users access to LPR data in a number of LPR-specific dashboards	Yes	
2.1.10 Dashboard will show LPR vehicle scans in an easy to read graphical format	Yes	
2.1.12 Contractor shall provide an option to purge data at specified intervals or dates	Yes	
2.1.12.1 Will have a notification process to assure compliance	Yes	
2.1.13 Data uploaded will only be shared at the discretion of an administrator designated by the San Diego County	Yes	
Sheriff's Department		
2.2 LPR CAMERAS		
2.7.1 Contractor shall have LPR systems capable of being installed on a fixed object (i.e. light pole), marked patrol vehicles, covert vehicles and speed trailers.	Yes	
2.7.2 Marked patrol vehicle camera mounting brackets must be compatible with Whelen, Code3, TOMAR, Federal Signal, Arjent S2 light bars	Yes	
2.7.3 Cameras shall be self-illuminating Infrared (IR) for effective license plate image capture in a variety of weather and lighting conditions	Yes	
2.7.4 LPR cameras shall be water-resistance with few moving parts that can be damaged	Yes	
2.7.5 LPR cameras shall have the ability to automatically capture all variations of California license plates, to include California dealer issued plates (paper plates)	Yes	
2.7.6 Cameras shall have a dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle for verification purposes	Yes	
2.7.7 Cameras shall be sealed to NEMA 6 (IP67) standards	Yes	
2.7.8 Dual lens cameras shall be capable of capturing up to 60 frames per second	Yes	

Use or disclosure of this proposal is subject to the restrictions on the cover page.

Specification	Compliant	Comment
2.7.9 Cameras shall have the ability to adjust shutter, brightness, and gain settings to ensure a high-quality image regardless of weather or lighting conditions	Yes	
2.7.10 The cameras shall be able to have a fixed focal point or target distance from the camera to the vehicle's license plate from 9 ½ feet to 30 feet	Yes	
2.7.11 The camera shall be capable of various configurations to capture plates in any of the following modes depending on the configuration:	Yes	
2.7.11.1 An adjacent lane on either side of the vehicle while driving through traffic and/or parking lots	Yes	
2.7.11.2 Traffic in an adjacent lane while parked on the side of the shoulder of a roadway	Yes	
2.7.11.3 Parked vehicles in parking lots	Yes	
2.3 LPR PROCESSOR		
2.3.1 Processor shall have a "self-trigger" mode to detect the presence of correctly mounted vehicle license plates in the camera's field of view for image capture from the camera	Yes	
2.3.2 Processor's installed in vehicles shall be equipped with an intelligent Power Supply Unit (PSU) that provides for a safe start and shut-down each time the vehicle's ignition is turned on and turned off	Yes	
2.3.3 Processor controls the power supplied to the cameras and provides video connection points for simplified system wiring	Yes	
2.1.11 LPR dashboard will show vehicle location, images captured and provide the ability to search using the license plate Contractor shall have LPR systems capable of being installed on a fixed object (i.e. light pole), marked patrol vehicles, covert vehicles and speed trailers.	Yes	
2.1.12.1.1 Provide notification of purge date.	Yes	From the server

Use or disclosure of this proposal is subject to the restrictions on the cover page.

Specification	Compliant	Comment
2.1.12.1.2 Provide confirmation and notification that specified data was purged.	Yes	From the server
COUNTY OF SAN DIEGO - REQUEST FOR BIDS (RFB # 10493)		
SHERIFF'S DEPARTMENT		
LICENSE PLATE READERS		
SECTION C: EXHIBIT A STATEMENT OF WORK		
Page 24 of 46		
2.3.4 Processor shall have at least four (4) LPR camera connections and multiple USB ports	Yes	
2.3.5 Vehicle mounted processors shall meet the environmental conditions associated with being mounted in a trunk	Yes	
2.4 LPR SOFTWARE		
2.4.1 Application software shall be capable of running on a Windows based mobile computer	Yes	
2.4.2 There shall be no Java programming or Java derivatives	Yes	
2.4.3 LPR system shall have real time alerting and the ability to program custom hotlist	Yes	
2.4.4 There shall be a secure login and password function on the LPR software; The user's access shall be controlled by an administrator designated by the San Diego County Sheriff's Department	Yes	
2.4.4.1 API capable of integrating user defined active directory	Yes with comment	SAML w/ IDP initiated SAML Assertion
2.4.5 The software shall provide live, simultaneous display of all the following data:		
2.4.5.1 The IR license plate image	Yes	
2.4.5.2 The license plate interpretation or system read	Yes	
2.4.5.3 A corresponding color overview of the vehicle displaying the captured IR license plate	Yes	
2.4.5.4 The date and time stamp	Yes	
2.4.5.5 Identification of the camera capturing the image	Yes	

Specification	Compliant	Comment
2.4.6 Software shall capture GPS coordinates for every recorded license reads	Yes	
2.4.7 Software shall have the ability to GPS stamp all the reads	Yes	
2.4.8 Software will give a unique audible and visible alert when a wanted license plate is discovered	Yes	
2.4.9 The Alert Screen remains displayed until acknowledged by the user, and, while displayed, the system continues to process license plate data in the background	Yes	
3 DEMONSTRATION OR SAMPLE		
determine if it meets the requirements stated. All specifications listed in the General Requirements shall be confirmed. All travel, demonstration supplies and/or shipping expenses shall be at the contractor's expense.	Yes	
4 INSTALLATION		
4.1 Contractor shall provide the option to purchase systems as a "kit" that includes all hardware, wiring and software for standard installations	Yes	
4.2 Contractor shall provide installation and warranty repair options on vehicles within San Diego County.	Yes	
4.3 Contractor shall provide a technician or representative to visit customer site for system start-up, configuration and commissioning of LPR system	Yes	
5 CUSTOMER SUPPORT		
5.1 The Contractor shall provide technical advice and sales support within 72 business hours .	Yes	
6 TRAINING		
6.1 The County reserves the right to request up to eight (8) hours of training at a San Diego County Sheriff's Department facility within 30 days of delivery at no additional charge. This is in addition to the requirement set forth in 4.3.	Yes	

Use or disclosure of this proposal is subject to the restrictions on the cover page.

Specification	Compliant	Comment
7 DELIVERY REQUIREMENTS		
7.1 Delivery address: San Diego County Sheriff's Department Attn: Ivy Scites - Grants Unit 9621 Ridgehaven Court San Diego, CA 92123	Yes	
8 INVOICE		
8.1 Invoices shall be sent to: San Diego County Sheriff's Department Attn: Ivy Scites - Grants Unit 9621 Ridgehaven Court San Diego, CA 92123	Yes	
8.2 Only new products shall be accepted. An LPR system that has been used in any way, refurbished, reconditioned, or gray market is unacceptable and will be rejected and returned.	Yes	
8.3 The County shall be given credit for damaged and returned items within five (5) business days.	Yes	
8.4 There shall be no restocking fees or other charges for returns of damaged or incorrect items.	Yes	
8.5 Deviations to the terms, conditions and/or specifications shall be conspicuously noted in writing by the respondent.	Yes	
9 LEAD TIME		
9.1 Department requested deliver lead time: 60 days.	Yes	

C.4 EXHIBIT B – INSURANCE REQUIREMENTS

MOTOROLA SOLUTIONS RESPONSE

Please see the 'redlined' responses noted below.

COUNTY OF SAN DIEGO - REQUEST FOR BIDS (RFB# **10493**)
SHERIFF'S DEPARTMENT
LICENSE PLATE READERS

SECTION C: EXHIBIT B INSURANCE REQUIREMENT – Motorola Solutions, Inc. clarifications

INSURANCE REQUIREMENTS FOR CONTRACTORS

Without limiting Contractor's indemnification obligations to County, Contractor shall provide at its sole expense and maintain for the duration of this contract, or as may be further required herein, insurance against claims for injuries to persons or damages to property which may arise from or in connection with the performance of the work hereunder and the results of the work by the Contractor, his agents, representatives, employees or subcontractors.

1. ~~Minimum~~ Scope of Insurance Coverage shall be at least as broad as:

A. Commercial General Liability, Occurrence form, Insurance Services Office form CG0001.

B. Automobile Liability covering all owned, non owned, hired auto Insurance Services Office form CA0001.

C. Workers' Compensation, as required by State of California and Employer's Liability Insurance.

D. Technology Liability (Errors & Omissions)

2. ~~Minimum~~ Limits of Insurance

Contractor shall maintain limits no less than:

A. Commercial General Liability including Premises, Operations, Products and Completed Operations, Contractual Liability, and Independent Contractors Liability: $1~~2~~,000,000 per occurrence for bodily injury, personal injury and property damage. The General Aggregate limit shall be $24,000,000.

B. Automobile Liability: $1,000,000 each accident for bodily injury and property damage.

C. Employer's Liability: $1,000,000 each accident for bodily injury or disease. Coverage shall include waiver of subrogation endorsement in favor of County of San Diego.

D. Technology Liability (Errors & Omissions): $1~~2~~,000,000 per claim ~~occurrence or claim~~ with an aggregate limit of not less than $24,000,000. This

coverage shall be maintained for a minimum of three years following termination or completion of Contractor's work pursuant to the Contract.

~~If the contractor maintains broader coverage and/or higher limits than the minimums shown above, the County requires and shall be entitled to the broader coverage and/or higher limits maintained by the Contractor. As a requirement of this contract, any available insurance proceeds in excess of the specified minimum limits and coverage stated above, shall also be available to the County of San Diego.~~

3. Self-Insured Retentions

Any self-insured retention or deductible under Contractor's policies herein shall be the Contractor's sole obligation. ~~must be declared to and approved by County Risk Management. At the option of the County, either: the insurer shall reduce or eliminate such self-insured retentions as respects the County, the members of the Board of Supervisors of the County and the officers, agents, employees and volunteers; or the Contractor shall provide a financial guarantee satisfactory to the County guaranteeing payment of losses and related investigations, claim administration, and defense expenses.~~

4. Other Insurance Provisions

The insurance policies are to contain, or be endorsed to contain, the following provisions:

A. Additional Insured Endorsement

The County of San Diego, the members of the Board of Supervisors of the County and the officers, agents, employees ~~and volunteers~~ of the County, individually and collectively are to be covered as additional insureds on the General Liability policy with respect to liability arising out of work or operations performed by or on behalf of the Contractor including materials, parts, or equipment furnished in connection with such work or operations and automobiles owned, leased, hired or borrowed by or on behalf of the Contractor. General Liability coverage can be provided in the form of an endorsement to the Contractor's insurance (at least as broad as ISO from ~~CG 2010 11 85 or both~~ CG 2010, CG 2026, CG 2033, or CG 2038; and CG 2037 form ~~sms if later revisions used).~~

B. Primary Insurance Endorsement

For any claims related to this project, the Contractor's insurance coverage, including any excess liability policies, shall be primary insurance at least as broad as ISO CG 2001 04 13 as respects the County, the members of the Board of

C. Each insurance policy required above shall state that in the event of cancellation of coverage ~~shall not be canceled, except with~~ notice will be provided to the County. Notice of Cancellation

D. Severability of Interest Clause

Coverage applies separately to each insured, except with respect to the limits of liability, and that an act or omission by one of the named insureds shall not reduce or avoid coverage to the other named insureds.

GENERAL PROVISIONS

5. Qualifying Insurers

All required policies of insurance shall be issued by companies which have been approved to do business in the State of California by the State Department of Insurance, and which hold a current policy holder's alphabetic and financial size category rating of not less than A, VII according to the current Best's Key Rating guide, or a company of equal financial stability that is approved in writing by County Risk Management.

6. Evidence of Insurance

Prior to commencement of this Contract, but in no event later than the effective date of the Contract, Contractor shall furnish the County ~~with a copy of the policy declaration and endorsement pages along with the~~ certificates of insurance and ~~amendatory~~ eendorsements ~~effecting coverage~~ required by this clause. ~~Policy declaration and~~ E~~e~~ndorsement pages shall be included with renewal certificates.

~~and amendatory endorsements submissions and shall be furnished to County within thirty days of the expiration of the term of any required policy. Contractor shall permit County at all reasonable times to inspect any required policies of insurance.~~

Failure to Obtain or Maintain Insurance; County's Remedies

Contractor's failure to provide insurance specified or failure to furnish certificates of insurance and amendatory endorsements or failure to make premium payments required by such insurance shall constitute a material breach of the Contract, and County may, at its option, terminate the Contract for any such default by Contractor.

7. No Limitation of Obligations

The foregoing insurance requirements as to the types and limits of insurance coverage to be maintained by Contractor, and any approval of said insurance by the County are not intended to and shall not in any manner limit or qualify the liabilities and obligations otherwise assumed by Contractor pursuant to the Contract, including, but not limited to, the provisions concerning indemnification.

8. Review of Coverage

County retains the right at any time to review the coverage, form and amount of insurance required herein and may require Contractor to obtain insurance reasonably sufficient in coverage, form and amount to provide adequate

protection against the kind and extent of risk which exists at the time a change in insurance is required.

9. Self-Insurance

Contractor may, with the prior written consent of County Risk Management, fulfill some or all of the insurance requirements contained in this Contract under a plan of self-insurance. Contractor shall only be permitted to utilize such self-insurance if in the opinion of County Risk Management, Contractor's (i) net worth, and (ii) reserves for payment of claims of liability against Contractor, are sufficient to adequately compensate for the lack of other insurance coverage required by this Contract. Contractor's utilization of self-insurance shall not in any way limit liabilities assumed by Contractor under the Contract.

10. Claims Made Coverage

If coverage is written on a "claims made" basis, the Certificate of Insurance shall clearly so state. In addition to the coverage requirements specified above, such policy shall provide that:

A. The policy retroactive date coincides with or precedes Contractor's commencement of work under the Contract (including subsequent policies purchased as renewals or replacements).

B. Contractor will make every effort to maintain similar insurance during the required extended period of coverage following expiration of the Contact.

C. If insurance is terminated for any reason, Contractor shall purchase an extended reporting provision of at least three years to report claims arising in connection with the Contract.

D. The policy allows for reporting of circumstances or incidents that might give rise to future claims.

12. Subcontractors' Insurance

Contractor shall require and verify that all subcontractors maintain insurance meeting all the requirements stated herein, and Contractor shall ensure that County is an additional insured on insurance required from subcontractors. Such Additional Insured endorsement shall be attached to the certificate of insurance in order to be valid and on a form at least as broad as ISO from CG 2010 11 85 or both CG 2010, CG 2026, CG 2033, or CG 2038; and CG 2037 forms if later revisions used. ~~If any sub contractor's coverage does not comply with the foregoing provisions, Contractor shall defend and indemnify the County from any damage, loss, cost, or expense, including attorneys' fees, incurred by County as a result of subcontractor's failure to maintain required coverage.~~

Waiver of Subrogation

Contractor hereby grants to County a waiver of their rights of subrogation which any insurer of Contractor may acquire against County by virtue of the payment of any loss. Contractor agrees to obtain any endorsement that may be necessary to affect this waiver of subrogation. The Workers' Compensation

policy shall be endorsed with a waiver of subrogation in favor of the County for all work performed by the Contractor, its employees, agents and subcontractors.

MOTOROLA SOLUTIONS RESPONSE

RFB # H. **Exception**. Motorola asserts it does not perform under Cost Accounting Standards ("CAS") covered contracts; (ii) does not accept contracts where cost or pricing data is required to be provided; (iii) does not need to have and maintain an estimating system such as described in DFARS 252.215-7002; (iv) does not generate labor hour estimates from an estimating system; (v) does not provide cost information; and (vi) does not calculate or submit cost-based indirect or labor rates so it cannot agree to be bound by the Uniform Administration Requirements of 2 CFR Part 200. Additionally, Motorola cannot agree to terms and conditions imposed by any federal agency without the ability to review such terms and conditions to ensure compliance so we respectfully request deletion of this clause.

C.5 EXHIBIT C – PRICING SCHEDULE

Description	MFG & Model	Estimated Quantity	Unit Price	Total	Notes
Mobile LPR 1 camera system, dual lens configuration in a single camera housing, featuring both an IR lens for plate capture and a color overview image of the vehicle	Vigilant Mobile LPR 4-Camera Reaper High Definition System	4	$7,500	$30,000	
Portable LPR 1 camera system, dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle	Vigilant Fixed LPR ReaperHD Camera with Sun Shield - 25mm Lens with Camera Cable - Standard ReaperHD Camera	10	$4,500	$45,000	
LPR Camera Mounting Brackets for Light Bar	Vigilant LPR Camera Mounting Brackets - Light Bar Mounting Style - Complete Set	4	$700	$2,800	
LPR Mounting for Portable system	Fixed LPR Camera Bracket	10	$349	$3,490	
LPR Processor	n/a	14 already incldued	n/a		Processers are included with Mobile and Installation "Kit" line items)
Modem (for mobile)	Cradlepoint IBR600C	4	500	$2,000	We typically use the existing modem, but can supply our own
Modem (for portable)	Cradlepoint IBR600C	10 already included	n/a		Modems included with "Installation Kit" line item

Use or disclosure of this proposal is subject to the restrictions on the cover page.

Description	MFG & Model	Estimated Quantity	Unit Price	Total	Notes
LPR Software (Mobile)	Vigilant LPR Basic Service Package for Hosted/Managed LPR Deployments	4 Units	$840	$3,360	
LPR Software (Portable)	Vigilant LPR Basic Service Package for Hosted/Managed LPR Deployments	10 Units	$210	$2,100	
LPR Speed Trailer complete package	Vigilant Basic Solar 2-Camera HD LPR Trailer with 80W panel	1	$19,995	$19,995	
Start-up, configuration, and commissioning of LPR Systems at Sheriff's facility to include all expenses such as travel	Vigilant System Start Up & Commissioning of 'In Field' LPR system	14	$0.00	$0	
Installation (4 Installs inlcuded for mobiles, County indicated they would use their own assets for "portable" installation)	Standard 4-Camera Vehicle Instalaltion	4	$800	$3,200	
Covert Installation in vehicle	Covert Installation on Vehicle TBD	1	$3,000	$3,000	
Installation "Kit", includes all hardware, wiring, and software for "do it yourself" standard installations (on poles & trailers)	Vigilant Fixed Camera Communications Box	5	$2,500	$12,500	Box contains processor, modem, and connection for 120v continuous power.
Training	Vigilant Training	8	$0	$0	Training is always free with Vigilant Solutions.
Shipping (Mobile)	Vigilant Shipping Charges (Mobile)	4	$130	$520	

Use or disclosure of this proposal is subject to the restrictions on the cover page.

Description	MFG & Model	Estimated Quantity	Unit Price	Total	Notes
Shipping (Portable)	Vigilant Shipping Charges (Fixed)	10	$55	$550	
Shipping (Trailer)	Crating and Shipping for Vigilant Trailer	1	$1,500	$1,500	Forklift required at delivery
			Total:	**$130,015**	
Additional Notes:					
All equipment comes with one year of hosting and warranty on LEARN.					
ARJIS API included under the Sheriff's exisitng arrangment with Vigilant.					
Ongoing hosting fees after year 1 will be in accoradance with the exisiting ESA between Vigilant and San Diego Sheriff.					

C.6 EXHIBIT D – FEDERAL GRANT REQUIREMENTS

RFB Exhibit D Federal Grant Requirements.
RFB # D.

MOTOROLA SOLUTIONS RESPONSE

Comply with Clarification: If selected for award, Motorola would be providing a commercial item available to its customers. Motorola therefore considers the requirements rights to inventions as described in this section are not applicable.

RFB # H.

MOTOROLA SOLUTIONS RESPONSE

Exception. Motorola asserts it does not perform under Cost Accounting Standards ("CAS") covered contracts; (ii) does not accept contracts where cost or pricing data is required to be provided; (iii) does not need to have and maintain an estimating system such as described in DFARS 252.215-7002; (iv) does not generate labor hour estimates from an estimating system; (v) does not provide cost information; and (vi) does not calculate or submit cost-based indirect or labor rates so it cannot agree to be bound by the Uniform Administration Requirements of 2 CFR Part 200. Additionally, Motorola cannot agree to terms and conditions imposed by any federal agency without the ability to review such terms and conditions to ensure compliance so we respectfully request deletion of this clause.

C.6.1 Form W-9

MOTOROLA SOLUTIONS RESPONSE

Motorola's Form W-9 is provided below.

Form **W-9**
(Rev. October 2018)
Department of the Treasury
Internal Revenue Service

Request for Taxpayer Identification Number and Certification

▶ **Go to *www.irs.gov/FormW9* for instructions and the latest information.**

Give Form to the requester. Do not send to the IRS.

Print or type. See Specific Instructions on page 3.

1 Name (as shown on your income tax return). Name is required on this line; do not leave this line blank.
Motorola Solutions, Inc.

2 Business name/disregarded entity name, if different from above

3 Check appropriate box for federal tax classification of the person whose name is entered on line 1. Check only **one** of the following seven boxes.

☐ Individual/sole proprietor or single-member LLC ☑ C Corporation ☐ S Corporation ☐ Partnership ☐ Trust/estate

☐ Limited liability company. Enter the tax classification (C=C corporation, S=S corporation, P=Partnership) ▶ _____

Note: Check the appropriate box in the line above for the tax classification of the single-member owner. Do not check LLC if the LLC is classified as a single-member LLC that is disregarded from the owner unless the owner of the LLC is another LLC that is **not** disregarded from the owner for U.S. federal tax purposes. Otherwise, a single-member LLC that is disregarded from the owner should check the appropriate box for the tax classification of its owner.

☐ Other (see instructions) ▶

4 Exemptions (codes apply only to certain entities, not individuals; see instructions on page 3):

Exempt payee code (if any) **5**

Exemption from FATCA reporting code (if any) **D**

(Applies to accounts maintained outside the U.S.)

5 Address (number, street, and apt. or suite no.) See instructions.
500 W. Monroe Street

Requester's name and address (optional)

6 City, state, and ZIP code
Chicago, IL 60661

7 List account number(s) here (optional)

Part I Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. The TIN provided must match the name given on line 1 to avoid backup withholding. For individuals, this is generally your social security number (SSN). However, for a resident alien, sole proprietor, or disregarded entity, see the instructions for Part I, later. For other entities, it is your employer identification number (EIN). If you do not have a number, see *How to get a TIN*, later.

Note: If the account is in more than one name, see the instructions for line 1. Also see *What Name and Number To Give the Requester* for guidelines on whose number to enter.

Social security number

			-			-				

or

Employer identification number

3	6	-	1	1	1	5	8	0	0

Part II Certification

Under penalties of perjury, I certify that:

1. The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me); and
2. I am not subject to backup withholding because: (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding; and
3. I am a U.S. citizen or other U.S. person (defined below); and
4. The FATCA code(s) entered on this form (if any) indicating that I am exempt from FATCA reporting is correct.

Certification instructions. You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and generally, payments other than interest and dividends, you are not required to sign the certification, but you must provide your correct TIN. See the instructions for Part II, later.

Sign Here | **Signature of U.S. person** ▶ [signature] | **Date** ▶ 1/6/2020

General Instructions

Section references are to the Internal Revenue Code unless otherwise noted.

Future developments. For the latest information about developments related to Form W-9 and its instructions, such as legislation enacted after they were published, go to *www.irs.gov/FormW9*.

Purpose of Form

An individual or entity (Form W-9 requester) who is required to file an information return with the IRS must obtain your correct taxpayer identification number (TIN) which may be your social security number (SSN), individual taxpayer identification number (ITIN), adoption taxpayer identification number (ATIN), or employer identification number (EIN), to report on an information return the amount paid to you, or other amount reportable on an information return. Examples of information returns include, but are not limited to, the following.

- Form 1099-INT (interest earned or paid)
- Form 1099-DIV (dividends, including those from stocks or mutual funds)
- Form 1099-MISC (various types of income, prizes, awards, or gross proceeds)
- Form 1099-B (stock or mutual fund sales and certain other transactions by brokers)
- Form 1099-S (proceeds from real estate transactions)
- Form 1099-K (merchant card and third party network transactions)
- Form 1098 (home mortgage interest), 1098-E (student loan interest), 1098-T (tuition)
- Form 1099-C (canceled debt)
- Form 1099-A (acquisition or abandonment of secured property)

Use Form W-9 only if you are a U.S. person (including a resident alien), to provide your correct TIN.

If you do not return Form W-9 to the requester with a TIN, you might be subject to backup withholding. See What is backup withholding, *later.*

Next

Bid

COUNTY OF SAN DIEGO - REQUEST FOR BIDS (RFB # **10493**)
SHERIFF'S DEPARTMENT
LICENSE PLATE READERS
SECTION A: COVER PAGE (P&C 600 FORM)

COUNTY OF SAN DIEGO
SECTION A-P&C 600 FORM
This is not an order

Issued: October 22, 2020

MAIL OR DELIVER TO:
COUNTY OF SAN DIEGO, RFB NO. 10493
DEPARTMENT OF PURCHASING & CONTRACTING
5560 OVERLAND AVE., SUITE 270
SAN DIEGO, CA 92123

AWARD WILL BE MADE TO THE LOWEST RESPONSIVE, RESPONSIBLE BIDDER BASED ON
[ ] ALL OR NONE
[ ] EACH LOT
[X] TOTAL PRICE
[ ] OTHER (SEE PRICING SCHEDULE)

UNSPSC commodity code**: 461716.0000**

FOR INFORMATION, PLEASE CONTACT:
PUNNITA DINMUONG, ASSISTANT PROCUREMENT SPECIALIST
PUNNITA.DINMUONG@SDCOUNTY.CA.GOV

BID OPENING DATE: NOVEMBER 5, 2020
BIDS MUST BE RECEIVED AT THE ABOVE ADDRESS PRIOR TO 11:00 A.M. ON DATE OF BID OPENING.

PLEASE STATE YOUR LOWEST PRICE F.O.B. DESTINATION AND BRAND NAME OR TRADE NAME IF APPLICABLE.
(Please use typewriter or black ink)
YOUR ENVELOPE MUST INCLUDE RFB NO. 10493

DESCRIPTION

THE COUNTY OF SAN DIEGO (COUNTY), SHERIFF'S DEPARTMENT HAS A REQUIREMENT FOR LICENSE PLATE READERS IN ACCORDANCE WITH THE TERMS & CONDITIONS AND THE STATEMENT OF WORK REFLECTED HEREIN.

INITIAL TERM: DATE OF AWARD – OCTOBER 31, 2021
1ST OPTION YEAR: NOVEMBER 1, 2021 – OCTOBER 31 2022
2ND OPTION YEAR: NOVEMBER 1, 2022 – OCTOBER 31, 2023

PRICING SUBMITTED IS TO REMAIN FIRM FIXED FOR THE TERM PERIOD IDENTIFIED ABOVE. ALL ITEMS WITHIN EACH TERM PERIOD MUST BE PRICED TO BE CONSIDERED RESPONSIVE. AWARD WILL BE MADE TO THE LOWEST RESPONSIVE, RESPONSIBLE OFFEROR BASED ON THE TOTAL PRICE. OFFEROR WHO SUBMITS THE LOW BID WILL BE DEEMED RESPONSIBLE BASED ON THE RESULTS OF THE PRE-AWARD SURVEY.

ARE YOU ABLE TO COMPLY WITH ALL ITEMS SPECIFIED WITHIN THE SCOPE OF WORK? YES X OR __NO

BIDDER ACKNOWLEDGES ADDENDUM NO. 1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

SUBJECT TO ACCEPTANCE WITHIN **90** DAYS

NAME AND ADDRESS OF BIDDER NEOLOGY INC

STREET, CITY, STATE, ZIP 13520 Evening Creek Dr N Suite 460, San Diego CA 92128

TELEPHONE: NUMBER (858) 391-0260

FAX TELEPHONE: (858)391-0264

E-MAIL: sales@pipstechnology.com

PAYMENT TERMS NET **30** DAYS OR % DAY

NAME AND TITLE OF PERSON AUTHORIZED TO SIGN OFFER:

SIGNATURE OFFEROR DATE

PRINTED NAME: Francisco Martinez de Velasco

PRINTED TITLE: CEO

NOTIFICATION OF AWARD

ACCEPTANCE AS TO ITEM(S) NUMBERED:

(VC NO.)

TOTAL AMOUNT AWARD NO.

(THIS SECTION FOR COUNTY USE ONLY)
COUNTY OF SAN DIEGO
BY: _____ DATE: _____
JOHN M. PELLEGRINO, DIRECTOR
DEPT OF PURCHASING & CONTRACTING

NAME AND TITLE OF CONTRACTING OFFICER

County of San Diego
Department of Purchasing and Contracting

REPRESENTATIONS AND CERTIFICATIONS

The following representations and certifications are to be completed, signed and returned with the offer (the term "offer" includes a bid, proposal, quote, statement of qualifications, or any other submission to provide goods and/or services).

1. BUSINESS TYPE

☒ For-profit ☐ Non-profit ☐ Government

2. INTERLOCKING DIRECTORATE

In accordance with Board of Supervisors Policy A-79, if Offeror is a non-profit and will be subcontracting with a related for-profit entity where an interlocking directorate, management or ownership relationship exists, Offeror must list all such entity(ies) on an attached separate sheet, and authorization must be sought from Board of Supervisors. If Offeror is a non-profit and does not submit such a list, Offeror certifies it has not entered into a subcontract relationship with a related for-profit entity.

List Attached? Yes ☐

3. BUSINESS REPRESENTATION

Offeror represents as a part of this offer the following information regarding the ownership, operation, and control of its business:

3.1. Are you a local business with a physical address within the County of San Diego? ☐ Yes ☐ No

3.2. Are you certified by the State of California as a:

☐ Disabled Veteran Business Enterprise(DVBE)
Certification #: _____

☐ Small Business Enterprise (SBE)
Certification #: _____

3.3. Are you certified by the U.S. Dept Of Veterans' Affairs as:

☐ Veteran Owned Small Business (VOSB)
Certification # _____

☐ Service Disabled Veteran Owned Small Business (SDVOSB)
Certification # _____

3.4. Estimated percentage of work in this offer to be performed or fulfilled locally (within the geographic boundaries of the County of San Diego): _____%

4. DEBARMENT, SUSPENSION, AND RELATED MATTERS

4.1. Offeror certifies to the best of its knowledge that neither it nor any of its officers:

4.1.1. Are presently debarred, suspended, declared ineligible, or voluntarily excluded from covered transactions by any state, local, or federal department or agency.

4.1.2. Have within a three (3) year period preceding this agreement been convicted of or had a civil judgment rendered against them for commission of fraud or criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or contract under a public transaction; violation of federal or state antitrust statutes; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;

4.2. Except as allowed for in Section 4.2.5, Offeror hereby certifies to the best of its knowledge that neither it nor any of its officers:

4.2.1 Are presently indicted for or otherwise criminally or civilly charged by a government entity (federal, state, or local) with the commission of any of the offenses enumerated in paragraph 4.1.2 of this certification;

4.2.2 Have within a three (3) year period preceding this agreement had one or more public transactions (federal, state or local) terminated for cause or default;

4.2.3 Are presently the target or subject of any investigation, accusation or charges by any federal, state or local agency or law enforcement, licensing, certification, ethics, or compliance body;

4.2.4 Are proposed for debarment by any state, local, or federal department or agency.

4.2.5 If Offeror is unable to certify Sections 4.2.1, 4.2.2, 4.2.3, or 4.2.4, it certifies that it has disclosed and attached to this Representations and Certifications the reason(s) it cannot do so. The disclosure must include the Section(s), specific relevant facts including dates, contracts, individuals involved, status of actions, and any other relevant information that prevent it from making the requested certification(s). The County reserves the right to disqualify an Offeror based upon information disclosed.

Disclosure Attached? Yes ☐

5. RELATED WORK

Offeror certifies to the best of its knowledge that, other than as disclosed in an attached separate sheet, it and its proposed subcontractors, agents, and consultants have not previously contracted with the County to perform work on or related to this project (e.g. preparing related studies or recommendations, components of the statement of work, or plans and specifications).

Disclosure Attached? Yes ☐

6. CURRENT COST OR PRICING

Offeror certifies to the best of its knowledge that cost and/or pricing data submitted with this offer, or specifically identified by reference if actual submission of the data is impracticable, are accurate, complete, and current as of the date signed below.

7. INDEPENDENT PRICING

Offeror certifies that in relation to this offer:

7.1. The prices in this offer have been arrived at independently, without consultation, communication, or agreement, for the purpose of restricting competition, as to any matter relating to such prices with other offerors, with any competitors, or with any County employee(s) or consultant(s) involved in this or related procurements;

7.2. Unless otherwise required by law, the prices that have been quoted in this offer have not been knowingly disclosed by the Offeror and will not knowingly be disclosed by the Offeror prior to opening, in the case of a bid, or prior to award, in the case of a proposal, directly or indirectly to any other Offeror or to any competitor or with any County employee(s) or consultant(s) involved in this or related procurements; and

7.3. No attempt has been made or will be made by the Offeror to induce any other person or firm to submit or not to submit an offer for the purpose of restricting competition.

8. ADDITIONAL DISCLOSURES

Offeror shall report in writing to the County Department of Purchasing and Contracting within five business days of discovering or having any reason to suspect any change in status as certified in the preceding paragraphs. Upon County's request, Offeror shall provide additional information supporting Offeror's Representations and Certifications. Offeror's obligations under this Section 8 shall continue until Offeror is no longer under consideration for award of a contract, or until termination or expiration of any resulting contract(s).

CERTIFICATION

The information furnished in Paragraphs 1 through 8 and in the accompanying offer is certified to be factual and correct as of the date submitted and this certification is made under penalty of perjury under the laws of the State of California.

Name: Jerry Burch Signature: _____

Title: Area Sales Manager Date: November 5, 2020

Company/Organization: Motorola Solutions, Inc.

SUBMIT THIS FORM AS DIRECTED IN THE REQUEST FOR SOLICITATION DOCUMENTS OR WITH THE OFFER

COUNTY OF SAN DIEGO

NONDISCLOSURE INDEMNIFICATION AGREEMENT

IF OFFEROR SUBMITS EXHIBIT CONFIDENTIAL/PROPRIETARY, THE FOLLOWING NONDISCLOSURE INDEMNIFICATION AGREEMENT MUST BE COMPLETED, SIGNED AND RETURNED WITH THE OFFER

This indemnification agreement ("Agreement") is made and entered into by and between the County of San Diego ("County") and Offeror Company/Organization Name: NEOLOGY INC ("Offeror") with reference to the following facts: _____

WHEREAS the County may receive a request for disclosure of Offeror's submission under the California Public Records Act, Government Code Section 6250, et seq.; and

WHEREAS, Offeror has included in its submission an exhibit entitled "*EXHIBIT – CONFIDENTIAL/PROPRIETARY*" containing records that Offeror has determined to constitute trade secrets or other proprietary information exempt from disclosure under the California Public Records Act; and

WHEREAS the County requires defense and indemnity from Offeror for the County's ongoing non-disclosure of Offeror's *EXHIBIT-CONFIDENTIAL/PROPRIETARY*;

NOW, THEREFORE, for good and valuable consideration and the mutual promises contained herein, the parties agree to the following:

1. The above recitals are incorporated herein by this reference.
2. Except as otherwise provided herein, the County will not release Offeror's *EXHIBIT-CONFIDENTIAL/PROPRIETARY* based on Offeror's representation that the records contained therein are proprietary and exempt from disclosure under the California Public Records Act and/or are trade secrets as that term is defined in Government Code Section 6250, et seq. Notwithstanding the foregoing, however, the County may release Offeror's *EXHIBIT-CONFIDENTIAL/PROPRIETARY* in the event of any of the following:
   a. Offeror fails to comply with the terms and conditions of this Agreement; or
   b. Offeror provides the County with written notice that some or all of the records may be released; or
   c. A court of competent jurisdiction orders the County to release the records and the County has exhausted or waived its appeal rights.
3. To the fullest extent allowed by law, the County shall not be liable for, and Offeror shall defend and indemnify County and its Board of Supervisors, officers, directors, employees and agents of County (collectively "County Parties"), against any and all claims, demands, liability, judgments, awards, fines, mechanics' liens or other liens, labor disputes, losses, damages, expenses, charges or costs of any kind or character, including attorneys' fees (whether incurred by County attorneys or attorneys employed by County) and court costs (hereinafter collectively referred to as "Claims"), related to Offeror's *EXHIBIT-CONFIDENTIAL/PROPRIETARY.*
4. Offeror waives any and all claims in law or equity and hereby releases the County Parties from any and all claims, deductibles, self-insured retentions, demands, liability, judgments, awards, fines, mechanics' liens or other liens, labor disputes, losses, damages, expenses, charges or costs of any kind or character, including attorneys' fees and court costs, which arise out of or are in any way connected to Offeror's *EXHIBIT-CONFIDENTIAL/PROPRIETARY*.

TO BE COMPLETED BY AN AUTHORIZED REPRESENTATIVE OF THE OFFEROR	
Offeror Company/Organization Name:	NEOLOGY INC
Authorized Representative Name:	Francisco Martinez de Velasco
Authorized Representative Title:	CEO
Signature:	Date: 11/2/2020

BASE YEAR
DATE OF AWARD – OCTOBER 31, 2021

DESCRIPTION	MFG & MODEL	ESTIMATED QUANTITY	UNIT PRICE	TOTAL
Mobile LPR 1 camera system, dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle	P720 - ALPR Camera	4	$ 2,400.00	$ 9,600.00
Portable LPR 1 camera system, dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle	P720 - ALPR Camera	10	$ 2,400.00	$ 24,000.00
LPR Camera Mounting Brackets for Light Bar	Lightbar Mount	4	$ 300.00	$ 1,200.00
LPR Mounting for Portable system	P720 - Portable Mount	10	$ 300.00	$ 3,000.00
LPR Processor	SX4e Processor	14	$ 1,595.00	$ 22,330.00
Modem	RUT240	14	$150.00	$2,100.00
LPR Software	Pagis OCR (inc. above)	14	$ 0.00	$ 0.00
LPR Speed Trailer complete package	Base LPR Trailer	1	$ 18,450.00	$ 18,450.00
Start-up, configuration, and commissioning of LPR Systems at Sheriff's facility to include all expenses such as travel	System Commissioning	14	$ 260.00	$ 3,640.00
Installation	Mobile Install	14	$ 300.00	$ 4,200.00
Covert Installation in vehicle	Covert Install	1	$ 1,200.00	$ 1,200.00
Installation "Kit", Includes all hardware, wiring and software for "do it yourself" standard installations (on poles & trailers)	Power Supply Enclosure kit	5	$ 1,200.00	$ 6,000.00
Training	Hourly Training	8	$ 150.00	$ 1,200.00
Shipping				$
			BASE YEAR SUBTOTAL:	$ 96,920.00

**Quantities are estimates only and not guaranteed

OPTION YEAR 1
NOVEMBER 1, 2021 – OCTOBER 31, 2022

DESCRIPTION	MFG & MODEL	ESTIMATED QUANTITY	UNIT PRICE	TOTAL
Mobile LPR 1 camera system, dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle	P720 - ALPR Camera	4	$ 2,400.00	$ 9,600.00
Portable LPR 1 camera system, dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle	P720 - ALPR Camera	10	$ 2,400.00	$ 24,000.00
LPR Camera Mounting Brackets for Light Bar	Lightbar Mount	4	$ 300.00	$ 1,200.00
LPR Mounting for Portable system	P720 - Portable Mount	10	$ 300.00	$ 3,000.00
LPR Processor	SX4e Processor	14	$ 1,595.00	$ 22,330.00
Modem	RUT240	14	$ 150.00	$2,100.00
LPR Software	Pagis OCR (inc. above)	14	$ 0.00	$0.00
LPR Speed Trailer complete package	Base LPR Trailer	1	$ 18,450.00	$ 18,450.00
Start-up, configuration and commissioning of LPR Systems at Sheriff's facility to include all expenses such as travel	System Commissioning	14	$ 260.00	$ 3,640.00
Installation	Mobile Install	14	$ 300.00	$ 4,200.00
Covert Installation	Covert Install	1	$ 1,200.00	$ 1,200.00
Installation "Kit", Includes all hardware, wiring and software for do it yourself standard installations (on poles & trailers)	Power Supply Enclosure kit	5	$ 1,200.00	$ 6,000.00
Training per hour	Hourly Training	8	$ 150.00	$ 1,200.00
Shipping				$
			OPTION YEAR 1 SUBTOTAL:	$ 96,920.00

**Quantities are estimates only and not guaranteed

OPTION YEAR 2
NOVEMBER 1, 2022 – OCTOBER 31, 2023

DESCRIPTION	MFG & MODEL	ESTIMATED QUANTITY	UNIT PRICE	TOTAL
Mobile LPR 1 camera system, dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle	P720 - ALPR Camera	4	$ 2,400.00	$ 9,600.00
Portable LPR 1 camera system, dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle	P720 - ALPR Camera	10	$ 2,400.00	$ 24,000.00
LPR Camera Mounting Brackets for Light Bar	Lightbar Mount	4	$ 300.00	$ 1,200.00
LPR Mounting for Portable system	P720 - Portable Mount	10	$ 300.00	$ 3,000.00
LPR Processor	SX4e Processor	14	$ 1,595.00	$ 22,330.00
Modem	RUT240	14	$ 150.00	$ 2,100.00
LPR Software	Pagis OCR (inc. above)	14	$ 0.00	$ 0.00
LPR Speed Trailer complete package	Base LPR Trailer	1	$ 18,450.00	$ 18,450.00
Start-up, configuration and commissioning of LPR Systems at Sheriff's facility to include all expenses such as travel	System Commissioning	14	$ 260.00	$ 3,640.00
Installation	Mobile Install	14	$ 300.00	$ 4,200.00
Covert Installation	Covert Install	1	$ 1,200.00	$ 1,200.00
Installation "Kit", Includes all hardware, wiring and software for do it yourself standard installations (on poles & trailers)	Power Supply Enclosure kit	5	$ 1,200.00	$ 6,000.00
Training per hour	Hourly Training	8	$ 150.00	$ 1,200.00
Shipping				$
			OPTION YEAR 2 SUBTOTAL:	$ 96,920.00

**Quantities are estimates only and not guaranteed

GRAND TOTAL (BASIS OF AWARD) :	$ 290,760.00

1. PRICING

1.1. Enter unit prices for each line item, Base Term Period, 1st Option Period, and 2nd Option Period tabs for each line item on the appropriate tab.

1.2. These worksheets have built-in formulas that will calculate the extended prices for each line item and each term period. The aggregate total for each term period will be automatically transferred to the Grand Total (Extended Price) where your total will be calculated.

1.3. The worksheets are locked/protected. The format and the contents of the worksheets should not be tampered with or altered in any way.

1.4. Bids must meet specifications provided.

1.5. All items must be priced to be considered responsive.

2. GENERAL REQUIREMENTS

2.1 A specifications sheet with pictures and operations manual for the product shall be submitted with the bid.

COMPANY:	Neology Inc
REPRESENTATIVE NAME:	Louis Wershaw
REPRESENTATIVE EMAIL:	lwershaw@neology.net
REPRESENTATIVE PHONE:	562-843-1066

Leading the innovation **in detection**

PIPS TECHNOLOGY
DETECTION INNOVATION

Increase your vision

new mobile solution

P720

mobile camera

& **SX4e** processor



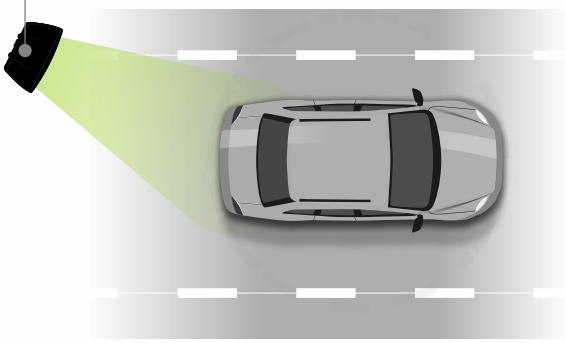
Extended field of view
- 2 lane coverage
- FOV increased by 42%
- 1280 x 720 @ 60fps
- New sensors for better image quality

Longer Capture Range
- Up to 45ft - 50% increase
- Improved low-light capability

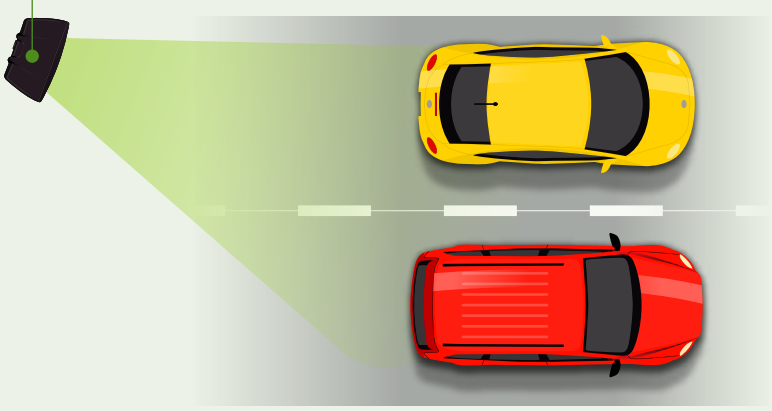
Minimal Upgrade Barrier
- Same low profile and small footprint as the P634 mobile camera
- Backward compatible with current PIPS™ brackets

Easy and flexible installation
- POE cable available in 15 ft to 100 ft
- Metal IP67 sealed connectors
- IP67 housing for outdoor operation

P634 camera field of view (Current)



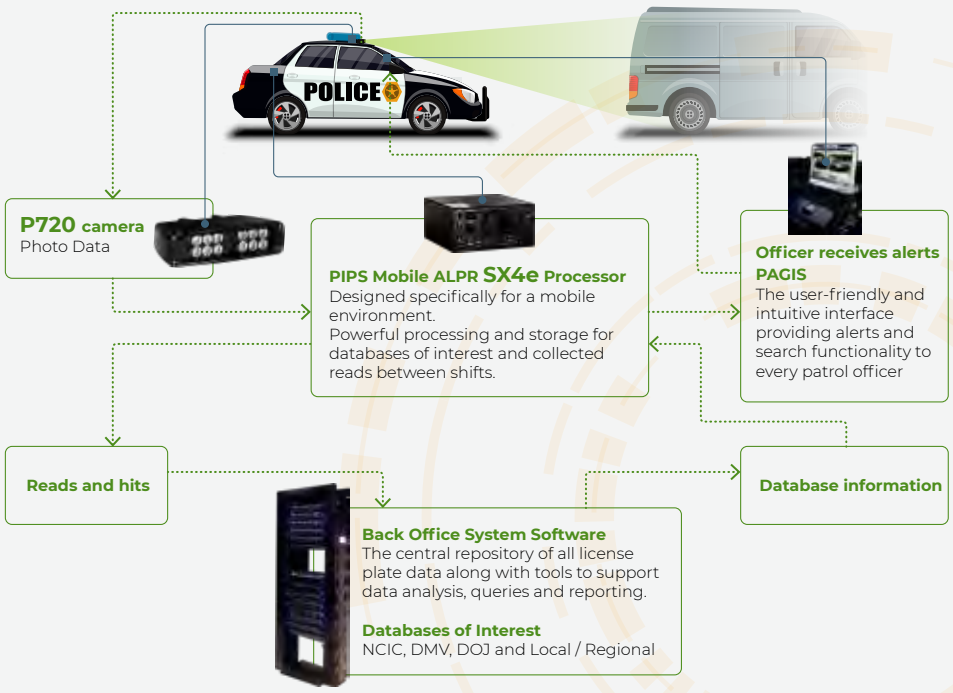
P720 camera field of view



Mobile ALPR Systems

Mobile ALPR Systems assist on-street patrol officers checking for criminal activity by capturing and analyzing license plates against known databases. This compact, rugged system has been IP67 certified and mounts securely below the lightbar for limited visual interference.

PIPS Mobile ALPR Solution is a force multiplier that increases officer productivity and safety with every deployment.



APPLICATIONS

On-street enforcement of:

- Stolen Vehicles
- Amber Alerts
- Unregistered Vehicles
- Wanted Criminals
- Parking Violations
- Be on the Lookout (BOLO)

FEATURES AND BENEFITS:

- Offers high resolution coverage for a full lane of traffic with up to two concurrent vehicles in the field of view.
- Instantly checks captured plates against one or more databases of interest to immediately alert officers of hits.
- Increases spatial awareness for improved officer safety.
- Enhances proactive, preventative enforcement by enabling more intelligent investigations and data sharing across jurisdictions.
- Back Office System Software (BOSS) stores all collected data in a central location to support data analysis, data queries and reporting for law enforcement investigations (in accordance with each jurisdiction's data retention policy).

For additional information, assistance or maintenance questions please contact Neology ALPR/ANPR support at:

PHONE: **833-PIPS-LPR (833-747-7577)**

- Option 1 for sales
- Option 2 for support

For the **U.S/Can and all other areas**:
Sales Enquiry Email: sales@pipstechnology.com
Support Request Email: support@pipstechnology.com

For **Europe, Middle East and Africa**:
Sales Enquiry Email: sales@pipstechnology.co.uk
Support Request Email: support@pipstechnology.co.uk

PIPS TECHNOLOGY DETECTION INNOVATION
is a trademark of Neology inc., and either registered or pending registration in several jurisdictions.

A NEOLOGY MOBILITY TECHNOLOGIES bussiness.

Neology Headquarters San Diego
Address: 13520 Evening Creek Drive Suite 460. San Diego, CA 92128

Neology UK Ltd.
Address: Form 1 Bartley Wood Business Park Hook Hampshire RG27 9XA

Neology Mexico
Plaza Carso II, Lago Zurich No.219-piso 10 C.P. 11529 Ciudad de Mexico

Next

Bid



County of San Diego Sherriff's Department

RFB #10493

November 5, 2020

COUNTY OF SAN DIEGO - REQUEST FOR BIDS (RFB # 10493)
SHERIFF'S DEPARTMENT
LICENSE PLATE READERS
SECTION A: COVER PAGE (P&C 600 FORM)

COUNTY OF SAN DIEGO
SECTION A-P&C 600 FORM
This is not an order

Issued: October 22, 2020

MAIL OR DELIVER TO:
COUNTY OF SAN DIEGO, RFB NO. 10493
DEPARTMENT OF PURCHASING & CONTRACTING
5560 OVERLAND AVE., SUITE 270
SAN DIEGO, CA 92123

AWARD WILL BE MADE TO THE LOWEST RESPONSIVE, RESPONSIBLE BIDDER BASED ON
[ ] ALL OR NONE
[ ] EACH LOT
[X] TOTAL PRICE
[ ] OTHER (SEE PRICING SCHEDULE)

UNSPSC commodity code: **461716.0000**

FOR INFORMATION, PLEASE CONTACT:
PUNNITA DINMUONG, ASSISTANT PROCUREMENT SPECIALIST
PUNNITA.DINMUONG@SDCOUNTY.CA.GOV

BID OPENING DATE: NOVEMBER 5, 2020
BIDS MUST BE RECEIVED AT THE ABOVE ADDRESS PRIOR TO 11:00 A.M. ON DATE OF BID OPENING.

PLEASE STATE YOUR LOWEST PRICE - $183,725.02
F.O.B. DESTINATION AND BRAND NAME OR TRADE NAME IF APPLICABLE. Portable Computer Systems, In
– Brand name Route1 dba PCS Mobile
(Please use typewriter or black ink)
YOUR ENVELOPE MUST INCLUDE RFB NO. 10493

DESCRIPTION

THE COUNTY OF SAN DIEGO (COUNTY), SHERIFF'S DEPARTMENT HAS A REQUIREMENT FOR LICENSE PLATE READERS IN ACCORDANCE WITH THE TERMS & CONDITIONS AND THE STATEMENT OF WORK REFLECTED HEREIN.

INITIAL TERM: DATE OF AWARD – OCTOBER 31, 2021
1ST OPTION YEAR: NOVEMBER 1, 2021 – OCTOBER 31 2022
2ND OPTION YEAR: NOVEMBER 1, 2022 – OCTOBER 31, 2023

PRICING SUBMITTED IS TO REMAIN FIRM FIXED FOR THE TERM PERIOD IDENTIFIED ABOVE. ALL ITEMS WITHIN EACH TERM PERIOD MUST BE PRICED TO BE CONSIDERED RESPONSIVE. AWARD WILL BE MADE TO THE LOWEST RESPONSIVE, RESPONSIBLE OFFEROR BASED ON THE TOTAL PRICE. OFFEROR WHO SUBMITS THE LOW BID WILL BE DEEMED RESPONSIBLE BASED ON THE RESULTS OF THE PRE-AWARD SURVEY.

ARE YOU ABLE TO COMPLY WITH ALL ITEMS SPECIFIED WITHIN THE SCOPE OF WORK? YES OR NO

BIDDER ACKNOWLEDGES ADDENDUM NO. 1 [x] 2 [x] 3 [x] 4 [x] 5 [ ]

SUBJECT TO ACCEPTANCE WITHIN **90** DAYS

PAYMENT TERMS NET **30** DAYS OR % DAY

NAME AND ADDRESS OF BIDDER – Portable Computer Systems, Inc.
4949 S. Syracuse Street, Suite 430
Denver, CO 80237-2747
STREET, CITY, STATE, ZIP

TELEPHONE: NUMBER (916) 204-0621
FAX TELEPHONE: ( )

E-MAIL: lauren.santillano@route1.com

NAME AND TITLE OF PERSON AUTHORIZED TO SIGN OFFER: Lauren Santillano

Lauren Santillano 11/5/2020
SIGNATURE OFFEROR DATE

PRINTED NAME: Lauren Santillano

PRINTED TITLE: VP Business Development

NOTIFICATION OF AWARD

ACCEPTANCE AS TO ITEM(S) NUMBERED:

(VC NO.)

(THIS SECTION FOR COUNTY USE ONLY)
COUNTY OF SAN DIEGO
BY: _____ DATE: _____
JOHN M. PELLEGRINO, DIRECTOR
DEPT OF PURCHASING & CONTRACTING

TOTAL AMOUNT AWARD NO. NAME AND TITLE OF CONTRACTING OFFICER

County of San Diego
Department of Purchasing and Contracting

REPRESENTATIONS AND CERTIFICATIONS

The following representations and certifications are to be completed, signed and returned with the offer (the term "offer" includes a bid, proposal, quote, statement of qualifications, or any other submission to provide goods and/or services).

1. **BUSINESS TYPE**
   ■ For-profit ☐ Non-profit ☐ Government
2. **INTERLOCKING DIRECTORATE**
   In accordance with Board of Supervisors Policy A-79, if Offeror is a non-profit and will be subcontracting with a related for-profit entity where an interlocking directorate, management or ownership relationship exists, Offeror must list all such entity(ies) on an attached separate sheet, and authorization must be sought from Board of Supervisors. If Offeror is a non-profit and does not submit such a list, Offeror certifies it has not entered into a subcontract relationship with a related for-profit entity.
   List Attached? Yes ☐
3. **BUSINESS REPRESENTATION**
   Offeror represents as a part of this offer the following information regarding the ownership, operation, and control of its business:
   - **3.1.** Are you a local business with a physical address within the County of San Diego? ☐ Yes ☒ No
   - **3.2.** Are you certified by the State of California as a:
     ☐ Disabled Veteran Business Enterprise(DVBE)
     Certification #: _____
     ☐ Small Business Enterprise (SBE)
     Certification #: _____
   - **3.3.** Are you certified by the U.S. Dept Of Veterans' Affairs as:
     ☐ Veteran Owned Small Business (VOSB)
     Certification # _____
     ☐ Service Disabled Veteran Owned Small Business (SDVOSB)
     Certification # _____
   - **3.4.** Estimated percentage of work in this offer to be performed or fulfilled locally (within the geographic boundaries of the County of San Diego): 50 %
4. **DEBARMENT, SUSPENSION, AND RELATED MATTERS**
   - **4.1.** Offeror certifies to the best of its knowledge that neither it nor any of its officers:
     - **4.1.1.** Are presently debarred, suspended, declared ineligible, or voluntarily excluded from covered transactions by any state, local, or federal department or agency.
     - **4.1.2.** Have within a three (3) year period preceding this agreement been convicted of or had a civil judgment rendered against them for commission of fraud or criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or contract under a public transaction; violation of federal or state antitrust statutes; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;
   - **4.2.** Except as allowed for in Section 4.2.5, Offeror hereby certifies to the best of its knowledge that neither it nor any of its officers:
     - **4.2.1** Are presently indicted for or otherwise criminally or civilly charged by a government entity (federal, state, or local) with the commission of any of the offenses enumerated in paragraph 4.1.2 of this certification;
     - **4.2.2** Have within a three (3) year period preceding this agreement had one or more public transactions (federal, state or local) terminated for cause or default;
     - **4.2.3** Are presently the target or subject of any investigation, accusation or charges by any federal, state or local agency or law enforcement, licensing, certification, ethics, or compliance body;
     - **4.2.4** Are proposed for debarment by any state, local, or federal department or agency.
     - **4.2.5** If Offeror is unable to certify Sections 4.2.1, 4.2.2, 4.2.3, or 4.2.4, it certifies that it has disclosed and attached to this Representations and Certifications the reason(s) it cannot do so. The disclosure must include the Section(s), specific relevant facts including dates, contracts, individuals involved, status of actions, and any other relevant information that prevent it from making the requested certification(s). The County reserves the right to disqualify an Offeror based upon information disclosed.
     Disclosure Attached? Yes ☐
5. **RELATED WORK**
   Offeror certifies to the best of its knowledge that, other than as disclosed in an attached separate sheet, it and its proposed subcontractors, agents, and consultants have not previously contracted with the County to perform work on or related to this project (e.g. preparing related studies or recommendations, components of the statement of work, or plans and specifications).
   Disclosure Attached? Yes ☐
6. **CURRENT COST OR PRICING**
   Offeror certifies to the best of its knowledge that cost and/or pricing data submitted with this offer, or specifically identified by reference if actual submission of the data is impracticable, are accurate, complete, and current as of the date signed below.
7. **INDEPENDENT PRICING**
   Offeror certifies that in relation to this offer:
   - **7.1.** The prices in this offer have been arrived at independently, without consultation, communication, or agreement, for the purpose of restricting competition, as to any matter relating to such prices with other offerors, with any competitors, or with any County employee(s) or consultant(s) involved in this or related procurements;
   - **7.2.** Unless otherwise required by law, the prices that have been quoted in this offer have not been knowingly disclosed by the Offeror and will not knowingly be disclosed by the Offeror prior to opening, in the case of a bid, or prior to award, in the case of a proposal, directly or indirectly to any other Offeror or to any competitor or with any County employee(s) or consultant(s) involved in this or related procurements; and
   - **7.3.** No attempt has been made or will be made by the Offeror to induce any other person or firm to submit or not to submit an offer for the purpose of restricting competition.
8. **ADDITIONAL DISCLOSURES**
   Offeror shall report in writing to the County Department of Purchasing and Contracting within five business days of discovering or having any reason to suspect any change in status as certified in the preceding paragraphs. Upon County's request, Offeror shall provide additional information supporting Offeror's Representations and Certifications. Offeror's obligations under this Section 8 shall continue until Offeror is no longer under consideration for award of a contract, or until termination or expiration of any resulting contract(s).

CERTIFICATION

The information furnished in Paragraphs 1 through 8 and in the accompanying offer is certified to be factual and correct as of the date submitted and this certification is made under penalty of perjury under the laws of the State of California.

Name: Lauren Santillano Signature: [signature]
Title: VP Business Development Date: 1/15/20
Company/Organization: Portable Computer Systems, Inc.

SUBMIT THIS FORM AS DIRECTED IN THE REQUEST FOR SOLICITATION DOCUMENTS OR WITH THE OFFER

COUNTY OF SAN DIEGO

NONDISCLOSURE INDEMNIFICATION AGREEMENT

IF OFFEROR SUBMITS EXHIBIT CONFIDENTIAL/PROPRIETARY, THE FOLLOWING NONDISCLOSURE INDEMNIFICATION AGREEMENT MUST BE COMPLETED, SIGNED AND RETURNED WITH THE OFFER

This indemnification agreement ("Agreement") is made and entered into by and between the County of San Diego ("County") and Offeror Company/Organization Name: Portable Computer Systems, Inc. ("Offeror") with reference to the following facts: Appendix – Genetec User Guides

WHEREAS the County may receive a request for disclosure of Offeror's submission under the California Public Records Act, Government Code Section 6250, et seq.; and

WHEREAS, Offeror has included in its submission an exhibit entitled "*EXHIBIT – CONFIDENTIAL/PROPRIETARY*" containing records that Offeror has determined to constitute trade secrets or other proprietary information exempt from disclosure under the California Public Records Act; and

WHEREAS the County requires defense and indemnity from Offeror for the County's ongoing non-disclosure of Offeror's *EXHIBIT-CONFIDENTIAL/PROPRIETARY*;

NOW, THEREFORE, for good and valuable consideration and the mutual promises contained herein, the parties agree to the following:

1. The above recitals are incorporated herein by this reference.
2. Except as otherwise provided herein, the County will not release Offeror's *EXHIBIT-CONFIDENTIAL/PROPRIETARY* based on Offeror's representation that the records contained therein are proprietary and exempt from disclosure under the California Public Records Act and/or are trade secrets as that term is defined in Government Code Section 6250, et seq. Notwithstanding the foregoing, however, the County may release Offeror's *EXHIBIT-CONFIDENTIAL/PROPRIETARY* in the event of any of the following:
   a. Offeror fails to comply with the terms and conditions of this Agreement; or
   b. Offeror provides the County with written notice that some or all of the records may be released; or
   c. A court of competent jurisdiction orders the County to release the records and the County has exhausted or waived its appeal rights.
3. To the fullest extent allowed by law, the County shall not be liable for, and Offeror shall defend and indemnify County and its Board of Supervisors, officers, directors, employees and agents of County (collectively "County Parties"), against any and all claims, demands, liability, judgments, awards, fines, mechanics' liens or other liens, labor disputes, losses, damages, expenses, charges or costs of any kind or character, including attorneys' fees (whether incurred by County attorneys or attorneys employed by County) and court costs (hereinafter collectively referred to as "Claims"), related to Offeror's *EXHIBIT-CONFIDENTIAL/PROPRIETARY.*
4. Offeror waives any and all claims in law or equity and hereby releases the County Parties from any and all claims, deductibles, self-insured retentions, demands, liability, judgments, awards, fines, mechanics' liens or other liens, labor disputes, losses, damages, expenses, charges or costs of any kind or character, including attorneys' fees and court costs, which arise out of or are in any way connected to Offeror's *EXHIBIT-CONFIDENTIAL/PROPRIETARY.*

TO BE COMPLETED BY AN AUTHORIZED REPRESENTATIVE OF THE OFFEROR	
Offeror Company/Organization Name:	Portable Computer Systems, Inc.
Authorized Representative Name:	Lauren Santillano
Authorized Representative Title:	VP Business Development
Signature:	Date: 11/5/20

BASE YEAR
DATE OF AWARD – OCTOBER 31, 2021

DESCRIPTION	MFG & MODEL	ESTIMATED QUANTITY	UNIT PRICE	TOTAL
Mobile LPR 1 camera system, dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle	AU-Z3-B-08F08F-850 including warranty. 5 years available.	4	$8,425.26	$33,701.04
Portable LPR 1 camera system, dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle	AU-K-V-Generic-LC including warranty. 5 years available.	10	$3,311.58	$33,115.79
LPR Camera Mounting Brackets for Light Bar	AU-H-Z3-B-LTBARMNT-DBL	4	$115.79	$463.16
LPR Mounting for Portable system	Included in portable LPR system costs.	10	$0	$0
LPR Processor	AU-K-P4Z3-BASE	14	$1,380.45	$19,326.30
Modem	CradlePoint IBR900 and associated hardware	14	$1,793.68	$25,111.58
LPR Software	Genetec Advantage also including support	14	$134.59	$1,884.26
LPR Speed Trailer complete package	Includes 1 portable camera (AU-K-V-Generic-LC), software (Genetec Advantage), training, and shipping on County provided trailer. If County wants Route1 to provide, trailer starts at $19,888 (Wanco).	1	$4,460.26	$4,460.26
Start-up, configuration, and commissioning of LPR Systems at Sheriff's facility to include all expenses such as travel	Includes both mobile and fixed LPR installations. Solar fixed LPR can be provided upon request.	14	$350	$4,900.00
Installation	Includes installation of both mobile and fixed LPR. Does not include trailer installation (see above). Solar fixed LPR can be provided upon request.	14	$875	$12,250.00
Covert Installation in vehicle	Installation	1	$1,775	$1,775

Installation "Kit", Includes all hardware, wiring and software for "do it yourself" standard installations (on poles & trailers)	Includes hardware (AU-K-V-Generic-LC), software (Genetec Advantage), and associated parts.	5	$6,953.83	$34,769.17
Training		8	$150	$1,200.00
Shipping		14	$128.67	$1,799.98
			BASE YEAR SUBTOTAL:	$174,756.54

**Quantities are estimates only and not guaranteed

OPTION YEAR 1
NOVEMBER 1, 2021 – OCTOBER 31, 2022

DESCRIPTION	MFG & MODEL	ESTIMATED QUANTITY	UNIT PRICE	TOTAL
Mobile LPR 1 camera system, dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle		4	$	$
Portable LPR 1 camera system, dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle		10	$	$
LPR Camera Mounting Brackets for Light Bar		4	$	$
LPR Mounting for Portable system		10	$	$
LPR Processor		14	$	$
Modem		14	$	$
LPR Software	Genetec Advantage also including support	14	$134.59	$1,884.26
LPR Speed Trailer complete package		1	$	$
Start-up, configuration and commissioning of LPR Systems at Sheriff's facility to include all expenses such as travel	Preventative Maintenance and travel (optional)	14	$128.57	$1,799.98
Installation		14	$	$
Covert Installation		1	$	$
Installation "Kit", Includes all hardware, wiring and software for do it yourself standard installations (on poles & trailers)		5	$	$
Training per hour	Optional	8	$150	$1,200.00
Shipping				$
			OPTION YEAR 1 SUBTOTAL:	$4,884.24

**Quantities are estimates only and not guaranteed

OPTION YEAR 2
NOVEMBER 1, 2022 – OCTOBER 31, 2023

DESCRIPTION	MFG & MODEL	ESTIMATED QUANTITY	UNIT PRICE	TOTAL
Mobile LPR 1 camera system, dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle		4	$	$
Portable LPR 1 camera system, dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle		10	$	$
LPR Camera Mounting Brackets for Light Bar		4	$	$
LPR Mounting for Portable system		10	$	$
LPR Processor			$	$
Modem		14	$	$
LPR Software	Genetec Advantage also including support	14	$134.59	$1,884.26
LPR Speed Trailer complete package		14 1	$	$
Start-up, configuration and commissioning of LPR Systems at Sheriff's facility to include all expenses such as travel	Preventative Maintenance and travel (optional)	14	$	$1,799.98
Installation			$	$
Covert Installation		14	$	$
Installation "Kit", Includes all hardware, wiring and software for do it yourself standard installations (on poles & trailers)		1 5	$	$
Training per hour	Optional	8	$150	$1,200.00
Shipping		8		$
			OPTION YEAR 2 SUBTOTAL:	$4,884.24

**Quantities are estimates only and not guaranteed

GRAND TOTAL (BASIS OF AWARD) :	$183.725.02	

1. PRICING

1.1. Enter unit prices for each line item, Base Term Period, 1st Option Period, and 2nd Option Period tabs for each line item on the appropriate tab.

1.2. These worksheets have built-in formulas that will calculate the extended prices for each line item and each term period. The aggregate total for each term period will be automatically transferred to the Grand Total (Extended Price) where your total will be calculated.

1.3. The worksheets are locked/protected. The format and the contents of the worksheets should not be tampered with or altered in any way.

1.4. Bids must meet specifications provided.

1.5. All items must be priced to be considered responsive.

2. GENERAL REQUIREMENTS

2.1 A specifications sheet with pictures and operations manual for the product shall be submitted with the bid.

COMPANY: Portable Computer Systems, Inc.

REPRESENTATIVE NAME: Lauren Santillano

REPRESENTATIVE EMAIL: lauren.santillano@route1.com

REPRESENTATIVE PHONE: 916-204-0621

AutoVu SharpZ3

Mobile Automatic License Plate Recognition System

High performance and edge-based mobile ALPR

The AutoVu™ SharpZ3 is a mobile automatic license plate recognition (ALPR) system that goes beyond traditional plate identification. It brings new levels of insight in vehicle analytics, situational awareness, and accuracy.

That's because the SharpZ3 is powered by the latest edge-based processing technology. Designed to combine high-performance and low power consumption, it lets you take full advantage of machine learning capabilities directly at the edge. And with its third optical sensor, the SharpZ3 can precisely position objects and vehicles to understand what's around the license plate, placing reads into context.

Expand your vision with the AutoVu SharpZ3.

Features

- Powered by AutoVu MLC machine learning based engine
- Built-in vehicle classification, plate origin and make and color recognition analytics
- Ultra-low reading latency
- 3 optical sensors
- Modular architecture designed to evolve seamlessly
- Optional advanced GPS positioning with dead reckoning
- Up to 4 high-definition ALPR cameras on the same base unit
- Unified with Genetec Security Center





Get more from your mobile ALPR system

Go beyond conventional mobile ALPR
With the latest neural networking technology built in, the SharpZ3 redefines what mobile ALPR can do. Not only does it deliver higher accuracy and reduce misreads, the SharpZ3 unlocks new insights through its expanded suite of vehicle analytics.

Capture the full picture
With its third optical sensor, the SharpZ3 effortlessly navigates complex urban environments. From flat and non-reflective plates to embossed designs and digital plates, the SharpZ3 can detect more plate designs than traditional units.

Evolve your system with ease
The SharpZ3 is designed with growth in mind. The modular chassis of the SharpZ3 will protect your investment and let you tap into new modules and capabilities over time. This reduces the complication and cost of hardware replacement.

AutoVu SharpZ3 Camera Specifications

ALPR camera sensors
1456(H) x 1088(V) progressive scan @30fps, monochrome, global shutter

ALPR capture range
Up to 63-foot (19-meter) range with retro-reflective license plates

ALPR camera lens options
8mm, 12mm, 16mm, 25mm

Context camera sensor
1456(H) x 1088(V) progressive scan @30fps, color, B&W night mode with 940nm illuminator, global shutter. JPEG still images and MJPEG video streaming

Context camera lens
Based on ALPR lens configuration: (4mm, 6mm, 8mm, 12mm)

Illuminators
Pulsed LED illuminator (740nm, 850nm, 940nm, 590nm)

Water-resistance | sealing
IEC 60529 IPx6, IPx7 | IEC 60529 IP6x

Dimensions
1.65 (h) x 5.12 (w) x 3.56 (d) inches (4.2 × 13 × 9 cm) | Excludes cabling and mounting bracket

Weight
1.2 lbs (0.54kg)

Color
Available in black/white

AutoVu SharpZ3 Base Unit Specifications

I/O
Base unit:
2x 10/100/1000 Base-T Ethernet ports (RJ45)
4x digital inputs (triggers), 0~32Vdc, opto-coupled
4x dry-contact outputs (relays): 2x 0.25A solid state relays, 2x 8A electromechanical relays
1x regulated 12V AUX output power, 200ma

Mounting options
Horizontal and vertical

Dimensions
3.6 (h) x 8.6 (w) x 9.3 (d) inches (9.1 × 21.8 × 23.6 cm).
Excludes cabling, cable racks and mounting brackets

Weight
Base unit: 4.4 lbs (2.0 kg)
ALPR module: 2-ports: 4.1 lbs (1.9 kg)
ALPR module: 4-ports: 4.4 lbs (2.0 kg)

Processors
Intel Atom Processor E3950
Additional dedicated machine-learning co-processor

Power
12/24Vdc nominal (9 to 32 Vdc)
Optional modules:
2x ALPR unit base module
Typical Power consumption: 50W
4x ALPR unit base module
Typical Power consumption: 98W

AutoVu SharpZ3 System Certification (Camera + Base unit)

Vibration
IEC 60068-2-64

Shock resistance
IEC 60068-2-27

Electromagnetic immunity & emissions
FCC part 15 Sub-part B | ICES-003 Issue 4 | CISPR32 / EN55032 | CISPR24 / EN55024 | CISPR25 / EN55025 | EN 50498

CE marking
EMC Directive 2014/30/EU; Automotive EMC Directive 2004/104/EC; RoHS Directive 2011/65/EU

Temperature
-40°F to 122°F (-40°C to 50°C) operating; -40°F to 185°F (-40°C to 85°C) storage
-40°F to 149°F (-40°C to 65°C) base unit operating, w/optional cooling pack
Certifications: IEC 60068-2-1 Category Ad and Ae | IEC 60068-2-2 Category Be | IEC 60068-2-14 Category Na
Includes hi-temp auto-shutoff protection

Genetec Inc.
genetec.com/locations
info@genetec.com
@genetec

© Genetec Inc., 2020. Genetec, AutoVu and the Genetec Logo are trademarks of Genetec Inc., and may be registered or pending registration in several jurisdictions. Other trademarks used in this document may be trademarks of the manufacturers or vendors of the respective products.

UPDATED:18-MAR-20

AutoVu™ SharpV

Automatic License Plate Recognition System

Dedicated, high performance, and edge based Fixed ALPR

The Genetec AutoVu™ SharpV is a specialized, all-in-one automatic license plate recognition (ALPR) camera designed to simplify deployments from specification through installation. Versatile and accurate, the SharpV is suited for fixed ALPR installations, such as monitoring entries and exits or capturing license plates at high-speeds on city-streets and highways.

The SharpV is ideally suited for a range of applications, from managing off-street parking lots and facilities to covering major city access points for wanted vehicles. The SharpV is also capable of simultaneously streaming ALPR and video data to Security Center, the Genetec security platform, where it can be unified with plate reads from mobile ALPR vehicles, surveillance camera streams, and access control events in a single system.



Features

- On-board ALPR processing ensures high-performance, scalability, and ultra low reading latency
- Varifocal lenses ease specification and design
- Power over Ethernet Plus (PoE+) enabled to simplify deployment
- IP67-rated enclosure allows for operation in extreme weather conditions and harsh environments
- Built-in illumination for around-the-clock operation
- Simultaneously read license plates and stream high-resolution contextual color video
- On-board I/Os for integration to induction loops or gates
- Dual lane feature available for America, Europe, ANZ, other regions*

Benefits

Intelligence at the Edge – With processing on-board, the SharpV brings ALPR intelligence to the edge of your system with ultra low reading latency. Since only plate read data needs to be transferred over the network, this means decreased data load on the network and server as all the image processing and analysis is done in the unit. The cameras are not dependent on the server, hence providing uninterrupted coverage even when connectivity goes down.

Unify on a Single Platform – The SharpV can be enrolled within Security Center as a surveillance camera for streaming and recording video. On-board I/Os can be used to trigger reads based on sensors to increase capture rates or open gates based on credentials associated to the plates.

Simplify Specification and Installation – The SharpV is built to facilitate deployment. As a varifocal PoE+ device, the reading distance, magnification and cabling are easily adjustable on site, reducing system design and specification effort. Meanwhile, the modern HTML5 web portal simplifies configurations and maintenance.

See more – Equipped with high-resolution ALPR and context cameras as well as on-board illumination, the SharpV covers a wide field-of-view and provides high-quality images and video, day or night.

* To verify Dual-lane feature availability in your region, contact your Genetec representative.

Specifications

ALPR camera sensor
1280 × 960 @ 30 fps; monochrome; global shutter

Capture range
Standard Range: 9–60 ft (3–18.25 m)
Long Range: 60–115 ft (18–35 m)

Dimensions
2.5 in × 7.6 in × 8.5 in (2.7 high with sunshield for black version)
(63 mm × 192 mm × 214 mm)

Weight
5.04 lb (2.29 kg)

Illuminator
Pulsed LED illuminator for effective use in
0 lux (total darkness) environments
940nm, 850nm, 740nm and 590nm illumination wavelengths available

Context camera sensor (not in ITS model)
1280 × 960 @ 30 fps; color; global shutter

Available color(s)
Security White / Black

Operating Temperature
-40°F to 140°F (-40°C to 65°C) ambient

On-board Analytics
Single-camera speed estimation, direction of travel and virtual loop

Power supply
PoE+ (Power-over-Ethernet) - 802.3at Type 2 (25.5 W)

Cabling
Cat5e cable (special connector provided for IP67 rating)

Sealing (Water/Dust Protection)
IEC 60529: IP66/IP67

Still image compression
JPEG compression for ALPR and Context still images

External interface
1 × 10/100/1000 Base-T Ethernet port

Video streaming
H.264 @ up to 30 fps; MJPEG @ up to 15 fps

Vibration & Shock
IEC 60068-2-64: 5~100Hz | 0.5 g rms
IEC 60068-2-27: 10g | 16ms half-sine
NEMA TS-2: 5~30 Hz | 0.5 g double-amplitude

Electromagnetic immunity & emissions
FCC part 15 Subpart B | ICES-003 Issue 4 | CISPR32 / EN55032 | CISPR 24 / EN 55024

EMC Directive (CE marking)
2014/30/EU

External I/Os
2 inputs / 2 outputs (opto-isolated)

Mounting
Pole and Wall Mount included





Genetec Inc.
genetec.com/locations
info@genetec.com
@genetec

© Genetec Inc., 2020. Genetec, AutoVu and the Genetec Logo are trademarks of Genetec Inc., and may be registered or pending registration in several jurisdictions. Other trademarks used in this document may be trademarks of the manufacturers or vendors of the respective products.

UPDATED:05-FEB-20

Operations and Security

AutoVu MLC

The new standard for accuracy in automatic license plate recognition

Security Center AutoVu™ MLC (Machine Learning Core) is the automatic license plate recognition (ALPR) engine embedded in the ALPR devices. It replaces the traditional rule-based engine used in ALPR solutions with a machine-based algorithm. This increases accuracy, capture rate, while reducing common misreads and false-positives.

Industry:
Parking Enforcement, Transportation, Law Enforcement, B&I

Applications:
LPR

Challenge

Fixed and mobile ALPR systems read thousands of license plates every day. This amplifies the impact of misreads and false positives, with every instance requiring human intervention. The popularity of ALPR in performance-sensitive applications, such as parking enforcement and automatic vehicle access control, means that every gap in performance leads to lost productivity and unnecessary alarms. These service interruptions not only cause customer dissatisfaction but also cost operators time and money.

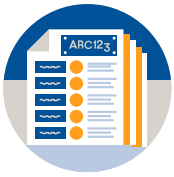
Pushing past the performance plateau

The performance of traditional ALPR technology is difficult to improve on. That's why a new approach is needed. AutoVu MLC leverages decades of ALPR images and a proprietary neural network to achieve new levels of plate-read performance. It has been optimized to run on current ALPR hardware already used by customers in the field; eliminating the need for the costly hardware often required by machine learning technology. AutoVu MLC reduces the number of misreads and false positives and increases the accuracy of advanced vehicle analytics, such as license plate origin detection. This increases automation efficiency, reduces the frequency of operator interventions, and helps officers act with confidence knowing that their data is accurate.

Key benefits

- Cover more ground per shift by reducing interruptions caused by misreads and false positives
- Ensure the smooth flow of vehicles at gated entrances
- Apprehend more offenders or vehicles of interest with improved accuracy and capture rate
- Get new insights on where visitors come from with high accuracy license plate origin detection
- Compatible with existing SharpX, SharpV, and Sharp 3 ALPR units

Applications



Law enforcement

AutoVu MLC boosts the performance of advanced vehicle analytics, such as the state of origin of a license plate. Police officers can act with increased confidence, by having more reliable information and more accurate reads right at their fingertips



Parking enforcement

False positives can drain parking management of resources as they are forced to validate and correct misreads. AutoVu MLC dramatically reduces the number of interruptions parking officers face so they can focus on improving efficiency and catching violators.



Vehicle access control

Accuracy is crucial when businesses trust you on the front line of their operations. Whether to identify scofflaws, black listed plates, your own staff, or even suppliers AutoVu MLC can be trusted to automate vehicle access control on your premises while limiting false positives.



Marketing & business intelligence

Offer a seamless experience to loyalty program and VIP members. AutoVu MLC can identify regular patrons more accurately, helping you get a better sense of your customers. Reduced false positives also save your team time by avoiding the hassle of unnecessary alerts to focus on your customers.

How ALPR performance affects your operations

Capture rate

The percentage of license plates that enter an ALPR camera's field of view and are read by the camera. The capture rate is the foundation of ALPR performance across all applications – detecting more license plates results in a higher chance to identify vehicles of interests or those not on a list of approved individuals.

Read rate

The percentage of detected license plates that are read properly. A perfect read means that each individual character on the license plate was read properly. Other methods can be used to improve vehicle matching capabilities. The process of fuzzy matching replaces similar characters, such as 'B' or '8', in the matching engine and can require only a partial set of characters to be matched to a list before alerting operators.

Misreads

Misreads have different impacts depending on how ALPR is applied in operations. When ALPR is used to identify vehicles on a list, such as an offender or vehicle of interest list, misreads can let a target vehicle go by unnoticed. When used to identify employee or contractor vehicles, misreads can prevent a gate from opening and stalling customers requiring a human operator to intervene.

False positives

When an ALPR camera identifies non-license plate text, such as lettering, roadside signage, or fences, and reads it as a license plate. This is especially problematic in applications where vehicles that are not present on a list generate an alert, such as permit enforcement.

False positives interrupt the work of operators and require corrections to be entered in the system. They can also reduce the confidence of ALPR system users in the data gathered by their system, leading to slower response while they try to validate the read before taking action.

How AutoVu MLC compares to traditional engines

	Rule-based engine	AutoVu MLC	Daily impact
Capture rate	93.9%	98.6%	+165 license plates captured
Perfect read rate	91.5%	97.8%	+368 license plate perfectly read
Fuzzy Matchable Rate	97.3%	99.7%	+244 matchable license plates
False positives	1.6%	0.1%	50 fewer false alerts

[1] Sample size: 1,511 license plates of various countries, including United States, Canada, Western Europe, etc. The Daily Impact column assumes an average of 3,500 reads per day.

Genetec Inc.
genetec.com/locations
info@genetec.com
@genetec

© 2019 Genetec, Inc. All rights reserved. Genetec, the Genetec logo, Federation, Omnicast, Synergis, and AutoVu are either registered trademarks or trademarks of Genetec. All other trademarks contained herein are the property of their respective owners.

AMLC_FN1EN

Per the Indemnification Agreement, all pages going forward are CONFIDENTIAL/PROPRIETARY



Security Center AutoVu™

SharpV Administrator Guide 13.2

Document last updated: September 15, 2020

Genetec™

Legal notices

©2020 Genetec Inc. All rights reserved.

Genetec Inc. distributes this document with software that includes an end-user license agreement and is furnished under license and may be used only in accordance with the terms of the license agreement. The contents of this document are protected under copyright law.

The contents of this guide are furnished for informational use only and are subject to change without notice. Genetec Inc. assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this guide.

This publication may not be copied, modified, or reproduced in any form or for any purpose, nor can any derivative works be created therefrom without Genetec Inc.'s prior written consent.

Genetec Inc. reserves the right to revise and improve its products as it sees fit. This document describes the state of a product at the time of document's last revision, and may not reflect the product at all times in the future.

In no event shall Genetec Inc. be liable to any person or entity with respect to any loss or damage that is incidental to or consequential upon the instructions found in this document or the computer software and hardware products described herein.

Genetec™, AutoVu™, AutoVu MLC™, Citywise™, Community Connect™, Curb Sense™, Federation™, Flexreader™, Genetec Airport Sense™, Genetec Citigraf™, Genetec Clearance™, Genetec ClearID™, Genetec Mission Control™, Genetec Motoscan™, Genetec Patroller™, Genetec Retail Sense™, Genetec Traffic Sense™, KiwiVision™Omnicast™, Privacy Protector™Sipelia™, Stratocast™, Streamvault™, Synergis™, Valcri™, their respective logos, as well as the Mobius Strip Logo are trademarks of Genetec Inc., and may be registered or pending registration in several jurisdictions.

KiwiSecurity™, KiwiVision™, Privacy Protector™ and their respective logos are trademarks of KiwiSecurity Software GmbH, and may be registered or pending registration in several jurisdictions.

Other trademarks used in this document may be trademarks of the manufacturers or vendors of the respective products.

Patent pending. Genetec™ Security Center, Omnicast™, AutoVu™, Stratocast™, Citigraf™, Genetec Clearance™, and other Genetec™ products are the subject of pending patent applications, and may be the subject of issued patents, in the United States and in other jurisdictions worldwide.

All specifications are subject to change without notice.

Document information

Document title: SharpV Administrator Guide 13.2

Original document number: EN.400.008-V13.2.B(1)

Document number: EN.400.008-V13.2.B(2)

Document update date: September 15, 2020

You can send your comments, corrections, and suggestions about this guide to documentation@genetec.com.

About this guide

This guide provides you with a complete source of information about the SharpV web portal and how to configure your SharpV cameras. It explains the basic settings you must configure before your SharpV can be used.

Last-minute updates can be found in the *SharpOS Release Notes*.

You'll still need to refer to the *Security Center Administrator Guide* since some of the configuration for ALPR is done in Security Center Config Tool. For example, information about configuring the ALPR Manager role and creating hotlists is covered in the *Security Center Administrator Guide*.

This guide assumes you are familiar with Security Center systems.

Notes and notices

The following notes and notices might appear in this guide:

- **Tip:** Suggests how to apply the information in a topic or step.
- **Note:** Explains a special case or expands on an important point.
- **Important:** Points out critical information concerning a topic or step.
- **Caution:** Indicates that an action or step can cause loss of data, security problems, or performance issues.
- **Warning:** Indicates that an action or step can result in physical harm, or cause damage to hardware.

IMPORTANT: Content in this guide that references information found on third-party websites was accurate at the time of publication, however, this information is subject to change without prior notice from Genetec Inc.

Contents

Preface

Legal notices ii
About this guide iii

Chapter 1: Getting started

About Security Center AutoVu™ 2
About the AutoVu™ SharpV 3
ALPR using machine learning 4
Specifications for the SharpV 5
Genetec™ server configurations for AutoVu™ systems 9
Storage requirement for ALPR images 11
Supported ALPR contexts 13
Supported dual-lane configurations 16
Supported plate origin recognition 17

Chapter 2: Introduction to the Sharp Portal

Logging on to the Sharp Portal 19
Sharp Portal interface overview 23
Viewing camera feeds 24
SharpV hardware inventory 26
Changing your logon password in the Sharp Portal 27
Rebooting a SharpV from the Sharp Portal 28
Importing and exporting settings 29
Synchronizing the SharpV clock 31

Chapter 3: SharpV software configuration

Security configuration in the Sharp Portal 33
- Installing the SharpV auto-generated certificate 33
- Installing a self-signed certificate 35
- Installing a signed certificate 37

Configuring SharpV network settings 39
- Connecting to a SharpV camera using the fallback IP address 39

Calibrating the SharpV zoom and focus 40
- Plate read distances for SharpV lenses 44

About SharpV exposure adjustment for indoor installations 45
- Setting custom SharpV ALPR camera exposure levels for indoor installations 45
- Setting custom SharpV context camera exposure levels for indoor installations 46

About SharpV exposure adjustment for outdoor installations 47
- Setting custom SharpV ALPR camera exposure levels for outdoor installations 47
- Setting SharpV ALPR camera exposure levels for reflective and non-reflective plates 48
- Troubleshooting outdoor exposure issues for the SharpV ALPR camera 50
- Troubleshooting outdoor exposure issues for the SharpV context camera 51

Configuring SharpV analytics 52
- About Sharp read strategies 54
- Configuring the SharpV to monitor dual lanes 56

Calibrating the virtual loop . . . 57
Calibrating speed estimation . . . 63
About matcher settings files . . . 66
Configuring where the SharpV sends its ALPR data . . . 69
SharpV camera connections to the ALPR Manager role . . . 70
SharpV communication ports . . . 71
Adding a SharpV camera to the ALPR Manager . . . 72
Upgrading a SharpV to use the LPM protocol . . . 75
About port forwarding for SharpV cameras using the LPM protocol . . . 76
About port forwarding for SharpV cameras using the Security Center (legacy) extension . . . 79
Adding a SharpV camera to the Archiver . . . 81
Configuring the SharpV FTP extension . . . 84
Modifications you can make to the SharpV FTP XML template . . . 84
Configuring the SharpV HTTP extension . . . 87
Examples of JSON and XML ALPR events for the SharpV HTTP extension . . . 88
Configuring Syslog for SharpV log files . . . 90

Chapter 4: Upgrade

Supported SharpOS update paths . . . 92
Updating a Sharp unit from the Sharp Portal . . . 93
Updating the SharpV Platform from the Sharp Portal . . . 95

Chapter 5: Sharp Portal reference

Sharp Portal - Overview page . . . 98
Sharp Portal - Camera feeds page . . . 100
Sharp Portal - Inventory page . . . 102
Sharp Portal - Network page . . . 103
Sharp Portal - Security page . . . 104
Sharp Portal - Exposure page . . . 106
Sharp Portal - Position and orientation page . . . 107
Sharp Portal - ALPR settings page . . . 108
Sharp Portal - Extension page . . . 110
Sharp Portal - Product improvement program page . . . 112
Sharp Portal - Recovery page . . . 113
Sharp Portal - Date and time page . . . 114
Sharp Portal - Power options page . . . 115
Sharp Portal - Maintenance page . . . 116
Sharp Portal - Logs page . . . 117
Sharp Portal - Log sources page . . . 118

Chapter 6: Troubleshooting for SharpV fixed installation

LED status on the SharpV camera unit . . . 120
Resetting a lost password for the Sharp Portal . . . 122

Glossary . . . 124

Where to find product information . . . 145
Technical support . . . 146

1

Getting started

This section includes the following topics:

- "About Security Center AutoVu™" on page 2
- "About the AutoVu™ SharpV" on page 3
- "ALPR using machine learning" on page 4
- "Specifications for the SharpV " on page 5
- "Genetec™ server configurations for AutoVu™ systems" on page 9
- "Storage requirement for ALPR images" on page 11
- "Supported ALPR contexts" on page 13
- "Supported dual-lane configurations" on page 16
- "Supported plate origin recognition" on page 17

About Security Center AutoVu™

The AutoVu™ automatic license plate recognition (ALPR) system automates license plate reading and identification, making it easier for law enforcement and for municipal and commercial organizations to locate vehicles of interest and enforce parking restrictions. Designed for both fixed and mobile installations, the AutoVu™ system is ideal for a variety of applications and entities, including law enforcement, municipal, and commercial organizations.

Depending on the Sharp hardware you install, you can use AutoVu™ in a fixed configuration such as on a pole in a parking lot, or in a mobile configuration such as on a patrol vehicle.

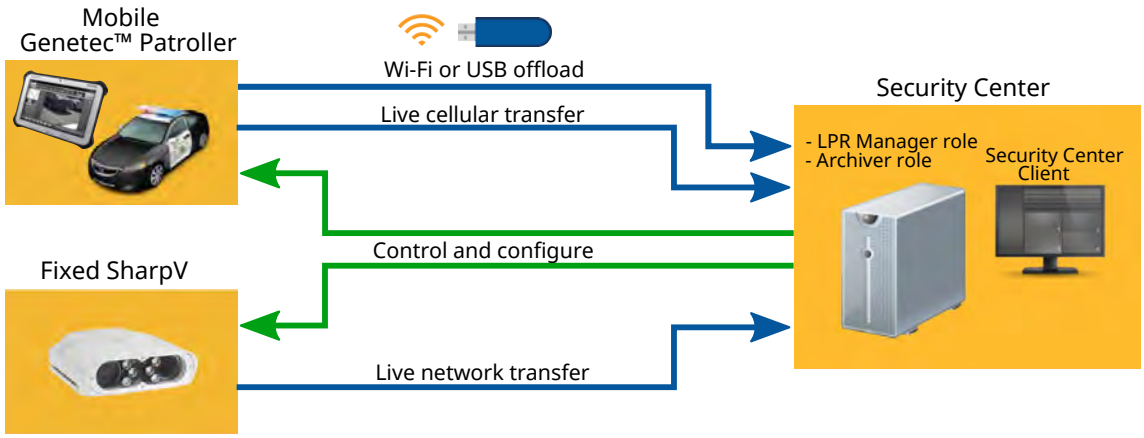
You can use AutoVu™ for the following:

- Scofflaw and wanted vehicle identification
- City-wide surveillance
- Parking enforcement
- Parking permit control
- Vehicle inventory
- Security
- Access control

AutoVu™ system architecture

AutoVu™ Sharp cameras capture license plate images, and send the data to Genetec Patroller™ or Security Center to verify against lists of vehicles of interest (hotlists) and vehicles with permits (permit lists).

The following diagram shows how a typical AutoVu™ system works:

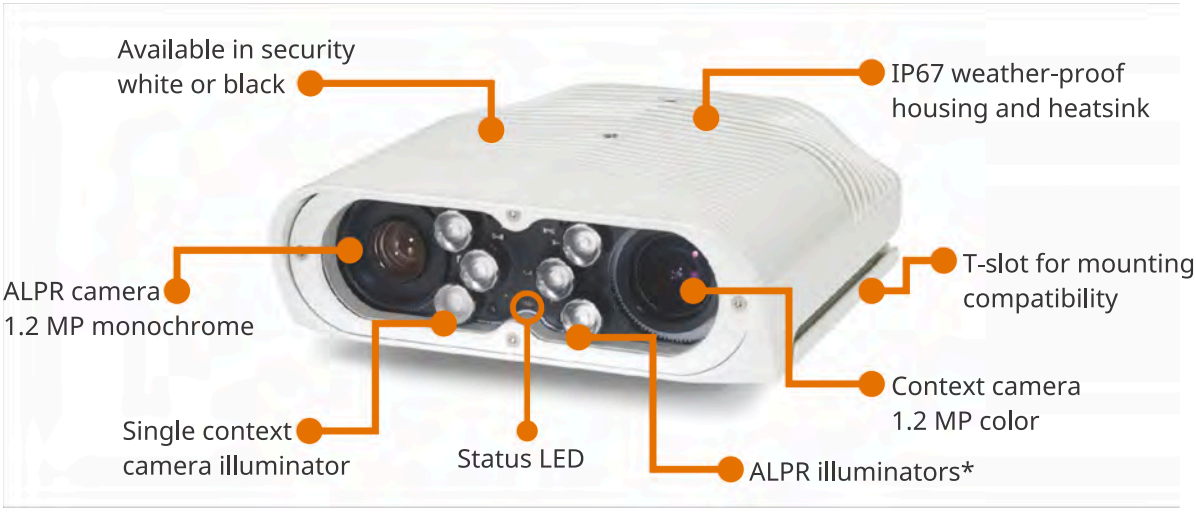


Example

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

About the AutoVu™ SharpV

The AutoVu™ SharpV is an all-in-one specialized automatic license plate recognition (ALPR) device which combines two high-definition cameras with onboard processing and illumination in a ruggedized, environmentally sealed unit.



* Depending on the camera options, the five ALPR illuminators might emit light that is visible in dark conditions. The single context camera illuminator does not emit visible light.

ALPR using machine learning

Sharp systems running SharpOS 13 use machine learning to classify license plates and to perform character recognition.

AutoVu MLC™

AutoVu MLC™ (Machine Learning Core) replaces traditional rule-based ALPR technology with machine learning-based algorithms to reduce common ALPR misreads and false positives. It is a proprietary technology of Genetec Inc. used in AutoVu™ Sharp hardware for license plate recognition.

Although off-the-shelf machine learning solutions are commercially available for ALPR, their results can be unpredictable. With our hardware and software engineering expertise, we have built the AutoVu MLC™ from the ground up. This includes developing a deep neural network (DNN), training the system with Sharp camera images, and optimizing the system to run on AutoVu™ hardware. The AutoVu MLC™ represents a significant reduction in the time that operators spend manually correcting plate reads.

As the AutoVu MLC™ continues to develop, we will apply it to more aspects of the ALPR process. You will be able to take advantage of these improvements with future SharpOS releases.

Specifications for the SharpV

Refer to the technical, mechanical, and environmental specifications when planning and deploying a SharpV camera.

Mechanical and environmental specifications

Hardware	Specification
ALPR camera sensor	1280 x 960 progressive scan 30 fps (60 Hz) or 25 fps (50 Hz), monochrome
Context camera sensor	1280 x 960 progressive scan 30 fps (60 Hz) or 25 fps (50 Hz), color (available on Standard model only) **NOTE:** Information on context cameras is not applicable to SharpV ITS cameras.
Capture range	• **Standard:** 2.75 - 18.25 m (9 - 60 ft) • **Long range:** 18.25 – 35 m (60 - 115 ft)
Dimensions (HxWxD)	63 x 192 x 214 mm (2.5 × 7.6 × 8.5 in.) Height including sunshield for black version: 69 mm (2.7 in.)
Weight	2.29 kg (5.04 lb)
Illuminator	Pulsed LED illuminator for effective use in 0 lux (total darkness) environments. Different illumination wavelengths are available.
Available colors	Security white or black
Operating temperature	• -40ºC to 65°C (-40ºF to 150ºF) ambient • -40ºC to 55°C (-40ºF to 130ºF) ambient for installations in India
On-board analytics	Single-camera speed estimation, direction of travel, virtual loop, and state name (North America and Europe)
Power supply	PoE+ (Power-over-Ethernet; 802.3at Type 2 (25.5 W))
Input rating	PoE+: 43 – 57V, 0.6 – 0.4A
Compression	MJPEG or H.264 video compression for ALPR and Context feeds; JPEG compression for ALPR and Context still images
External interface	1 x 10/100/1000 Base-T Ethernet port
External I/O	• 2 inputs (Opto-isolated, DC polarized) • 2 outputs (Opto-isolated, dry)
Mounting	Pole mount and wall mount included.

Network cable specifications

Hardware	Specification
Cable rating	CAT5e or higher (special connector provided for IP67 rating)
Shielding	Shielded or unshielded
Conductor gauge	24 AWG
Conductor arrangement	Straight-through EIA-568A or EIA-568B
Cable diameter	The RJ45 connector that is shipped with the system accepts CAT5e cable diameters in the range 4.8 - 6.7 mm (0.19 - 0.26 in.). The bayonet shell supports cable diameters in the range 4 - 8 mm (0.16 - 0.31 in.).
Cable length	Maximum 100 m (330 ft)
Environmental	The network cable must be waterproof and UV-resistant, with a temperature rating appropriate for your climate.
PoE+ standard	Power-over-Ethernet; 802.3at Type 2 (25.5 W) **NOTE:** • Not all hardware that is labeled "PoE+" meets the IEEE 802.3at standard that is required for use with the SharpV. • Ensure that the total power consumption of all hardware connected to the PoE+ source does not exceed the power budget of the PoE+ source. Each SharpV camera must be supplied with 25.5 W.

Input / output specifications

Hardware	Specification
Inputs	
Number of inputs	2
Input rating	0 VDC - 30 VDC
Guaranteed ON state threshold	5.75 V
Guaranteed OFF state threshold	4.80 V
Overvoltage protection	Included
Reverse voltage protection	Included
Input type	Opto-isolated, DC polarized
Outputs	
Number of outputs	2
Output rating	30 V / 100 mA

Hardware	Specification
On-state voltage	Von = <1.0 V @ 2 mA Von = <2.5 V @ 100 mA
Overcurrent (overload) protection	Included
Reverse voltage protection	Included
Output type	Opto-isolated, dry

Input / output cable specifications

Hardware	Specification
Cable diameter	The I/O cable assembly is compatible with cable diameters in the range 4 - 8 mm (0.16 - 0.31 in.). **NOTE:** Two different cable seals are included with the I/O cable assembly. Refer to the manufacturer's instructions to determine which seal to install for the diameter of cable you are using.
Wire gauge	The I/O cable assembly can support a maximum wire gauge of 20 AWG. The cable's voltage rating must be suitable for the SharpV I/O specifications and must conform to electrical codes in your region.
Weather rating	The cable must be waterproof, UV resistant, and must be rated for outdoor installation in accordance with your region.

SharpV mounting specifications

Hardware	Specification
Mounting bolts	Type M6 x 1mm
Mounting hole distance	70 mm (2 3/4 in.)
Mounting hole depth	9.5 mm (3/8 in.)

Certifications and compliance

Compliance	Specification
Safety	IEC/EN 62471. Photobiological safety of lamps and lamp systems **WARNING:** Depending on the LED illuminator wavelength option selected for the camera hardware, the light emitted from the device might be visible or invisible to the eye. To limit the danger to your eyes caused by infrared light, stay at least 20 cm (8 in.) from the front of the camera. Ensure that the camera installation location prevents or discourages anyone from looking at the face of the camera from within this distance.
Electromagnetic immunity and emissions	FCC part 15 Subpart B | ICES-003 Issue 4 | CISPR32 / EN55032 | CISPR 24 / EN 55024

Compliance	Specification
EMC Directive (CE marking)	2014/30/EU
Vibration and shock	Random : IEC 60068-2-64; 5-100Hz; 0.5g; 3 axes; 1 hours/axis Sinusoidal, endurance : NEMA TS-2 Test 2.2.8.4; 30Hz, 3 axes; 1 hours/axis Shock resistance : IEC60068-2-27 / NEMA TS-2 Test 2.2.9; 10g; 3 axes, 3 shocks per direction per axis
Water resistance and sealing	IEC 60529 IPx6, IPx7 | IEC 60529 IP6x

Part numbers



Component	Signification
A	SharpV prefix
B	Color: **W** (white) or **B** (black)
C	Range: • **S (standard):** 2.75 - 18.25 m (9 - 60 ft) • **L (long range):** 18.25 – 35 m (60 - 115 ft)
D	Illumination: LED illumination in nanometers
E	Camera option: **LC** (ALPR and context) or **L** (ITS - Intelligent Traffic Systems: ALPR only)

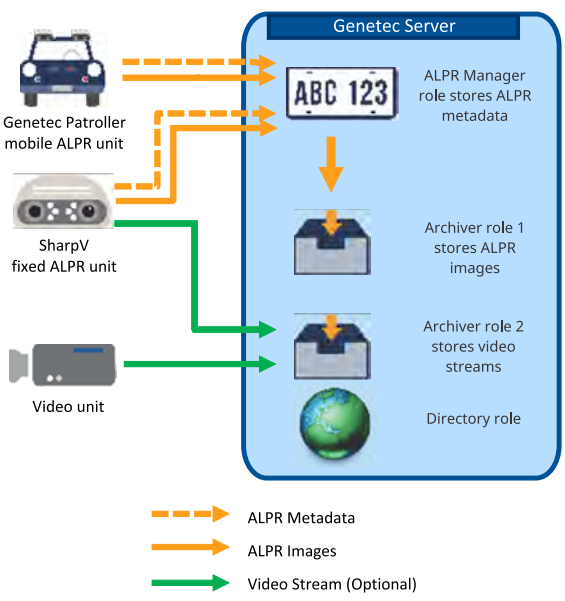
Genetec™ server configurations for AutoVu™ systems

Depending on the requirements of the system, you can install the AutoVu™ system on one server or distribute the load over multiple servers.

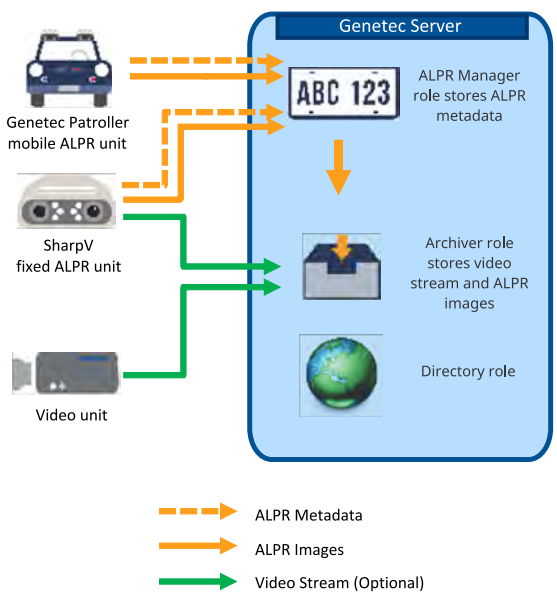
Single server

In a single-server system, the ALPR Manager, Archiver, and Directory roles are configured on the same server. For better performance, you can configure separate Archiver roles for ALPR and video.

Recommended server configuration



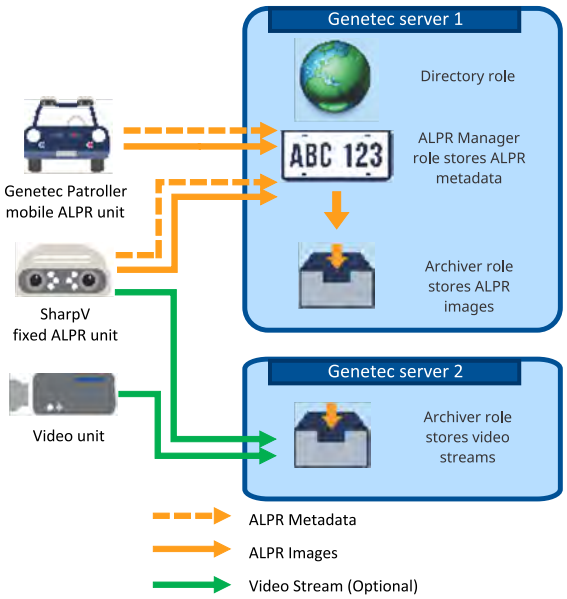
Small system server configuration



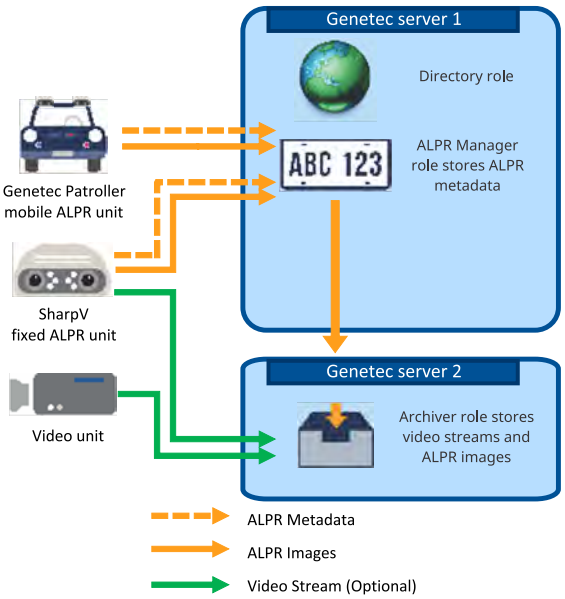
Multiple servers

In a multiple-server system, the Archiver role is installed on a separate server from the ALPR Manager and Directory roles. For better performance, you can configure separate Archiver roles for ALPR and video.

Recommended server configuration



Small system server configuration



Storage requirement for ALPR images

The images associated with the reads and hits are stored on disk in G64 files by an Archiver. You can estimate the disk space required to store these images if you know the average number of reads and hits processed by the ALPR Manager per day.

For every license plate read or hit processed by the ALPR Manager, the Archiver stores a set of four images:

- One context camera image (in either high resolution or low resolution)
- One ALPR camera image (cropped to show only the license plate)
- One context camera thumbnail image
- One ALPR camera thumbnail image

The size of the image set depends on the model of the Sharp camera and whether the context camera is configured to take images in high resolution or low resolution.

Use the following formula to estimate the disk space you need for the desired image retention periods.

```
Disk space = (ReadsPD x ImageSize x ReadIRP) + (HitsPD x ImageSize x HitIRP)
```

where:

- **ReadsPD:** Average number of reads per day.
- **ImageSize:** Estimated image size per read (depends on the Sharp model and configuration).
- **ReadIRP:** Read image retention period (see ALPR Manager's **Properties** tab).
- **HitsPD:** Average number of hits per day.
- **HitIRP:** Hit image retention period (see ALPR Manager's **Properties** tab).

If your patrol vehicles are equipped with wheel imaging cameras, double the number of hits per day in your formula (there is typically one wheel image per hit).

The following table gives you the rough estimates of the image size per read based on the Sharp model and configuration.

Type of image	Sharp VGA or XGA	SharpV	SharpZ3
High-resolution configuration			
Context camera image	~50 KB	~120 KB	~160 KB
ALPR camera image (cropped)	~3 KB	~3 KB	~2 KB
Context camera thumbnail image	~3 KB	~3 KB	~2 KB
ALPR camera thumbnail image	~1 KB	~1 KB	~1 KB
Total image size per read:	~57 KB	~127 KB	~165 KB
Low-resolution configuration			
Context camera image	~18 KB	-	-
ALPR camera image (cropped)	~3 KB	~3 KB	-
Context camera thumbnail image	~3 KB	~3 KB	-

Type of image	Sharp VGA or XGA	SharpV	SharpZ3
ALPR camera thumbnail image	~1 KB	~1 KB	-
Total image size per read:	~25 KB	-	-

NOTE: If a read or hit is protected and must be kept beyond its specified retention period, it will require more disk space for its associated images than what is calculated for a single event. Because the Archiver stores multiple ALPR images in a single G64 file, if one image in the file is protected, then all other images in the file are also protected. This uses up more disk space over time. However, an image whose corresponding read or hit has been deleted can no longer be read because the G64 files are encrypted.

If the Archiver is assigned to more than one ALPR Manager, add the numbers for all ALPR Manager roles together.

Supported ALPR contexts

ALPR contexts are created for specific regions in order to optimize ALPR for the license plates of that region.

NOTE: To help us improve the performance of regional contexts, click **Configuration** > **Connectivity** > **Product improvement** and register this camera to participate in the **Product improvement program**.

ALPR contexts are available for the following license plates:

Asia-Pacific

- Australia (optimized for New South Wales)
- Hong Kong
- India
- Japan
- Mongolia
- Northern territory (Australia)
- New Zealand
- Queensland (Australia)
- Singapore
- Sri Lanka[20]
- Turkmenistan
- Vietnam
- Western Australia

Caribbean and Latin America

- Argentina
- ArgentinaMulti[17]
- Bahamas
- Bermuda
- Brazil
- Cayman Islands
- Chile
- Colombia
- Costa Rica
- Dominican Republic
- Mexico
- Mexico Jalisco
- Paraguay
- Peru
- St-Maarten

Europe/Middle East/Africa

- Abu Dhabi
- Abu Dhabi WithPrefix[18]
- Algeria
- Arabic Peninsula[1]
- Azerbaijan
- Bahrain
- Belgium[9]
- BelgiumMulti[10]
- BelgiumMultiVanity[11]
- Denmark
- Dubai
- DubaiWithPrefix[18]
- Europe[2]
- Europe One and Two Lines[3]
- France
- Great Britain
- General European context
- Germany
- Iceland
- Ireland
- Italy
- Ivory Coast
- Jordan
- Kazakhstan
- Kuwait
- Lebanon
- Monaco
- Morocco
- Netherlands
- Norway
- Oman[4]
- Poland
- Portugal
- Qatar
- QatarMilitary[12]
- Romania
- Saudi Arabia
- Sharjah
- Sharjah WithPrefix[18]
- Slovakia
- South Africa
- Spain
- Sweden
- Switzerland
- Turkey
- TurkeyOnly[13]
- United Arab Emirates[5]
- United Arab Emirates WithPrefix[18]

North America

- Alabama
- Alaska
- Alberta
- Arizona
- British Columbia
- British Columbia Fixed[14]
- California
- Colorado
- Connecticut
- Delaware
- Florida
- General US context
- Georgia
- Georgia_3Chars[21]
- Hawaii
- Idaho
- Illinois
- Indiana
- Iowa
- Kansas
- Kentucky
- KentuckyIndiana
- Louisiana
- Maine
- Manitoba
- Maryland
- Massachusetts
- MassachusettsIR[15]
- Michigan
- Minnesota
- Mississippi
- Montana
- Nebraska
- Nevada
- New Brunswick
- Newfoundland
- New Hampshire
- New Jersey
- New Mexico
- New York
- New York City[16]
- North Carolina
- North Dakota
- Northeast states[6]
- Nova Scotia
- Ohio
- Oklahoma
- Ontario
- Oregon
- Pennsylvania
- PennsylvaniaDelaware[6]
- Prince Edward Island
- Quebec
- Rhode Island
- Saskatchewan
- South Carolina
- South Dakota
- Tennessee
- Texas
- Utah and Neighbors[8]
- Vermont
- Virginia
- Washington State[19]
- Wisconsin
- Wyoming
- Yukon

[1]Includes Saudi Arabia, Bahrain, Kuwait, and UAE.

[2]General European context for one-line plates.

[3]General European context for one-line and two-line plates.

[4]Only standard Omani plates are supported (wide-format, black-on-white, and black-on-yellow). License plates issued by neighboring countries are not supported.

[5]Includes Abu Dhabi, Dubai, and Sharjah plates.

[6]Includes Delaware, New York, Pennsylvania, and Vermont plates.

[7]Includes Pennsylvania, Delaware, Florida, Vermont, and New York plates.

[8]Includes Utah, Oregon, Montana, and North Dakota plates.

[9]Supports one-line plates with five or more characters.

[10]Supports one-line and two-line plates with five or more characters.

[11]Supports one-line and two-line plates with three or more characters. Note that this context can produce many false positive reads.

[12]Exposure settings are optimized for non-reflective military plates. Note that performance with standard plates might be reduced.

[13]Excludes the letters Q, W, and X. Note that foreign plates that contain these characters are not read correctly.

[14]Optimized for fixed installations.

[15]Optimized for SharpV cameras with 850nm IR illuminators.

[16]Exposure settings are optimized for non-reflective taxi plates. Note that performance with standard plates might be reduced.

[17]Supports standard and motorcycle plates.

[18]*WithPrefix* includes characters that are present on the plate, but are separate from the license plate read.

[19]Specialized ALPR contexts available for ABMER (590 nm) and IR (850nm) illuminators.

[20]Supports Latin characters only.

[21]Supports plates with three or more characters. Note that using this context might increase the false positive count.

Supported dual-lane configurations

Dual-lane configurations are created for specific regions where dual-lane license plate recognition is available.

Dual-lane license plate recognition is available for the following countries:

Asia-Pacific

- Australia
- Hong Kong
- Sri Lanka
- Mongolia
- New Zealand
- Vietnam

Caribbean/Latin America

- Bahamas
- Bermuda
- Cayman Islands
- Chile
- Colombia
- Costa Rica
- Dominican Republic
- Mexico
- Peru

Europe/Middle East/Africa

- Algeria
- Belgium
- Denmark
- France
- Great Britain
- Germany
- Italy
- Iceland
- Ireland
- Kazakhstan
- Netherlands
- Monaco
- Norway
- Poland
- Portugal
- Romania
- Slovakia
- South Africa
- Spain
- Sweden
- Switzerland
- Turkey

North America

- United States of America (USA)
- Canada

Supported plate origin recognition

In addition to reading the number on a license plate, the SharpV can also read the state, province, or country. Plate origin recognition is performed on a best-effort basis, and is not necessarily available for the same plates that have a supported ALPR context.

Plate origin recognition is supported for the following plates:

Europe/Middle East/Africa

- Abu Dhabi (AD)
- Ajman (AJ)
- Bahrain (BRN)
- Belgium (B)
- Denmark (DK)
- Dubai (DUB)
- France (F)
- Fujairah (FUJ)
- Germany (D)
- Great Britain (GB)
- Italy (I)
- Kuwait (KWT)
- Netherlands (NL)
- Norway (N)
- Poland (PL)
- Portugal (P)
- Ras al Khaimah (RAK)
- Romania (RO)
- Saudi Arabia (KSA)
- Sharjah (SHJ)
- Slovakia (SK)
- Switzerland (CH)
- Spain (E)
- Umm al Qaiwain (UAQ)

North America

- Alabama (AL)
- Alaska (AK)
- Alberta (AB)
- Arizona (AZ)
- Arkansas (AR)
- British Columbia (BC)
- California (CA)
- Colorado (CO)
- Connecticut (CT)
- Delaware (DE)
- District of Columbia (DC)
- Florida (FL)
- Georgia (GA)
- Hawaii (HI)
- Idaho (ID)
- Illinois (IL)
- Indiana (IN)
- Iowa (IA)
- Kansas (KS)
- Kentucky (KY)
- Louisiana (LA)
- Maine (ME)
- Manitoba (MB)
- Maryland (MD)
- Massachusetts (MA)
- Michigan (MI)
- Minnesota (MN)
- Mississippi (MS)
- Missouri (MO)
- Montana (MT)
- Nebraska (NE)
- Nevada (NV)
- New Brunswick (NB)
- Newfoundland and Labrador (NL)
- New Hampshire (NH)
- New Jersey (NJ)
- New Mexico (NM)
- New York (NY)
- North Carolina (NC)
- North Dakota (ND)
- Nova Scotia (NS)
- Ohio (OH)
- Oklahoma (OK)
- Ontario (ON)
- Oregon (OR)
- Pennsylvania (PA)
- Price Edward Island (PEI)
- Rhode Island (RI)
- Quebec (QC)
- Saskatchewan (SK)
- South Carolina (SC)
- South Dakota (SD)
- Tennessee (TN)
- Texas (TX)
- US Government (GOV)
- Utah (UT)
- Vermont (VT)
- Virginia (VA)
- Washington (WA)
- West Virginia (WV)
- Wisconsin (WT)
- Wyoming (WY)
- Yukon (YT)

2

Introduction to the Sharp Portal

This section includes the following topics:

- "Logging on to the Sharp Portal" on page 19
- "Sharp Portal interface overview" on page 23
- "Viewing camera feeds" on page 24
- "SharpV hardware inventory" on page 26
- "Changing your logon password in the Sharp Portal" on page 27
- "Rebooting a SharpV from the Sharp Portal" on page 28
- "Importing and exporting settings" on page 29
- "Synchronizing the SharpV clock" on page 31

Logging on to the Sharp Portal

To configure SharpV cameras, you must log on to the Sharp Portal.

Before you begin

- You need to know the IP address or name of the SharpV camera you want to connect to:
  - **SharpV:** You can find the SharpV name (for example, SharpV12345) on the label on the back of the unit.
  - **Fallback IP address:** If you cannot connect to a SharpV on your network, you can try connecting using the camera's fallback IP address. For more information, see Connecting to a SharpV camera using the fallback IP address on page 39.

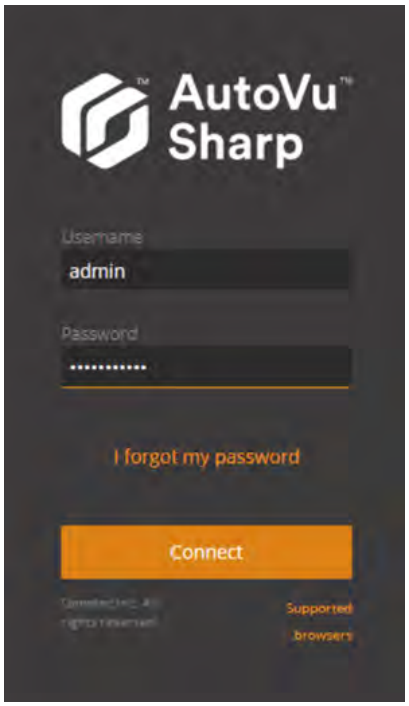
What you should know

- You can access the Sharp Portal using the following browsers:
  - Microsoft Edge version 41 and later
  - Google Chrome version 46 and later
- To ensure that camera feeds are displayed correctly, only open one instance of the Sharp Portal at a time.
- To log onto the portal, the SharpV must be provided with PoE+ power that conforms to IEEE 802.3at standards. If the camera encounters power issues, a warning is displayed and you can see details in the *SharpV Portal - Logs* page. For more information on specifications for the SharpV, see the *AutoVu SharpV Deployment Guide*.

To log on to the Sharp Portal:

1. Open your Web browser, and go to `https://<SharpV name or IP address>`.
2. Enter the **Username** and **Password**.
   - If you have already logged on and changed the default password, enter your **Username** and **Password** and click **Connect**.
   - If this is the first time you are logging on to the Sharp Portal for this unit, enter the default credentials
     - **Username:** admin
     - **Password:** Genetec

3 Click **Connect**.



4 Select the power line frequency that corresponds to the installation location.

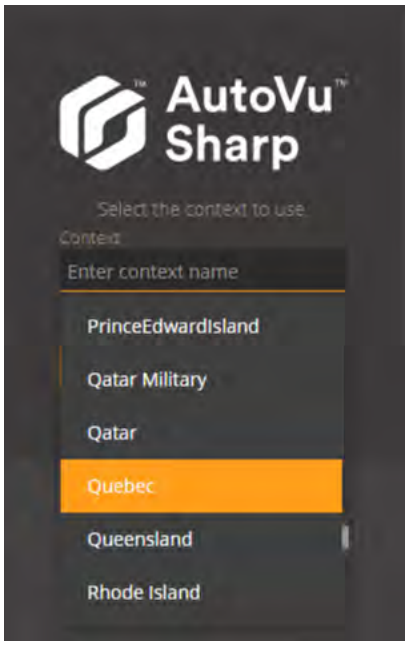


- **60 Hz:** Generally used in North America and South America
- **50 Hz:** Generally used in Africa, Australia, Asia, and Europe

NOTE: For more information on the power line frequency used in your installation location, click here.

5 Click **Enter context name** and select which regional context to use.

NOTE: You can change the regional context when you configure analytics for the SharpV.



6 Click **Next**.

7 Enter and confirm a new password.

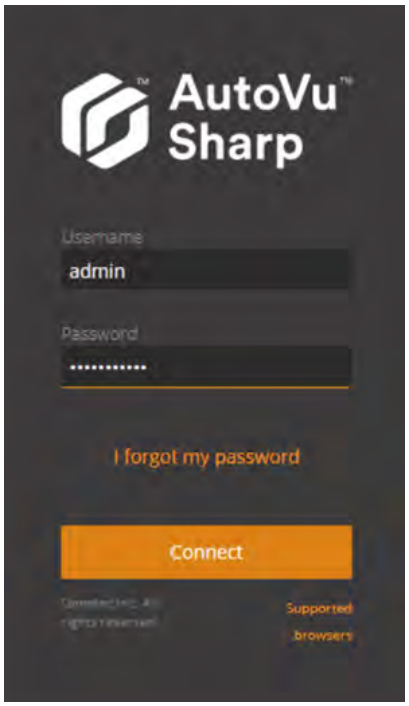


NOTE: You cannot modify the username.

8 Click **Next**.

9 You are redirected to the logon page. Enter the **Username** and new **Password**, then click **Connect**.

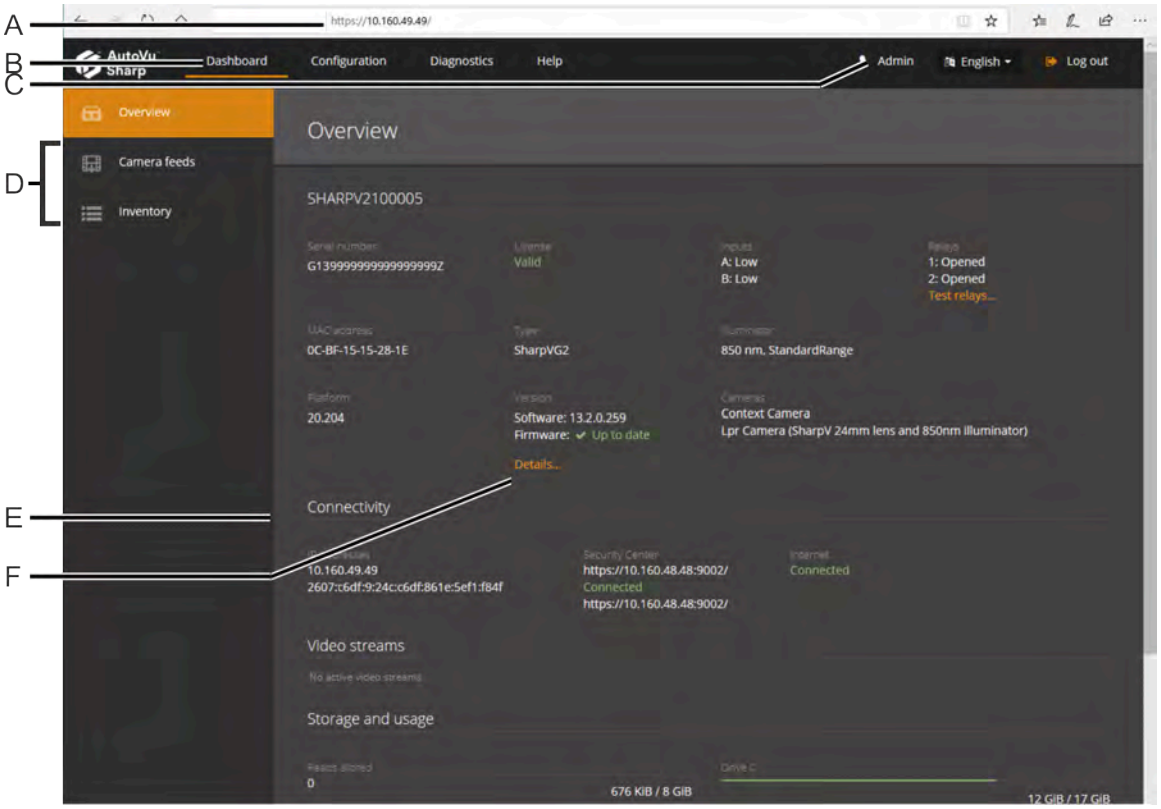
10 Click **Connect**.



After successfully logging on, the Sharp Portal opens to the **Overview** page of the **Dashboard** menu.

Sharp Portal interface overview

To familiarize yourself with the Sharp Portal, you can take a tour of the main areas of the user interface.



A	Sharp Portal address	Type the SharpV name or the IP address. The format is `https://Sharp12345` or `https://192.168.10.100`
B	Menu	Displays the main categories of the Sharp Portal.
C	Current user	Shows the current user and log out command.
D	Pages	Shows the available pages for the selected portal menu.
E	Sections	Shows the available information, status, or settings for the selected portal page.
F	Additional information	Orange text indicates that the text is clickable. This can indicate a hyperlink, can trigger actions, or can display additional information.

Viewing camera feeds

You can use the camera feed to test and align Sharp cameras.

To view the Sharp unit camera feed:

1 Log on to the Sharp Portal.

2 From the **Dashboard** menu, select the *Camera feeds* page.

The *Camera feeds* page displays the feeds from the selected Sharp unit and recent license plate reads from the unit.

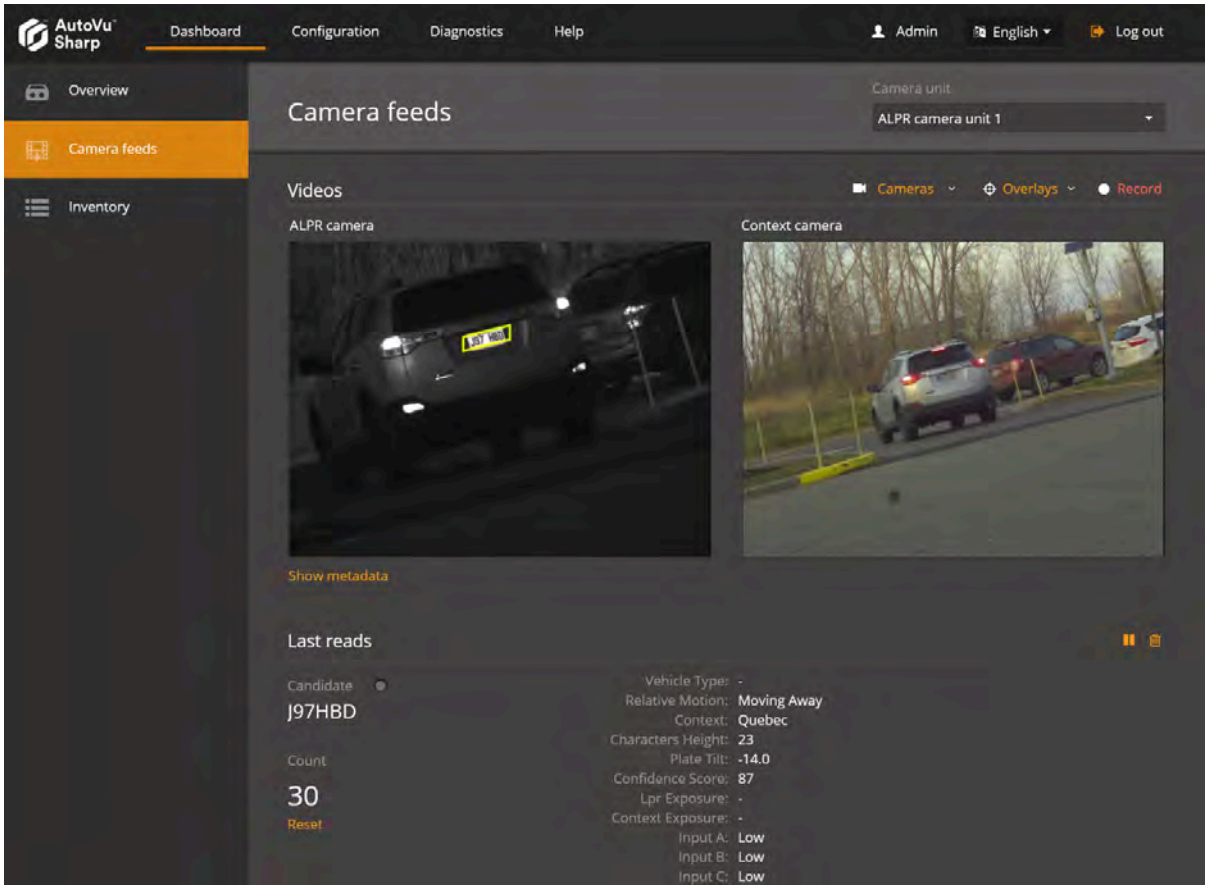
The following options are available in the *Camera feeds* page:

- **Camera unit:** The SharpV camera unit *ALPR camera unit 1* is displayed.
- **Cameras:** Select which of the two SharpV camera feeds to display.

  NOTE: Information on context cameras is not applicable to SharpV ITS cameras.
- **Overlays:**
  - **Crosshairs:** Select this option to display crosshairs in the ALPR or context camera window.
  - **Bounding box:** Select this option to display the yellow bounding box around detected plates in the ALPR camera window.
  - **Region of interest:** A region of interest limits plate detection to a specific part of the field of view. This can be used to ensure that the system focuses on the best region to capture plates or to exclude plates passing in certain regions.
- **Record:** Click the **Record** button to capture a series of context and ALPR images directly from the *Camera feeds* window and save them to your computer as a .zip file for debugging purposes.

NOTE:

- Using the **Record** feature increases CPU usage.
- To use this feature, you cannot use the camera's auto-generated certificate. You must install a self-signed certificate that includes the IP address of the camera.



After you finish

To reduce network bandwidth, after you have finished viewing the camera feeds, select **No camera** from the **Cameras** menu, or navigate to a different page of the Sharp Portal.

SharpV hardware inventory

The **Dashboard** > **Inventory** page in the Sharp Portal displays information on SharpV system hardware.

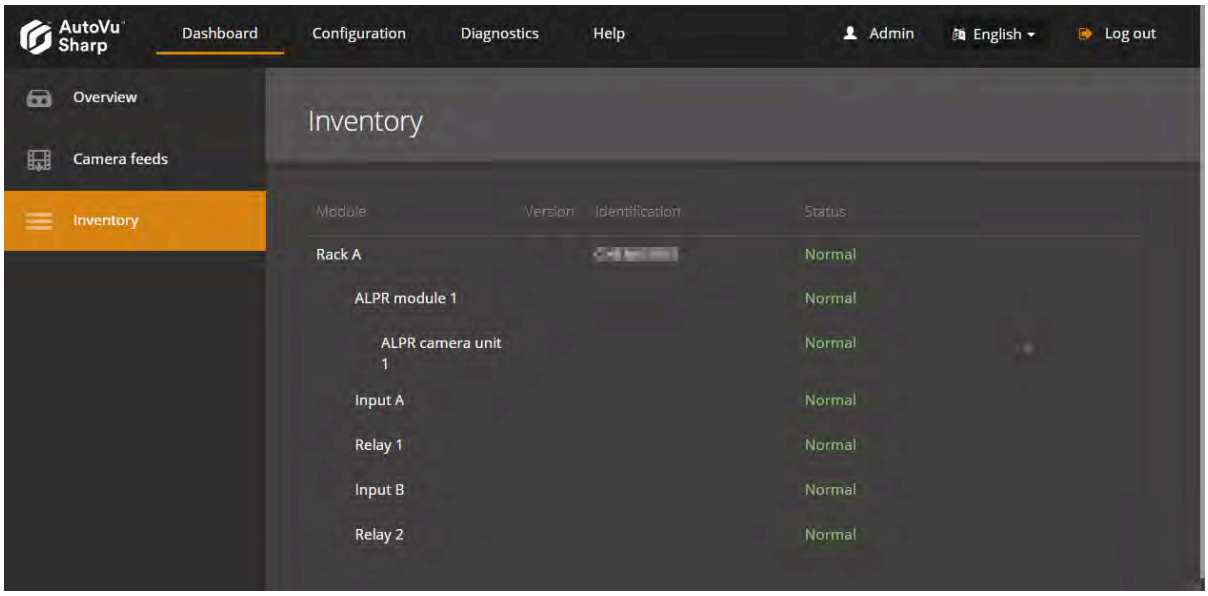
The *Inventory* page is available from the **Dashboard** menu. The page displays the status of the hardware components of the system and allows you to identify camera units by blinking their LEDs.

NOTE: To see the most recent information in the *Inventory* page, you must refresh the web page.

The *Inventory* page provides the following information:

- **Module:** Displays the name of the component.
- **Version:** Displays the component's firmware version.
- **Identification:** Displays a unique identifier of the component, such as its name or serial number.

  NOTE: The serial number is also printed on the component sticker.
- **Status:** Displays the health status of the component.
- **Blink LED:** Blinks the LED on SharpV camera.



Changing your logon password in the Sharp Portal

For security reasons, you might need to change the logon password for the Sharp unit. You can do this in the Sharp Portal.

To change your password:

1. Log on to the Sharp Portal.
2. From the **Configuration** menu, select the **Security** page.
3. In the **Access** section, click **Modify password**.
4. Enter your old password, then enter and confirm your new password.
5. Click **Apply**.

Rebooting a SharpV from the Sharp Portal

Certain configuration procedures require you to reboot the SharpV camera. You can do this from the Sharp Portal.

To reboot the SharpV:

1 Log on to the Sharp Portal.
2 From the **Configuration** menu, select the **Maintenance** page.
3 Click the **Reboot unit** button.

The connection to the Sharp Portal is momentarily lost.

4 Wait approximately 2 minutes to allow the Sharp Portal to restart.

Importing and exporting settings

You can export SharpV settings for use as diagnostic information if required by the AutoVu™ Support team. You can also use the exported settings file to restore the configuration of the SharpV unit or to copy the configuration to another unit.

What you should know

- You can only import settings from the same Sharp model, for example, a SharpV can only import settings from another SharpV.
- You cannot export a configuration from a newer SharpOS version to an older SharpOS version.
- **WARNING:** When you import settings to a SharpV, the camera's current configuration is lost with some exceptions, including:
  - Sharp Portal password
  - Network static configuration
  - Certificates
  - Product improvement program registration
- Battery monitoring settings are unaffected by the import operation.

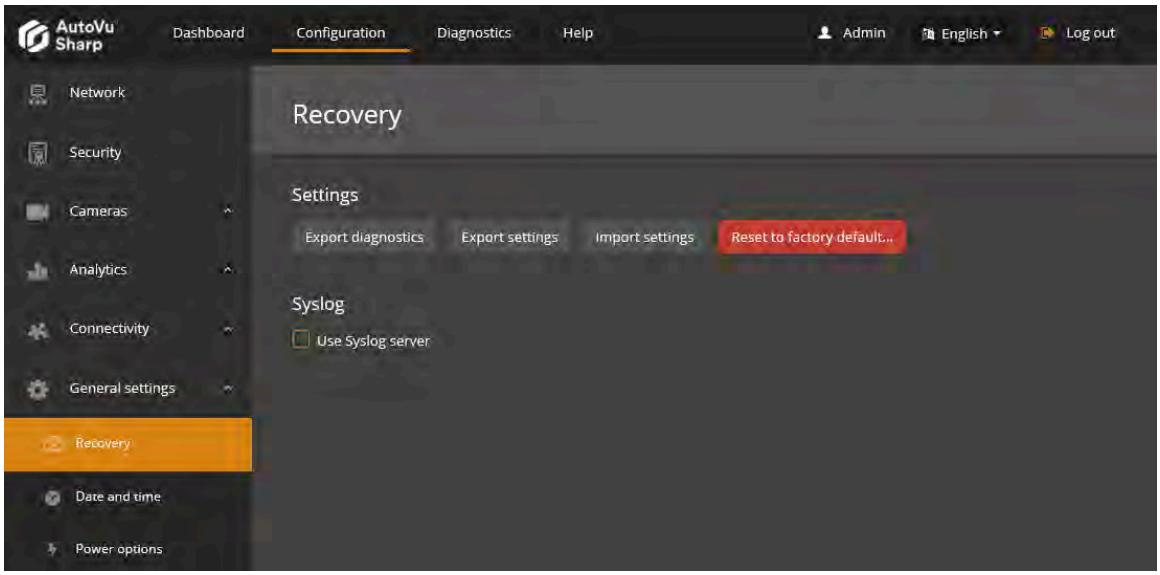
To export SharpV settings:

1 Log on to the Sharp Portal of the SharpV that you want to export settings from.

2 From the **Configuration** menu, click **General settings > Recovery**.

3 From the **Settings** section, select one of the following options:

- **Export diagnostics:** Export a file that includes SharpV diagnostics and SharpV settings.
- **Export settings:** Exports configuration and diagnostic settings as a .zip file. You can use the .zip file for technical support, or you can import the settings to another Sharp unit for quick configuration



The system prepares the files and displays the message "Download succeeded".

4 Save the diagnostics .zip file to a location that is accessible to the browser that is used to view the portal and to the Windows user that will be importing the file. The file is named with the date and time the file was created, for example, `Diagnostics-2020-02-25_12_49_36`.

To import SharpV settings:

1 Log on to the Sharp Portal of the SharpV that you want to import settings to.

2 From the **Configuration** menu, click **General settings > Recovery**.
3 From the **Settings** section, click **Import settings**.
4 Enter the path and filename, or browse to the ZIP file with the SharpV settings you want to import and click **Yes, import**.
5 Follow the on-screen instructions and import the settings to the camera.

Synchronizing the SharpV clock

You can configure the SharpV camera to synchronize time and date settings with the computer you are using to access the Sharp Portal. Alternatively, you can synchronize the date and time with an NTP server or with the Security Center server.

What you should know

By default, the SharpV synchronizes its time and date settings with the active extension defined in the *Configuration* > *Connectivity* > *Extension* page. If you select a different extension, you must manually update the **Date and time** selection in the *Configuration* > *General settings* > *Date and time* page.

To synchronize the SharpV clock:

1 Log on to the Sharp Portal.

2 From the **Configuration** menu, select the **General settings > Date and time** section.

3 Select one of the following options:

- **No synchronization:** The camera does not synchronize with any server (not recommended).

  If you select **Synchronize with client browser now**, the camera performs a one-time synchronization with the date and time of the client browser.

  IMPORTANT: Do not synchronize the SharpV clock with the client browser unless you are connecting to the Sharp Portal from the server (computer hosting the ALPR Manager role). If you synchronize clocks with a computer other than the server, the camera's reads and hits might not have accurate timestamps.
- **NTP server:** The camera synchronizes with an NTP server. Typically, the NTP server is either a foreign computer or a server within your organization that synchronizes itself with an external NTP server. The latter is recommended if synchronization is crucial to your organization. Click **Server** and enter the URL of the machine running the NTP server. Clicking **Test connection** tests the connection between the camera and the NTP server. The camera synchronizes with the NTP server every hour.
- **Active extension (default):** If you select **Active extension (Security Center)**, the camera's date and time are synchronized with the Security Center server that the camera is connected to. The camera synchronizes with the **Security Center** server upon connection, then again every 12 hours.

  NOTE: If you have not yet configured the active extension (see Configuring where the SharpV sends its ALPR data on page 69), you can select **Active extension**, and it will be updated when you configure the extension.

  NOTE: The **Active extension** option displays whichever extension is currently selected for the camera in *Configuration* > *Extensions*, however, selecting this option has no effect if you are using an extension type other than **Security Center** (not valid for FTP, HTTP, and so on).
- **LPM protocol:** When you add a SharpV camera to the ALPR Manager using the LPM Protocol, the camera's date and time are automatically synchronized with the LPM Protocol.

  NOTE: By default, LPM protocol is not an available setting. When a SharpV (SharpOS 12.7 and later) is manually added to the ALPR Manager (Security Center 5.8 and later), the LPM protocol is automatically selected as the unit's extension type and for date and time synchronization.

4 Click **Save**.

3

SharpV software configuration

This section includes the following topics:

- "Security configuration in the Sharp Portal" on page 33
- "Configuring SharpV network settings" on page 39
- "Calibrating the SharpV zoom and focus" on page 40
- "About SharpV exposure adjustment for indoor installations" on page 45
- "About SharpV exposure adjustment for outdoor installations" on page 47
- "Configuring SharpV analytics" on page 52
- "Configuring where the SharpV sends its ALPR data" on page 69
- "Configuring the SharpV FTP extension" on page 84
- "Configuring the SharpV HTTP extension" on page 87
- "Configuring Syslog for SharpV log files" on page 90

Security configuration in the Sharp Portal

SharpV cameras must communicate using TLS encryption (HTTPS) using either the certificate that is auto-generated on the SharpV, a new self-signed certificate, or a signed certificate from your own public key infrastructure (PKI) or from a Certificate Authority such as VeriSign.

Consider the following:

- The first time you log on to the Sharp Portal, a self-signed certificate is generated and HTTPS is activated by default.
- You must install the certificate on all machines that communicate with the SharpV camera. This includes the servers hosting the ALPR Manager, the Archiver, and all machines that connect to the Sharp Portal
- You can install multiple certificates and then select a certificate to activate.

  IMPORTANT: If the current certificate is a signed certificate, deleting the certificate signing request prevents the certificate from being reinstalled.
- To capture context and ALPR images directly from the SharpV using the **Record** button on the *Camera feeds* window of the Sharp Portal, you cannot use the camera's auto-generated certificate. You must install a signed or self-signed certificate that includes the IP address of the camera as the *common name*.
- If the IP address of the SharpV changes, you must regenerate and reinstall the signed or self-signed certificate.

Installing the SharpV auto-generated certificate

If the SharpV unit uses its auto-generated certificate for HTTPS communication, you must install the certificate on all machines that communicate with the Sharp unit.

Before you begin

Read about how the Sharp Portal must be encrypted.

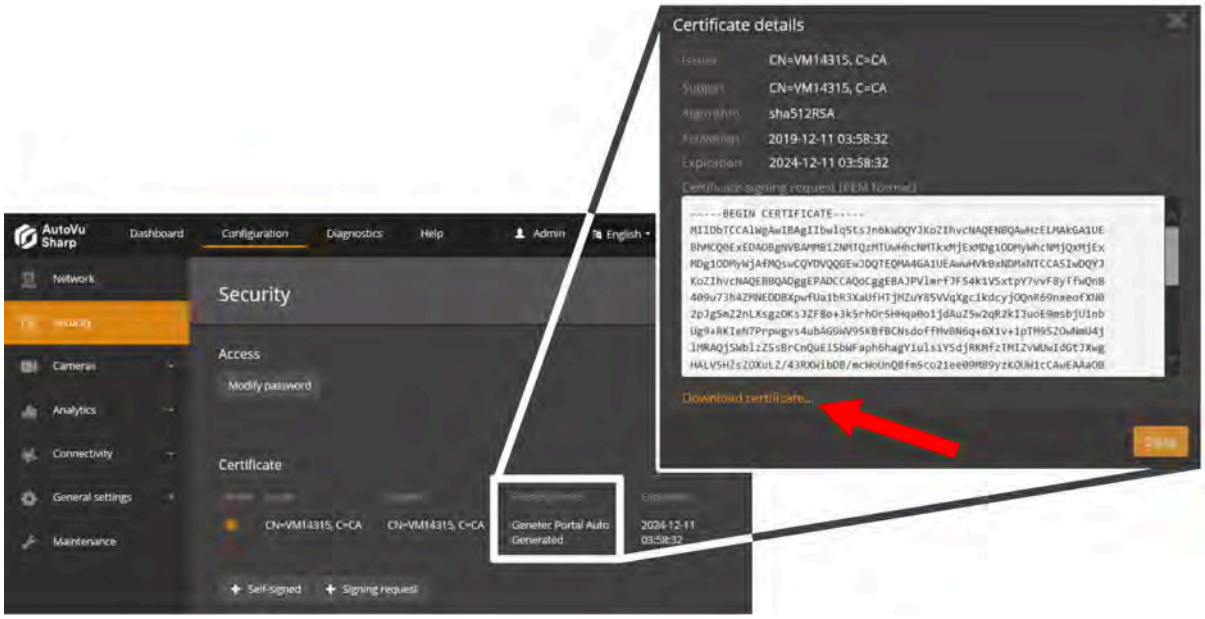
What you should know

- IPv6 static addresses are not supported.

To install the auto-generated certificate on a workstation:

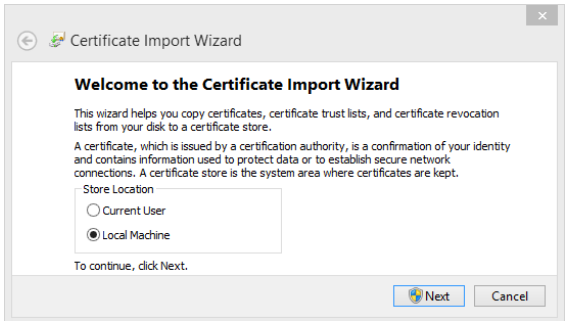
1 On the machine where you want to register the certificate, log on as an Administrator.
2 Log on to the Sharp Portal.
3 From the **Configuration** menu, select the *Security* page.
4 Click the certificate with the **Friendly name**: *Genetec Portal Auto Generated*.
The *Certificate details* are displayed.

5 Click **Download certificate** and save the certificate file as prompted by your browser.

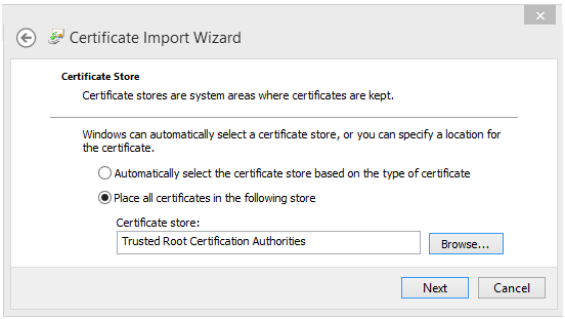


6 Double-click the *certificate.cer* file and click **Install Certificate**.

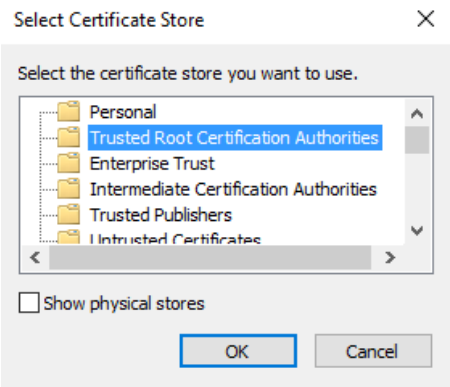
7 The *Certificate Import Wizard* prompts you to select a store location. Select **Local Machine** and click **Next**.



8 The wizard prompts you to select the certificate store you want to use. Select **Place all certificates in the following store** and click **Browse**.



9 From the **Select Certificate Store** window, select **Trusted root certification Authorities** and click **OK**.



10 Click **Next** to continue, and click **Finish** to close the wizard.
The system displays the message: *The import was successful*.

11 Close all web browsers and open the Windows Task Manager to ensure that no browser processes are running in the background.

12 Log on to the Sharp Portal. You are automatically logged on in HTTPS mode.

A lock icon ( ) in the browser's address bar indicates that you are now logged on to the SharpV with a secure connection.

Installing a self-signed certificate

If the SharpV unit uses a self-signed certificate for HTTPS communication, you must install the certificate on all machines that communicate with the Sharp unit.

Before you begin

Read about how the Sharp Portal must be encrypted.

What you should know

IPv6 static addresses are not supported.

To encrypt connection to the Sharp Portal using a self-signed certificate:

1 On the machine where you want to register the certificate, log on as an Administrator.
2 Log on to the Sharp Portal.
3 From the **Configuration** menu, select the *Security* page.
4 From the **Certificate** section, select **+ Self-signed**.
5 Enter the required information for the certificate and click **OK**.

- The **Country** field requires a two-letter country code.
- If you are also using the certificate to connect to the Archiver, the **Sharp's common name** (Sharp's IP address if connecting to the Archiver) defined in the certificate must be the Sharp unit's IP address, not the Sharp name.

The message *Operation succeeded* is displayed and the signing request is added to the certificate list.

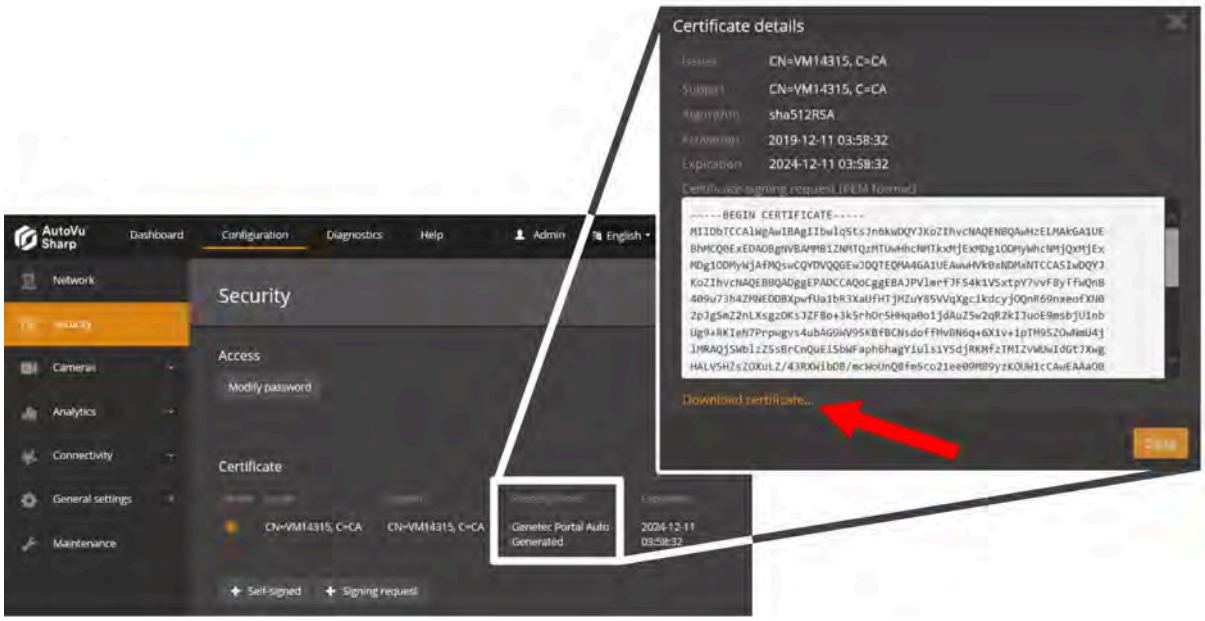
6 Click the **Active** button for the certificate.
7 Click **Save and reboot** and click **OK** to confirm the reboot.

NOTE: Depending on the browser you are using, you might receive warnings because the certificate is not signed by a trusted certificate authority.

To install the certificate on a workstation:

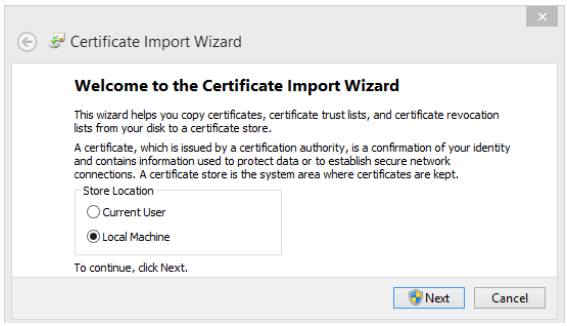
1 Click on the certificate to display the *Certificate details*.

2 Click **Download certificate** and save the certificate file as prompted by your browser.

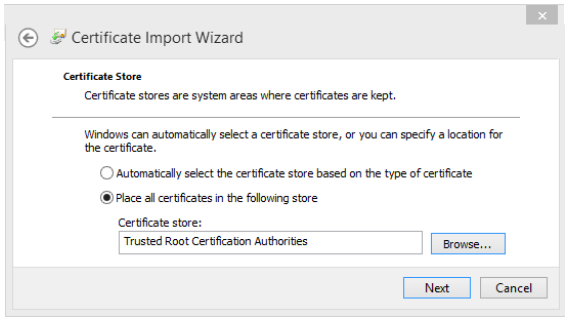


3 Double-click the *certificate.cer* file and click **Install Certificate**.

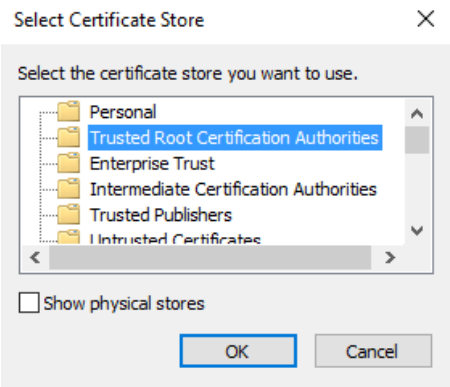
4 The *Certificate Import Wizard* prompts you to select a store location. Select **Local Machine** and click **Next**.



5 The wizard prompts you to select the certificate store you want to use. Select **Place all certificates in the following store** and click **Browse**.



6 From the **Select Certificate Store** window, select **Trusted root certification Authorities** and click **OK**.



7 Click **Next** to continue, and click **Finish** to close the wizard.
The system displays the message: *The import was successful*.
8 Close all web browsers and open the Windows Task Manager to ensure that no browser processes are running in the background.
9 Log on to the Sharp Portal. You are automatically logged on in HTTPS mode.
A lock icon ( ) in the browser's address bar indicates that you are now logged on to the SharpV with a secure connection.

Installing a signed certificate

If the SharpV unit uses a signed certificate from your own public key infrastructure (PKI) or from a Certificate Authority such as VeriSign, you must install the certificate on all machines that communicate with the SharpV unit.

Before you begin

Read about how the Sharp Portal must be encrypted.

What you should know

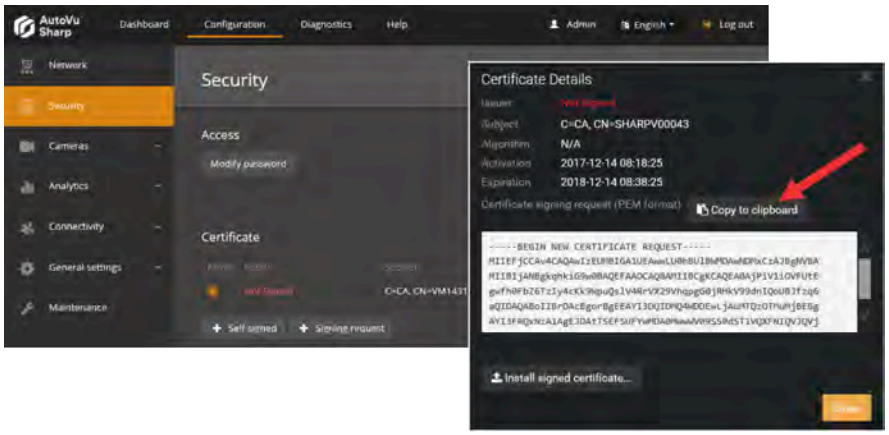
IPv6 static addresses are not supported.

To encrypt the connection to the Sharp Portal using a signed certificate:

1 On the machine where you want to register the certificate, log on as an Administrator.
2 Log on to the Sharp Portal.
3 From the **Configuration** menu, select the *Security* page.
4 Click **+ Signing request**.
5 Enter the required information for the certificate signing request and click **OK**.
NOTE:
- The **Country** field requires a two-letter country code.
- If you are also using the certificate to connect to the Archiver, the **Sharp's common name** (Sharp's IP address if connecting to the Archiver) defined in the certificate must be the Sharp unit's IP address, not the Sharp name.

The message *Operation succeeded* is displayed and the signing request is added to the certificate list with *not signed* displayed for the **Issuer**.
6 Click on the certificate to display the *Certificate details*.

7 Click **Copy to clipboard**.



8 Send the certificate signing request to a certificate authority.

IMPORTANT: Do not delete the signing request if it has been used to request a certificate.

You will receive an SSL certificate signed by the certificate authority.

9 In the *Certificate Details* window, click **Install signed certificate** then browse to the certificate location and click **Open**.

10 Click **Save**.

The system displays the message: *Installed signed certificate... successful*.

11 Refresh the browser (F5).

The certificate is displayed in the **Certificate** list.

12 Click the **Active** button for the certificate.

13 Click **Save and reboot** and click **OK** to confirm the reboot.

When the system comes back online, notice that the URL displays that you are in HTTPS mode. A lock icon (🔒) in the browser's address bar indicates that you are now logged on to the SharpV with a secure connection.

Configuring SharpV network settings

You can configure the SharpV to use Dynamic Host Configuration Protocol (DHCP) or a static IP address.

What you should know

DHCP is used by default if no option is selected on the Network page of the Sharp Portal.

To configure the SharpV's network settings:

1 Log on to the Sharp Portal.
2 From the **Configuration** menu, select the **Network** page.
3 Select one of the following:
   - **Use DHCP:** This is the default mode for SharpV cameras. Select DHCP if you are connecting the Sharp to a DHCP server, which assigns the required IP address. When you are on a DHCP server with DNS capability, you can connect to the SharpV using the SharpV name (for example, SharpV12345) rather than the IP address (for example, 192.168.10.100).
   - **Use static IP address:** Select this option to use a static address for the SharpV.

     NOTE: IPv6 static addresses are not supported.

     IMPORTANT: If you are streaming video to the Security Center Archiver role, ensure that the SharpV IP address does not change.
4 If you selected **Use static IP address** configure the following:
   - **IP adress:** Type the new IP address you want to assign to the SharpV. 10.0.0.1 is the default.
   - **Subnet mask:** Type the new **Subnet mask** if applicable. 255.255.0.0 is the default.
   - **Gateway:** Type the new **Gateway** if applicable. 10.0.0.0 is the default.
   - **DNS:** Type the new **DNS** if applicable. 10.0.0.0 is the default.
5 Click **Save**.

Connecting to a SharpV camera using the fallback IP address

If you cannot connect to a SharpV camera on your network, you can try connecting to the camera by using the camera's fallback IP address.

What you should know

- You may need to connect to the camera using the fallback IP address if, for example, the DHCP server is not available.
- If the camera is powered up and is not connected to the network for a few minutes, the fallback IP address will be available.
- The fallback IP address is only available if the camera is in DHCP mode.

To connect to a camera using the fallback IP address:

1 If there is more than one Sharp camera on the network, isolate the camera by connecting it directly to a computer with the use of a PoE+ injector.
2 Connect to the camera using the fallback IP address (192.168.10.100).
3 Reconfigure the camera as required and reconnect to the network.

Calibrating the SharpV zoom and focus

To ensure that the SharpV reads license plates clearly and that the plate characters appear in an acceptable size, you must adjust the zoom and focus of your SharpV camera.

Before you begin

- Read about optimal reading distance for plate reads for the SharpV.
- Install a stationary license plate to adjust the SharpV camera's zoom and focus. If this necessitates closing a lane of traffic, observe all local regulations. Alternatively, you can adjust the zoom and focus by pointing the camera to the side of the street and placing the stationary plate at the expected distance for plate reads. When the camera is pointed back to the traffic lane, you must evaluate plate read images to adjust the focus.

What you should know

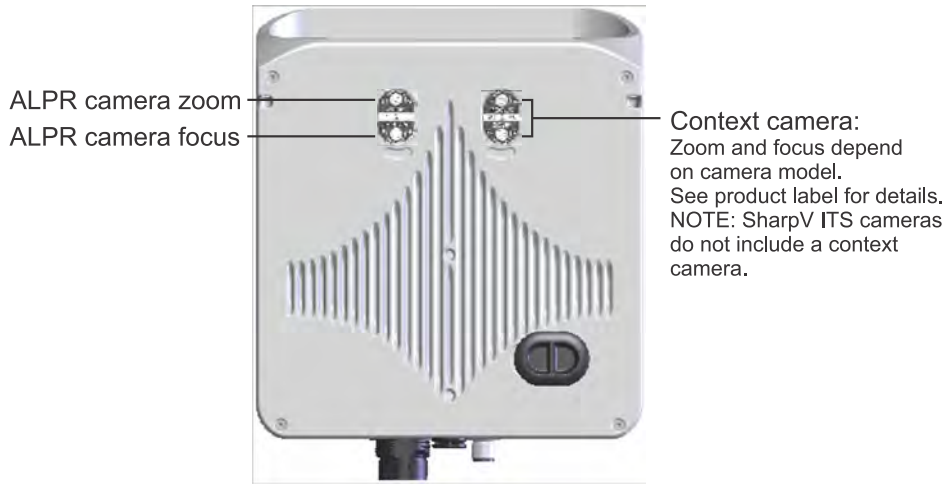
- The system captures plate reads more accurately if characters are between 25 and 60 pixels high in the images acquired by the ALPR camera. The optimal size of license plate characters is 30 pixels high.

  NOTE: If the SharpV is configured for dual-lane plate reading, the characters must be from 10 to 40 pixels high. For more information, see Configuring the SharpV to monitor dual lanes on page 56.
- The position of the zoom and focus adjustment screws on the context camera might be reversed depending on whether you are installing the SharpV SR (Standard-Range) or LR (Long-Range). Refer to the product sticker on the camera for specific adjustment screw information.

  NOTE: Information on context cameras is not applicable to SharpV ITS cameras.

Zoom and focus adjustment screws

The SharpV includes zoom and focus adjustment screws for the ALPR camera and the context camera. You can access the adjustment screws by removing the rubber plugs on the bottom of the camera. A hex key is provided for making the adjustments.



The following information appears on the zoom / focus adjustment label:

Label	Description
Zoom: T/W	Telephoto/wide

Label	Description
Focus: F/N	Far/near
LPR / CTX	ALPR camera/context camera
SR / LR	Standard range/long range

To adjust the zoom and focus of the ALPR camera:

1 Open the Sharp Portal `https://<Sharp name or IP address>`.

By default, the SharpV is configured to use DHCP. If no DHCP server is available on the network, you can use the IP address `192.168.10.100` to access the SharpV.

2 If this is the first time you are logging on the portal, you are prompted to change the password for security reasons. For more information, see Logging on to the Sharp Portal on page 19.

NOTE: If you forget your password, you can reset it from the logon page.

3 From the **Configuration** menu, select **Cameras > Zoom and focus**.

4 From the **Select your camera** drop-down list, select the **ALPR Camera**.

The live feed of the ALPR camera is displayed.

5 Adjust the exposure as required for the best plate image.

NOTE: The SharpV camera only uses the exposure setting that are visible in the *Zoom and Focus* page during the adjustment process. After the camera has been adjusted, this setting is ignored and the camera returns to the configured exposition settings.

6 Adjust the camera's zoom level.

a) Select **Show ruler**. A ruler is displayed on the ALPR camera image. Drag the ruler so that it appears next to the license plate.

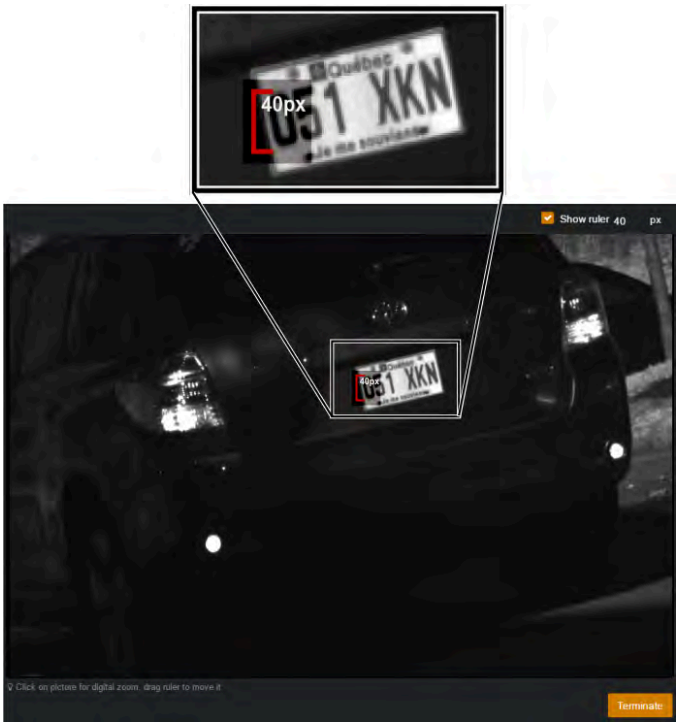
b) Enter a new pixel (px) value to change the size of the ruler on the page to match the height of the license plate characters.

c) Adjust the zoom and alignment so that the image has the largest field of view and the longest plate transit time, while keeping the height of the plate characters in the image between 25 - 60 pixels. The optimal performance is 30 pixels.

NOTE:

- If the SharpV is configured for dual-lane plate reading, the characters must be from 10 to 40 pixels high. For more information, see Configuring the SharpV to monitor dual lanes on page 56.
- When you change the camera's zoom level, the focus is lost. You need to perform a basic focus adjustment each time you change the zoom level so that you have a relatively clear view of the license plate.

TIP: Click on the license plate to use digital zoom. There are three zoom levels: 1:1, 2:1, and 4:1. A preview of the zoomed area is displayed in the top right corner of the image.



7 Adjust the camera focus.

a) Focus the camera on a stationary plate located at the mid-point of the vehicle's expected trajectory.

b) Click the image to digitally zoom in on the plate.

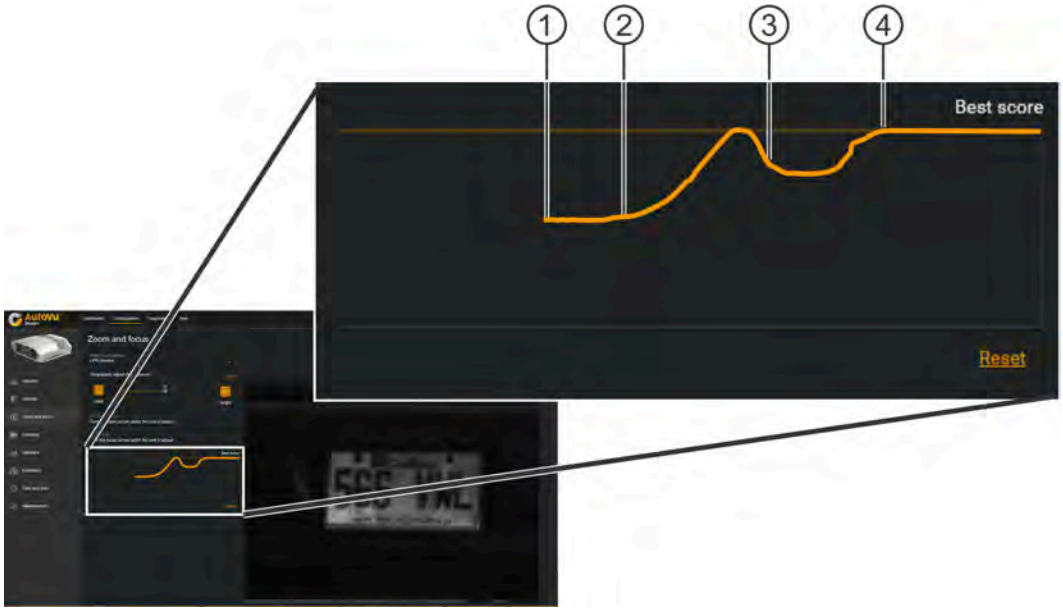
NOTE:

- Use the **Best score** graph to visually monitor when the optimal setting is reached for the focus while you are adjusting the screws on the bottom of the SharpV, two orange lines are displayed.

The 'bold' orange line indicates the current focus value. The 'dim' orange line indicates the best focus that has been achieved since the graph was last reset.

- For best results, make sure that there is no movement in the camera's field of view when using the **Best score** graph.

Example:



c) Click **Reset** to start the focus adjustment (1).
d) Start turning the focus adjustment screw for the ALPR camera (2). For this example, the screw is being turned clockwise.

   Both the bold and dim orange lines move higher on the graph and are intersecting.
e) At a certain point, the bold line starts to move lower on the graph and the lines are no longer intersecting (3). At this point you have exceeded the best focus.

   It is important to note that the dim orange line now displays the best focus point.
f) Start turning the adjustment screw in the opposite direction (for this example, counter-clockwise).
g) When the bold line reaches the level of the dim line (4), the focus adjustment is completed. Click **Done**.

To adjust the zoom and focus of the context camera:

Adjust the context camera using the same method described for the ALPR camera, with the following exceptions:

- You can focus the camera's context image based on the image's sharpness, but you can also use the graph tool to help you fine-tune the focus.
- The pixel height of the license plate characters is not important when adjusting the context camera. You must only ensure that the vehicle is clear and recognizable in the image.
- If you need to adjust the zoom and focus of the context camera in low light conditions, enable the IR illuminator. To enable the IR illuminator, click **Configuration > Cameras > Zoom and focus > Enable flash**. The IR illuminator enables you to see the image more clearly; however, the video feed from the context camera is converted to a black and white image.
- If you adjust the zoom and focus of the context camera in very bright conditions (sunlight), you might need to use very low level on the exposure level slider. At very low levels, the camera iris aperture is reduced. If the focus is adjusted in this position, the result might not be optimal because focus quality can degrade in lower light conditions. The web portal displays a warning to indicate when such conditions exist. To achieve the best possible focus quality, you should not adjust the focus in very bright sunlight.

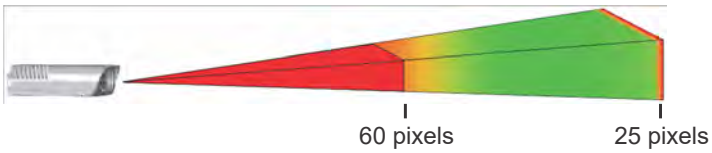
NOTE: Information on context cameras is not applicable to SharpV ITS cameras.

8 Click **Done**.

Plate read distances for SharpV lenses

The maximum plate reading distance and field of view that SharpV cameras can support depend on the lens type and zoom setting of the camera.

For optimal performance, respect the following installation distances for standard and long-range SharpV cameras.



Lens type	Zoom level	60 pixels (maximum)	25 pixels (minimum)
Standard lens	Reading distance	2.75 m (9 ft)	18.25 m (60 ft)
Long-range lens	Reading distance	18.25 m (60 ft)	35 m (115 ft)

About SharpV exposure adjustment for indoor installations

By default, the SharpV is configured to automatically adjust exposure settings for changing light conditions when capturing license plate reads. Alternatively, if you are installing a SharpV camera indoors, for example, in an underground parking lot, you can define fixed values for the camera's iris, shutter time, and gain settings. Doing this can result in more consistent exposure for ALPR and context images.

IMPORTANT: Modifying the SharpV exposure settings can greatly impact ALPR performance. Vanity plates, or plates that are damaged or dirty can have different reflective properties. Improving the exposure using a stationary test plate can result in reduced ALPR performance on every-day traffic which includes plates with a wide range of reflective properties. You must test the system after modifying these settings.

Setting custom SharpV ALPR camera exposure levels for indoor installations

If the default exposure settings do not produce acceptable results, you can adjust the iris, shutter time, and gain settings of the SharpV ALPR camera to work best with your indoor installation.

Before you begin

- Ensure that the lighting conditions match what is expected during normal camera operation.
- Adjust the zoom and focus of the camera.

What you should know

- In a correctly-exposed license plate image, the characters and the plate state are dark and well-defined, and the background is white or very bright.



- In the ALPR image, it is normal that the surroundings of the plate are under-exposed while the plate itself is correctly-exposed. In the ALPR image, make sure that the plate is correctly exposed and ignore the quality of the surroundings.

To adjust the ALPR camera exposure settings:

1. Log on to the Sharp Portal.
2. From the **Configuration** menu, select **Cameras > Zoom and focus**.
3. From the **Select your camera** drop-down list, select the **ALPR Camera**.
   The live feed of the ALPR camera is displayed.
4. Select the **Show ruler** check box.
5. Place a stationary license plate in front of the camera so that the character height is 25 pixels.
   IMPORTANT: Do not modify the focus. The license plate might appear out of focus, but you are only adjusting the exposure in these steps.
6. From the **Configuration** menu, select **Cameras > Exposure**.
7. From the **Select your camera** drop-down list, select the **ALPR camera**.
   The live feed from the ALPR camera is displayed.
8. From the **Exposure** drop-down list, select **Fixed (indoor)**.
   Gain, **Exposure time** and **Iris** settings are displayed.
9. Clear the **Iris** check box.

10 Open the iris to 100% by moving the slider to the right.
11 Set the **Gain** level to the minimum default value (0).
12 Adjust the **Exposure time** to be as high as possible without resulting in an over-exposed image.
13 If you reach the maximum **Exposure time** level and the plate image is still too dark, increase the **Gain** level and adjust the **Exposure time** until you are satisfied with the plate image.

TIP: Increasing the gain level introduces noise in the image. Keep the gain as low as possible.

14 When you are satisfied with the appearance of the plate images in the video feed window, click **Save**.
The system displays the message: *Configuration saved successfully*.

Setting custom SharpV context camera exposure levels for indoor installations

If the default exposure settings do not produce acceptable results, you can adjust the shutter time, and gain settings of the SharpV context camera to work best with your indoor installation.

Before you begin

- Ensure that the lighting conditions match what is expected during normal camera operation.
- Adjust the zoom and focus of the camera.

What you should know

- Adjusting the exposure settings of the context camera has no impact on ALPR performance. Performing this procedure simply improves the quality of the context image.
- If you configure a long exposure time, you might notice motion blur in the context image. This is not apparent when using a fixed license plate for calibration, and might require adjustment after testing the camera in normal operation.
- Information on context images is not applicable to SharpV ITS cameras.

To adjust the context camera exposure settings:

1 Log on to the Sharp Portal.
2 From the **Configuration** menu, select **Cameras > Exposure**.
3 From the **Select your camera** drop-down list, select the **Context camera**.
The live feed from the context camera is displayed.
4 From the **Lighting type** drop-down list, select the setting that best describes the installation's normal lighting conditions.
5 From the **Exposure** drop-down list, select **Fixed (indoor)**.
Gain and **Exposure time** settings are displayed.
6 Set the **Gain** level to the minimum default value (0).
7 Adjust the **Exposure time** until you are satisfied with the image and license plates are clearly visible.
8 If you reach the maximum **Exposure time** level and the plate image is still too dark, increase the **Gain** level.

NOTE: If, due to poor lighting, the plate image is still not visible even after increasing the gain level, or if increasing the gain level adds too much noise to the image, you can select **Enable illuminator** to turn on the camera's IR illuminator. The IR illuminator makes the plate more visible, but removes color from the context image.

9 When you are satisfied with the appearance of the plate images in the video feed window, click **Save**.
The system displays the message *Configuration saved successfully*.

About SharpV exposure adjustment for outdoor installations

For SharpV cameras that are installed outdoors, we recommend that you keep the default exposure settings. If you notice that license plates are often under-exposed (too dark) or over-exposed (too bright), you can adjust the exposure settings. However, there are many factors to consider in order to account for changing lighting conditions.

IMPORTANT: Modifying the SharpV exposure settings can greatly impact ALPR performance. Vanity plates, or plates that are damaged or dirty can have different reflective properties. Improving the exposure using a stationary test plate can result in reduced ALPR performance on every-day traffic which includes plates with a wide range of reflective properties. You must test the system after modifying these settings.

Setting custom SharpV ALPR camera exposure levels for outdoor installations

If the default exposure settings do not produce acceptable results, you can adjust the iris, shutter time, and gain settings of the SharpV ALPR camera to work best with your outdoor installation.

Before you begin

- Ensure that the lighting conditions match what is expected during normal camera operation.
- Adjust the zoom and focus of the camera.

What you should know

- In a correctly-exposed license plate image, the characters and the plate state are dark and well-defined, and the background is white or very bright.



- In the ALPR image, it is normal that the surroundings of the plate are under-exposed while the plate itself is correctly-exposed. Make sure that the plate is correctly exposed and ignore the quality of the surroundings.
- The ranges for the **Exposure time** and **Gain** settings must be large enough to allow good quality images in all lighting conditions, but you should reduce the range as much as possible. If the range is too large, it increases the risk of over-exposure or under-exposure. It is normal that the SharpV constantly varies the exposure of the ALPR camera in order to get a correct exposure of a plate.
- Modifying settings to improve read performance at night can have a negative impact on read performance during the day, and vice versa. Therefore, you must test the settings both at night and during the day (under sun illumination).
- If the SharpV is expected to read both embossed and flat license plates, perform the day instructions with the flat plate and the night instructions with the embossed plate.

Adjust the ALPR camera under sun illumination:

1. Place a stationary license plate as close to the camera as possible while still being within range for the camera to capture plate reads.
2. Log on to the Sharp Portal.
3. From the **Configuration** menu, click **Cameras > Exposure**.
4. From the **Select your camera** menu, select the **ALPR camera**.

   The live feed from the ALPR camera is displayed. Do not modify the focus. The license plate might appear out of focus, but you are only adjusting the exposure in these steps.

5 From the **Exposure** drop-down list, select **Range (outdoor)**.
Gain, **Exposure time** and **Iris** settings are displayed.
6 Set the **Gain** and **Exposure time** minimum and maximum levels to their minimum values.
7 Clear the **Iris** check box.
8 Move the **Iris** slider towards the right as much as possible without over-exposing image.
9 When you are satisfied with the appearance of the plate images in the video feed window, click **Save**.
The system displays the message *Configuration saved successfully*.

Adjust the ALPR camera at night:

1 Place a stationary license plate as far from the camera as possible while still being within range for the camera to capture plate reads.
2 Log on to the Sharp Portal.
3 From the **Configuration** menu, select **Cameras > Exposure**.
4 From the **Select your camera** drop-down list, select the **ALPR camera**.
The live feed from the ALPR camera is displayed. Do not modify the focus. The license plate might appear out of focus, but you are only adjusting the exposure in these steps.
5 From the **Exposure** drop-down list, select **Range (outdoor)**.
Gain, **Exposure time** and **Iris** settings are displayed.
6 Increase the **Exposure Time** maximum as much as possible without getting an over-exposed image.
7 If the **Exposure Time** is set at the maximum value and the image is still dark, increase the **Gain** maximum until you are satisfied with the image.
8 When you are satisfied with the appearance of the plate images in the video feed window, click **Save**.
The system displays the message *Configuration saved successfully*.

Setting SharpV ALPR camera exposure levels for reflective and non-reflective plates

If the license plates in your region include both reflective and non-reflective plates, you can configure the SharpV camera's exposure settings to look for both plate types.

Before you begin

- Adjust the zoom and focus of the camera.
- To calibrate the exposure, reflective and non-reflective plates must be visible in the video feed. For best results, place stationary reflective and non-reflective license plates as far from the camera as possible while still being within range for the camera to capture plate reads. If this is not possible due to traffic, you can still evaluate the exposure by monitoring moving vehicles, however, you must familiarize yourself with local license plate types so that you can visually identify reflective and non-reflective plates in the image.

What you should know

- When you configure a SharpV for reflective and non-reflective plates, each frame of the ALPR camera video feed alternates between the optimal exposure settings for the two plate types. As a result, a license plate only appears with the correct exposure in half of the image frames. This means that when the system selects the best image to associate with a plate read, fewer possible candidates are available.
- The following procedure includes steps that must be performed in darkness followed by steps that must be performed in sunlight. You can calibrate the exposure remotely using the Sharp Portal, assuming the required license plates are visible in the video feed.

- In a correctly-exposed license plate image, the characters and the plate state are dark and well-defined, and the background is white or very bright.



IMPORTANT: Modifying the exposure settings can greatly impact ALPR performance. You must test the system after modifying these settings.

- In the ALPR image, it is normal that the surroundings of the plate are under-exposed while the plate itself is correctly-exposed. Make sure that the plate is correctly exposed and ignore the quality of the surroundings.

Adjust the ALPR camera in darkness:

1. Log on to the Sharp Portal.
2. From the **Configuration** menu, click **Cameras > Exposure**.
3. From the **Select your camera** menu, select the **ALPR camera**.
   The live feed from the ALPR camera is displayed.
4. From the **Exposure** menu, select **Reflective and non-reflective**.
   The camera automatically detects the lighting conditions and selects the **Night** adjustment.
5. Move the **Non-reflective plates** slider to the right as much as possible without over-exposing the image.
   NOTE: For this adjustment, ignore the exposure of any reflective plates in the video feed.
6. Move the **Reflective plates** slider towards the right as much as possible without over-exposing the image.
   NOTE: For this adjustment, ignore the exposure of any non-reflective plates in the video feed.
7. Clear the **Iris** check box and move the slider to the right as much as possible without over-exposing image.
8. When you are satisfied with the appearance of the plate images in the video feed window, click **Save**.
   The system displays the message *Configuration saved successfully*.

Adjust the ALPR camera under sunlight:

1. Log on to the Sharp Portal.
2. From the **Configuration** menu, click **Cameras > Exposure**.
3. From the **Select your camera** menu, select the **ALPR camera**.
   - The live feed from the ALPR camera is displayed.
   - **Reflective and non-reflective** is already selected as the **Exposure** type.
   - The camera automatically detects the lighting conditions and selects the **Sunlight** adjustment.
4. Move the **Non-reflective plates** slider to the right as much as possible without over-exposing the image.
   NOTE: For this adjustment, ignore the exposure of any reflective plates in the video feed.
5. Move the **Reflective plates** slider to the right as much as possible without over-exposing the image.
   NOTE: For this adjustment, ignore the exposure of any non-reflective plates in the video feed.
6. Do not adjust the **Iris** settings. The adjustment you made for the night configuration also applies for the sunlight configuration.
7. When you are satisfied with the appearance of the plate images in the video feed window, click **Save**.
   The system displays the message *Configuration saved successfully*.

Troubleshooting outdoor exposure issues for the SharpV ALPR camera

You can resolve exposure adjustment issues that result in under-exposed or over-exposed license plate images in fixed SharpV installations.

If ALPR images (or some specific plate models) are always too dark at night:

1. Make the first adjustments under sun illumination.
2. Set the **Gain** and **Exposure time** minimum and maximum levels to the minimum value.
3. Increase the **Iris** value as much as possible without over-exposing the plate.
4. Perform the remaining exposure adjustment at night.
5. Increase the maximum **Exposure time** value until you are satisfied with the plate images.
6. If you reach the maximum **Exposure time** level and the ALPR images are still too dark, increase the maximum **Gain** value.

If ALPR images are often too dark at night:

In this case, the exposure setting range might be too large, causing exposure to be too low. To reduce the range, start by increasing the minimum values. Because higher minimum values might lead to over-exposure for daytime reads, perform the adjustment during the day.

In this case, the exposure setting range might be too large, causing exposure to be too low. You can reduce the range by increasing the minimum values, but you should do this carefully because increasing the minimum values can cause over-exposure during the day. Therefore, this adjustment should be done during the day.

1. Make the adjustment under sun illumination.
2. Increase the minimum **Exposure time** value as much as possible without compromising image quality.
3. If the minimum **Exposure time** value reaches its maximum value, then you can increase the minimum **Gain** value. Test to make sure image quality is still satisfactory.

If ALPR images (or some specific plate models) are always too dark even under sunlight:

1. Make the adjustment under sun illumination.
2. Increase the **Iris** value as much as possible without over-exposing the plate.
3. If the **Iris** reaches its maximum value and the plate is still under-exposed, increase the maximum **Exposure time** level as much as possible without over-exposing the plate.
4. If the maximum **Exposure time** reaches its maximum value and the plate is still under-exposed, increase the maximum **Gain** value one step at the time until you are satisfied with the images.

If ALPR images (or some specific plate models) are always too bright under sunlight:

1. Make the adjustment under sun illumination.
2. Decrease the minimum **Gain** value until you are satisfied with the plate images.
3. If you reach the minimum **Gain** level and the ALPR images are still too bright, decrease the minimum **Exposure time** value.
4. If you reach the minimum **Exposure time** level and the ALPR images are still too bright, decrease the iris aperture until you are satisfied with the plate images.

If ALPR images are often too bright under sunlight:

In this case, the exposure setting range might be too large, causing exposure to be too high. You can reduce the range by decreasing the maximum values, but you should do this carefully because decreasing the maximum values can cause under-exposure at night. Therefore, this adjustment should be done during the night.

1. Make the adjustment at night.

2 Decrease the maximum **Gain** value as much as possible without compromising image quality.
3 If the maximum **Gain** value reaches its minimum value, then you can decrease the maximum **Exposure time** value. Test to make sure image quality is still satisfactory.
4 If you reach the minimum **Exposure time** level and you are still not satisfied with the image quality, perform the complete day and night exposure adjustment again.

Troubleshooting outdoor exposure issues for the SharpV context camera

You can resolve exposure adjustment issues that result in under-exposed or over-exposed license context images in fixed SharpV installations.

If context images are blurry on fast-moving vehicles:

1 Make the adjustment at night.
2 Decrease the maximum **Exposure time** value until the blur caused by vehicle motion is acceptable.

If context images are noisy during the night:

1 Make the adjustment at night.
2 (Optional) Select **Enable illuminator**. This allows the camera to turn on the IR illuminator under dark conditions, but removes color from the image as the light level diminishes.
3 Decrease the maximum **Gain** value. This prevents the camera from amplifying the noise, but it can result in darker images.

If context images are too dark during the night:

1 Make the adjustment at night.
2 (Optional) Select **Enable illuminator**. This allows the camera to turn on the IR illuminator under dark conditions, but this progressively removes color from the image as the light level diminishes.
3 Increase the maximum **Exposure time** value until you are satisfied with the image quality. However, do not exceed the level that causes unacceptable motion blur on fast-moving vehicles.
4 If you reach the maximum **Exposure time** value and the image is still too dark, increase the maximum **Gain** value.

If context images are too bright during the day:

1 Make the adjustment under sun illumination.
2 Decrease the minimum **Gain** value until you are satisfied with the image quality.
3 If you reach the minimum **Gain** value and the image is still too bright, decrease the minimum **Exposure time** value.

Configuring SharpV analytics

You can configure the analytics performed by the SharpV, such as which plates the SharpV will read, and whether the SharpV should attempt to read the plate origin and vehicle make.

To configure SharpV analytics:

1 Log on to the Sharp Portal.

2 From the **Configuration** menu, click **Analytics** > **ALPR settings**.

3 From the **Context** menu, select which license plates will be most commonly read by the SharpV.

NOTE: For more information on the available regional contexts, see Supported ALPR contexts on page 13.

TIP: To help us improve the performance of regional contexts, click **Configuration** > **Connectivity** > **Product improvement** and register this camera to participate in the **Product improvement program**.

4 Under **Camera orientation**, select the pictograph that describes how the road appears from the camera's perspective. This helps the system to determine the direction that vehicles are traveling.

5 To ignore parked vehicles, signs, and other static objects, select the **Optimize for static image background** check box.

IMPORTANT:

- Not recommended if only a small part of the image background is static, for example, if many moving trees are visible. This is less likely to happen in installations where the camera is tilted downwards.
- It is not recommended to use this feature in conjunction with Virtual Loop when vehicles are traveling at speed above 50 km/h (30 MPH).

6 If a compatible regional context is selected, the **Zones** field is displayed, which lets you configure the SharpV for single or dual-lane plate reading. For more information, see Configuring the SharpV to monitor dual lanes.

7 From the **Reading mode** drop-down list, select one of the following reading modes:

- **Continuous:** Select this for plates to be captured continuously. This is the default setting.
- **Conditional:** Select this to capture plate reads continuously as long as the selected input signal meets the condition defined (high/low).
- **Single read on trigger:** Select this option to force the SharpV to capture a plate read after a signal is received from an electrical trigger, or after a Security Center event-to-action or hot action. This configuration is useful for controlling vehicle access to gated parking lots. You can configure the plate read capture to occur before or after the trigger is activated.

8 (Optional) If you selected **Single read on trigger**, click **Add trigger** and configure the following:

a) Under **Trigger**, select when an input (A or B) triggers a plate read based on its state (Low or High). For example, you can specify that **Input A** triggers a plate read when it **transitions to** a **Low** state. You can also select an **External** input such as a Security Center event-to-action or hot action.

b) Under **Capture window**, specify when the SharpV starts capturing (in milliseconds) and whether to do it **before** or **after** the trigger. You also need to specify the **Duration** (in milliseconds) that the SharpV will attempt to capture a plate read.

c) Under **If no plates**, indicate how long (in milliseconds) to wait after a trigger before capturing a context image of the vehicle. Select the **Use the ALPR image as context image** option, when you want an image from the ALPR camera to be used for the *no plate read*.

NOTE: Information on context images is not applicable to SharpV ITS cameras.

9 From the **Read strategy** list, select a read strategy. The following tables gives general recommendations based on the installation type. For more information, see About Sharp read strategies on page 54

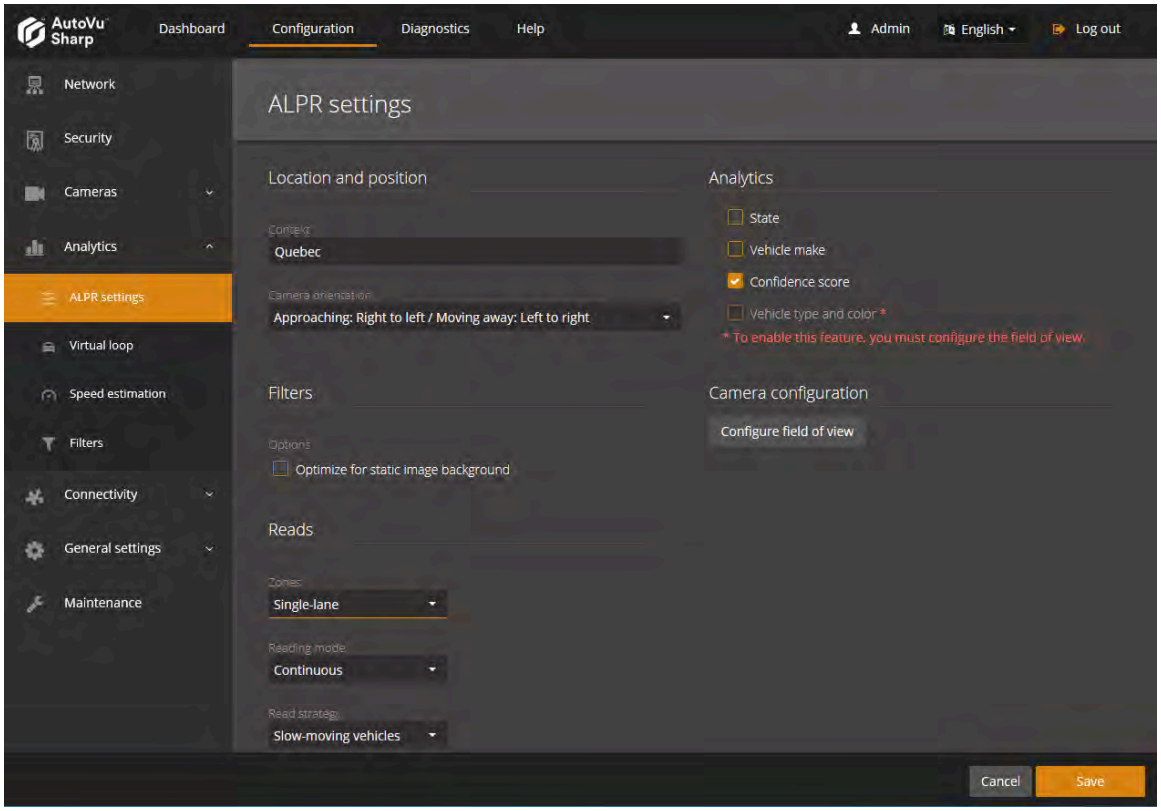
10 Under **Analytics**, select the contents of the plate you would like the SharpV to attempt to read. You can select the following:

NOTE: You can add the state, vehicle make, and confidence score as annotation fields in Security Center to query for this information in Security Desk reports.

- **State:** Select this option if you want the SharpV unit to attempt read the license plate origin. Depending on the region, this can refer to the issuing state, province, or country.
- **Vehicle make:** Select this option if you want the SharpV unit to attempt to read the vehicle's make from the brand or logo (Honda, Toyota, and so on).

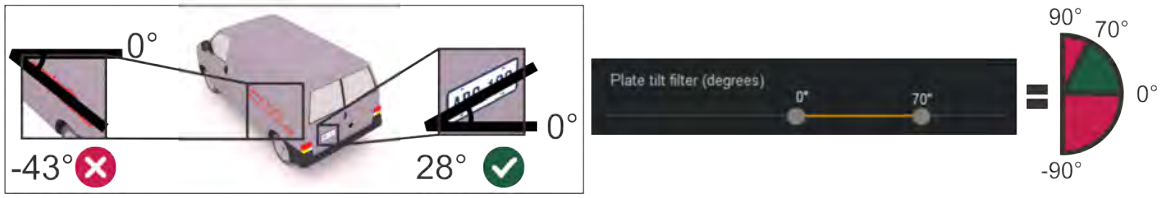
  NOTE: This setting is not recommended for MLPI installations.
- **Confidence score:** The SharpV assigns a confidence score percentage to each license plate read. This value indicates how confident the SharpV is in the accuracy of the read.

  NOTE: License plates that contain similar characters such as *8* and *B* are more difficult to read and generally produce reads with a lower confidence score.
- **Vehicle type and color:** Select this option if you want to include the vehicle type and vehicle color with plate reads. Based on the context image, the Sharp unit can detect if the vehicle is a bus, passenger vehicle, motorcycle, pickup, truck, work van, or an unknown vehicle type. In addition, the Sharp unit can detect if the vehicle is black, white, blue, brown, green, gray, orange, red, or yellow. Colors excluding white and black are also assigned *light*, *neutral*, or *dark* according to the color analysis.



11 If the SharpV is installed at a high angle, it might detect the lettering on the side of passing vehicles and produce false positive reads. Set the **Plate tilt filter** to ignore text unless it appears at the correct angle in the image.

NOTE: The plate tilt value is displayed in the **Last read** section of the *Camera feeds* page. It is also included as an annotation field which can then be included in read reports.

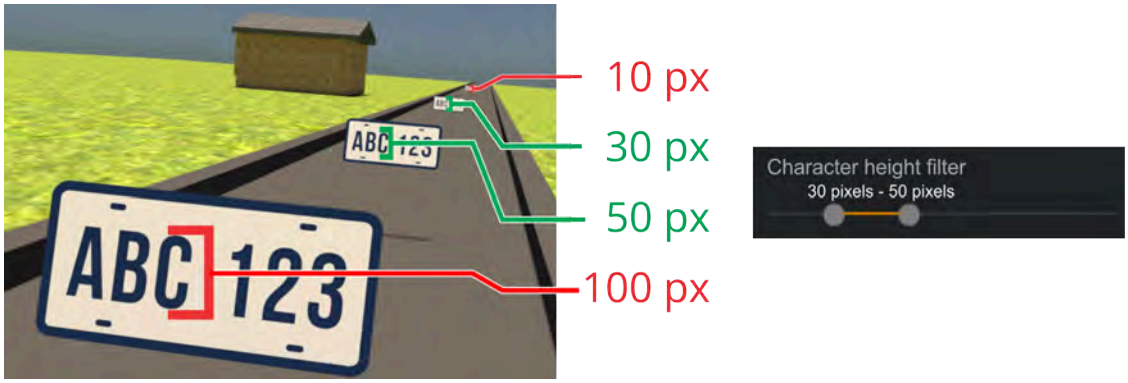


12 If the SharpV is installed at a low angle and license plates have a long transit time through the image, you can improve the read rate by setting the **Character height filter** to ignore license plates until they appear at the right height in the image.

TIP: The system captures plate reads more accurately if characters are between 25 and 60 pixels high in the images acquired by the ALPR camera. The optimal size of license plate characters is 30 pixels high. You can measure the pixel height on the **Configuration > Cameras > Zoom and focus** page.

NOTE:

- If the SharpV is configured for dual-lane plate reading, the characters must be from 10 to 40 pixels high. For more information, see Configuring the SharpV to monitor dual lanes on page 56.
- The character height is displayed in the **Last read** section of the *Camera feeds* page. It is also included as an annotation field which can then be included in read reports.



13 Click **Save**.

About Sharp read strategies

When you define a read strategy analytic for a Sharp camera, it optimizes how the camera captures license plate reads based on the expected vehicle speed and behavior.

Read strategies for fixed and mobile Sharp cameras

There are several scenarios where ALPR might be required. If vehicles generally pass the Sharp at the same speed, you can enable a read strategy to optimize ALPR performance for that scenario. For example, a mobile unit on a law enforcement vehicle must read license plates at a higher speed and frequency than a fixed unit used to control a gate. The read strategy analytic takes advantage of these differences to minimize duplicated and missed license plate reads. Each read strategy automatically configures the optimal internal values for the scenario.

- **Slow moving vehicle:** Select this strategy for fixed Sharp cameras monitoring parking lots and for mobile Sharp cameras used for parking enforcement. Generally results in better ALPR accuracy, but occasionally misses or duplicates plate reads.

- **Fast moving vehicle:** Select this strategy for fixed Sharp cameras monitoring highways and for mobile Sharp cameras used for law enforcement. This strategy obtains ALPR reads quickly, but often duplicates reads if the plate is in the field of view for a long time.
- **Gate control:** Select this when vehicles must come to a stop when the license plates are read. For example, select this option for a SharpV camera that is monitoring a gated parking lot entrance or toll booth.
- **Free-Flow:** Select this when AutoVu™ Free-Flow is enabled on the ALPR Manager. This strategy improves the accuracy of the parking lot occupancy calculation.

  NOTE: When using the Free-Flow read strategy, the system waits for the vehicle to exit the field of view before selecting the best plate read. You might notice a delay of a few seconds when monitoring live plate reads. For this reason, we do not recommend using this strategy when the camera relays are also used to control a physical gates.

ALPR scenario	Slow moving vehicle	Fast moving vehicle	Gate control	Free-Flow
Mobile				
Parking enforcement	✔			
Law enforcement		✔		
Fixed				
Highways		✔		
Parking lots	✔			
Parking lots (AutoVu™ Free-Flow)				✔
Gate control			✔	

Read strategy characteristics

Characteristic	Slow moving vehicle	Fast moving vehicle	Gate control	Free-Flow
Missed plate reads	More frequent	Less frequent	Less frequent	More frequent
Duplicated plate reads	More frequent	More frequent if plates are in the field of view for a long time.	Less frequent	Less frequent
Latency	Medium-low	Low	Medium	High
ALPR accuracy	Better	Good	Best	Best

Configuring the SharpV to monitor dual lanes

In certain situations, it is possible for the SharpV to monitor two lanes of traffic. If dual-lane monitoring is available in your region, you can configure the camera to identify two lanes in the field of view.

Before you begin

- Install the SharpV between the two lanes, for example, on an overpass. If the camera cannot be installed exactly between the two lanes, a certain amount of offset can be accounted for in the following steps.
- Adjust the focus and zoom of the camera.

  NOTE: When monitoring dual lanes, characters should be from 10 to 40 pixels high. This is smaller than the standard pixel height requirements (25 - 60 pixels). As a result, license plate capture performance might be affected. When using this feature, it is recommended that you test the system's performance.
- Select a compatible regional context. For the complete list of countries that currently support Dual-lane feature, see Supported dual-lane configurations.

What you should know

IMPORTANT: When the SharpV is configured to monitor dual lanes, the virtual loop, speed estimation, and region of interest features are unavailable.

IMPORTANT: In the dual-lane mode, motorcycle plates are not read bySharpV cameras.

IMPORTANT: Using the SharpV dual-lane monitoring feature reduces the ALPR performance of the camera. Do not configure the SharpV for dual-lane license plate detection if you are monitoring parking occupancy using AutoVu™ Free-Flow in Security Center.

- The SharpV can detect vehicles moving in either direction, assuming the vehicles have front and rear license plates.
- One read strategy analytic (for example, for slow-moving vehicles) applies to both lanes.

To configure the SharpV to monitor dual lanes:

1 Log on to the Sharp Portal.
2 From the **Configuration** menu, select **Analytics** > **ALPR settings**.
3 From the **Zones** menu, select **Dual lane**.

NOTE: The **Zones** menu is only displayed if a compatible regional **Context** is selected.

4 Define the center line between the two lanes.

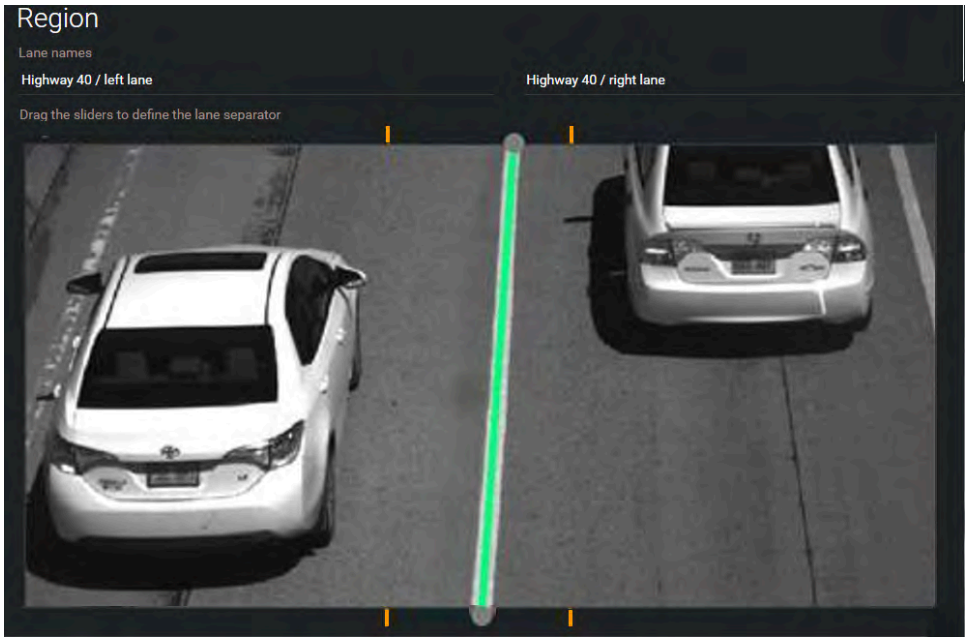
a) From the **Configuration** menu, select **Cameras** > **Region**.

b) Enter descriptive **Lane names**.

For example: `Highway 40 / left lane`

NOTE: To include this information in Security Desk reports, you can add "Lane" as annotation field in Security Center.

c) Drag the sliders to define the lane separator position.



d) When you are satisfied with the appearance of the lanes in the video feed window, click **Save**.

The system displays the message: *Configuration saved successfully.*

Calibrating the virtual loop

For parking applications where the license plate capture rate is critical, the SharpV virtual loop feature can detect vehicles with damaged or dirty license plates that are not detected by the SharpV ALPR camera. The plate numbers of these vehicles can then be manually modified in Security Desk.

Before you begin

- Install the SharpV camera in a fixed location, following the positioning guidelines.
- Adjust the zoom and focus of the camera.

IMPORTANT: To use the virtual loop, the zoom level of the ALPR and context cameras must be adjusted so that the context camera field of view is more than double the width of the ALPR camera field of view.

NOTE: If you move the location of the camera, or if you modify the zoom and focus or the pan and tilt angles of the camera, you must reconfigure and recalibrate the virtual loop detection zone.

What you should know

- For best results when using the virtual loop feature, ensure that the detection area is well illuminated. If there is not enough light for reliable operation, the virtual loop is temporarily disabled until lighting conditions improve.
- To be detected by the virtual loop, at least 25% of the vehicle must pass through the red detection zone and at least 20% of the vehicle must pass through the orange ALPR field of view, in any order. The vehicle must also either enter or exit the context camera field of view, depending on the settings you choose.

- You must respect the recommended SharpV positioning guidelines. For more information, see the *SharpV Handbook*.
- It is not recommended to use Virtual loop in conjunction with the **Optimize for static image background** feature when vehicles travel faster than 50 km/h (30 MPH).
- For the calibration to finish quickly, choose a time when vehicles are expected to be traveling in the appropriate direction in the designated area.
- The virtual loop feature is not available on SharpV ITS cameras.
- You cannot use the virtual loop as a trigger for gate control.
- This feature is not supported if the SharpV is configured for dual-lane plate reading.

To configure SharpV virtual loop:

1 Log on to the Sharp Portal.

2 From the **Configuration** menu, select the **Analytics > Virtual loop** page.

3 Click **Enable**.

The camera saves the configuration and displays the message "Configuration saved successfully".

4 Click **Configure**.

The status LED on the SharpV flashes red and green during the configuration.

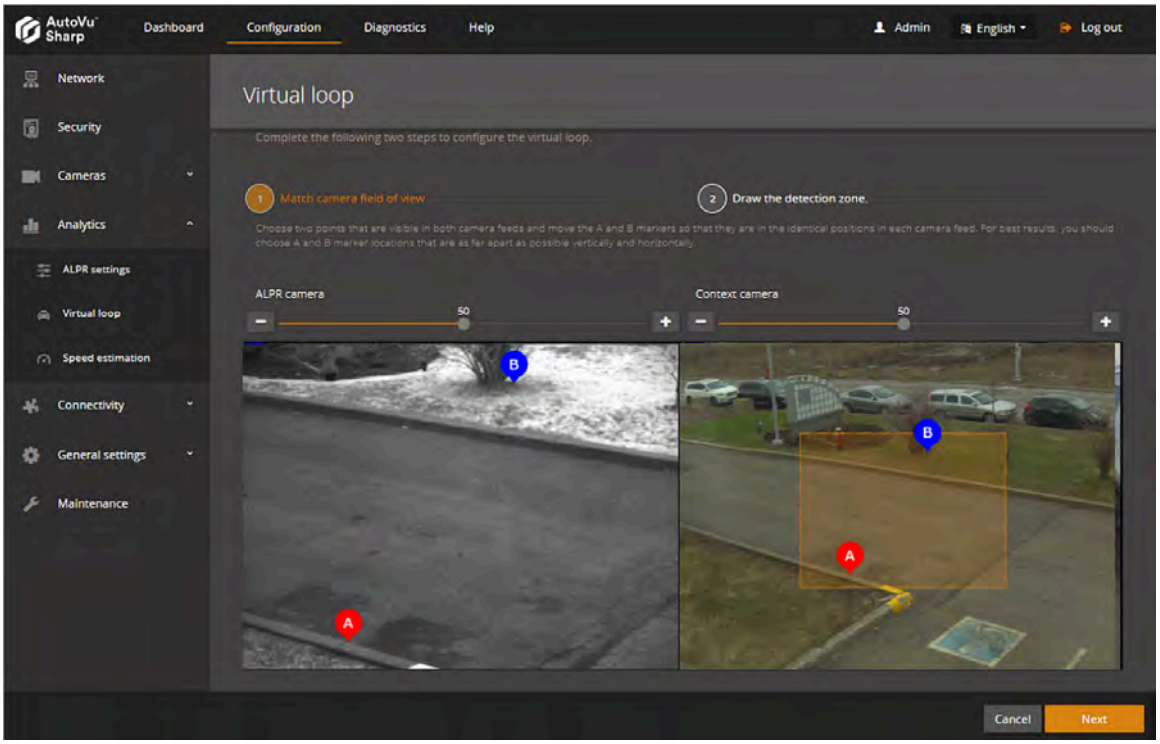
5 Match the markers.

a) In the virtual loop configuration page, the video feeds from the ALPR camera and context camera are displayed with an *A* and *B* marker for each camera. Choose two points that are visible in both camera feeds and move the A and B markers so that they are in the identical positions in each camera feed. When the markers are close to the correct position, an orange box appears in the context camera video feed. Fine tune the marker positioning so that the orange box matches the field of view of the ALPR camera.

NOTE:

- For best results, choose *A* and *B* marker locations that are as far apart as possible vertically and horizontally.
- If either of the video feeds are too dark or too bright to accurately place the markers, you can temporarily adjust the brightness using the sliders located above each video feed. When the calibration is finished, the exposure returns to its default mode.

b) Click **Next**.



6 Configure a detection zone.

a) To configure the system to detect vehicles that are moving in a specific direction, select one of the following detection modes from the drop-down list:

- Enters the field of view in the detection zone.
- Exits the field of view in the detection zone.
- Enters or exits the field of view in the detection zone.

b) To draw a detection zone in the camera video feed, create a polygon by clicking on at least three points.

NOTE:

- Clicking in the field of view clears any existing polygon. You can also click **Clear the zone** to remove an existing polygon.
- To draw a polygon that covers the entire context camera field of view, click **Select all** and use the *Enters or exits the field of view in the detection zone* setting.

Consider the following when drawing the detection zone:

- The polygon must touch the border of the image. This is necessary for all direction of travel settings, for example, *Enters the field of view in the detection zone*.
- The polygon lines cannot intersect.
- To be detected, at least 25% of the visible part of the vehicle must pass through the red detection zone (if configured) when the vehicle enters or exits the image. The vehicle must also cover at least 20% of the orange ALPR field of view somewhere along its trajectory.
- Try to draw your detection zone so that cyclists and pedestrians do not pass through the zone. For example, if you have too many false detections when you draw a polygon far from the camera and use the *Exits the field of view in the detection zone* setting, try drawing a polygon close to the camera and use the *Enters the field of view in the detection zone* setting.

For more information, see Virtual loop detection zone examples on page 61.

c) When you have finished drawing the polygon, click **Done**.

The system displays *In progress - Waiting for 5 more vehicles* and counts down the number of license plate reads that are required for calibration to finish. During this calibration, the system evaluates the expected vehicle size and trajectory.

NOTE:

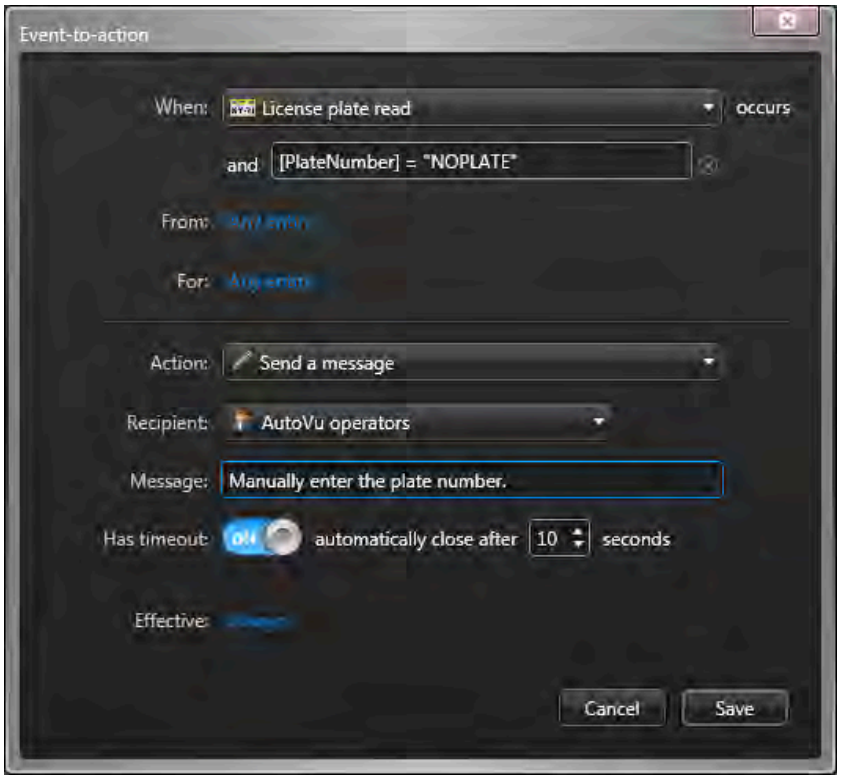
- The system completes the calibration on its own. No further steps are required.
- If, before the calibration ends, you make any other change to the SharpV configuration, the calibration is restarted.

After you finish

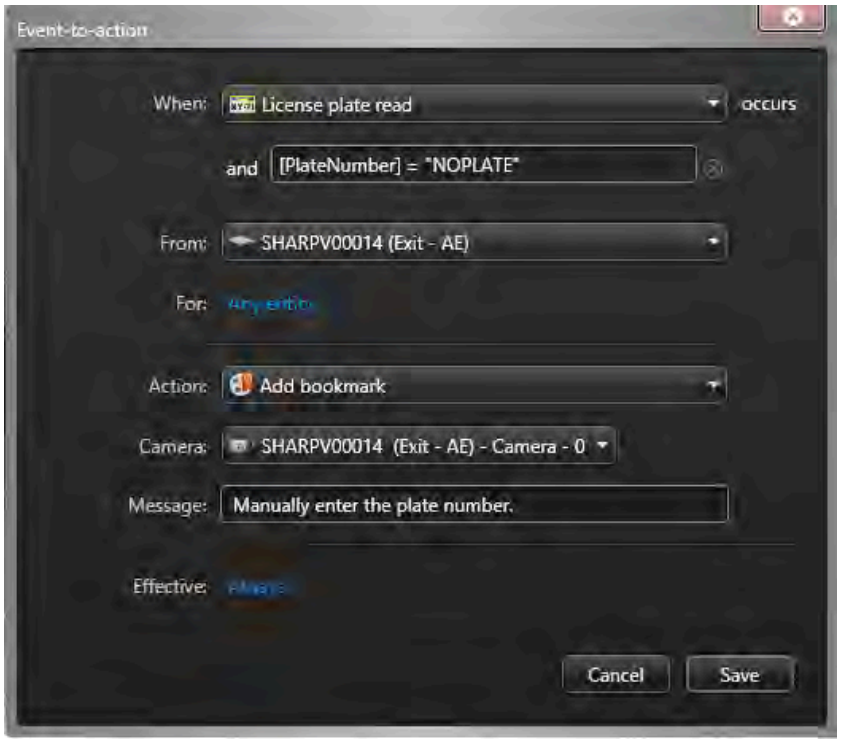
- For troubleshooting purposes, virtual loop diagnostic information is available from the **Diagnostics > Logs** page. Before calibration, using the *VehicleDetection* source, and after calibration using the *VehicleDetection (verbose)* source (must be enabled from the **Sources to log** drop-down list).
- If the ALPR camera fails to capture a vehicle's license plate and the vehicle is then detected by the virtual loop, the license plate event sent by the SharpV uses the string *NOPLATE*. To let the operator know that the

license plate needs to be manually modified, you can configure an event-to-action in Config Tool to trigger an alarm, to send a message, or to add a bookmark.

Example: Event-to-action to send a message



Example: Event-to-action to create a bookmark



Virtual loop detection zone examples

To reduce the number of false detections when using the virtual loop feature in a fixed SharpV installation, you must consider the guidelines for drawing the detection zone.

Virtual loop detection zone guidelines:

- The polygon must touch the border of the image. This is necessary for all direction of travel settings, for example, *Enters the field of view in the detection zone*.
- The polygon lines cannot intersect.
- To be detected, at least 25% of the visible part of the vehicle must pass through the red detection zone (if configured) when the vehicle enters or exits the image. The vehicle must also cover at least 20% of the orange ALPR field of view somewhere along its trajectory.
- Try to draw your detection zone so that cyclists and pedestrians do not pass through the zone. For example, if you have too many false detections when you draw a polygon far from the camera and use the *Exits the field of view in the detection zone* setting, try drawing a polygon close to the camera and use the *Enters the field of view in the detection zone* setting.

Issue: The detection zone does not touch the edge of the field of view

- **Bad:** The detection zone polygon (drawn in red) covers the parking lot entrance, but it does not touch the edge of the context camera field of view. With this detection zone, no vehicles are detected.



- **Good:** The detection zone touches the edge of the context camera field of view. To detect only vehicles exiting the parking lot, use the *Enters the field of view in the detection zone* setting.



Issue: Vehicles do not leave the field of view

- **Bad:** To be detected, vehicles must exit the context camera field of view. Some of the parking spaces in this parking lot are within the detection zone. As a result, the vehicles in those spaces are not detected.



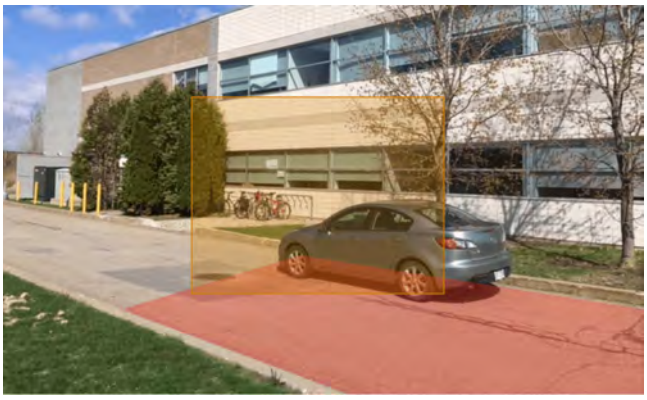
- **Good:** To correct this issue, the camera angle has been lowered (which requires zoom and focus recalibration) and the *Enters the field of view in the detection zone* setting is used.

  Alternatively, you could reduce the size of the context camera's field of view so that the vehicles in the parking lot are not visible.

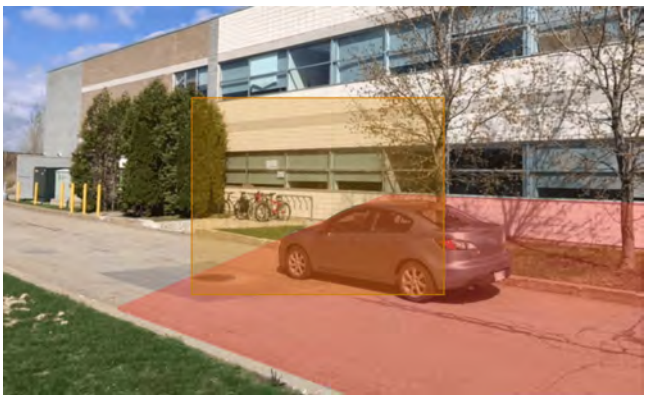


Issue: 25% of the vehicle is not within the detection zone

- **Bad:** In this example, the detection zone is drawn to match the road. Especially when the camera is installed close to the ground, this can mean that vehicles are excluded.



- **Good:** To correct this issue, when drawing the detection zone, consider the path and size of vehicles as they pass through the field of view.



Calibrating speed estimation

For systems that include a fixed SharpV camera, you can configure the camera to include an estimated vehicle speed when performing license plate reads.

Before you begin

- Install the SharpV camera in a fixed location. To use this feature, cameras should be installed higher than the level of the license plates with respect to the road. This means a camera installation height of at least 1.5 m (5 ft). The camera should be pointing downward with respect to the horizontal by at least 5°.
- Adjust the zoom and focus of the camera.

  NOTE: If you modify the zoom and focus or the pan and tilt angles of the camera, you must recalibrate speed estimation.
- Configure the ALPR context. Do this so that the speed and measurement units are displayed in the format for your region.

What you should know

- For more accurate speed estimation, vehicles that pass the camera during calibration should travel at a constant speed of at least 30 km/h (20 mph). This recommendation only applies during calibration. In general, the system can estimate speeds for vehicles moving slower than 30 km/h (20 mph).
- **To calibrate speed estimation, the system needs the following, in any order:**
  - At least one license plate read from a calibration vehicle with a known speed. You can do this by driving the calibration vehicle at a specific speed, or by using a radar device to detect the speed of a passing vehicle.
  - 20 additional license plate reads. You do not need to know the speed of these vehicles.

    NOTE: For the calibration to finish quickly, choose a time when vehicles are expected to be traveling in the appropriate direction in the designated area. If no traffic is expected to pass during the calibration, you can use one vehicle to make 20 passes in front of the camera, leaving at least 15 seconds between passes.
- This feature is not supported if the SharpV is configured for dual-lane plate reading.

To configure SharpV speed estimation:

1 Log on to the Sharp Portal.
2 From the **Configuration** menu, select the **Analytics > Speed estimation** page.
3 Click **Enable**.

The camera saves the configuration and displays the message "Configuration saved successfully".

4 Click **Start calibration**.

The system starts to capture license plate reads for calibration and displays *Calibrating...*. A counter indicates the number of plate reads remaining to complete the calibration.

If you use a calibration vehicle moving at a specific speed:

1 From the main speed estimation screen, click **Edit**.

2 Click **Plate number** and enter the license plate of the calibration vehicle.

3 Click **Add**.

The system displays the message: *The system is now expecting to read a plate for this vehicle. The vehicle should maintain a constant speed.*

When the system detects the calibration plate, it displays the license plate read with a time stamp.

4 Click **Validate**.

Two images of the calibration plate are displayed.

5 As shown in the following image, the orange line in each image must follow the bottom of the characters and must be as wide as the license plate. If required, move the end points to correct the line placement.

IMPORTANT: Speed estimation accuracy depends on precise positioning of the end points.



6 Enter the **Speed** at which the vehicle was traveling when it was read by the SharpV camera.

7 The **Width** of the plate is entered for you based on the ALPR context that you have configured. If necessary, modify the plate width.

8 (Optional) For more accuracy, measure the distance from the ground to the bottom of the calibration vehicle's license plate and enter the measurement in the **Distance from ground to plate** field.

9 Click **Validate**.

A green check mark is displayed over the calibration plate, indicating that the step is complete.

NOTE: You can add plate numbers for additional calibration vehicles. This is not required, but can increase speed estimation accuracy.

If you use a radar device to detect the speed of a passing vehicle:

1 From the main speed estimation screen, click **Edit**.

2 Click **Advanced** on the right side of the screen.

The license plates from passing vehicles are displayed.

3 Take note of the license plate of a passing vehicle and use your radar device to detect the vehicle's speed.

4 Click the license plate image of the vehicle with the known speed.

Two images of the calibration plate are displayed.

5 The orange line on each image must follow the bottom of the characters and must be as wide as the license plate. If required, move the end points to correct the line placement.

IMPORTANT: Speed estimation accuracy depends on precise positioning of the end points.

6 Enter the **Speed** of the vehicle as detected by your radar device.

7 The **Width** of the plate is entered for you based on the ALPR context that you have configured. If necessary, modify the plate width.

8 Click **Save**.

The camera captures 20 license plate reads:

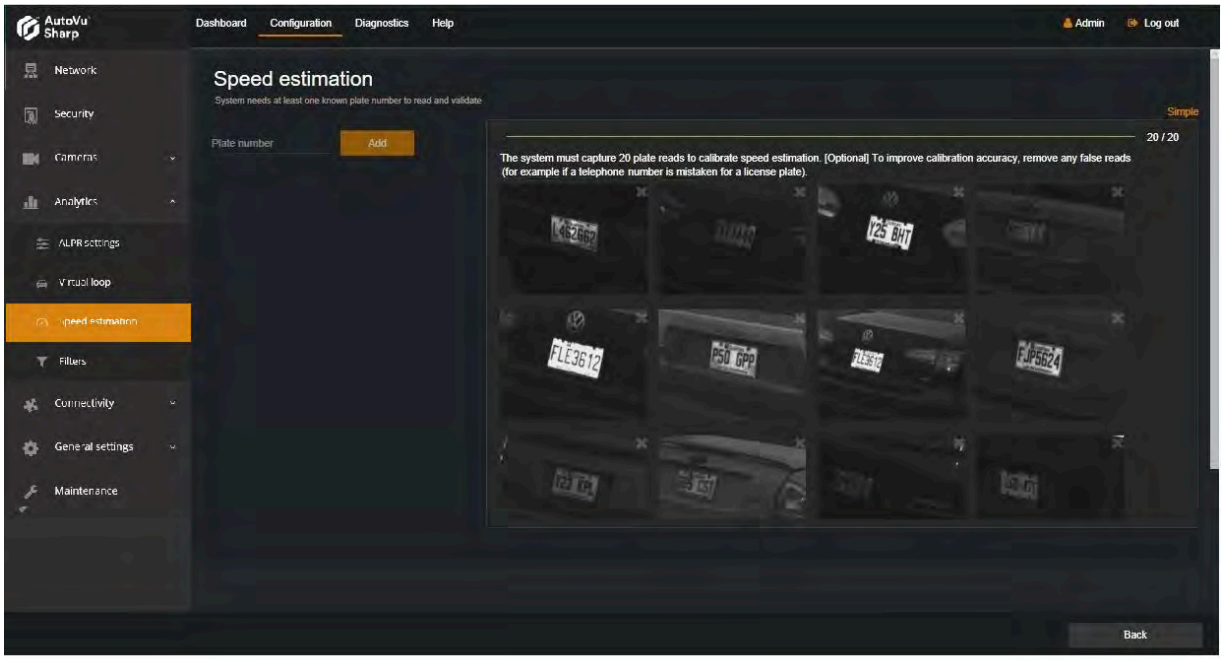
The system must analyze plate reads from 20 passing vehicles. The vehicles can be traveling at any speed and you do not need to know the speed of these vehicles. There is no user action required for this step, however, you can improve speed estimation accuracy by editing the plate reads using the following steps:

NOTE: It might take more than 20 vehicle passes to complete the calibration.

1 From the main speed estimation screen, click **Edit**.

2 Click **Advanced** on the right side of the screen.

The license plates from passing vehicles are displayed.



3 If you notice an incorrect plate read, for example, if a sticker on the back of a vehicle was mistaken for a license plate, delete the image.

4 You can click on an image to display two images of the license plate. You can inspect the position of the end points of the orange line. If the position is inaccurate, you can either move the end points to correct the line placement or delete the image.

5 Click **Back** to return to the main speed estimation screen.

When the system has successfully read 20 license plates, and when you have entered the speed of at least one license plate, the **State** displayed on the main calibration screen is *Ready*.

When the speed estimation calibration is complete, vehicle speed is displayed in the *Live Feed* page of the portal. It is also possible to configure the vehicle speed to be included as an annotation field in Security Center. For more information, see the *Security Center Administrator Guide*.

About matcher settings files

When dirty or damaged license plates are misread by a Sharp camera, different methods are available for matching the plate read to a permit. Which matcher settings file you need to configure depends on the AutoVu™ installation type.

The following ALPR matcher files and settings are available:

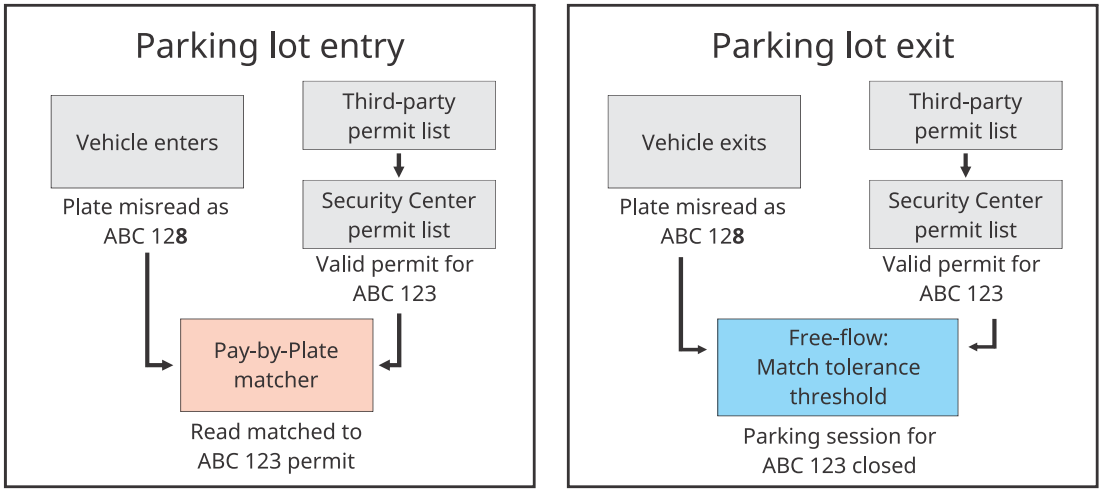
ALPR matcher	File or setting	Location
General matcher	MatcherSettings.xml	*C:\Program Files\Genetec Security Center X.X.*
Pay-by-Plate Sync matcher	*Genetec.Plugins.MobilePBP.dll.config*	*C:\Program Files (x86)\Security Center Plugins\MobilePBP*
AutoVu™ Free-Flow setting	Match tolerance threshold	*AutoVu™ Free-Flow* section of the ALPR Manager *Properties* page

Fixed SharpV cameras using AutoVu™ Free-Flow and the Pay-by-Plate Sync plugin

In this case, the Pay-by-Plate Sync matcher settings are used to validate license plate reads at the parking lot entrance against the Security Center permit file that has been updated with third party permits by Pay-by-Plate Sync.

The **Match tolerance threshold** setting is used to close parking sessions if the plate is misread at the parking lot exit.

NOTE: In the following example, the matcher settings allow one OCR equivalent character.

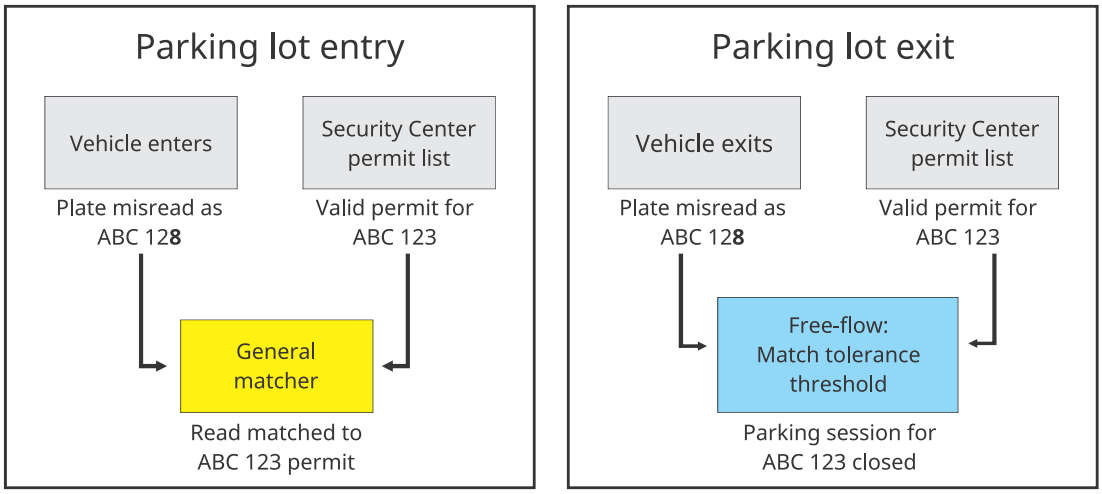


Fixed SharpV cameras using AutoVu™ Free-Flow without the Pay-by-Plate Sync plugin

In this case, the general matcher file is used to validate license plate reads at the parking lot entrance against the Security Center permit list. No third-party lists are involved in this scenario.

The **Match tolerance threshold** setting is used to close parking sessions if the plate is misread at the parking lot exit.

NOTE: In the following example, the matcher settings allow one OCR equivalent character.

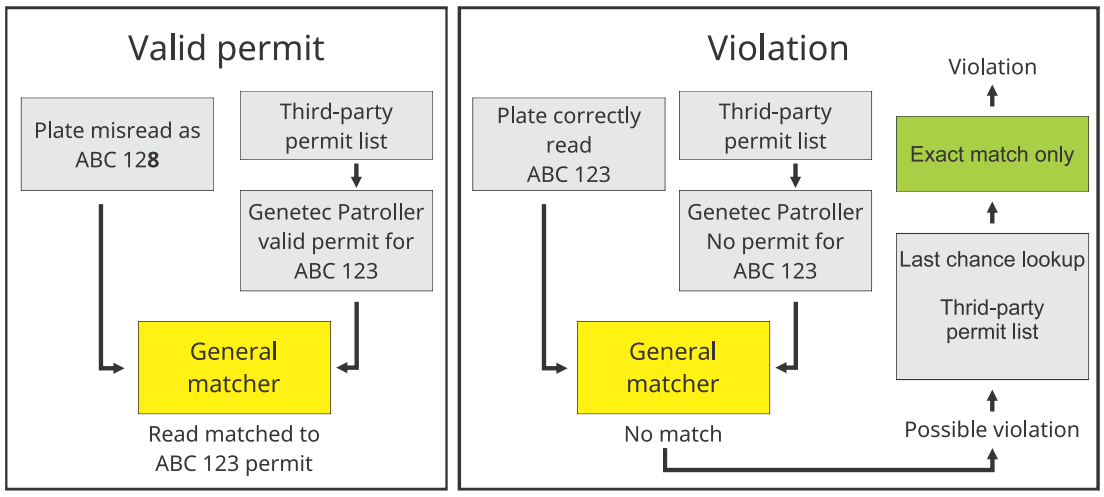


Mobile cameras using the Pay-by-Plate Sync plugin

In this case, the general matcher file is used to validate license plate reads against the Genetec Patroller™ permit file that has been updated with third party permits by Pay-by-Plate Sync.

When the system performs a last chance lookup to verify that the permit has not recently been added to the list, no matcher settings are applied. Only an exact match triggers a violation.

NOTE: In the following example, the matcher settings allow one OCR equivalent character.

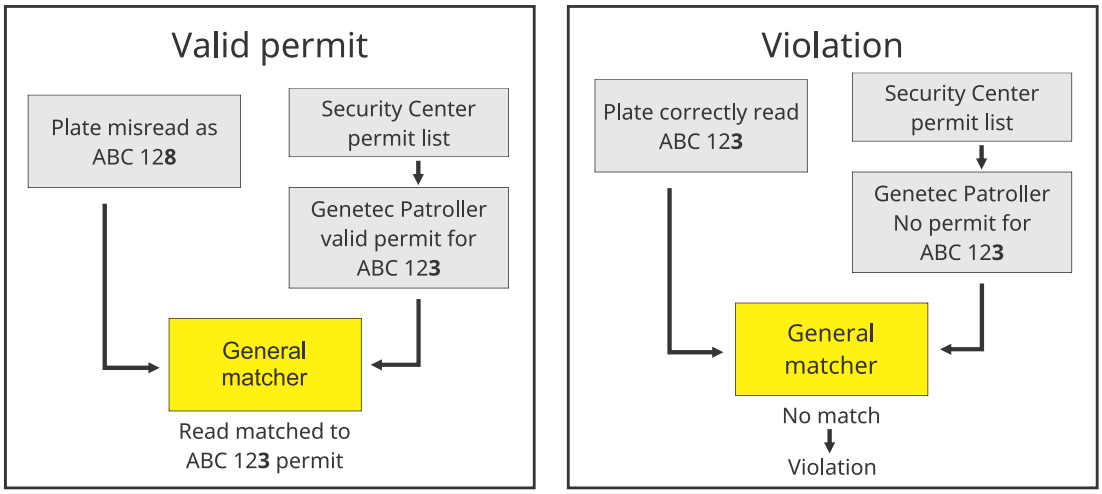


Mobile SharpX cameras without the Pay-by-Plate Sync plugin

In this case, the general matcher file is used to validate license plate reads against the Genetec Patroller™ permit file that has been updated with the current Security Center permit list.

When the system performs a last chance lookup to verify that the permit has not recently been added to the list, no matcher settings are applied. Only an exact match triggers a violation.

NOTE: In the following example, the matcher settings allow one OCR equivalent character.


Valid permit
Plate misread as ABC 128
Security Center permit list
Genetec Patroller valid permit for ABC 123
General matcher
Read matched to ABC 123 permit
Violation
Plate correctly read ABC 123
Security Center permit list
Genetec Patroller No permit for ABC 123
General matcher
No match
Violation

Configuring where the SharpV sends its ALPR data

Depending on whether you want to receive license plate read information in Security Center, or an FTP or HTTP server, you must configure where the SharpV sends its ALPR data accordingly.

What you should know

- For SharpV cameras that have been upgraded to SharpOS 12.7 or later and have been upgraded to use the LPM Protocol, or for new SharpV cameras that were shipped with SharpOS 12.7 or later, you do not need to select an extension. When you add the camera to the ALPR Manager using the LPM protocol, the setting is added and automatically selected.
- If the SharpV is connected to Security Center, plate reads are automatically stored if the connection is lost. The SharpV can store up to 20 000 plate reads with their associated images.
- For FTP and HTTP extensions, plate reads and images are automatically stored if the connection is lost, however, you can disable edge storage using the **Retain data when the connection is lost** setting in the extension configuration. To reduce cellular data usage, you can also configure whether the ALPR and context images are exported.

To configure the SharpV extension:

1 Log on to the Sharp Portal.
2 From the **Configuration** menu, select the **Connectivity > Extension** page.
3 From the **Extension type** drop-down list, select one of the following:
   - **FTP:** Use this option to send ALPR data to an FTP server. You can configure the FTP XML template which can be integrated by third-party applications. For more information, see Configuring the SharpV FTP extension on page 84.
   - **HTTP:** Use this option to send ALPR data to an HTTP server. You can configure the system to send the data in XML or JSON format. For more information and examples of the exported XML and JSON files, see Configuring the SharpV HTTP extension on page 87.
   - **Security Center (Legacy):** Use this option to send ALPR data to the ALPR Manager. Use this option if you are connecting the SharpV to Security Center 5.7 or earlier.
     - **This unit manages the connection to Security Center:** Use this **only** if the autodiscovery of the connected SharpV does not work (see SharpV camera connections to Security Center) or if you cannot manually add the SharpV to the ALPR Manager. You must enter the **Server** address and **Port** of the server running the ALPR Manager role. For example, if a SharpV is connected to a WiFi router, and the camera's IP address is then changed, the ALPR Manager cannot detect the change automatically, so you can use this to reconnect to the Security Center computer.
       IMPORTANT: When using this option, no failover is available if the server connection is lost.
     - **Discovery port:** Port on which the SharpV listens for discovery requests. This port number must match the discovery port entered on the ALPR Manager *Properties* page.
       NOTE: When setting the discovery port, do not use port 5050 as it is reserved for the logger service.
     - **Control port:** Used in Security Center Config Tool when creating a new ALPR unit (SharpV) manually.
   - **Security Center (LPM protocol):** Use this option to send ALPR data to the ALPR Manager (Security Center 5.8 or later).

     NOTE:

     - By default, LPM protocol is not an available extension. When a SharpV (SharpOS 12.7 and later) is manually added to the ALPR Manager (Security Center 5.8 and later), the LPM protocol is automatically selected as the unit's extension type.
     - When a SharpV is upgraded to SharpOS 12.7 or later, you must still upgrade the unit to use the LPM protocol before you connect to Security Center.
4 Click **Save**.

After you finish

Synchronize the SharpV clock.

SharpV camera connections to the ALPR Manager role

If you want to send ALPR data from a SharpV camera to Security Center, you must first enroll the camera in the Security Center *ALPR* task under *Roles and units*.

When connecting to Security Center 5.8 or later, the SharpV uses the LPM protocol to manage the connection (when manually added). If the LPM protocol is not enabled on the SharpV, other connection methods are available.

For information on configuring ALPR Managers for fixed AutoVu™ system, refer to the *Security Center Administrator Guide*.

Adding a camera using the LPM protocol

This is the preferred method for adding a Sharp to the ALPR Manager. The LPM protocol provides a secure and reliable connection.

Connection Method	When to use this method	Requirements
Manually add the camera in Security Center: You can add the camera to the ALPR Manager in Config Tool's *ALPR* task.	If your camera can be upgraded to SharpOS 12.7, this is the recommended method.	• SharpOS 12.7 or higher with LPM protocol enabled • Security Center 5.8 or higher • You must know the IP address and the username and password used to access the Sharp Portal .

Adding a camera that does not use the LPM protocol

For cameras where the SharpOS version is earlier than 12.7, the easiest way to add a SharpV camera in Security Center is to configure the ALPR Manager to discover the camera. If this connection method is not possible, you can add the camera manually in Security Center or in the camera's web portal.

NOTE: If you are connecting a SharpV camera, it is recommended that you upgrade it to SharpOS 12.7 or higher, and enable the secure and reliable LPM protocol connection.

Connection Method	When to use this method	Requirements
Configure the ALPR Manager to discover the camera: You can configure the ALPR Manager's *Discovery port* to find the camera on the subnet.	This is the preferred method if the camera and Security Center are on the same subnet.	To use this method, you must set the same *Discovery port* in the ALPR Manager's *Properties* tab and in the camera's web portal. The camera and Security Center must be on the same subnet.

Connection Method	When to use this method	Requirements
Manually add the camera in Security Center: You can add the camera to the ALPR Manager in Config Tool's *A* task.	Use this method when the camera and Security Center are on different subnets within the same LAN. You can use this method if the *Discovery port* is not available, however the *Discovery port* can be changed in Security Center and in the camera's web portal. **NOTE:** • You cannot use this method if communication must go across the Internet. • If the camera is behind a NAT, you must configure port forwarding.	To use this method, you must know the IP address, port (80 or 443), and its control port (default 8001). The camera and Security Center must be on the same network.
Add a SharpV from the camera's web portal: You can force a connection from the camera's web portal when you select the *Security Center* extension and select **Connect to Security Center**. For assistance, contact your Genetec™ representative.	Use this method if the camera and Security Center must communicate across the Internet and where the network topology includes NATs. **NOTE:** If the camera is behind a NAT, you must configure port forwarding.	To use this method, you must enter the *Hostname* or *IP address* and *port* (listening port) of the Security Center computer.

SharpV communication ports

For SharpV cameras to communicate with Security Center, the correct communication ports must be defined.

The following table lists the default network ports used for SharpV communication with Security Center:

Computer	Inbound	Outbound	Port usage
SharpV	TCP 8001		Control port.
	TCP 2323		Used by the SharpV to determine which extension to load.
	UDP 5000		Used to discover SharpV units connected to the network.
		TCP 8731	Default listening port.
		9001	LPM protocol.
	80		Used for HTTP communication with Security Center.
	443		Used for HTTPS communication with Security Center.
	RTSP 554		Used to set up, start, and stop the SharpV H.264 video stream.

Adding a SharpV camera to the ALPR Manager

To send ALPR data from the camera to Security Center, you must add the camera to an ALPR Manager.

Before you begin

- To add a camera in Security Center, you must first configure an ALPR Manager role.
- If your SharpV was shipped with SharpOS 12.7 or later and you are manually adding the SharpV to Security Center, you do not need to upgrade it to use the LPM protocol. If your SharpV camera is running an earlier SharpOS 12.x version, it is recommended that you upgrade the camera and enable the LPM protocol to take advantage of this secure and reliable connection to Security Center.

  NOTE: If a camera uses the LPM protocol to connect to Security Center, the **Active extension** in the Sharp Portal is set to *Security Center (LPM protocol)*.

What you should know

- The steps for adding the camera to the ALPR Manager depend on the SharpOS version running on the camera. For more information, see SharpV camera connections to the ALPR Manager role.
- If the SharpOS running on the camera is 12.6 or earlier, you can still connect by configuring the Security Center, HTTP, or FTP extensions in the Sharp Portal.

To manually add a camera running SharpOS 12.7 or later:

1 From the Config Tool home page, click the *ALPR* task and select **Roles and units**.

2 Select the **ALPR Manager** role from the drop-down list.

3 Click **ALPR unit**.

The **Creating a unit** dialog box opens.

4 Enter a **Name** for the camera.

5 Enter the camera's IPv4 or IPv6 **IP address**.

NOTE: If the camera is behind a NAT, enter the IP address of the NAT, and the port of the NAT which has been associated to port 443 of the camera.

6 This SharpOS version requires HTTPS communication. Enter **Port** 443.

NOTE: If the camera is behind a NAT, enter the IP address of the NAT, and the port of the NAT which has been associated to port 443 of the camera.

7 From the **Location** list, assign the camera to an area entity.



8 Click **Next**.

9 Enter the **Username** and **Password** used to log onto the Sharp Portal and click **Next**.

10 Review the settings and click **Create**.

To manually add a camera running SharpOS 12.6 or earlier:

1 From the Config Tool home page, click the *ALPR* task and select **Roles and units**.

2 Select the **ALPR Manager** role from the drop-down list.

3 Click **ALPR unit**.

The **Creating a unit** dialog box opens.

4 Enter a **Name** for the camera.

5 Enter the Sharp unit's IPv4 or IPv6 **IP address**.

6 Enter **Port** 443 for HTTPS or 80 for HTTP, according to the Sharp unit's configuration.

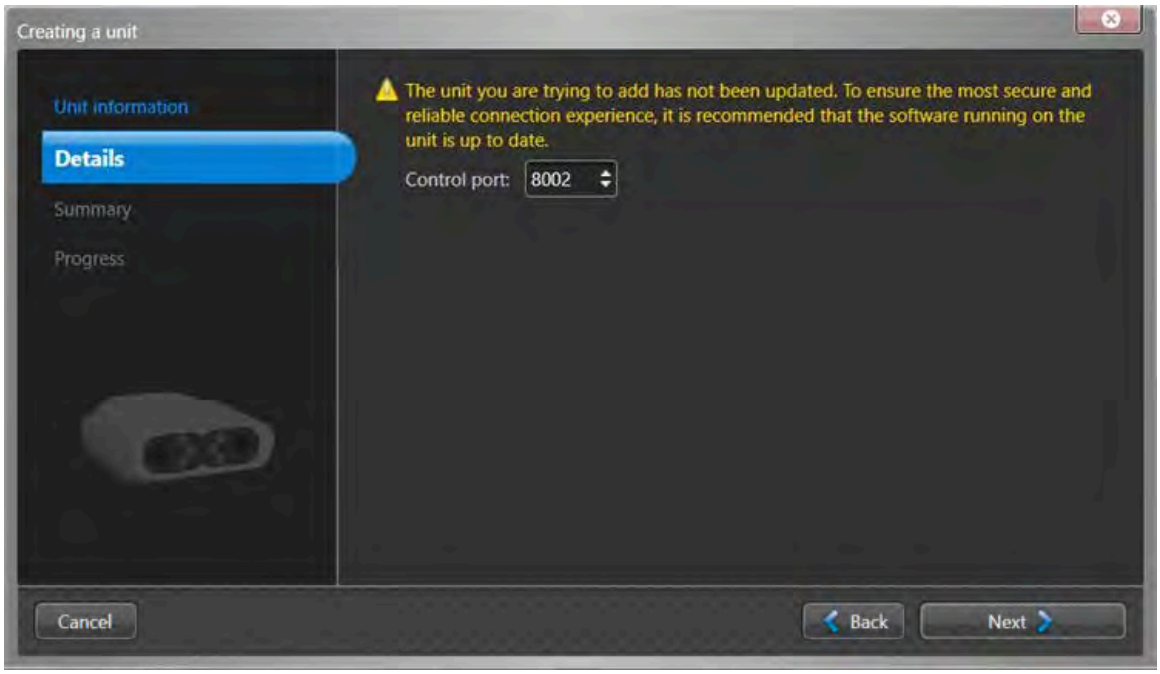
7 From the **Location** list, assign the camera to an area entity.



8 Click **Next**.

9 Enter the camera's **Control port** (default: 8001).

This information should match what is displayed in the Sharp Portal configuration page.



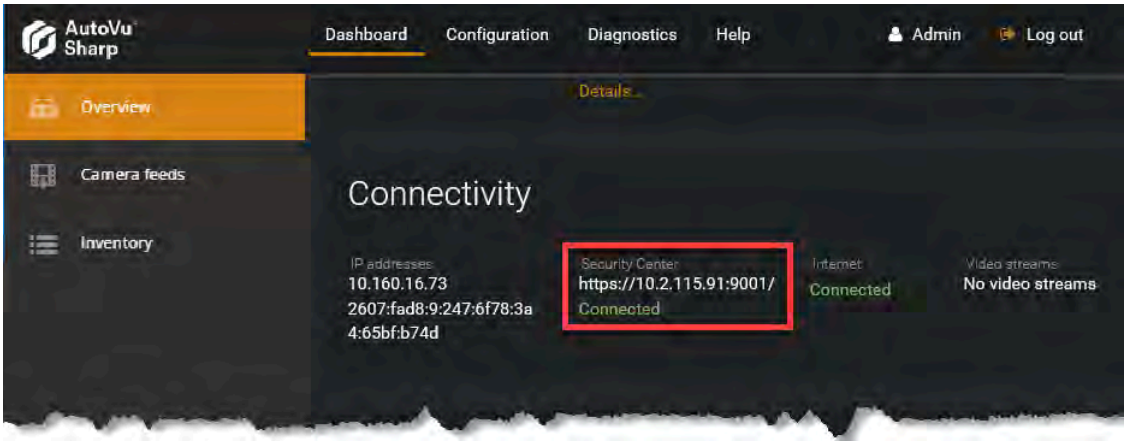
10 Click **Next**.

11 Review the settings and click **Create**.

IMPORTANT: When using the LPM protocol, the Extension in the Sharp Portal is automatically set to *None*. Do not change the extension.

- The new camera is added under the selected ALPR Manager.

- In the following image, the `https://` address prefix indicates that the unit is connected to Security Center using the LPM protocol.



Related Topics

About port forwarding for SharpV cameras using the LPM protocol on page 76
About port forwarding for SharpV cameras using the Security Center (legacy) extension on page 79

Upgrading a SharpV to use the LPM protocol

The License Plate Management (LPM) protocol provides a Sharp camera with a secure and reliable connection to Security Center. When The LPM protocol is enabled on a Sharp camera, the protocol manages the camera's connection to the ALPR Manager role.

Before you begin

- Minimum SharpOS version: 12.7

  NOTE: If your SharpV was shipped with SharpOS 12.7 or later and you are manually adding the SharpV to Security Center, you do not need to upgrade it to use the LPM protocol.
- Minimum Security Center version: 5.8

What you should know

- After you upgrade your SharpV to 12.7 or later, you can still connect to Security Center using the **Active extension:** *Security Center (Legacy)* until you upgrade to the LPM protocol.
- If the LPM protocol is enabled on the camera, Security Center can only connect to the camera using the LPM protocol.
- If a camera uses the LPM protocol to connect to Security Center, the **Active extension** in the Sharp Portal is set to *Security Center (LPM protocol)*.
- You cannot revert the LPM protocol upgrade.

To upgrade a SharpV camera to use the LPM protocol:

1 From the Config Tool home page, click the *ALPR* task and select **Roles and units**.
2 Select the **ALPR Manager** role from the drop-down list.
3 Expand the list of cameras under the ALPR Manager and select the SharpV camera.

4 At the bottom of the screen, click **Unit** and select **Upgrade to LPM protocol**.

The *Upgrade to LPM Protocol* window opens.



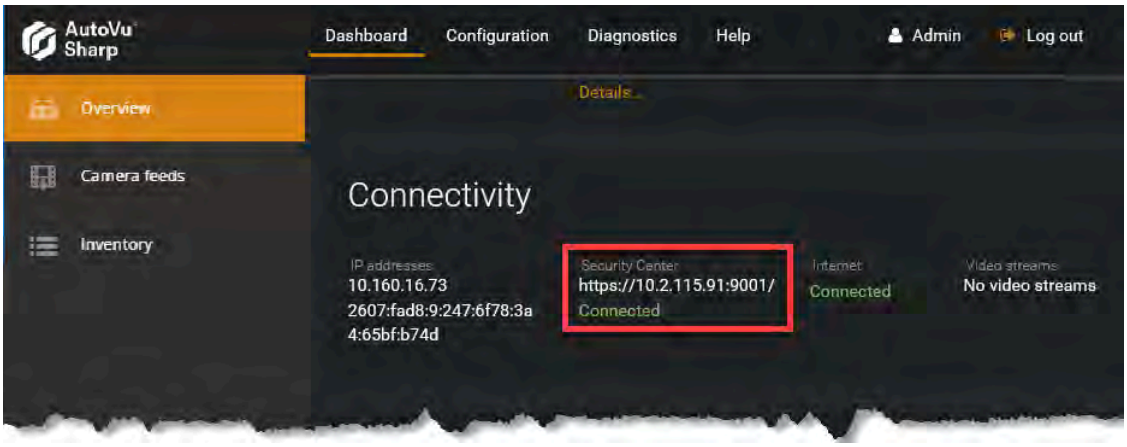
5 Enter the HTTPS **Port** of the unit (default = 443).

6 Click **Next**.

7 Enter the **Username** and **Password** used to log onto the Sharp Portal and click **Next**.

8 Review the settings and click **Upgrade**.

The Sharp Portal shows that the camera is connected to Security Center. The LPM protocol listening port (default = 9001) is appended to the IP address, indicating that the LPM protocol is managing the connection to Security Center.



About port forwarding for SharpV cameras using the LPM protocol

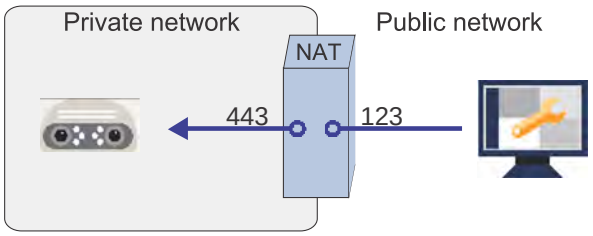
For SharpV cameras that use the LPM protocol to connect to Security Center, if either the SharpV or the ALPR Manager role is behind a Network address translation (NAT) device, additional configuration is required.

IMPORTANT: Consider the following when designing your system:

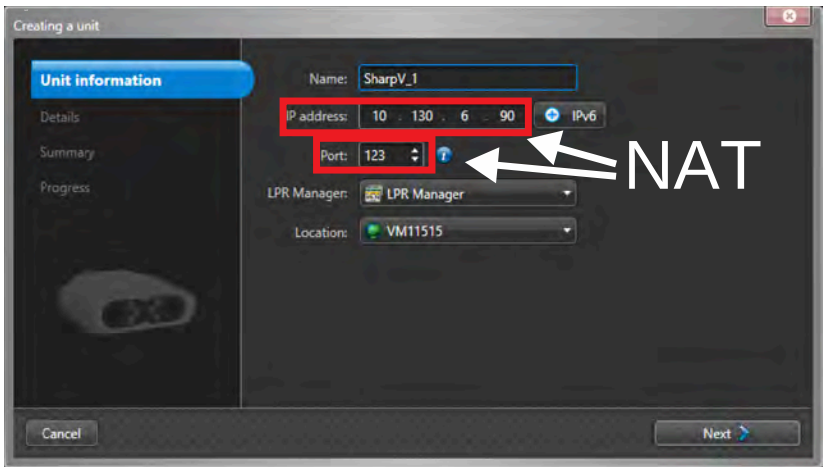
- If the SharpV camera or the ALPR Manager role are behind a NAT, it is not possible to configure a failover server.
- If you have a multi-server system where the Directory and the ALPR Manager roles are installed on different machines, it is not possible to configure NAT port forwarding for the ALPR Manager role.

The SharpV is behind a NAT

In this case, you must configure port forwarding to forward the port of the NAT to the IP address and port of the ALPR Manager. For example, if port 123 is available on the NAT, configure port forwarding to point to port 443 on the SharpV.

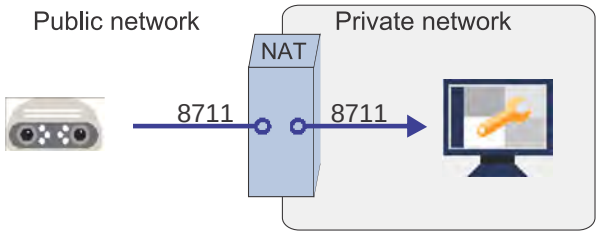


- When adding the SharpV to the ALPR Manager using the *Create a unit* wizard, enter the IP address and port of the NAT.

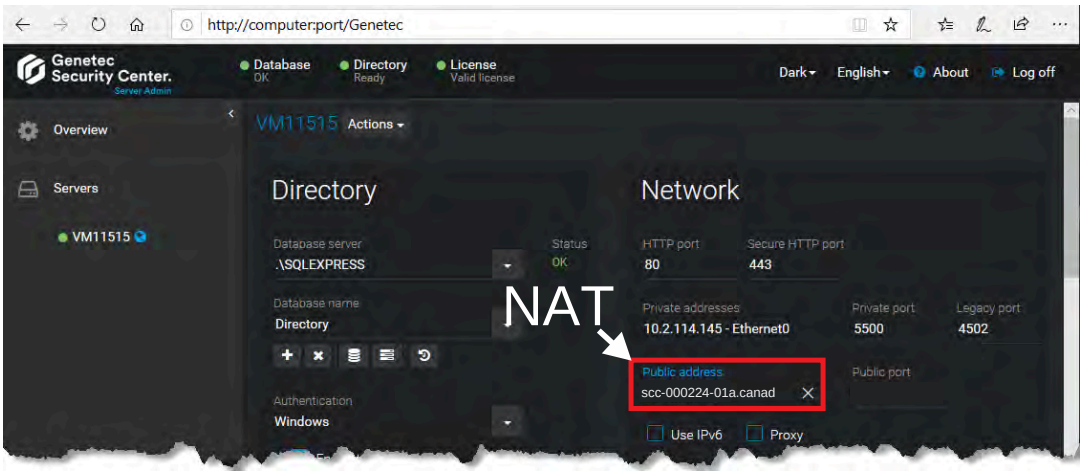


The ALPR Manager role is behind a NAT

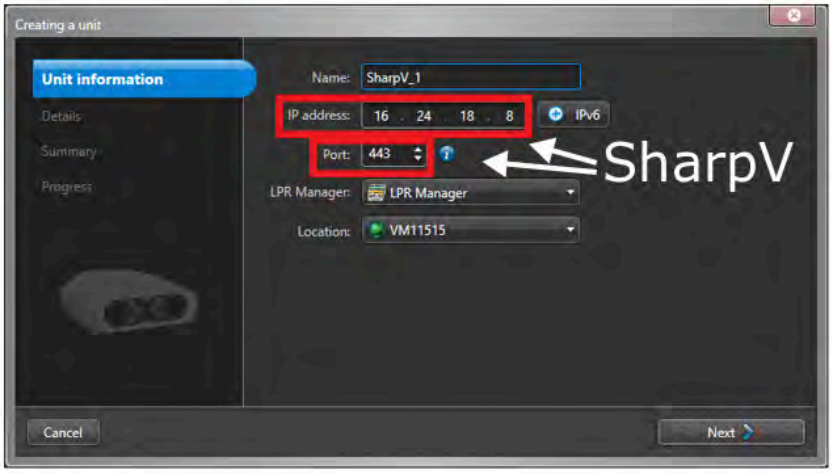
In this case, you must configure the ALPR Manager listening port to match the inbound port that is configured on the NAT. For example, if port 8711 is available on the NAT and the firewall rules have been configured accordingly, configure port forwarding to point to port 8711 on the ALPR Manager.



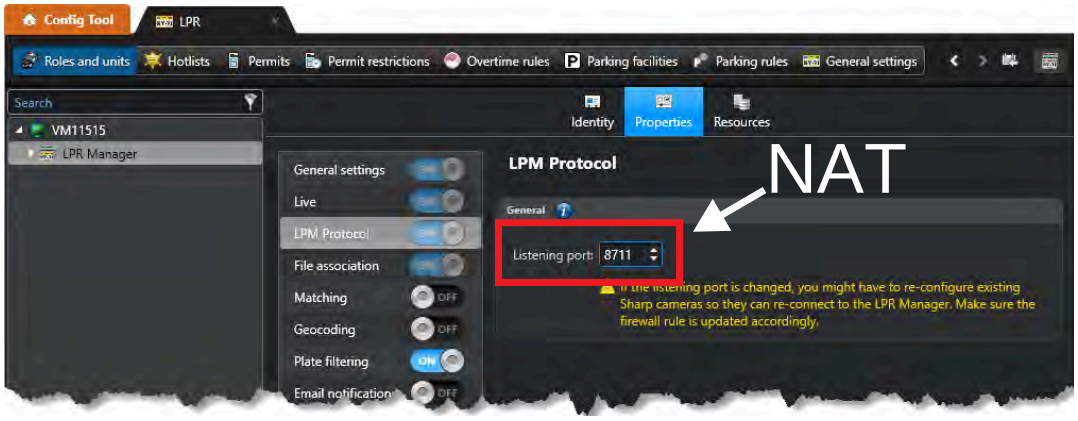
- In the Server Admin **Public address** field, enter the hostname or IP address.



- When adding the SharpV to the ALPR Manager using the *Create a unit* wizard, enter the IP address and port of the SharpV.



- Update the port that the ALPR Manager will be listening on. In this example where the NAT is configured to use port 8711, you would change the LPM protocol **Listening port** from the default port (9001) to port 8711.



Related Topics

Adding a SharpV camera to the ALPR Manager on page 72

SharpV camera connections to the ALPR Manager role

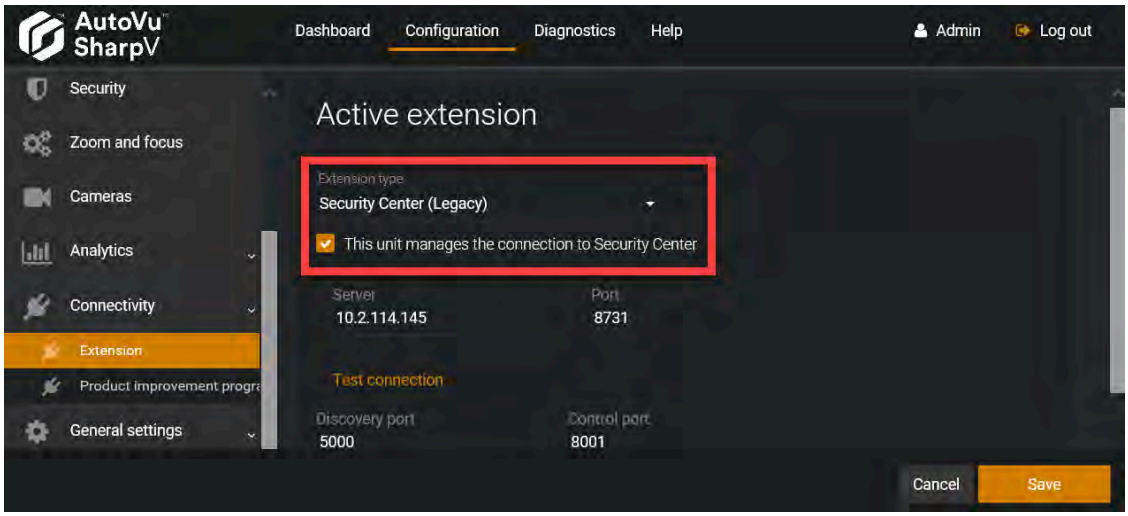
About port forwarding for SharpV cameras using the Security Center (legacy) extension

For SharpV cameras that use the Security Center (legacy) extension to connect to Security Center, if either the SharpV or the ALPR Manager role is behind a Network address translation (NAT) device, additional configuration is required.

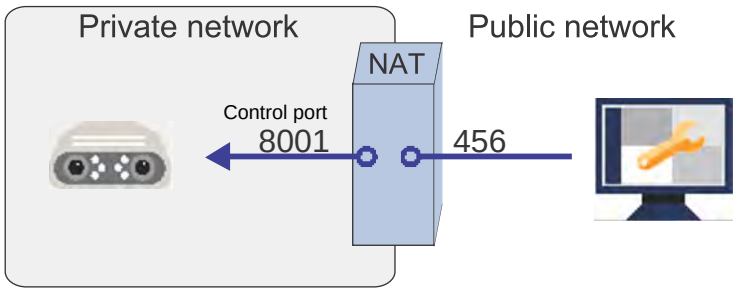
The SharpV is behind a NAT

- **If the SharpV manages the connection:**

  In this case, the SharpV connection to Security Center is forced using the **This unit manages the connection to Security Center** setting in the Sharp Portal.



  Configure port forwarding to forward the port of the NAT to the IP address and port 8001 (control port) of the SharpV.



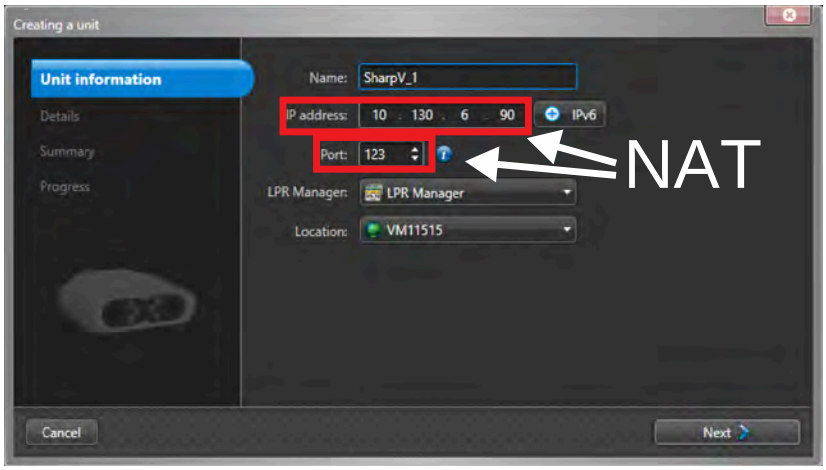
- **If the ALPR Manager role manages the connection:**

  The SharpV does not support the legacy extension when the ALPR Manager role manages the connection.

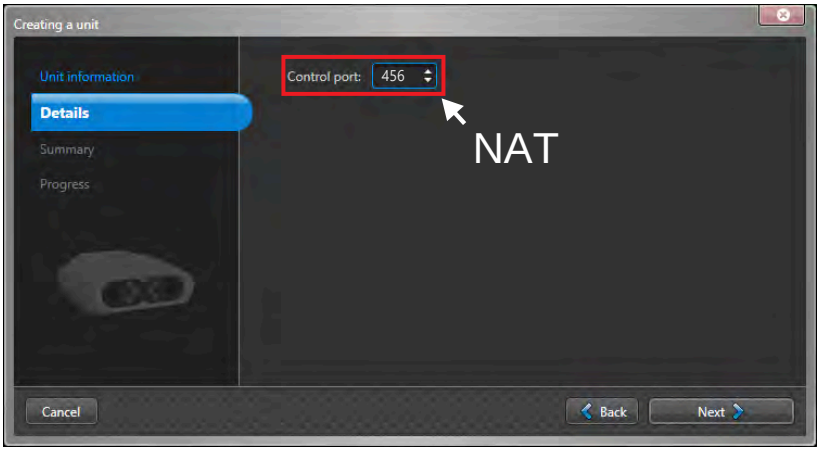
- When adding the SharpV to the ALPR Manager using the *Create a unit* wizard, enter the IP address and port of the NAT.

  NOTE: The **Port** in this screen corresponds to the port the SharpV is configured to listen to for HTTP traffic. By default, legacy SharpV cameras listen for HTTP traffic on port 80, however if you have

configured the device to use HTTPS, it will be listening for HTTP traffic on port 443. In such a case, you must configure the NAT to port forward HTTP traffic to port 443 instead of port 80.

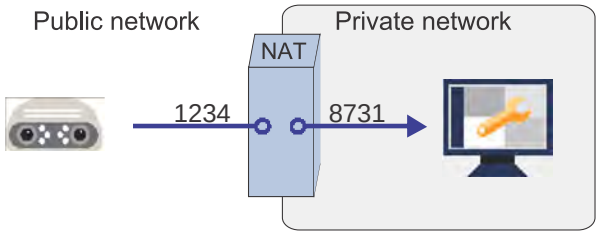


In the *Details* page, enter the port of the NAT that is configured to port forward to the control port (8001).

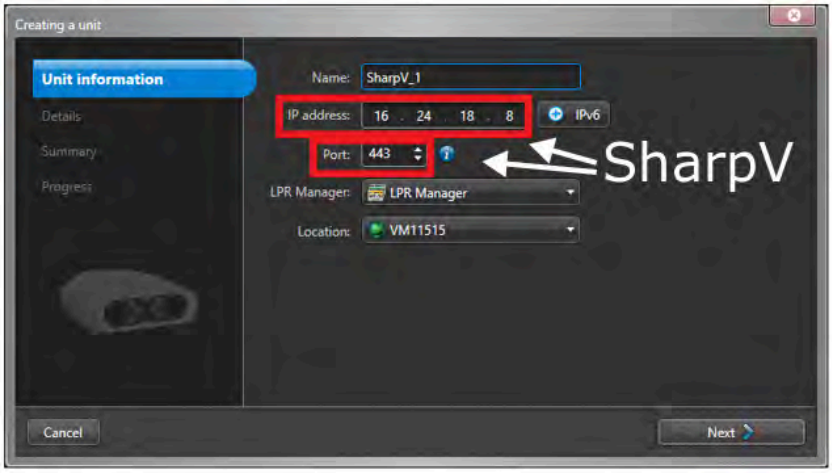


The ALPR Manager role is behind a NAT

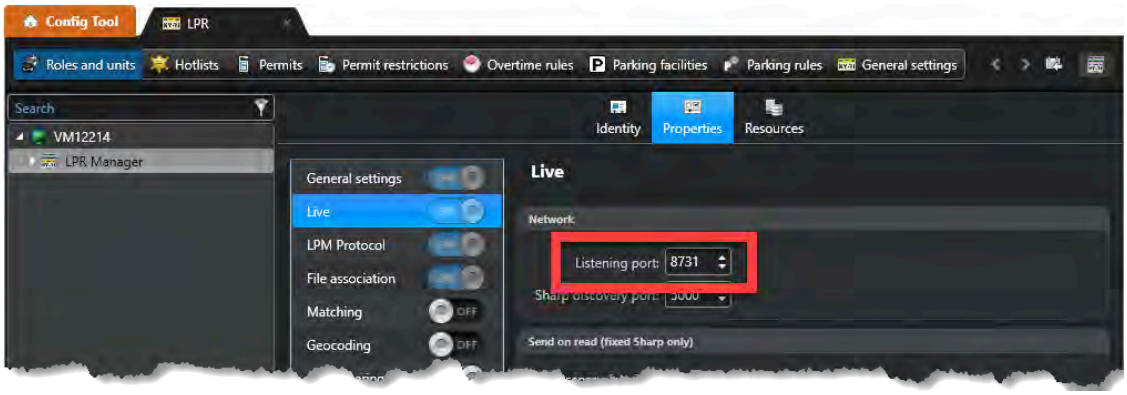
In this case, you must configure port forwarding to point to the listening port of the ALPR Manager. For example, if port 1234 is available on the NAT, configure port forwarding to point to port 8731 (listening port) on the ALPR Manager.



- When adding the SharpV to the ALPR Manager using the *Create a unit* wizard, enter the IP address and port of the SharpV.



- The listening port is defined in the **Live** settings on the ALPR Manager's *Properties* tab.



Related Topics

Adding a SharpV camera to the ALPR Manager on page 72
SharpV camera connections to the ALPR Manager role

Adding a SharpV camera to the Archiver

To store the ALPR images that are associated with the reads and hits, you must add the Sharp camera to the Archiver.

Before you begin

- Set up the Archiver role for ALPR. For more information, see the *Security Center Administrator Guide*.
- Log on to the camera's web portal and change the default password.

  NOTE: You cannot use the default SharpV credentials when adding the camera to the Archiver.
- By default, SharpV cameras are in DHCP mode. To add the context camera to the Archiver, you must configure the camera to use a static IP address that is defined in the web portal.
- By default, SharpV units include a self-signed certificate that uses the common name of the SharpV (for example, SharpV12345). To add the SharpV to the Archiver, you must generate a new certificate (signed or self-signed) that uses the camera's IP address instead of the common name.

What you should know

- By default, the Archiver uses the H.264 stream from SharpV cameras. If you want to use the MJPEG stream, you can select it in the *Video* task from the SharpV camera's screen.
- Information on context cameras is not applicable to SharpV ITS cameras.

To manually add a camera to a Security Center Archiver:

1 From the Config Tool home page, open the *Video* task.

2 Click **Add an entity** > **Video unit**.

The *Manual add* dialog box opens.

3 If you have multiple Archiver roles, select one to manage the unit from the **Archiver** drop-down list.

4 From the **Manufacturers** drop-down list, select **AutoVu™**.

5 From the **Product type** drop-down list, select **All**.

6 Enter the **IP address** of the video unit.

- Select **IPv4** or **IPv6** and enter the **IP address**.
- If your network supports DHCP, enter the assigned **IP address**.

  NOTE: If this address is subject to change, click **Hostname** to enter the hostname of the unit.

To add multiple units in a single operation, enter a range ( ) of IP addresses .

7 Enter the **HTTP port** for the unit (default = 80).

NOTE: If the unit uses HTTPS, enter the HTTP port (80) here. You will enter the HTTPS port in the following steps.

8 Select the **Authentication** method for the camera.

- **Default logon:** The camera uses the default logon defined for the Archiver in the *Extensions* tab. Using this method, you can define the same logon credentials for multiple cameras.

  IMPORTANT: You cannot use the default logon when adding a SharpV camera. You must use the credentials you configured when you first logged on to the SharpV portal.
- **Specific:** Enter the logon credentials for the camera. Turn on **Use HTTPS** if you have applied a certificate.

  NOTE: Sharp cameras running SharpOS 12.7 or later must use HTTPS communication.

9 From the **Location** drop-down, assign the camera to an area entity.

10 Click **Add**.



The notification tray displays the message "Adding unit started". If successful, it displays the message "Unit added successfully".

The camera is added under the selected Archiver.

Configuring the SharpV FTP extension

You can configure the SharpV to send ALPR data to an FTP server. ALPR data that is sent to an FTP server can then be integrated by third-party applications.

What you should know

You can only configure one extension for the SharpV camera.

To configure the SharpV for FTP:

1 Log on to the Sharp Portal.
2 From the **Configuration** menu, select the **Connectivity > Extension** page.
3 From the **Active extension** section, select **FTP** from the **Extension type** drop-down menu.
4 Configure the following:

- **Server:** Enter the FTP server name and location for the ALPR data. You'll need the server name, port number (if different than the standard FTP server port 21), and the name of the folder. For example, *ftp://<ServerName>:<PortNumber>/<FolderNameOnServer>/*.
- **Username:** Enter the username for the FTP server.
- **Password:** Enter the password for the FTP server.
- **Content Template:** ALPR data is sent in XML format, using the template shown. You can change certain elements if you choose.
- **Export context images:** Export the context image (in JPEG format).

NOTE: Information on context images is not applicable to SharpV ITS cameras.

- **Export ALPR images:** Export the plate image (in JPEG format).
- **Retain data when the connection is lost:** If the check box is selected, plate read events are saved locally in the SharpV's database if the connection with the FTP server is lost. The SharpV can store up to 20 000 plate read events, however, note that event size varies based on the complexity of the scene being observed. The system tries to re-connect with the server every 30 seconds. Stored reads are pushed to the server when the connection is re-established. If the check box is cleared, the SharpV does not store reads locally if the connection with the FTP server is lost. You can see how many reads are stored on the SharpV in the *Dashboard* > *Overview* > *Storage and usage* section.

  NOTE: If there are any plate reads in the SharpV's database, clearing this check box and saving the configuration deletes the plate reads.

5 Click **Test connection** to test the connection to the FTP server.
6 Click **Send sample** to send a test plate to verify that the system can connect to the server using these settings.
7 Click **Save**.

Modifications you can make to the SharpV FTP XML template

The XML code defines the structure of the XML files generated by the SharpV. You can re-sort or remove any of the fields. The XML file name consists of the SharpV name and a unique identification number (for example, SHARPV12345_6ee17b00-82c1-466b-9fd6-003417bc82c4_lpr.xml).

Template:

```
<?xml version="1.0" encoding="utf-8"?>
<AutoVu>
   <Plate>#PLATE_READ#</Plate>
   <State>#CUSTOM_FIELDS#{State Name}</State>
   <UTCDate>#DATE_UTC#{yyyy:MM:dd}</UTCDate>
```

```
   <UTCTime>#TIME_UTC#{HH:mm:ss.fff}</UTCTime>
   <CameraName>#CAMERA_NAME#</CameraName>
   <SourceName>#SHARP_NAME#</SourceName>
   <ContextImage>#CONTEXT_IMAGE#</ContextImage>
   <PlateImage>#PLATE_IMAGE#</PlateImage>
   <LongitudeX>#LONGITUDE#</LongitudeX>
   <LatitudeY>#LATITUDE#</LatitudeY>
   <Guid>#GUID#</Guid>
</AutoVu>
```

Note the following:

- Hotlist matching is not supported.
- `LocalDate, LocalTime, UTCDate, UTCTime,` and `TimeZone` display the Windows date and time properties.
- `CameraName` is set in the Genetec Patroller™ Config Tool.
- `SourceName` is the SharpV name (e.g. Sharp12345).
- `ContextImage` and `PlateImage` are encoded into text.

  NOTE: Information on context images is not applicable to SharpV ITS cameras.
- `Guid` is the unique identification of the event read.
- If using FTP with GPS coordinates, you'll need to add longitude and latitude fields.
- You can add the following custom fields to the template:
  - **Confidence score:** The Sharp assigns a confidence score percentage to each license plate read. This value indicates how confident the Sharp is in the accuracy of the read. You can add the confidence score associated with the plate read to the XML using the following field:

    `<ConfidenceScore>#CUSTOM_FIELDS#{Confidence Score}</ConfidenceScore>`
  - **Lane:** If dual-lane monitoring is configured for the Sharp, you can add the lane name associated with the plate read to the XML using the following field:

    `<Lane>#CUSTOM_FIELDS#{Lane}</Lane>`
  - **Relative Motion:** When the Sharp reads a plate, it detects and displays if the vehicle is approaching or moving away. To use this field, add the following line to the XML:

    `<RelativeMotion>#CUSTOM_FIELDS#{Relative Motion}</RelativeMotion>.`
  - **Speed:** For systems that include a fixed Sharp camera, you can configure the camera to export the vehicle's estimated speed. You can add the speed of the vehicle associated with the plate read to the XML using the following field:

    `<Speed>#CUSTOM_FIELDS#{Speed}</Speed>`
  - **State Name:** The Sharp attempts to read the plate's origin in addition to the plate number (some plates include the issuing state or province). This may not be possible for all types of license plates. To use this field, add `<State>#CUSTOM_FIELDS#{State Name}</State>` to the XML, and then select *State* on the **Analytics** page of the **Configuration** menu in the Sharp Portal.

    NOTE: The ALPR context you are using must support the state name feature.
  - **Vehicle Type:** Certain license plates include character symbols that identify specific vehicle types (for example, taxi, transport, and so on). If the Sharp can read these symbols, it displays the vehicle type along with the other read and hit information. To use this field, add the following line to the XML:

    `<VehicleType>#CUSTOM_FIELDS#{Vehicle Type}</VehicleType>.`

Example

```
<?xml version="1.0" encoding="utf-8"?>
<AutoVu>
   <Plate>#PLATE_READ#</Plate>
   <LocalDate>#DATE_LOCAL#{HH:mm:ss}</LocalTime>
   <UTCDate>#DATE_UTC#{yyyy:MM:dd}</UTCDate>
   <UTCTime>#TIME_UTC#{HH:mm:ss.fff}</UTCTime>
   <TimeZone>#TIME_ZONE#</TimeZone>
   <CameraName>#CAMERA_NAME#</CameraName>
```

```
   <SourceName>#SHARP_NAME#</SourceName>
   <ContextImage>#CONTEXT_IMAGE#</ContextImage>
   <PlateImage>#PLATE_IMAGE#</PlateImage>
   <LongitudeX>#LONGITUDE#</LongitudeX>
   <LatitudeY>#LATITUDE#</LatitudeY>
   <Guid>#GUID#</Guid>
</AutoVu>
```

Configuring the SharpV HTTP extension

You can configure the SharpV to send ALPR data to an HTTP server instead of to Security Center. ALPR data that is sent to an HTTP server can then be integrated by third-party applications.

What you should know

You can only configure one extension for the SharpV camera.

To configure the SharpV for HTTP:

1 Log on to the Sharp Portal.
2 From the **Configuration** menu, select the **Connectivity > Extension** page.
3 From the **Active extension** section, select **HTTP** from the **Extension type** drop-down menu.
4 Configure the following:

- **Server:** Enter the URL of the server that receives the ALPR data. For example, *https://address:port/path/*. Both *http://* and *https://* are supported.
- **Format:** Select the format you want to send the ALPR data in. You can select either **JSON** or **XML** format.
- **Username:** Enter the username for the HTTP server (basic authentication).
- **Password:** Enter the password for the HTTP server (basic authentication).
- **Export context images:** Export the context image (in JPEG format).

NOTE: Information on context images is not applicable to SharpV ITS cameras.

- **Export ALPR images:** Export the plate image (in JPEG format).
- **Retain data when the connection is lost:** If the check box is selected, plate reads are saved locally in the SharpV's database if the connection with the HTTP server is lost. The SharpV can store up to 20 000 plate read events, however, note that event size varies based on the complexity of the scene being observed. The system tries to re-connect with the server every 30 seconds. Stored reads are pushed to the server when the connection is re-established. If the check box is cleared, the SharpV does not store reads locally if the connection with the HTTP server is lost. You can see how many reads are stored on the SharpV in the *Dashboard* > *Overview* > *Storage and usage* section.

  NOTE: If there are any plate reads in the SharpV's database, clearing this check box and saving the configuration deletes the plate reads.
- **Anonymize ALPR data:** The camera *hashes* the license plate using the SHA-1 algorithm. When you add an alphanumeric *salt (cryptography)* to the license plate number, it increases the security of the hashed output. Adding the same salt on all of the cameras in a network means that the same license plate produces an identical hash on all cameras. This allows the external system to recognize the identical hashes as a the same vehicle while still maintaining privacy.

  IMPORTANT: If the salt is changed after it is set, it must also be changed on all other cameras. Changing the salt breaks the link between old reads and new reads.
- **Ignore certificate errors:** Select this option when sending ALPR data to an HTTPS server that does not have a trusted certificate. The SharpV will not send the ALPR data to an HTTPS server that does not have a trusted certificate unless you select this option.

5 Click **Send sample** to send a test plate to verify that the system can connect to the server using these settings.
6 Click **Save**.

Examples of JSON and XML ALPR events for the SharpV HTTP extension

When you send ALPR data to an HTTP server, you can configure the SharpV system to send the data in XML or JSON format.

JSON format sample:

The following is an example of a license plate read event in JSON format.

NOTE: The binary image data has been removed from the example.

```
{ "ContextCameraName" : "Context Camera",
  "ContextImage" : "",
  "Id" : "32cf870a-46aa-4cfd-914b-00062d98e93a",
  "Latitude" : 0.0,
  "Longitude" : 0.0,
  "LprCameraName" : "Lpr Camera",
  "PlateAnalytics" : [ { "Key" : "State Name",
        "Score" : -1.0,
        "Value" : "-"
      },
      { "Key" : "Vehicle Type",
        "Score" : 1.0,
        "Value" : "-"
      },
      { "Key" : "Relative Motion",
        "Score" : -1.0,
        "Value" : "-"
      },
      { "Key" : "Context",
        "Score" : 1.0,
        "Value" : "US"
      },
      { "Key" : "Characters Height",
        "Score" : 1.0,
        "Value" : "70"
      }
    ],
  "PlateImage" : "",
  "PlateRead" : "AA7D2",
  "SourceUrl" : "SHARPV12345",
  "Timestamp" : "2016-08-29T08:42:45.797"
}
```

XML format sample:

The following is an example of a license plate read event in XML format.

NOTE: The binary image data has been removed from the example.

```
<Plate>
  <ContextCameraName>Context Camera</ContextCameraName>
  <ContextImage/>
  <Id>32cf870a-46aa-4cfd-914b-00062d98e93a</Id>
  <Latitude>0.0</Latitude>
  <Longitude>0.0</Longitude>
  <LprCameraName>Lpr Camera</LprCameraName>
  <PlateAnalytics>
    <PlateAnalytics>
      <Key>State Name</Key>
      <Score>-1.0</Score>
      <Value>-</Value>
    </PlateAnalytics>
    <PlateAnalytics>
      <Key>Confidence Score</Key>
      <Score>1</Score>
    <Value>100</Value>
```

```
    </PlateAnalytics>
  </PlateAnalytics>
  <PlateImage/>
  <PlateRead>AA7D2</PlateRead>
  <SourceUrl>SHARPV12345</SourceUrl>
  <Timestamp>2016-10-21T21:35:04.8627622+00:00</Timestamp>
</Plate>
```

Plate read event parameters

The following parameters are included in JSON and XML files that are exported to the HTTP server:

Parameter	Value type	Description
ContextCameraName	String	Name of the color context camera that generated the read event. **NOTE:** Information on context cameras is not applicable to SharpV ITS cameras.
ContextImage	Binary	Color context image of the scene. Base64 encoded JPEG image. **NOTE:** Information on context images is not applicable to SharpV ITS cameras.
Id	Guid	Unique identifier for the read event.
Latitude	Double	Decimal latitude of the SharpV camera.
Longitude	Double	Decimal longitude of the SharpV camera.
LprCameraName	String	Name of the license plate recognition camera that generated the read event.
PlateAnalytics	Array of analytics	Each analytic object is composed of a data triplet. This array is of variable size. The amount of analytic objects received depends on the SharpV camera's configuration.
Key (analytic triplet)	String	Name of the analytic.
Score (analytic triplet)	Float (-1.0 or 1.0)	Indicates if the analytic value is reliable (1.0) or not (-1.0).
Value (analytic triplet)	String	Value of the analytic.
PlateImage	Binary	Black and white cropped license plate image. Base64 encoded JPEG image.
PlateRead	String	Detected license plate number.
SourceUrl	String	Unique name of the SharpV camera.
Timestamp	DateTime	Date and time of the read event (UTC) in the following format: yyyy-MM-ddTHH:mm:ss:fff.

Configuring Syslog for SharpV log files

For installations that include multiple SharpV cameras, the *Syslog* feature allows you to configure a central repository for all SharpV log entries.

Before you begin

- You will need a Syslog server that is accessible by the SharpV camera.

What you should know

- The SharpV syslog feature is compliant with the RFC 5424 protocol.
- Whether you use the Syslog feature or not, SharpV logs will be available on Sharp Portal's *Diagnostics* > *Logs* page.

To configure a repository for SharpV log files:

1 Log on to the Sharp Portal.
2 From the **Configuration** menu, select the **General settings > Recovery** page.
3 Select the **Use Syslog server** checkbox.
4 In the **Server** field, enter the address of the server.

NOTE: Syslog server configurations do not support IPv6 addresses.

5 In the **Port** field, enter the port.
6 From the **Network Protocol** drop-down, select UDP or TCP.
7 Click **Test connection** to test the connection.
8 Click **Save**.

4

Upgrade

This section includes the following topics:

- "Supported SharpOS update paths" on page 92
- "Updating a Sharp unit from the Sharp Portal" on page 93
- "Updating the SharpV Platform from the Sharp Portal" on page 95

Supported SharpOS update paths

To update SharpOS, you must follow the required update path for the current software version of your Sharp unit.

SharpV update paths

Current SharpOS version	Update path
SharpOS 12.0 or higher	Download the *.zip* file and update to SharpOS 13.2.

SharpZ3 update paths

Not supported: SharpOS 13.2 is for SharpV camera units only.

Updating a Sharp unit from the Sharp Portal

To benefit from the most recent security improvements, it is recommended to upgrade the unit's SharpOS and platform software from the Sharp Portal.

Before you begin

- Ensure you are following the correct upgrade path for the Sharp unit. For more information, see Supported SharpOS update paths on page 92.

What you should know

- **IMPORTANT:** When the SharpOS is updated, all plate reads that are stored locally on the SharpV are deleted.
- You can update the Sharp unit's platform package or SharpOS package.
  - **Platform package:** Updates Windows 10 with the latest security patches.
  - **SharpOS package:** Updates the SharpOS installed on the Sharp.

    IMPORTANT:

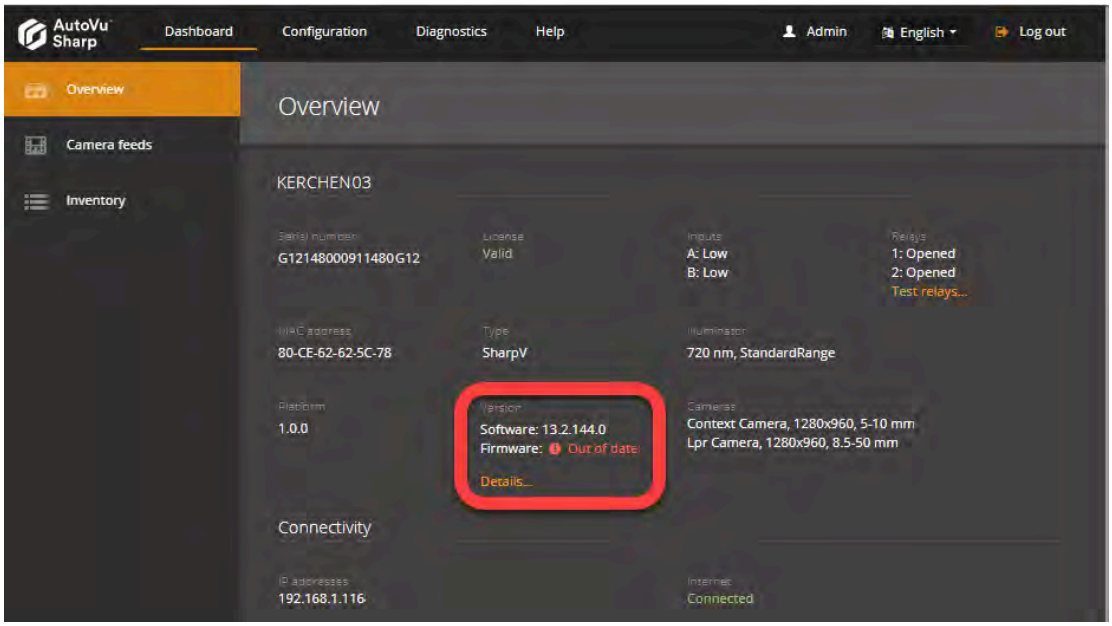
    - When the SharpOS is updated, all plate reads that are stored locally on the Sharp unit are deleted.
    - If you need to update both the SharpOS software and the platform software, update the SharpOS first.

To update the unit's SharpOS or platform package:

1 Log on to the Sharp Portal.

2 To verify that the firmware needs to be updated, click **Dashboard** > **Overview**. If **Firmware** shows the message *Out of date*, continue with the update steps.

The following example shows a SharpV unit that can be updated to a more recent SharpOS version.



3 Download the update package from GTAP. Save the *.gpack* file on the local machine you are using to log on to the Sharp Portal.

4 From the **Configuration** menu, select **Maintenance**.

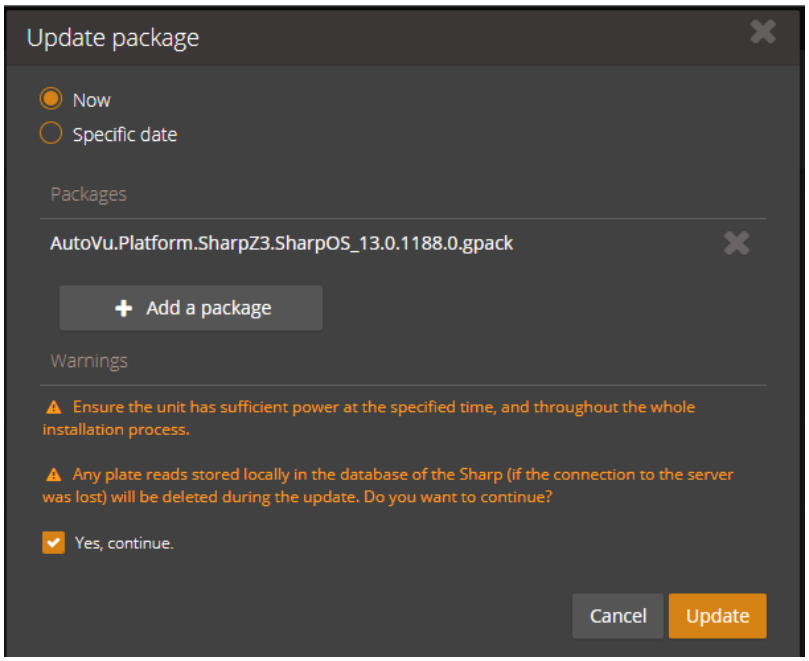
5 In the *Packages* section, click the **Update** button for the SharpOS.

6 In the *Update package* dialog box, choose when to run the update.
   - Click **Now** to run the update immediately.
   - Click **Specific date** to schedule the update for off-peak hours.

7 Click **Add a package**, find the update *.gpack* file, and then click **Open**.

8 Acknowledge the warnings and click **Update** or click **Schedule** if you set a specific date for the update.

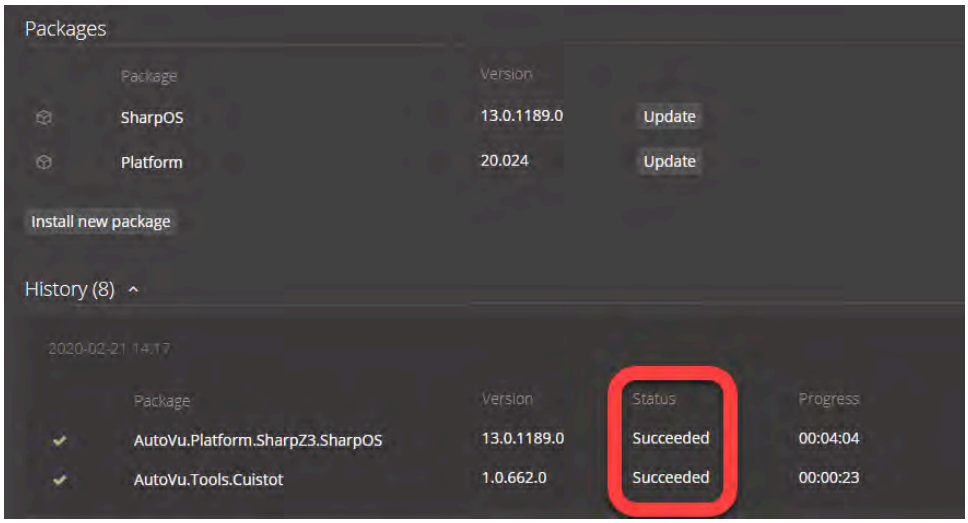
IMPORTANT: Whether you configure the update for **Now** or for a **Specific date**, the package is transferred to the Sharp unit immediately. Do not close or navigate away from the browser page until the transfer is complete.



The files are transferred to the Sharp unit and the update process begins.

NOTE: At certain points in the update process, the progress bar might not move for several minutes. It can take up to 30 minutes to complete the update.

If the update is successful, the new platform version is displayed and the **History** displays that the update *Succeeded*.



Updating the SharpV Platform from the Sharp Portal

To benefit from the most recent security improvements, it is recommended to upgrade the unit's platform software from the Sharp Portal.

Before you begin

- If you need to update the SharpOS software as well as the SharpV platform software, update the SharpOS first.
- SharpV platform update packages are available from GTAP. Save the *AutoVu.Platform.SharpV.Platform_XX.XXX.X.gpack* file on the local machine you are using to log on to the Sharp Portal.

What you should know

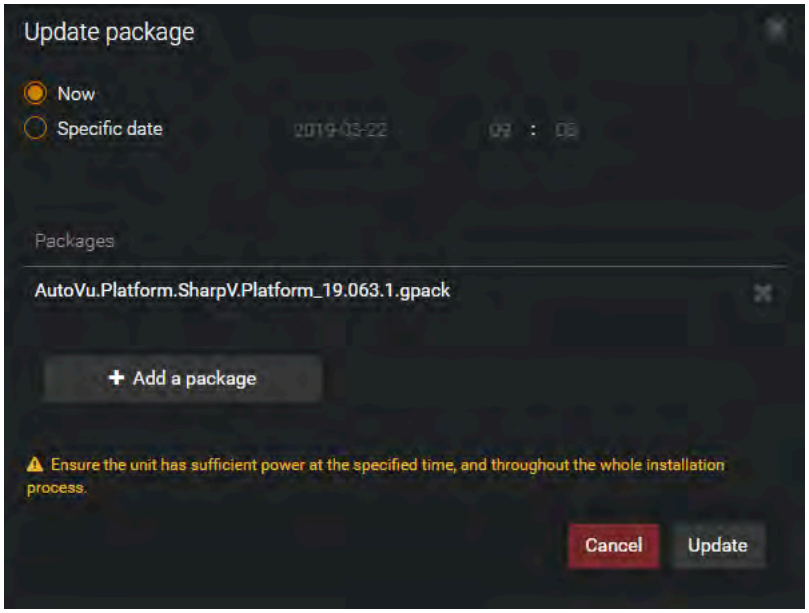
After you start the update, you cannot navigate away from the page without canceling the update.

To update the unit's platform version:

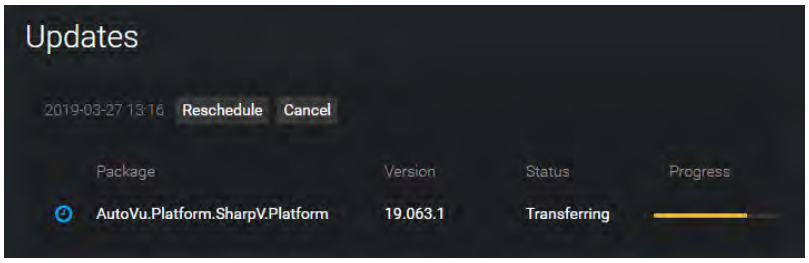
1 Log on to the Sharp Portal.
2 From the **Configuration** menu, select the **Maintenance** page.
3 From the **Packages** section, click the **Update** button for **Platform**.

NOTE: If you want to update the SharpOS and platform simultaneously, click **Install new package**.

4 In the **Update package** dialog box, choose to run the update **Now**, or click **Specific date** to schedule the update for off-peak hours.
5 Click **Add a package**, find the update *.gpack* file, and then click **Open**.

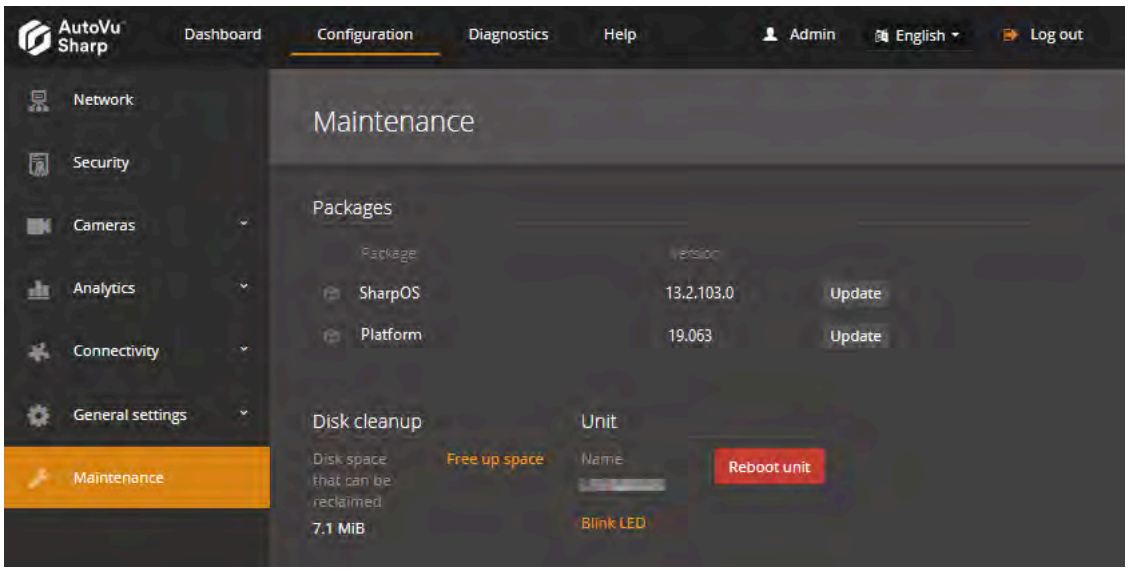


6 Click **Update** or **Schedule** if you set a specific date for the update).



The files are transferred to the SharpV.

When the update is finished, the new platform version is displayed.



5

Sharp Portal reference

This section includes the following topics:

- "Sharp Portal - Overview page" on page 98
- "Sharp Portal - Camera feeds page" on page 100
- "Sharp Portal - Inventory page" on page 102
- "Sharp Portal - Network page " on page 103
- "Sharp Portal - Security page" on page 104
- "Sharp Portal - Exposure page" on page 106
- "Sharp Portal - Position and orientation page" on page 107
- "Sharp Portal - ALPR settings page" on page 108
- "Sharp Portal - Extension page" on page 110
- "Sharp Portal - Product improvement program page" on page 112
- "Sharp Portal - Recovery page" on page 113
- "Sharp Portal - Date and time page" on page 114
- "Sharp Portal - Power options page" on page 115
- "Sharp Portal - Maintenance page" on page 116
- "Sharp Portal - Logs page" on page 117
- "Sharp Portal - Log sources page" on page 118

Sharp Portal - Overview page

This section lists the settings found in the *Overview* page of the Sharp Portal and provides general information about the SharpV, such as serial number, license, IP address, input and relay status, and so on.

To navigate to the *Overview* page, click **Configuration** > **Overview**.

Camera info

The following information is displayed:

- **Serial number:** Displays the SharpV hardware serial number.
- **License:** Displays whether the SharpV license is valid, invalid, or missing.
- **Inputs:** Displays the inputs on the SharpV and whether the input is in a **High** or **Low** state. A high-state input is indicative of a voltage of 5.75 V or higher. A low-state input is indicative of a voltage of 4.80 V or lower.
- **Relays:** Displays the SharpV relays and whether the relay state is **Opened** or **Closed**. The SharpV has two 0.25 A solid-state relays and two 8 A electromechanical relays.
- **Test relays:** Click to toggle your configured relay between **Opened** and **Closed** to validate the configuration.
- **Mac address:** Displays the MAC address of the SharpV. This information might be requested if you contact technical support.
- **Type:** Displays the type of Sharp unit.
- **Illuminator:** Displays the camera's LED wavelength and range option.
- **Platform:** Displays the software image installed on the SharpV. If you contact technical support, you might be asked to provide this number.
- **Version:**
  - **Software:** Displays the SharpOS version currently installed.
  - **Firmware:** Displays the update status of the Sharp unit.
  - **Details:** Provides additional information about the versions of the files and components included in the package.

  Displays the SharpOS package version. You can use this information to confirm that your SharpV is up to date.
- **Cameras:** Select which of the two SharpV camera feeds to display.

  NOTE: Information on context cameras is not applicable to SharpV ITS cameras.
- **Location:** Displays the coordinates of the SharpV camera: the camera's position must be configured in Security Center. Click **Locate on map** to display the camera's position on a map.

Connectivity

The following information is displayed:

- **IP addresses:** Displays the IPv4 and IPv6 addresses of the SharpV.
- **Internet:** Displays whether the SharpV is connected to the Internet.
- **Video streams:** If the SharpV has been added to the Security Center Archiver and is being used to monitor video, then the camera name, client IP address, frame rate, and encoding format are listed for each stream.

Storage and usage

You can view information about reads stored on the SharpV, CPU usage, and memory usage. Indicator lines, usually green or orange, are provided so you can see the status. If an indicator line stays red for a prolonged period of time, it indicates either high CPU activity or that there is a problem.

- **Reads stored:** Indicates the reads stored in the database of the SharpV. The number of reads is also displayed.
- **Memory:** Displays information on the system's RAM memory.
- **CPU (Total):** Indicates the total CPU usage of the SharpV. Click **Show details** to see the usage for each CPU.

Last activities

- **Unit rebooted:** Indicates the last time the unit was restarted.
- **Software restarted:** Indicates the last time the PlateReader software was restarted.

Sharp Portal - Camera feeds page

This section lists the settings found in the *Camera feeds* page of the Sharp Portal. Use the *Camera feeds* page to view the live feeds of the context camera and ALPR camera.

NOTE: Some of the fields described in this section do not apply to auxiliary cameras.

To navigate to the *Camera feeds* page, click **Dashboard** > **Camera feeds**.

Camera feeds

The **Camera feeds** section displays the live video feeds for both the Context camera and the ALPR camera. You can also view information about the live video feed such as the **FPS**, **Resolution**, **Exposure time**, and so on.

NOTE: Some of the fields described in this section do not apply to auxiliary cameras.

NOTE: Information on context cameras is not applicable to SharpV ITS cameras.

Videos

- **Camera unit:** The SharpV camera unit *ALPR camera unit 1* is displayed.
- **Cameras:** Select which of the two SharpV camera feeds to display.

  NOTE: Information on context cameras is not applicable to SharpV ITS cameras.
- **Overlays:**
  - **Crosshairs:** Select this option to display crosshairs in the ALPR or context camera window.
  - **Bounding box:** Select this option to display the yellow bounding box around detected plates in the ALPR camera window.
  - **Region of interest:** A region of interest limits plate detection to a specific part of the field of view. This can be used to ensure that the system focuses on the best region to capture plates or to exclude plates passing in certain regions.
- **Record:** Click the **Record** button to capture a series of context and ALPR images directly from the *Camera feeds* window and save them to your computer as a .zip file for debugging purposes.

  NOTE:
  - Using the **Record** feature increases CPU usage.
  - To use this feature, you cannot use the camera's auto-generated certificate. You must install a self-signed certificate that includes the IP address of the camera.

Metadata

- **FPS (actual/average):** Displays the FPS of the context camera. This is the framerate processed by the ALPR engine.
- **Resolution:** Displays the resolution of the camera's video feed.
- **Exposure time:** Displays the **Exposure** time of the video frame.
- **Gain:** Displays the **Gain** of the video frame.
- **Iris:** Displays the **Iris** aperture of the video feed as a percentage.
- **Illuminator:** (Context camera only) Displays the intensity of light of the illuminator (as a percentage) on the Context camera.

Last reads

- **Candidate:** Every read detected is displayed in this field as a potential read candidate. The camera can read up to 30 frames (reads) per second. The **Read strategy** configured on the **Analytics** page determines which read candidate will be used as the final read.

NOTE:

- The list contains the reads that have been made in this portal session. Exiting the session resets the list.
- The list is of limited length and older reads are automatically removed.
- Clicking on an entry pauses the list. Clicking Play resumes the list refresh and adds new reads that were received while the list was paused.

Sharp Portal - Inventory page

This section lists the settings found in the *Inventory* page of the Sharp Portal. Use the *Inventory* page to view a list of hardware components along with their firmware versions and status.

To navigate to the *Inventory* page, click **Dashboard** > **Inventory**.

The following information is displayed:

NOTE: Additional functionality is available for certain hardware components, such as blinking the LED or connecting to a configuration portal.

- **Module:** Displays the name of the component.
- **Version:** Displays the component's firmware version.
- **Identification:** Displays a unique identifier of the component, such as its name or serial number.

  NOTE: The serial number is also printed on the component sticker.
- **Status:** Displays the health status of the component.

Sharp Portal - Network page

The *Network* page is available from the **Configuration** menu. Use the *Network* page to configure the SharpV to use Dynamic Host Configuration Protocol (DHCP) or a static IP address.

IPv4 network settings

NOTE: DHCP is used by default if no option is selected.

- **Use DHCP:** Select this option to connect the SharpV to a DHCP server, which assigns the required IP address. On a network with DHCP and DNS servers, you can connect to the SharpV using the SharpV name (for example, SharpV1234) rather than the IP address (for example, 192.168.10.100).
- **Use static IP address:** Select this option to use a static address for the SharpV.

  IMPORTANT: You must use a static IP address if you want to stream video to the Security Center Archiver role.
  You can modify the following:

  - **IP address:** Type the new IP address you want to assign to the SharpV. The default is 10.0.0.1.
  - **Subnet mask:** Type the new **Subnet mask** if applicable. The default is 255.255.0.0.
  - **Gateway:** Type the new **Gateway** if applicable. The default is 10.0.0.0.
  - **DNS:** Type the new **DNS** if applicable. The default is 10.0.0.0.

Sharp Portal - Security page

This section lists the settings found in the *Security* page of the Sharp Portal. Use the *Security* page to change the password and to manage certificates and permissions.

To navigate to the *Security* page, click **Configuration** > **Security**.

Access

- **Modify password:** Click **Modify password** to change the password for the SharpV.

  NOTE: If you forget your password, you can reset it from the logon page.

Certificate

Displays the signed and self-signed certificates that have been installed in the trusted root store of the SharpV. You can install multiple certificates and select which certificate to activate.

To activate a certificate, select the **Active** button for the certificate and click **Save and reboot**.

To delete a certificate click **X** and click **Save**.

NOTE: You can delete certificates, but you must leave at least one certificate on the SharpV.

- **+ Self-signed:** Click to create a self-signed certificate. In the *Create a self-signed certificate* dialog box, you must enter a two-letter **Country** code, the **Common name** of the SharpV, one or more **IP addresses**, and you must define the **Validity (in years)**. The other fields are optional.

  NOTE:

  - If you use a self-signed certificate, you must also install the certificate on your client machine. For example, the machine used to log on to the Sharp Portal.
  - If a certificate signature is issued by a certificate authority that is not included in the list of Windows of third-party root certificate authorities (CA), or if your organization has its own public key infrastructure (PKI) which manages signatures, you must add the CA to the platform software running on the SharpV so that the host can validate the chain of trust. For more information, see KBA-78971: Adding a certificate to a pre-12.8 SharpV from an unknown certificate authority on the Genetec™ TechDoc Hub.
- **+ Signing request:** Click to create a certificate signing request. A certificate signing request must be created for your server before you can order a signed certificate from a trusted Certificate Authority. You must enter a two letter **Country** code, the **Common name** of the SharpV, and the **IP address** in the *Create a certificate signing request* dialog box. The other fields are optional.

  IMPORTANT: If the SharpV has been added to the Security Center Archiver and is being used to monitor video, you must enter the IP address of the SharpV and not the SharpV name.

  NOTE: The signing request is deleted when the certificate is signed.

Permissions

- **Accept remote reboot requests:** Select this option so that the SharpV can be rebooted from Security Center.
- **Remote assistance:** Click **Enable for 1 hour** to grant remote access for technical support. The time and date when access expires is displayed. Click **Disable now** to end the remote assistance session.

  NOTE: After one hour, the remote assistance session ends. If the AutoVu™ Support team needs additional time to resolve the issue, you can extend the remote assistance session. An audible reminder alerts you if the RDP session will soon expire.

Unit

- **Run in covert mode:** Select this option to turn off the LED on the Sharp camera unit, making it less noticeable.

  IMPORTANT: Selecting this option does not mean that the LED will never be illuminated. For example, if there is a serious error with the SharpV, the LED will blink to indicate that there is a problem.

Sharp Portal - Exposure page

This section lists the settings found in the *Exposure* page of the Sharp Portal. Use the *Exposure* page to adjust the exposure of the license plates in the ALPR image.

To navigate to the *Exposure* page, click **Configuration** > **Cameras** > **Exposure**.

The following information is displayed:

- **Select your camera:** Select the camera to configure.
- **(Context camera only) Lighting type:** Select a lighting type from the menu.

  NOTE: Information on context cameras is not applicable to SharpV ITS cameras.
- **Lighting type:** Select a lighting type from the menu:
  - **Auto (Default):** Select this option to have the SharpV automatically adjust the lighting settings (white balance) according to the surroundings.
  - **Fixed (Sun):** Select this option if advised by the customer support team.
- **Exposure:** Choose from the following:
  - **Default:** Select this option to have the SharpV automatically adjust the exposure settings.
  - **Fixed (indoor):** Select this option when constant lighting conditions are available. Use the sliders to adjust the **Gain** and **Exposure time**, until the overall brightness and clarity you want for the image is achieved.
  - **Range (outdoor):** Select this option for variable lighting conditions outdoors. Use the sliders to adjust the **Gain** and **Exposure time**, until the overall brightness and clarity you want for the image is achieved.
- **(ALPR camera only) Click the picture to define region of interest:** Defining a region of interest restrict the readable area to a portion of the field of view as configured by the user. Define a region of interest by clicking points on the image to create a perimeter. Click **Clear the region of interest** to delete the region.
- **(Context camera only) Allow illuminator:** Select this to enable the IR illuminator in low light conditions. If **Exposure** is set to **Fixed (indoor)**, the IR illuminator is fixed to On or Off depending on **Allow illuminator** check box. If **Exposure** is set to **Range (outdoor)**, the illuminator is automatically turned On or Off depending on light conditions. However, the IR illuminator can be completely turned off by clearing the **Allow illuminator** check box.

  NOTE: Information on context cameras is not applicable to SharpV ITS cameras.

Sharp Portal - Position and orientation page

This section lists the settings found in the *Position and orientation* page of the Sharp Portal. Use the *Position and orientation* page to define SharpV camera positions on the patrol vehicle roof.

To navigate to the *Position and orientation* page, click **Configuration** > **Cameras** > **Position and orientation**.

The following information is displayed:

- **Enable:** When enabled, the system estimates the GNSS position of the license plate of the target vehicle.

Position

- **Left/right:** Define how far the camera is installed to the left (0 to -400 cm) or to the right (0 to 400 cm) of the GNSS antenna.
- **Rear/front:** Define how far the camera is installed to the rear (0 to -1000 cm) or to the front (0 to 1000 cm) of the GNSS antenna.
- **Below/above:** Define how far the camera is installed below (0 to -400 cm) or above (0 to 400 cm) the GNSS antenna.

Orientation

- **Pan:** Define how far the camera is panned to the left (-90°) or to the right (90°) from a straight forward view (0°).
- **Tilt:** Define how far the camera is tilted to the up (45°) or down (-45°) from a level installation (0°).
- **Roll:** Define how far the camera is rolled counter-clockwise (-45°) or clockwise (45°) from a level installation (0°).

Sharp Portal - ALPR settings page

This section lists the settings found in the *ALPR settings* page of the Sharp Portal Use the *ALPR settings* page to configure the analytics used for the license plates read by the SharpV.

To navigate to the *ALPR settings* page, click **Configuration** > **Analytics** > **ALPR settings**.

The following information is displayed:

Location

- **Context:** Select which plate origin the SharpV is reading.

Analytics:

- **State:** Select this option if you want the SharpV unit to attempt read the license plate origin. Depending on the region, this can refer to the issuing state, province, or country.
- **Vehicle make:** Select this option if you want the SharpV unit to attempt to read the vehicle's make from the brand or logo (Honda, Toyota, and so on).

  NOTE: This setting is not recommended for MLPI installations.
- **Confidence score:** The SharpV assigns a confidence score percentage to each license plate read. This value indicates how confident the SharpV is in the accuracy of the read.

  NOTE: License plates that contain similar characters such as *8* and *B* are more difficult to read and generally produce reads with a lower confidence score.
- **Vehicle type and color:** Select this option if you want to include the vehicle type and vehicle color with plate reads. Based on the context image, the Sharp unit can detect if the vehicle is a bus, passenger vehicle, motorcycle, pickup, truck, work van, or an unknown vehicle type. In addition, the Sharp unit can detect if the vehicle is black, white, blue, brown, green, gray, orange, red, or yellow. Colors excluding white and black are also assigned *light*, *neutral*, or *dark* according to the color analysis.

Reads

- **Reading mode:** Select one of the following reading modes:
  - **Continuous:** Select this for plates to be captured continuously. This is the default setting.
  - **Conditional:** When this option is selected, the SharpV captures plate reads continuously as long as the selected input signal meets the condition defined (high/low). You must select an input and specify whether the state is high or low.
  - **Continuous with virtual loop:** This option is automatically selected when you enable the virtual loop feature. With this option, a parking lot gate can still be activated for vehicles with damaged or dirty license plates which cannot be detected by the SharpV ALPR camera.
  - **Single read on trigger:** Select this option so the SharpV captures a plate read after a signal is received from an electrical trigger, or after a Security Center event-to-action or hot action. This configuration is useful for controlling vehicle access to gated parking lots. You can configure the plate read capture to occur before or after the trigger is activated.
  - **Add trigger:** Select to add a trigger. You must configure the following;

- **When**. Select which input receives the trigger signal and indicate the state of the input (**Low** or **High**). You can also select an **External** input (Security Center event to-action or hot action).
- **Capture Window**.
  - **Start X ms before/after trigger**. The capture can occur up to X ms before or after the trigger is activated.
  - **Duration X ms**. The system attempts to capture a plate read for up to 30000 ms. 4000 ms is the default value.
    IMPORTANT: The capture window cannot end before the time the trigger is activated.
- **If no plates**.
  - **Capture image X ms after trigger**. If no plate is read during the time specified in the **Capture window**, a "no plate" read is logged and the system captures a context image of the vehicle so the read can be manually edited.
  - **Use ALPR image as context image**. An image from the ALPR camera is used to replace the context image for the "no plate" read.
    NOTE: Information on context images is not applicable to SharpV ITS cameras.

Read strategy

- **Slow moving vehicle:** Select this when vehicles are traveling slowly when their license plates are read. For example, select this option to monitor parking lot entrances where you require fast plate read results. Note that you might notice duplicate plate reads with this strategy.
- **Fast moving vehicle:** Select this when vehicles are traveling at moderate to high speeds when the license plates are read. For example, select this option for a SharpV overlooking a highway.

Sharp Portal - Extension page

This section lists the settings found in the *Extension* page of the Sharp Portal. Use the *Extension* page to configure where the SharpV sends ALPR data.

To navigate to the *Extension* page, click **Configuration** > **Connectivity** > **Extension**.

The following information is displayed:

Extension type: None

- **None:** Plate reads are stored locally on the SharpV and can only be retrieved using the Reads API which is an external application.

Extension type: FTP

Sends ALPR data to an FTP server. Configure the following:

- **Server:** Enter the server name and location of the FTP server.
- **Username:** Enter the username for the server.
- **Password:** Enter the password for the username.
- **Content Template:** ALPR data is sent in XML format, using the template shown. You can change certain elements if you choose.
- **Set default template:** Reverts to the default template values.
- **Export context images:** Export the context image (in JPEG format).
- **Export ALPR images:** Export the plate image (in JPEG format).
- **Retain data when the connection is lost:** Select this option for plate reads to be saved locally in the SharpV database if the connection with the server is lost. The system attempts to reconnect with the server every 30 seconds. Stored reads are pushed to the server when the connection is reestablished.

  IMPORTANT: If there are any plate reads in the SharpV database, clearing this check box and saving the configuration deletes the plate reads.
- **Send sample:** Verifies that the system can connect to the server and send a sample read file using the configured settings.

HTTP / HTTPS

- **Server:** Enter the server name and location of the third party receiving HTTP server.
- **Format:** Select the format you want to send the ALPR data in. You can select either **JSON** or **XML** format.
- **Username:** Enter the username for the server.
- **Password:** Enter the password for the username.
- **Anonymize ALPR data:** The camera *hashes* the license plate using the SHA-1 algorithm. When you add an alphanumeric *salt (cryptography)* to the license plate number, it increases the security of the hashed output. Adding the same salt on all of the cameras in a network means that the same license plate produces an identical hash on all cameras. This allows the external system to recognize the identical hashes as a the same vehicle while still maintaining privacy.

  IMPORTANT: If the salt is changed after it is set, it must also be changed on all other cameras. Changing the salt breaks the link between old reads and new reads.
- **Ignore certificate errors:** Select this option when sending ALPR data to an HTTPS server that does not have a trusted certificate. The SharpV does not send the ALPR data to an HTTPS server that does not have a trusted certificate unless you select this option.
- **Export context images:** Export the context image (in JPEG format).
- **Export ALPR images:** Export the plate image (in JPEG format).

- **Retain data when the connection is lost:** Select this option for plate reads to be saved locally in the SharpV database if the connection with the server is lost. The system attempts to reconnect with the server every 30 seconds. Stored reads are pushed to the server when the connection is reestablished.

  IMPORTANT: If there are any plate reads in the SharpV database, clearing this check box and saving the configuration deletes the plate reads.

Patroller

Sends ALPR data to Genetec Patroller™. Configure the following:

- **Discovery port:** Port on which the SharpV listens for discovery requests. This port number must match the discovery port entered on the Genetec Patroller™ Config Tool *Cameras* page.

Sharp Portal - Product improvement program page

This section lists the settings found in the *Product improvement program* page of the Sharp Portal. Use the *Product improvement program* page to configure the delay period to send images from SharpV camera to servers at Genetec Inc.

To navigate to the *Product improvement program* page, click **Configuration** > **Connectivity** > **Product improvement**.

The following information is displayed:

Product improvement program

- **Activate program:** Select one of the following activation modes:
  - **Not Active:** Select this option if you are not participating in the program.
  - **Always activated (recommended):** Select this option if you are participating in the program. When this option is selected, the SharpV camera sends images to Genetec Inc. cloud systems continuously as long as there is an established connection.
  - **Activated for:** Select this option if you want send images for a support case. You can choose a delay period from the menu.
    NOTE: When a delay period has been selected and the program is active, an expiration date and time is displayed.
  - **Support case number (optional):** If you activate the program for a support case, enter the support case number provided by Genetec™ Technical Support.
- **Agreement:** Select the check box to agree to terms and conditions of the product improvement program feature.

Sharp Portal - Recovery page

This section lists the settings found in the *Recovery* page of the Sharp Portal. Use the *Recovery* page to import or export settings and to configure a Syslog server.

To navigate to the *Recovery* page, click **Configuration** > **General settings** > **Recovery**.

The following information is displayed:

Settings

- **Export diagnostics:** Export a file that includes SharpV diagnostics and SharpV settings.
- **Export settings:** Exports configuration and diagnostic settings as a .zip file. You can use the .zip file for technical support, or you can import the settings to another Sharp unit for quick configuration
- **Import settings:** Imports configuration settings from a .zip file exported from another Sharp. You can use this .zip file to quickly configure your Sharp. After you import the settings, the Plate Reader service restarts automatically.

  IMPORTANT: You can only import settings from a similar Sharp (same model and SharpOS version).
- **Reset to factory default:** Click to reset the SharpV to use the factory default settings. A message confirms the reset and offers to optionally clear the network settings as well. Note that certificates are not cleared in a factory reset.

Syslog

- **Use Syslog server:** Select this option to configure a central repository for all SharpV log entries.
  - **Server:** Enter the IP address or name of the server.
    NOTE: Syslog server configurations do not support IPv6 addresses.
  - **Port:** Enter the port number of the syslog server.
  - **Network protocol:** Select UDP or TCP.

Sharp Portal - Date and time page

This section lists the settings found in the *Date and time* page of the Sharp Portal. Use the *Date and time* page to configure how you want to configure the internal clock of the SharpV.

To navigate to the *Date and time* page, click **Configuration** > **General settings** > **Date and time**.

The following information is displayed:

- **Settings:** Select one of the following settings.
  - **No synchronization:** The SharpV uses its own clock.
  - **NTP server:** Enter the URL of a known time server (for example, *time.windows.com*). The SharpV clock synchronizes with this server on startup and then every hour. You can test the connection at any time by clicking **Test connection**.
  - **Active extension:** Click to synchronize the SharpV clock with the clock on the Security Center server it is connected to. The SharpV clock synchronizes with the Security Center server clock upon connection, then every 24 hours.
    IMPORTANT: Selecting this option has no effect if you are using any of the other extension types (FTP, HTTP, and so on). It can only be used when the active extension type is configured as Security Center (legacy). The active extension is configured on the **Configuration > Connectivity > Extension** page.
  - **LPM protocol:** When you add a SharpV camera to the ALPR Manager using the LPM Protocol, the camera's date and time are automatically synchronized with the LPM Protocol.
    NOTE: By default, LPM protocol is not an available setting. When a SharpV (SharpOS 12.7 and later) is manually added to the ALPR Manager (Security Center 5.8 and later), the LPM protocol is automatically selected as the unit's extension type and for date and time synchronization.
  - **Synchronize with client browser now:** Click to synchronize the date and time with the client machine you are using to connect to the Sharp Portal Portal. The camera performs a one-time synchronization.
    IMPORTANT: Do not synchronize the SharpV clock with the client browser unless you are connecting to the Sharp Portal from the server hosting the ALPR Manager role. If you synchronize clocks with a computer other than the Security Center server, the camera's reads and hits might not have accurate timestamps.
- **Date and time format:** Select the date and time format to be used in the Sharp Portal.
  - **International:** Selecting the International option displays the date and time in the format: YYYY-MM-DD HH:MM:SS
  - **Imperial:** Selecting the Imperial option displays the date and time in the format: DD/MM/YYYY H:MM:SS AM/PM

Sharp Portal - Power options page

This section lists the settings found in the *Power options* page of the Sharp Portal. Use the *Power options* page to configure the camera based on the power grid of the installation location.

To navigate to the *Power options* page, click **Configuration** > **General settings** > **Power options**.

The following information is displayed:

- **Power line frequency:** Select the power line frequency that corresponds to the installation location.
  - **60 Hz:** Generally used in North America and South America
  - **50 Hz:** Generally used in Africa, Australia, Asia, and Europe

NOTE: For more information on the power line frequency used in your installation location, click here.

Sharp Portal - Maintenance page

This section lists the settings found in the *Maintenance* page of the Sharp Portal. Use the *Maintenance* page to update software or reboot the unit.

To navigate to the *Maintenance* page, click **Configuration** > **Maintenance**.

The following information is displayed:

- **Update:** Update the SharpOS software or the platform OS with latest security updates.
- **Free up space:** Space is freed up by deleting log files, untransmitted reads, and clearing the update cache.
- **Reboot unit:**
- **Blink LED:** Click to blink the LED on the SharpV for about a minute. This is useful when you have multiple units and you want to physically identify the one you are configuring.

Sharp Portal - Logs page

This section lists the settings found in the *Logs* page of the Sharp Portal. Use the *Logs* page to run reports and generate logs about the status of the SharpV. You can filter by a specific source, message, and so on. Log reports can also be exported to a .zip file by selecting **Export settings** on the *Maintenance* page.

To navigate to the *Logs* page, click **Diagnostics** > **Logs**.

The following information is displayed:

- **Severity:** Click the icons to choose which severity types you want to include in the report query. You can choose from the following:
  - Error
  - Warning
  - Information
  - Debug
  - Performance
- **Source:** Select the source that you want to include in the report query.
- **Message:** Enter a message. Only logs containing the message string entered are displayed on the query.
- **Time:** Select a time range.
- **Search:** Click to run the query.
- **Pause:** Click to pause the auto-refresh on the query. This is useful when you want to stop new entries from coming in so you can focus on a particular entry. Click **Resume** to activate the auto-refresh on the query.
- **Download all logs in a text file:** Click to download in a text file.

  NOTE: The filters on this page apply only to the visual report. The log file always contains a full, unfiltered list of events.

Sharp Portal - Log sources page

This section lists the settings found in the *Log sources* page of the Sharp Portal. Use the *Log sources* page to activate sources and to specify the level of verbosity.

To navigate to the *Log sources* page, click **Diagnostics** > **Log sources**.

The following information is displayed:

- **Sources to log:** Select the sources from which to generate a log. For example, if you only want to generate log events related to Plate Reader, select **Plate Reader** from the list.

  NOTE:

  - A source that contains *Verbose* in its name might generate a lot of disk activity.
  - When a log entry contains an exception, a small box icon is displayed under the **Exception** column. Click on the box to see the exception details.

6

Troubleshooting for SharpV fixed installation

This section includes the following topics:

- "LED status on the SharpV camera unit" on page 120
- "Resetting a lost password for the Sharp Portal" on page 122

LED status on the SharpV camera unit

The status LED on the SharpV camera unit responds according to the status of the system.

The following table describes how the SharpV camera's LED behaves in response to the SharpV system's status:



State	Description	LED (red or green)
Off	Unit is powered-off.	Off
Covert mode	The camera is configured in covert mode. Following camera startup, the LED is deactivated.	Off
Catastrophic failure	The camera is shut down due to a critical error, for example, an over-temperature alarm. In this state, you cannot connect to the camera.	Slow red blinking (0.5 seconds off – 0.5 seconds on)
Major failure	Plate Reader is down. You might be able to connect to the camera and you might be able to see the logs.	Three red blinks per second
Performance issues or minor failure	Plate Reader is running with important performance issues, for example, failure of the illuminator .	One short red blink per second
PoE+ failure	The PoE power supply has failed to negotiate IEEE 802.3at (POE+, or 25.5 W). PlateReader will not run, but the Sharp Portal might be accessible. Check the SharpV logs. For more information, see the network cable requirements for SharpV cameras.	One long red blink and one short green blink per second
Camera update	Plate Reader is down during the camera update, but is expected to come back online after the update is complete.	Five green blinks per second

State	Description	LED (red or green)
Locate camera	After clicking **Blink LED** in the Sharp Portal, the LED blinks for 10 seconds.	Slow red and green alternating (0.5 seconds each)
Focus mode	The camera's focus and zoom are being adjusted in the Sharp Portal.	Fast red and green alternating (0.25 seconds each)
Normal mode	The camera is running normally.	Solid green
Camera startup	The camera is booting up.	One green blink per second

Resetting a lost password for the Sharp Portal

If you forget your password to the Sharp Portal, you can reset the password using the **I forgot my password** button on the Sharp Portal logon screen.

Before you begin

To reset a lost password, you need the yellow *Important information* sticker that was shipped with the SharpV camera. If you do not have the sticker, you must contact the AutoVu™ Support team.



What you should know

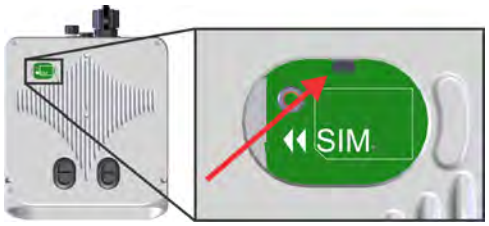
- As a step in the password reset procedure, you must press the reset button on the SharpV camera. Alternatively, if you do not have physical access to the camera, you are given the option to present a known license plate to the camera.
- You can use this procedure for SharpV cameras running SharpOS 12.3 SR1 or later.

To reset a lost password for the Sharp Portal:

1 From the Sharp Portal logon screen, click **I forgot my password**.
2 Enter the 32-character unit access code. You can find the unit access code on the yellow sticker that was provided with the SharpV camera.
3 Click **Next**.
4 For added security, and to ensure that the password cannot be reset remotely, you must select one of the following validation methods:
   - **Press the reset button:** To use this validation method, you must have physical access to the camera.
   - **Read a plate number:** To use this validation method, you are prompted to enter a plate number, and then have the camera read the plate.

To validate by pressing the reset button:

1 Select **Use the reset button** and click **Next**.
   The message *Press and hold the Sharp reset button for 2 seconds* is displayed.
2 Press and hold the reset button for 2 seconds.
   The reset button is located behind the rubber plug as indicated in the following image:



   NOTE: If you do not press the reset button within two hours, the password recovery operation is canceled.

   The message *Reset button pressed. Please wait.* is displayed.
3 When prompted, enter and confirm the new Sharp Portal password.
4 Click **Apply**.
   The message *The portal password has been changed* is displayed.
5 Log on to the Sharp Portal using your new password.

6 Store your password safely for future use.

To validate by reading a plate number:

1 Select **Read a plate number**.
2 Enter the number of a license plate that you can use to generate a plate read on the camera.
3 Click **Next**.
4 The message *Waiting for the Sharp to read plate ABC123* is displayed.
5 Use the plate to generate a read on the camera.

NOTE: If the camera does not read the plate within two hours, the password recovery operation is canceled.

6 When the camera reads the plate, the message *Plate number read. Please wait* is displayed.
7 When prompted, enter and confirm the new Sharp Portal password.
8 Click **Apply**.
The message *The portal password has been changed* is displayed.
9 Log on to the Sharp Portal using your new password.
10 Store your password safely for future use.

Glossary

authorized user An authorized user is a user who can see (has the right to access) the entities contained in a partition. Users can only exercise their privileges on entities they can see.

access right An access right is the basic right users must have over any part of the system before they can do anything with it. Other rights, such as viewing and modifying entity configurations, are granted through privileges. In the context of a Synergis™ system, an access right is the right granted to a cardholder to pass through an access point at a given date and time.

action An action is a user-programmable function that can be triggered as an automatic response to an event, such as door held open for too long or object left unattended, or that can be executed according to a specific time table.

active alarm An active alarm is an alarm that has not yet been acknowledged.

Active Directory Active Directory is a directory service created by Microsoft, and a type of role that imports users and cardholders from an Active Directory and keeps them synchronized.

Activity trails Activity trails is a type of maintenance task that reports on the user activity related to video, access control, and ALPR functionality. This task can provide information such as who played back which video recordings, who used the Hotlist and permit editor, who enabled hotlist filtering, and much more.

agent An agent is a subprocess created by a Security Center role to run simultaneously on multiple servers for the purpose of sharing its load.

alarm An alarm is a type of entity that describes a particular trouble situation that requires immediate attention and how it can be handled in Security Center. For example, an alarm can indicate which entities (usually cameras and doors) best describe it, who must be notified, how it must be displayed to the user, and so on.

alarm acknowledgement An alarm acknowledgement is a user response to an alarm. In Security Center, the default acknowledgement and alternate acknowledgement are the two variants of alarm acknowledgements. Each variant is associated to a different event so that specific actions can be programmed based on the alarm response selected by the user.

Alarm monitoring Alarm monitoring is a type of operation task that allows you to monitor and respond to alarms (acknowledge, forward, snooze, and so on) in real time, as well as review past alarms.

Alarm report	Alarm report is a type of investigation task that allows you to search and view current and past alarms.
ALPR camera	An Automatic License Plate Recognition (ALPR) camera is a camera connected to an ALPR unit that produces high resolution close-up images of license plates.
ALPR Frequency Monitor	The Stakeout - ALPR Frequency Monitor plugin tracks how often vehicles are detected by fixed Sharp cameras. The system can alert Security Desk users if vehicles without whitelisted license plates have exceed the configured threshold.
ALPR Manager	The ALPR Manager role manages and controls the patrol vehicle software (Genetec Patroller™), Sharp cameras, and parking zones. The ALPR Manager stores the ALPR data (reads, hits, timestamps, GPS coordinates, and so on) collected by the devices.
ALPR rule	ALPR rule is a method used by Security Center and AutoVu™ for processing a license plate read. An ALPR rule can be a hit rule or a parking facility.
ALPR unit	An ALPR unit is a device that captures license plate numbers. An ALPR unit typically includes a context camera and at least one ALPR camera.
area	In Security Center, an area entity represents a concept or a physical location (room, floor, building, site, and so on) used for grouping other entities in the system.
area view	The area view is a view that organizes the commonly used entities such as doors, cameras, tile plugins, intrusion detection areas, zones, and so on, by areas. This view is primarily created for the day to day work of the security operators.
asset	An asset is a type of entity that represents any valuable object with an RFID tag attached, thus allowing it to be tracked by an asset management software.
Audit trails	Audit trails is a type of maintenance task that reports on the configuration changes of the selected entities in the system and also indicates the user who made the changes.
automatic enrollment	Automatic enrollment is when new IP units on a network are automatically discovered by and added to Security Center. The role that is responsible for the units *broadcasts* a discovery request on a specific port, and the units listening on that port respond with a message that contains the connection information about themselves. The role then uses the information to configure the connection to the unit and enable communication.
automatic license plate recognition	Automatic license plate recognition (ALPR) is an image processing technology used to read license plate numbers.

	ALPR converts license plate numbers cropped from camera images into a database searchable format.
AutoVu™	The AutoVu™ automatic license plate recognition (ALPR) system automates license plate reading and identification, making it easier for law enforcement and for municipal and commercial organizations to locate vehicles of interest and enforce parking restrictions. Designed for both fixed and mobile installations, the AutoVu™ system is ideal for a variety of applications and entities, including law enforcement, municipal, and commercial organizations.
AutoVu MLC™	AutoVu MLC™ (Machine Learning Core) replaces traditional rule-based ALPR technology with machine learning-based algorithms to reduce common ALPR misreads and false positives. It is a proprietary technology of Genetec Inc. used in AutoVu™ Sharp hardware for license plate recognition.
block face (2 sides)	A block face (2 sides) is a type of parking regulation characterizing an overtime rule. A block face is the length of a street between two intersections. A vehicle is in violation if it is seen parked within the same block over a specified period of time. Moving the vehicle from one side of the street to the other does not make a difference.
Breakout box	The breakout box is the proprietary connector box of Genetec Inc. for AutoVu™ mobile solutions that use Sharp cameras. The breakout box provides power and network connectivity to the Sharp units and the in-vehicle computer.
broadcast	Broadcast is the communication between a single sender and all receivers on a network.
canvas	Canvas is one of the panes found in the Security Desk's task workspace. The canvas is used to display multimedia information, such as videos, maps, and pictures. It is further divided into three panels: the tiles, the dashboard, and the properties.
certificate	Designates one of the following: (1) *digital certificate*; (2) *SDK certificate*.
City Parking Enforcement	City Parking Enforcement is a Genetec Patroller™ software installation that is configured for the enforcement of parking permit and overtime restrictions.
City Parking Enforcement with Wheel Imaging	City Parking Enforcement with Wheel Imaging is a *City Parking Enforcement* installation of a Genetec Patroller™ application that also includes wheel imaging. The use of maps is mandatory and the mobile AutoVu™ system must include navigation hardware.
Config Tool	Config Tool is the Security Center administrative application used to manage all Security Center users and to configure

	all Security Center entities such as areas, cameras, doors, schedules, cardholders, patrol vehicles, ALPR units, and hardware devices.
Conflict resolution utility	Conflict resolution utility is a tool that helps you resolve conflicts caused by importing users and cardholders from an Active Directory.
context camera	A context camera is a camera connected to an ALPR unit that produces a wider angle color image of the vehicle whose license plate was read by the ALPR camera.
Copy configuration tool	The Copy configuration tool helps you save configuration time by copying the settings of one entity to many others that partially share the same settings.
covert hit	A covert hit is a read (captured license plate) that is matched to a covert hotlist. Covert hits are not displayed on the Genetec Patroller™ screen, but can be displayed in Security Desk by a user with proper privileges.
covert hotlist	Covert hotlists allow you to ensure the discretion of an ongoing investigation or special operation. When a hit is identified, only the authorized officer at the Security Center station is notified, while the officer in the patrol vehicle is not alerted. This enables enforcement officials to assign multiple objectives to the vehicle and back-end systems, while not interrupting the priorities of officers on duty.
custom event	A custom event is an event added after the initial system installation. Events defined at system installation are called system events. Custom events can be user-defined or automatically added through plugin installations. Unlike system events, custom events can be renamed and deleted.
custom field	A custom field is a user-defined property that is associated with an entity type and is used to store additional information that is useful to your organization.
Daily usage per patroller entity	Daily usage per patroller entity is a type of investigation task that reports on the daily usage statistics of a selected patrol vehicle (operating time, longest stop, total number of stops, longest shutdown, and so on) for a given date range.
dashboard	A dashboard is one of the three panels that belong to the canvas in Security Desk. It contains the graphical commands (or widgets) pertaining to the entity displayed in the current tile.
database server	A database server is an application that manages databases and handles data requests made by client applications. Security Center uses Microsoft SQL Server as its database server.
Directory	The Directory role identifies a Security Center system. It manages all entity configurations and system-wide settings.

	Only a single instance of this role is permitted on your system. The server hosting the Directory role is called the *main server*, and must be set up first. All other servers you add in Security Center are called *expansion servers*, and must connect to the main server to be part of the same system.
Directory Manager	The Directory Manager role manages the Directory failover and load balancing in order to produce the high availability characteristics in Security Center.
Directory server	A Directory server is any one of the multiple servers simultaneously running the Directory role in a high availability configuration.
discovery port	A discovery port is a port used by certain Security Center roles (Access Manager, Archiver, ALPR Manager) to find the units they are responsible for on the LAN. No two discovery ports can be the same on one system.
district	A district is a type of parking regulation characterizing an overtime rule. A district is a geographical area within a city. A vehicle is in violation if it is seen within the boundaries of the district over a specified period of time.
dynamic permit	In a system that uses the Pay-by-Plate Sync plugin, a dynamic permit holds a list of vehicles that is updated by a third-party permit provider. For example, in a system where vehicle owners pay for parking at a kiosk or using a mobile phone app, the list of vehicles are dynamically managed by a third-party permit provider.
enforce	To enforce is to take action following a confirmed hit. For example, a parking officer can enforce a scofflaw violation (unpaid parking tickets) by placing a wheel boot on the vehicle.
entity	Entities are the basic building blocks of Security Center. Everything that requires configuration is represented by an entity. An entity can represent a physical device, such as a camera or a door, or an abstract concept, such as an alarm, a schedule, a user, a role, a plugin, or an add-on.
entity tree	An entity tree is the graphical representation of Security Center entities in a tree structure, illustrating the hierarchical nature of their relationships.
event	An event indicates the occurrence of an activity or incident, such as access denied to a cardholder or motion detected on a camera. Events are automatically logged in Security Center. Every event has an entity as its main focus, called the event source.

event-to-action	An event-to-action links an action to an event. For example, you can configure Security Center to trigger an alarm when a door is forced open.
expansion server	An expansion server is any server machine in a Security Center system that does not host the Directory role. The purpose of the expansion server is to add to the processing power of the system.
failover	Failover is a backup operational mode in which a role (system function) is automatically transferred from its primary server to a secondary server that is on standby. This transfer between servers occurs only if the primary server becomes unavailable, either through failure or through scheduled downtime.
federated entity	A federated entity is any entity that is imported from an independent system through one of the Federation™ roles.
federated system	A federated system is a independent system (Omnicast™ or Security Center) that is unified under your local Security Center via a Federation™ role, so that the local users can view and control its entities, as if they belong to the local system.
Federation™	The Federation™ feature joins multiple, independent Genetec™ IP security systems into a single virtual system. With this feature, Security Center users can view and control entities that belong to remote systems, directly from their local Security Center system.
Fuzzy matching	Environmental factors such as dirt or snow can partially obstruct license plate characters and increase the likelihood of partial plate reads occurring. In addition, similarly shaped letters and numbers, like “2” and “Z” or, “8”, “B”, and “0”, can also reduce plate read accuracy. Fuzzy matching lets AutoVu™ compare reads not only to exact matches in hotlists, but also to potential or probable matches.
Genetec™ Server	Genetec™ Server is the Windows service that is at the core of Security Center architecture, and that must be installed on every computer that is part of the Security Center's pool of servers. Every such server is a generic computing resource capable of taking on any role (set of functions) you assign to it.
geocoding	Geocoding is the process of finding associated geographic coordinates (latitude and longitude) from a street address.
ghost patroller entity	A ghost patroller entity is automatically created by the ALPR Manager when the AutoVu™ license includes the XML Import module. In Security Center, all ALPR data must be associated to a Genetec Patroller™ entity or an ALPR unit corresponding to a fixed Sharp camera. When you import ALPR data from an external source via a specific ALPR Manager using the XML Import module, the system uses the ghost entity to represent

	the ALPR data source. You can formulate queries using the ghost entity as you would with a normal entity.
Geographic Information System	Geographic Information System (GIS) is a system that captures spatial geographical data. Map Manager can connect to third-party vendors that provide GIS services in order to bring maps and all types of geographically referenced data to Security Center.
Global Cardholder Synchronizer	The Global Cardholder Synchronizer role ensures the two-way synchronization of shared cardholders and their related entities between the local system (sharing guest) where it resides and the central system (sharing host).
global entity	A global entity is an entity that is shared across multiple independent Security Center systems by virtue of its membership to a global partition. Only cardholders, cardholder groups, credentials, and badge templates are eligible for sharing.
global partition	Global partition is a partition that is shared across multiple independent Security Center systems by the partition owner, called the sharing host.
hardware integration package	A hardware integration package, or HIP, is an update that can be applied to Security Center. It enables the management of new functionalities (for example, new video unit types), without requiring an upgrade to the next Security Center release.
Hardware inventory	Hardware inventory is a type of maintenance task that reports on the characteristics (unit model, firmware version, IP address, time zone, and so on) of access control, video, intrusion detection, and ALPR units in your system.
Health history	Health history is a type of maintenance task that reports on health issues.
Health Monitor	The Health Monitor role monitors system entities such as servers, roles, units, and client applications for health issues.
Health statistics	Health statistics is a maintenance task that gives you an overall view of the health of your system by reporting on the availability of selected system entities such as roles, video units, and doors.
High availability	High availability is a design approach that enables a system to perform at a higher than normal operational level. This often involves failover and load balancing.
hit	A hit is a license plate read that matches a hit rule, such as a hotlist, overtime rule, permit, or permit restriction. A Genetec Patroller™ user can choose to reject or accept a hit. An accepted hit can subsequently be enforced.

hit rule	Hit rule is a type of ALPR rule used to identify vehicles of interest (called "hits") using license plate reads. The hit rules include the following types: hotlist, overtime rule, permit, and permit restriction.
Hits	Hits is a type of investigation task that reports on hits reported within a selected time range and geographic area.
hot action	A hot action is an action mapped to a PC keyboard function key (Ctrl+F1 through Ctrl+F12) in Security Desk for quick access.
hotlist	A hotlist is a list of wanted vehicles, where each vehicle is identified by a license plate number, the issuing state, and the reason why the vehicle is wanted (stolen, wanted felon, Amber alert, VIP, and so on). Optional vehicle information might include the model, the color, and the vehicle identification number (VIN).
Hotlist and permit editor	Hotlist and permit editor is a type of operation task used to edit an existing hotlist or permit list. A new list cannot be created with this task, but after an existing list has been added to Security Center, users can edit, add, or delete items from the list, and the original text file is updated with the changes.
hotspot	Hotspot is a type of map object that represents an area on the map which requires special attention. Clicking on a hotspot displays associated fixed and PTZ cameras.
identity provider	A trusted, external system that administers user accounts, and is responsible for providing user authentication and identity information to relying applications over a distributed network.
illuminator	An illuminator is a light in the Sharp unit that illuminates the plate, thereby improving the accuracy of the images produced by the ALPR camera.
inactive entity	An inactive entity is an entity that is shaded in red in the entity browser. It signals that the real world entity it represents is either not working, offline, or incorrectly configured.
incident	An incident is an unexpected event reported by a Security Desk user. Incident reports can use formatted text and include events and entities as support material.
Incidents	Incidents is a type of investigation task that allows you to search, review, and modify incident reports.
intrusion detection area	An intrusion detection area is an entity that represents a zone (sometimes called an area) or a partition (group of sensors) on an intrusion panel.
Intrusion detection area activities	*Intrusion detection area activities* is a type of investigation task that reports on activities (master arm, perimeter arm, duress, input trouble, and so on) in selected intrusion detection areas.

intrusion detection unit	An intrusion detection unit is an entity that represents an intrusion device (intrusion panel, control panel, receiver, and so on) that is monitored and controlled by the Intrusion Manager role.
Intrusion detection unit events	*Intrusion detection unit events* is a type of investigation task that reports on events (AC fail, battery fail, unit lost, input trouble, and so on) related to selected intrusion detection units.
Intrusion Manager	The Intrusion Manager role monitors and controls intrusion detection units. It listens to the events reported by the units, provides live reports to Security Center, and logs the events in a database for future reporting.
intrusion panel	An intrusion panel (also known as alarm panel) is a wall-mounted unit where the alarm sensors (motion sensors, smoke detectors, door sensors, and so on) and wiring of the intrusion alarms are connected and managed.
Inventory management	Inventory management is a type of operation task that allows you to add and reconcile license plate reads to a parking facility inventory.
Inventory report	Inventory report is a type of investigation task that allows you to view a specific inventory (vehicle location, vehicle length of stay, and so on) or compare two inventories of a selected parking facility (vehicles added, vehicles removed, and so on).
I/O linking	I/O (input/output) linking is controlling an output relay based on the combined state (normal, active, or trouble) of a group of monitored inputs. A standard application is to sound a buzzer (through an output relay) when any window on the ground floor of a building is shattered (assuming that each window is monitored by a "glass break" sensor connected to an input).
IPv4	IPv4 is the first generation Internet protocol using a 32-bit address space.
IPv6	IPv6 is a 128-bit Internet protocol that uses eight groups of four hexadecimal digits for address space.
Keyhole Markup Language	Keyhole Markup Language (KML) is a file format used to display geographic data in an Earth browser such as Google Earth and Google Maps.
Law Enforcement	Law Enforcement is a Genetec Patroller™ software installation that is configured for law enforcement: the matching of license plate reads against lists of wanted license plates (hotlists). The use of maps is optional.
license key	A license key is the software key used to unlock the Security Center software. The license key is specifically generated for each computer where the Directory role is installed. To obtain

	your license key, you need the *System ID* (which identifies your system) and the *Validation key* (which identifies your computer).
license plate inventory	A license plate inventory is a list of license plate numbers of vehicles found in a parking facility within a given time period, showing where each vehicle is parked (sector and row).
license plate read	A license plate read is a license plate number captured from a video image using ALPR technology.
live hit	A live hit is a hit matched by the Genetec Patroller™ and immediately sent to the Security Center over a wireless network.
live read	A live read is a license plate captured by the patrol vehicle and immediately sent to Security Center over a wireless network.
load balancing	Load balancing is the distribution of workload across multiple computers.
logical ID	Logical ID is a unique ID assigned to each entity in the system for ease of reference. Logical IDs are only unique within a particular entity type.
Logons per Patroller	Logons is a type of investigation task that reports on the logon records of a selected patrol vehicle.
long term	Long term is a type of parking regulation characterizing an overtime rule. The *long term* regulation uses the same principle as the *same position* regulation, but the parking period starts on one calendar date and ends on another calendar date. No more than one overtime rule can use the long term regulation in the entire system.
LPM protocol	The License Plate Management (LPM) protocol provides a Sharp camera with a secure and reliable connection to Security Center. When The LPM protocol is enabled on a Sharp camera, the protocol manages the camera's connection to the ALPR Manager role.
macro	A macro is a type of entity that encapsulates a C# program that adds custom functionalities to Security Center.
main server	The main server is the only server in a Security Center system hosting the Directory role. All other servers on the system must connect to the main server to be part of the same system. In a high availability configuration where multiple servers host the Directory role, it is the only server that can write to the Directory database.
manual capture	Manual capture is when license plate information is entered into the system by the user and not by the ALPR.
map link	A map link is a map object that brings you to another map with a single click.

map mode	Map mode is a Security Desk canvas operating mode that replaces tiles and controls with a geographical map showing all active, georeferenced events in your system. Switching to Map mode is a feature of AutoVu™ and Genetec Mission Control™, and requires a license for one of these products.
map object	Map objects are graphical representations of Security Center entities or geographical features, such as cities, highways, rivers, and so on, on your maps. With map objects, you can interact with your system without leaving your map.
map view	A map view is a defined section of a map.
master arm	Master arm is arming an intrusion detection area in such a way that all sensors attributed to the area would set the alarm off if one of them is triggered.
Mobile Admin	(Obsolete as of SC 5.8 GA) Mobile Admin is a web-based administration tool used to configure the Mobile Server.
Genetec™ Mobile	Official name of the map-based Security Center mobile application for Android and iOS devices.
Mobile Data Computer	Mobile Data Computer is a tablet computer or ruggedized laptop used in patrol vehicles to run the Genetec Patroller™ application. The MDC is typically equipped with a touch-screen with a minimum resolution of 800 x 600 pixels and wireless networking capability.
Mobile License Plate Inventory	Mobile License Plate Inventory (MLPI) is the Genetec Patroller™ software installation that is configured for collecting license plates and other vehicle information for creating and maintaining a license plate inventory for a large parking area or parking garage.
Mobile Server	The Mobile Server role provides Security Center access on mobile devices.
Monitoring	The *Monitoring* task is a type of operation task that you can use to monitor and respond to real-time events that relate to selected entities. Using the *Monitoring* task, you can also monitor and respond to alarms.
Move unit	Move unit tool is used to move units from one manager role to another. The move preserves all unit configurations and data. After the move, the new manager immediately takes on the command and control function of the unit, while the old manager continues to manage the unit data collected before the move.
multi-tenant parking	If you use AutoVu™ Free-Flow to manage transient parking and contract permit parking in parking zones, installing the AutoVu™

	Free-Flow plugin allows you to manage parking lots where parking spots are leased to tenants.
Navigator box	The Navigator box is a proprietary in-vehicle device of Genetec Inc. that provides GPS coordinates and odometer readings to Genetec Patroller™. Because it taps into the vehicle's odometry signal, it is more accurate than a standard GPS device. The Navigator box can be used with any type of AutoVu™ mobile deployment that requires positioning information, but it is required for City Parking Enforcement with Wheel Imaging.
network	The network entity is used to capture the characteristics of the networks used by your system so that proper stream routing decisions can be made.
network address translation	Network address translation is the process of modifying network address information in datagram (IP) packet headers while in transit across a traffic routing device, for the purpose of remapping one IP address space into another.
network view	The network view is a browser view that illustrates your network environment by showing each server under the network they belong to.
new wanted	A new wanted is a manually entered hotlist item in Genetec Patroller™. When you are looking for a plate that does not appear in the hotlists loaded in the Genetec Patroller™, you can enter the plate in order to raise a hit if the plate is captured.
notification tray	The notification tray contains icons that allow quick access to certain system features, and also displays indicators for system events and status information. The notification tray display settings are saved as part of your user profile and apply to both Security Desk and Config Tool.
OCR equivalence	OCR equivalence is the interpretation of OCR (Optical Character Recognition) equivalent characters performed during license plate recognition. OCR equivalent characters are visually similar, depending on the plate's font. For example, the letter "O" and the number "0", or the number "5" and the letter "S". There are several pre-defined OCR equivalent characters for different languages.
Omnicast™	Security Center Omnicast™ is the IP video management system (VMS) that provides organizations of all sizes the ability to deploy a surveillance system adapted to their needs. Supporting a wide range of IP cameras, it addresses the growing demand for HD video and analytics, all the while protecting individual privacy.
Omnicast™ compatibility pack	Omnicast™ compatibility pack is the software component that you need to install to make Security Center compatible with an Omnicast™ 4.x system.

Omnicast™ Federation™	The Omnicast™ Federation™ role connects an Omnicast™ 4.x system to Security Center. That way, the Omnicast™ entities and events can be used in your Security Center system.
output behavior	An output behavior is a type of entity that defines a custom output signal format, such as a pulse with a delay and duration.
overtime rule	An overtime rule is a type of entity that defines a parking time limit and the maximum number of violations enforceable within a single day. Overtime rules are used in city and university parking enforcement. For university parking, an overtime rule also defines the parking area where these restrictions apply.
parking facility	A parking facility is a type of entity that defines a large parking area as a number of sectors and rows for the purpose of inventory tracking.
parking lot	A parking lot is a polygon that defines the location and shape of a parking area on a map. By defining the number of parking spaces inside the parking lot, Security Center can calculate its percentage of occupancy during a given time period.
parking zone	The parking zones that you define in Security Center represent off-street parking lots where the entrances and exits are monitored by Sharp cameras.
partition	A partition is a type of entity that defines a set of entities that are only visible to a specific group of users. For example, a partition could include all areas, doors, cameras, and zones in one building.
partition administrator	(Obsolete) Beginning in Security Center 5.7 GA, privileges that used to be exclusive to administrators can now be granted individually, making the concept of *partition administrator* obsolete.
patroller entity	A patroller entity in Security Center represents a patrol vehicle equipped with an in-vehicle computer running Genetec Patroller™ software.
Patroller Config Tool	Genetec Patroller™ Config Tool is the Genetec Patroller™ administrative application used to configure Patroller-specific settings, such as adding Sharp cameras to the in-vehicle LAN, enabling features such as Manual Capture or New Wanted, and specifying that a username and password are needed to log on to Genetec Patroller™.
Patrol vehicle tracking	Patrol vehicle tracking is a type of investigation task that allows you to replay the route followed by a patrol vehicle on a given date on a map, or view the current location of patrol vehicles on a map.

perimeter arm
Perimeter arm is arming an intrusion detection area in such a way that only sensors attributed to the area perimeter set the alarm off if triggered. Other sensors, such as motion sensors inside the area, are ignored.

permit
A permit is a type of entity that defines a single parking permit holder list. Each permit holder is characterized by a category (permit zone), a license plate number, a license issuing state, and optionally, a permit validity range (effective date and expiry date). Permits are used in both city and university parking enforcement.

permit hit
A permit hit is a hit that is generated when a read (license plate number) does not match any entry in a permit or when it matches an invalid permit.

permit restriction
A permit restriction is a type of entity that applies time restrictions to a series of parking permits for a given parking area. Permit restrictions can be used by patrol vehicles configured for University Parking Enforcement and for systems that use the AutoVu™ Free-Flow feature.

Plan Manager
Plan Manager is a module of Security Center that provides interactive mapping functionality to better visualize your security environment.

Plate Reader
Plate Reader is the software component of the Sharp unit that processes the images captured by the ALPR camera to produce license plate reads, and associates each license plate read with a context image captured by the context camera. The Plate Reader also handles the communications with the Genetec Patroller™ and the ALPR Manager. If an external wheel imaging camera is connected to the Sharp unit, the Plate Reader also captures wheel images from this camera.

plugin
A plugin (in lowercase) is a software component that adds a specific feature to an existing program. Depending on the context, plugin can refer either to the software component itself or to the software package used to install the software component.

plugin role
A plugin role adds optional features to Security Center. A plugin role is created by using the *Plugin* role template. By default, it is represented by an orange puzzle piece in the *Roles* view of the *System* task. Before you can create a plugin role, the software package specific to that role must be installed on your system.

Point of sale
Point of sale (POS) is a system that typically refers to the hardware and software used for checkouts - the equivalent of an electronic cash register. These systems are used to capture detailed transactions, authorize payments, track inventory, audit sales, and manage employees. Point of sale systems are

	used in supermarkets, restaurants, hotels, stadiums, casinos, retail establishments.
primary server	Primary server is the default server chosen to perform a specific function (or role) in the system. To increase the system's fault-tolerance, the primary server can be protected by a secondary server on standby. When the primary server becomes unavailable, the secondary server automatically takes over.
private IP address	A private IP address is an IP address chosen from a range of addresses that are only valid for use on a LAN. The ranges for a private IP address are: 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.16.255.255, and 192.168.0.0 to 192.168.255.255. Routers on the Internet are normally configured to discard any traffic using private IP addresses.
private task	A private task is a saved task that is only visible to the user who created it.
privilege	Privileges define what users can do, such as arming zones, blocking cameras, and unlocking doors, over the part of the system they have access rights to.
public task	A public task is a saved task that can be shared and reused among multiple Security Center users.
Reads	Reads is a type of investigation task that reports on license plate reads performed within a selected time range and geographic area.
Reads/hits per day	Reads/hits per day is a type of investigation task that reports on license plate reads performed within a selected time range and geographic area.
Reads/hits per zone	Reads/hits per zone is a type of investigation task that reports on the number of reads and hits per parking area for a selected date range.
Report Manager	Report Manager is a type of role that automates report emailing and printing based on schedules.
report pane	Report pane is one of the panes found in the Security Desk task workspace. It displays query results or real-time events in a tabular form.
reverse geocoding	Reverse geocoding is an AutoVu™ feature that translates a pair of latitude and longitude into a readable street address.
role	A role is a software component that performs a specific job within Security Center. To execute a role, you must assign one or more servers to host it.

same position	Same position is a type of parking regulation characterizing an overtime rule. A vehicle is in violation if it is seen parked at the exact same spot over a specified period of time. Genetec Patroller™ must be equipped with GPS capability in order to enforce this type of regulation.
schedule	A schedule is a type of entity that defines a set of time constraints that can be applied to a multitude of situations in the system. Each time constraint is defined by a date coverage (daily, weekly, ordinal, or specific) and a time coverage (all day, fixed range, daytime, and nighttime).
scheduled task	A scheduled task is a type of entity that defines an action that executes automatically on a specific date and time, or according to a recurring schedule.
Software Development Kit	The Software Development Kit (SDK) allows end-users to develop custom applications or custom application extensions for Security Center.
secondary server	A secondary server is any alternate server on standby intended to replace the primary server in the case the latter becomes unavailable.
Security Center	Security Center is a truly unified platform that blends IP video surveillance, access control, license plate recognition, intrusion detection, and communications within one intuitive and modular solution. By taking advantage of a unified approach to security, your organization becomes more efficient, makes better decisions, and responds to situations and threats with greater confidence.
Security Center Federation™	The Security Center Federation™ role connects a remote, independent Security Center system to your local Security Center. That way, the remote system's entities and events can be used in your local system.
Security Center Mobile	(Obsolete) See Mobile Server and Genetec™ Mobile.
Security Desk	Security Desk is the unified user interface of Security Center. It provides consistent operator flow across all of the Security Center main systems, Omnicast™, Synergis™, and AutoVu™. The unique task-based design of Security Desk lets operators efficiently control and monitor multiple security and public safety applications.
server	A server is a type of entity that represents a server machine on which the Genetec™ Server service is installed.
Server Admin	Server Admin is the web application running on every server machine in Security Center that allows you to configure the settings of Genetec Server. Server Admin also allows you to configure the Directory role on the main server.

sharing guest A sharing guest is a Security Center system that has been given the rights to view and modify entities owned by another Security Center system, called the sharing host. Sharing is done by placing the entities in a global partition.

sharing host Sharing host is a Security Center system that gives the right to other Security Center systems to view and modify its entities by putting them up for sharing in a global partition.

Sharp EX Sharp EX is the Sharp unit that includes an integrated image processor and supports two standard definition NTSC or PAL inputs for external cameras (ALPR and context cameras).

SharpOS SharpOS is the software component of a Sharp unit. SharpOS is responsible for everything related to plate capture, collection, processing, and analytics. For example, a SharpOS update can include new ALPR contexts, new firmware, Sharp Portal updates, and updates to the Sharp's Windows services (Plate Reader, HAL, and so on).

Sharp Portal Sharp Portal is a web-based administration tool used to configure Sharp cameras for AutoVu™ systems. From a web browser, you log on to a specific IP address (or the Sharp name in certain cases) that corresponds to the Sharp you want to configure. When you log on, you can configure options such as selecting the ALPR context (for example, Alabama, Oregon, Quebec), selecting the read strategy (for example, fast moving or slow moving vehicles), viewing the Sharp's live video feed, and more.

Sharp unit The Sharp unit is a proprietary ALPR unit of Genetec Inc. that integrates license plate capturing and processing components, as well as digital video processing functions, inside a ruggedized casing.

Sharp VGA Sharp VGA is a Sharp unit that integrates the following components: an infrared illuminator; a standard definition (640 x 480) ALPR camera for plate capture; an integrated image processor; an NTSC or PAL color context camera with video streaming capabilities.

SharpX SharpX is the camera component of the SharpX system. The SharpX camera unit integrates a pulsed LED illuminator that works in total darkness (0 lux), a monochrome ALPR camera (1024 x 946 @ 30 fps), and a color context camera (640 x 480 @ 30 fps). The ALPR data captured by the SharpX camera unit is processed by a separate hardware component called the AutoVu™ ALPR Processing Unit.

Sharp XGA Sharp XGA is a Sharp unit that integrates the following components: an infrared illuminator; a high-definition (1024 x 768) ALPR camera for plate capture; an integrated image

	processor; an NTSC or PAL color context camera with video streaming capabilities and optional internal GPS.
SharpX VGA	SharpX VGA is the camera component of the SharpX system. The SharpX VGA camera unit integrates a pulsed LED illuminator that works in total darkness (0 lux), a monochrome ALPR camera (640 x 480 @ 30 fps), and a color context camera (640 x 480 @ 30 fps). The ALPR data captured by the SharpX VGA camera unit is processed by a separate hardware component called the AutoVu™ ALPR Processing Unit.
standard schedule	A standard schedule is a type of schedule entity that may be used in all situations. Its only limitation is that it does not support daytime or nighttime coverage.
static permit	In a system that uses the Pay-by-Plate Sync plugin, a static permit holds a list of vehicle license plates that is not updated by a third-party permit provider. For example, a list of employee vehicles that are authorized to park in the lot are manually maintained as a static list.
Synergis™	Security Center Synergis™ is the IP access control system (ACS) that heightens your organization's physical security and increases your readiness to respond to threats. Supporting an ever-growing portfolio of third-party door control hardware and electronic locks, it allows you to leverage your existing investment in network and security equipment.
system event	A system event is a predefined event that indicates the occurrence of an activity or incident. System events are defined by the system and cannot be renamed or deleted.
System status	System status is a type of maintenance task that monitors the status of all entities of a given type in real time, and allows you to interact with them.
task	A task is the central concept on which the entire Security Center user interface is built. Each task corresponds to one aspect of your work as a security professional. For example, use a monitoring task to monitor system events in real-time, use an investigation task to discover suspicious activity patterns, or use an administration task to configure your system. All tasks can be customized and multiple tasks can be carried out simultaneously.
taskbar	A taskbar is a user interface element of the Security Center client application window, composed of the Home tab and the active task list. The taskbar can be configured to appear on any edge of the application window.

task cycling	A task cycling is a Security Desk feature that automatically cycles through all tasks in the active task list following a fixed dwell time.
task workspace	A task workspace is an area in the Security Center client application window reserved for the current task. The workspace is typically divided into the following panes: canvas, report pane, controls, and area view.
threat level	Threat level is an emergency handling procedure that a Security Desk operator can enact on one area or the entire system to deal promptly with a potentially dangerous situation, such as a fire or a shooting.
tile	A tile is an individual window within the canvas, used to display a single entity. The entity displayed is typically the video from a camera, a map, or anything of a graphical nature. The look and feel of the tile depends on the displayed entity.
tile ID	The tile ID is the number displayed at the upper left corner of the tile. This number uniquely identifies each tile within the canvas.
tile mode	Tile mode is the main Security Desk canvas operating mode that presents information in separate tiles.
tile pattern	The tile pattern is the arrangement of tiles within the canvas.
tile plugin	A tile plugin is a software component that runs inside a Security Desk tile. By default, it is represented by a green puzzle piece in the area view.
timeline	A timeline is a graphic illustration of a video sequence, showing where in time, motion, and bookmarks are found. Thumbnails can also be added to the timeline to help the user select the segment of interest.
twilight schedule	A twilight schedule is a type of schedule entity that supports both daytime and nighttime coverages. A twilight schedule cannot be used in all situations. Its primary function is to control video related behaviors.
unit	A unit is a hardware device that communicates over an IP network that can be directly controlled by a Security Center role. We distinguish four types of units in Security Center: • Access control units, managed by the Access Manager role • Video units, managed by the Archiver role • ALPR units, managed by the ALPR Manager role • Intrusion detection units, managed by the Intrusion Manager role

Unit discovery tool	Starting with Security Center 5.4 GA the Unit discovery tool has been replaced by the Unit enrollment tool.
Unit replacement	Unit replacement is a tool that is used to replace a failed hardware device with a compatible one, while ensuring that the data associated to the old unit gets transferred to the new one. For an access control unit, the configuration of the old unit is copied to the new unit. For a video unit, the video archive associated to the old unit is now associated to the new unit, but the unit configuration is not copied.
University Parking Enforcement	University Parking Enforcement is a Genetec Patroller™ software installation that is configured for university parking enforcement: the enforcement of scheduled parking permits or overtime restrictions. The use of maps is mandatory. Hotlist functionality is also included.
unreconciled read	A unreconciled read is a MLPI license plate read that has not been committed to an inventory.
user	A user is a type of entity that identifies a person who uses Security Center applications and defines the rights and privileges that person has on the system. Users can be created manually or imported from an Active Directory.
user group	A user group is a type of entity that defines a group of users who share common properties and privileges. By becoming member of a group, a user automatically inherits all the properties of the group. A user can be a member of multiple user groups. User groups can also be nested.
user level	A user level is a numeric value assigned to users to restrict their ability to perform certain operations, such as controlling a camera PTZ, viewing the video feed from a camera, or staying logged on when a threat level is set. Level 1 is the highest user level, with the most privileges.
validation key	A validation key is a serial number uniquely identifying a computer that must be provided to obtain the license key.
vehicle identification number	A vehicle identification number (VIN) is an identification number that a manufacturer assigns to vehicles. This is usually visible from outside the vehicle as a small plate on the dashboard. A VIN can be included as additional information with license plate entries in a hotlist or permit list, to further validate a hit and ensure that it is the correct vehicle.
virtual zone	A virtual zone is a zone entity where the I/O linking is done by software. The input and output devices can belong to different units of different types. A virtual zone is controlled by the Zone Manager and only works when all the units are online. It can be armed and disarmed from Security Desk.

watchdog	Watchdog is a Security Center service installed alongside the Genetec Server service on every server computer. The watchdog monitors the Genetec Server service, and restarts it if abnormal conditions are detected.
Web-based SDK	The Web-based SDK role exposes the Security Center SDK methods and objects as web services to support cross-platform development.
Web Client	Security Center Web Client is the web application that gives users remote access to Security Center so that they can monitor videos, investigate events related to various system entities, search for and investigate alarms, and manage cardholders, visitors, and credentials. Users can log on to Web Client from any computer that has a supported web browser installed.
Web Map Service	Web Map Service (WMS) is a standard protocol for serving georeferenced map images over the Internet that are generated by a map server using data from a GIS database.
wheel imaging	Wheel imaging is a virtual tire-chalking technology that takes images of the wheels of vehicles to prove whether they have moved between two license plate reads.
widget	A widget is a component of the graphical user interface (GUI) with which the user interacts.
Windows Communication Foundation	Windows Communication Foundation (WCF) is a communication architecture used to enable applications, in one machine or across multiple machines connected by a network, to communicate. Genetec Patroller™ uses WCF to communicate wirelessly with Security Center.
zone	A zone is a type of entity that monitors a set of inputs and triggers events based on their combined states. These events can be used to control output relays.
Zone activities	Zone activities is a type of investigation task that reports on zone related activities (zone armed, zone disarmed, lock released, lock secured, and so on).
Zone Manager	Zone Manager is a type of role that manages virtual zones and triggers events or output relays based on the inputs configured for each zone. It also logs the zone events in a database for zone activity reports.
Zone occupancy	Zone occupancy is a type of investigation task that reports on the number of vehicles parked in a selected parking area, and the percentage of occupancy.

Where to find product information

You can find our product documentation in the following locations:

- **Genetec™ TechDoc Hub:** The latest documentation is available on the TechDoc Hub. To access the TechDoc Hub, log on to Genetec™ Portal and click TechDoc Hub. Can't find what you're looking for? Contact documentation@genetec.com.
- **Installation package:** The Installation Guide and Release Notes are available in the Documentation folder of the installation package. These documents also have a direct download link to the latest version of the document.
- **Help:** Security Center client and web-based applications include help, which explains how the product works and provide instructions on how to use the product features. To access the help, click **Help**, press F1, or tap the **?** (question mark) in the different client applications.

Technical support

Genetec™ Technical Assistance Center (GTAC) is committed to providing its worldwide clientele with the best technical support services available. As a customer of Genetec Inc., you have access to TechDoc Hub, where you can find information and search for answers to your product questions.

- **Genetec™ TechDoc Hub:** Find articles, manuals, and videos that answer your questions or help you solve technical issues.

  Before contacting GTAC or opening a support case, it is recommended to search TechDoc Hub for potential fixes, workarounds, or known issues.

  To access the TechDoc Hub, log on to Genetec™ Portal and click TechDoc Hub. Can't find what you're looking for? Contact documentation@genetec.com.
- **Genetec™ Technical Assistance Center (GTAC):** Contacting GTAC is described in the Genetec™ Lifecycle Management (GLM) documents: Genetec™ Assurance Description and Genetec™ Advantage Description.

Additional resources

If you require additional resources other than the Genetec™ Technical Assistance Center, the following is available to you:

- **Forum:** The Forum is an easy-to-use message board that allows clients and employees of Genetec Inc. to communicate with each other and discuss many topics, ranging from technical questions to technology tips. You can log on or sign up at https://gtapforum.genetec.com.
- **Technical training:** In a professional classroom environment or from the convenience of your own office, our qualified trainers can guide you through system design, installation, operation, and troubleshooting. Technical training services are offered for all products and for customers with a varied level of technical experience, and can be customized to meet your specific needs and objectives. For more information, go to http://www.genetec.com/support/training/training-calendar.

Licensing

- For license activations or resets, please contact GTAC at https://gtap.genetec.com.
- For issues with license content or part numbers, or concerns about an order, please contact Genetec™ Customer Service at customerservice@genetec.com, or call 1-866-684-8006 (option #3).
- If you require a demo license or have questions regarding pricing, please contact Genetec™ Sales at sales@genetec.com, or call 1-866-684-8006 (option #2).

Hardware product issues and defects

Please contact GTAC at https://gtap.genetec.com to address any issue regarding Genetec™ appliances or any hardware purchased through Genetec Inc.



Security Center AutoVu™

SharpZ3 Administrator Guide 13.1

Document last updated: June 30, 2020

Genetec™

Legal notices

©2020 Genetec Inc. All rights reserved.

Genetec Inc. distributes this document with software that includes an end-user license agreement and is furnished under license and may be used only in accordance with the terms of the license agreement. The contents of this document are protected under copyright law.

The contents of this guide are furnished for informational use only and are subject to change without notice. Genetec Inc. assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this guide.

This publication may not be copied, modified, or reproduced in any form or for any purpose, nor can any derivative works be created therefrom without Genetec Inc.'s prior written consent.

Genetec Inc. reserves the right to revise and improve its products as it sees fit. This document describes the state of a product at the time of document's last revision, and may not reflect the product at all times in the future.

In no event shall Genetec Inc. be liable to any person or entity with respect to any loss or damage that is incidental to or consequential upon the instructions found in this document or the computer software and hardware products described herein.

Genetec™, AutoVu™, AutoVu MLC™, Citywise™, Community Connect™, Curb Sense™, Federation™, Flexreader™, Genetec Airport Sense™, Genetec Citigraf™, Genetec Clearance™, Genetec ClearID™, Genetec Mission Control™, Genetec Motoscan™, Genetec Patroller™, Genetec Retail Sense™, Genetec Traffic Sense™, Omnicast™, Sipelia™, Stratocast™, Streamvault™, Synergis™, Valcri™, their respective logos, as well as the Mobius Strip Logo are trademarks of Genetec Inc., and may be registered or pending registration in several jurisdictions.

KiwiSecurity™, KiwiVision™, Privacy Protector™ and their respective logos are trademarks of KiwiSecurity Software GmbH, and may be registered or pending registration in several jurisdictions.

Other trademarks used in this document may be trademarks of the manufacturers or vendors of the respective products.

Patent pending. Genetec™ Security Center, Omnicast™, AutoVu™, Stratocast™, Citigraf™, Genetec Clearance™, and other Genetec™ products are the subject of pending patent applications, and may be the subject of issued patents, in the United States and in other jurisdictions worldwide.

All specifications are subject to change without notice.

Document information

Document title: SharpZ3 Administrator Guide 13.1

Original document number: EN.430.004-V13.1.1B(2)

Document number: EN.430.004-V13.1.1B(2)

Document update date: June 30, 2020

You can send your comments, corrections, and suggestions about this guide to documentation@genetec.com.

About this guide

This guide provides you with a complete source of information about the SharpZ3 web portal and how to configure your SharpZ3 cameras. It explains the basic settings you must configure before your SharpZ3 can be used.

You can customize your AutoVu™ SharpZ3 system to fit several different deployment types (for example, parking enforcement or law enforcement).

Depending on the type of deployment you require, you might not need to perform all of the steps listed in this document. For installation and configuration information related to your AutoVu™ solution, follow the steps in the appropriate deployment overview.

WARNING: Only AutoVu™-certified personnel should set up and install AutoVu™ systems. Read all of the procedures in this guide before installing an AutoVu™ system. Failure to follow the supplied instructions or information might result in loss of data or damage to hardware and will void the warranty.

Notes and notices

The following notes and notices might appear in this guide:

- **Tip:** Suggests how to apply the information in a topic or step.
- **Note:** Explains a special case or expands on an important point.
- **Important:** Points out critical information concerning a topic or step.
- **Caution:** Indicates that an action or step can cause loss of data, security problems, or performance issues.
- **Warning:** Indicates that an action or step can result in physical harm, or cause damage to hardware.

IMPORTANT: Content in this guide that references information found on third-party websites was accurate at the time of publication, however, this information is subject to change without prior notice from Genetec Inc.

Contents

Preface

Legal notices . . . ii
About this guide . . . iii

Chapter 1: Getting started

About Security Center AutoVu™ . . . 2
ALPR using machine learning . . . 3
Specifications for the SharpZ3 . . . 4
Genetec™ server configurations for AutoVu™ systems . . . 7
Storage requirement for ALPR images . . . 9
Supported ALPR contexts . . . 11
Supported plate origin recognition . . . 14

Chapter 2: Introduction to the Sharp portal

About the Sharp Portal . . . 16
Logging on to the Sharp Portal . . . 17
Changing your logon password in the Sharp Portal . . . 21
Sharp Portal interface overview . . . 22
Viewing camera feeds . . . 24
SharpZ3 hardware inventory . . . 26
Rebooting the SharpZ3 ALPR module . . . 27
Synchronizing the SharpZ3 clock . . . 28
Configuring battery monitoring . . . 29

Chapter 3: SharpZ3 camera configuration

Security configuration in the Sharp Portal . . . 32
- Installing the SharpZ3 auto-generated certificate . . . 32
- Installing a self-signed certificate . . . 34
- Installing a signed certificate . . . 36

About SharpZ3 exposure adjustment . . . 38
- Setting custom SharpZ3 ALPR camera exposure levels . . . 38
- Troubleshooting outdoor exposure issues for the SharpZ3 ALPR camera . . . 39
- Troubleshooting outdoor exposure issues for the SharpZ3 context camera . . . 40

Configuring SharpZ3 position and location . . . 41
Associating wheel-imaging cameras with SharpZ3 camera units . . . 43
Configuring SharpZ3 analytics . . . 46
Configuring where the SharpZ3 sends its ALPR data . . . 48
About SharpZ3 network settings . . . 49
- Configuring the SharpZ3 system to use a specific IP address range . . . 50

Configuring the SharpZ3 FTP extension . . . 53
- Modifications you can make to the SharpZ3 FTP XML template . . . 54

Configuring the SharpZ3 HTTP/HTTPS extension . . . 56
- Examples of JSON and XML ALPR events for the SharpZ3 HTTP extension . . . 57

Configuring Syslog for SharpZ3 log files . . . 60
Importing and exporting settings . . . 61

Chapter 4: Troubleshooting for SharpZ3 installation

LED status on the SharpZ3 camera unit 64
Resetting a lost password for the Sharp Portal 67

Chapter 5: Updating the system

Updating a Sharp unit from the SharpOS 13 Sharp Portal 70

Chapter 6: Sharp Portal reference

Sharp Portal - Overview page 74
Sharp Portal - Camera feeds page 76
Sharp Portal - Inventory page 78
Sharp Portal - Network page 79
Sharp Portal - Security page 80
Sharp Portal - Exposure page 82
Sharp Portal - Position and orientation page 83
Sharp Portal - Auxiliary cameras page 84
Sharp Portal - ALPR settings page 85
Sharp Portal - Extension page 86
Sharp Portal - Product improvement program page 88
Sharp Portal - Recovery page 89
Sharp Portal - Date and time page 90
Sharp Portal - Power options page 91
Sharp Portal - Maintenance page 92
Sharp Portal - Logs page 93
Sharp Portal - Log sources page 94

Glossary 95

Where to find product information 111
Technical support 112

1

Getting started

This section includes the following topics:

- "About Security Center AutoVu™" on page 2
- "ALPR using machine learning" on page 3
- "Specifications for the SharpZ3 " on page 4
- "Genetec™ server configurations for AutoVu™ systems" on page 7
- "Storage requirement for ALPR images" on page 9
- "Supported ALPR contexts" on page 11
- "Supported plate origin recognition" on page 14

About Security Center AutoVu™

The AutoVu™ automatic license plate recognition (ALPR) system automates license plate reading and identification, making it easier for law enforcement and for municipal and commercial organizations to locate vehicles of interest and enforce parking restrictions. Designed for both fixed and mobile installations, the AutoVu™ system is ideal for a variety of applications and entities, including law enforcement, municipal, and commercial organizations.

Depending on the Sharp hardware you install, you can use AutoVu™ in a fixed configuration such as on a pole in a parking lot, or in a mobile configuration such as on a patrol vehicle.

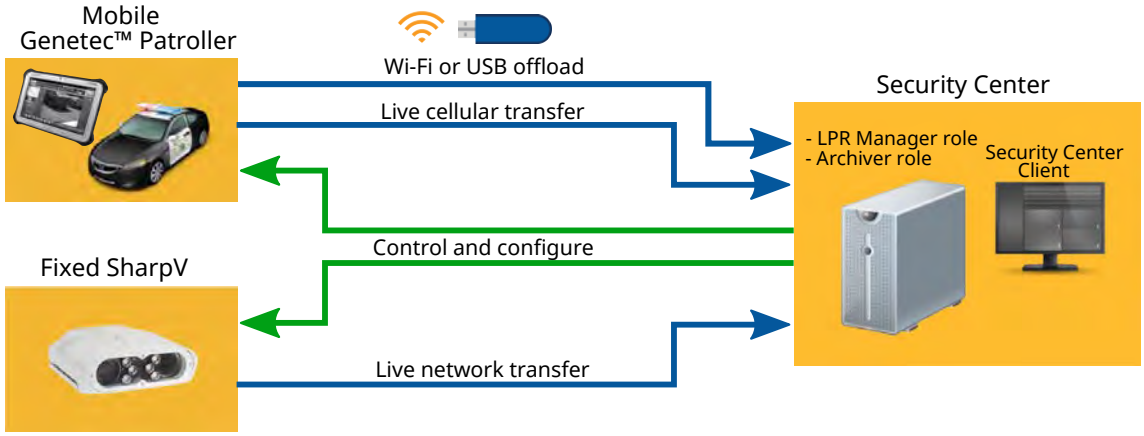
You can use AutoVu™ for the following:

- Scofflaw and wanted vehicle identification
- City-wide surveillance
- Parking enforcement
- Parking permit control
- Vehicle inventory
- Security
- Access control

AutoVu™ system architecture

AutoVu™ Sharp cameras capture license plate images, and send the data to Genetec Patroller™ or Security Center to verify against lists of vehicles of interest (hotlists) and vehicles with permits (permit lists).

The following diagram shows how a typical AutoVu™ system works:



Example

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages. If using Internet Explorer, the video might not display. To fix this, open the **Compatibility View Settings** and clear **Display intranet sites in Compatibility View**.

ALPR using machine learning

Sharp systems running SharpOS 13 use machine learning to classify license plates and to perform character recognition.

AutoVu MLC™

AutoVu MLC™ (Machine Learning Core) replaces traditional rule-based ALPR technology with machine learning-based algorithms to reduce common ALPR misreads and false positives. It is a proprietary technology of Genetec Inc. used in AutoVu™ Sharp hardware for license plate recognition.

Although off-the-shelf machine learning solutions are commercially available for ALPR, their results can be unpredictable. With our hardware and software engineering expertise, we have built the AutoVu MLC™ from the ground up. This includes developing a deep neural network (DNN), training the system with Sharp camera images, and optimizing the system to run on AutoVu™ hardware. The AutoVu MLC™ represents a significant reduction in the time that operators spend manually correcting plate reads.

As the AutoVu™ MLC continues to develop, we will apply it to more aspects of the ALPR process. You will be able to take advantage of these improvements with future SharpOS releases.

Specifications for the SharpZ3

Refer to the technical, mechanical, and environmental specifications when planning and deploying a SharpZ3 system.

SharpZ3 camera specifications

Specification	Details
ALPR camera sensors	1456(H) x 1088(V) progressive scan @30fps, monochrome, global shutter
ALPR capture range	Up to 63-foot (19-meter) range with retro-reflective license plates
ALPR camera lens options	8mm, 12mm, 16mm, 25mm
Context camera sensor	• 1456(H) x 1088(V) progressive scan @30 fps • Color • B&W night mode with 940nm illuminator • Global shutter • JPEG still images and MJPEG video streaming
Context camera lens	Based on ALPR lens configuration: 4mm, 6mm, 8mm, 12mm
Illuminator	• Pulsed LED illuminator (740nm, 850nm, 940nm, 590nm)
Water-resistance | sealing	IEC 60529 IPx6, IPx7 | IEC 60529 IP6x
Dimensions	1.65 (h) x 5.12 (w) x 3.56 (d) inches (4.2 x 13 x 9 cm) | Excludes cabling and mounting bracket
Weight	1.2 lbs (0.54 kg)
Color	Available in black/white

SharpZ3 base unit specifications

Specification	Details
I/O	Base unit: 2x 10/100/1000 Base-T Ethernet ports (RJ45) 4x digital inputs (triggers), 0~32Vdc, opto-coupled 4x dry-contact outputs (relays): 2x 0.25A solid state relays, 2x 8A electromechanical relays 1x regulated 12V AUX output power, 200ma
Mounting options	Horizontal and vertical
Dimensions	3.6 (h) x 8.6 (w) x 9.3 (d) inches (9.1 x 21.8 x 23.6 cm). Excludes cabling, cable racks and mounting brackets

Specification	Details
Weight	Base unit: 4.4 lbs (2.0 kg) ALPR module: 2-ports: 4.1 lbs (1.9 kg) ALPR module: 4-ports: 4.4 lbs (2.0 kg)
Processors	Intel Atom Processor E3950 Intel Myriad X VPU (machine-learning co-processor)
Power	12/24Vdc nominal (9 to 32 Vdc) **Optional modules:** 2x ALPR base unit module: Typical power consumption: 50W 4x ALPR base unit module: Typical power consumption: 98W

SharpZ3 system certification (camera and base unit)

Specification	Details
Vibration	IEC 60068-2-64
Shock resistance	IEC 60068-2-27
Electromagnetic immunity and emissions	FCC part 15 Sub-part B | ICES-003 Issue 4 | CISPR32 / EN55032 | CISPR35 / EN55035 | CISPR25 / EN55025 | EN 50498
CE marking	EMC Directive 2014/30/EU; Automotive EMC Directive 2004/104/EC; RoHS Directive 2011/65/EU
Temperature	-40°F to 122°F (-40°C to 50°C) operating; -40°F to 185°F (-40°C to 85°C) storage -40°F to 149°F (-40°C to 65°C) base unit operating, w/optional cooling pack Certifications: IEC 60068-2-1 Category Ad | IEC 60068-2-2 Category Bd | IEC 60068-2-14 Category Na Includes hi-temp auto-shutoff protection

Part numbers



Component	Signification
A	SharpZ3 prefix
B	Color: **W** (white) or **B** (black)

Component	Signification	
C	Primary ALPR lens:	• **Focal length:** 8 mm, 12 mm, 16 mm, 25 mm • **Filter:** F: Monochrome sensor with filter M: Monochrome sensor without filter C: Color sensor with filter
D	Secondary ALPR lens:	
E	LED	• **Illumination:** 590 nm, 740 nm, 850 nm, 940 nm

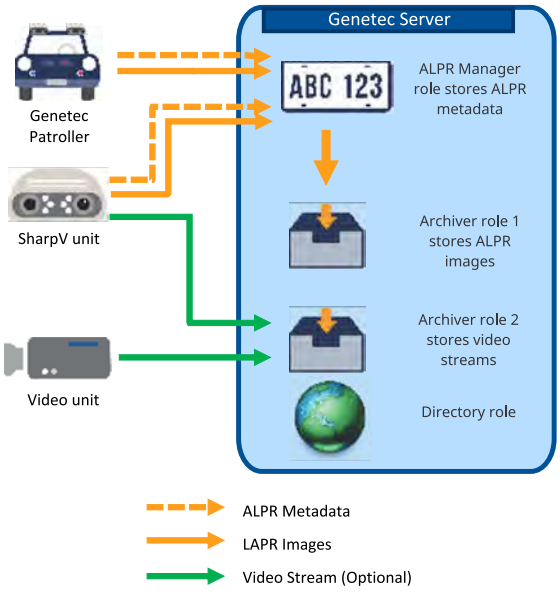
Genetec™ server configurations for AutoVu™ systems

Depending on the requirements of the system, you can install the AutoVu™ system on one server or distribute the load over multiple servers.

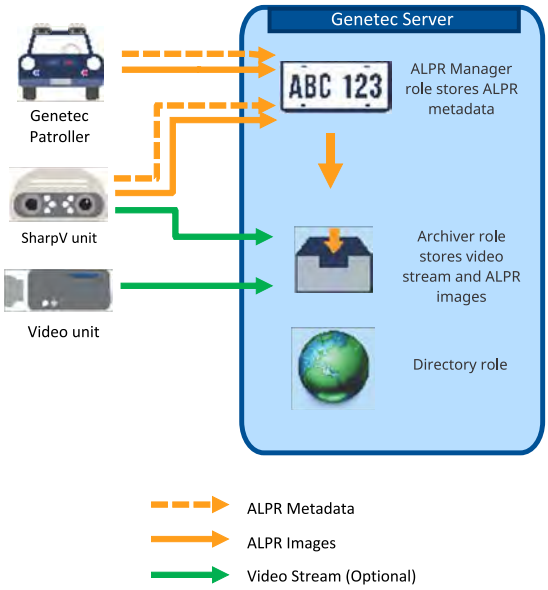
Single server

In a single-server system, the ALPR Manager, Archiver, and Directory roles are configured on the same server. For better performance, you can configure separate Archiver roles for ALPR and video.

Recommended server configuration



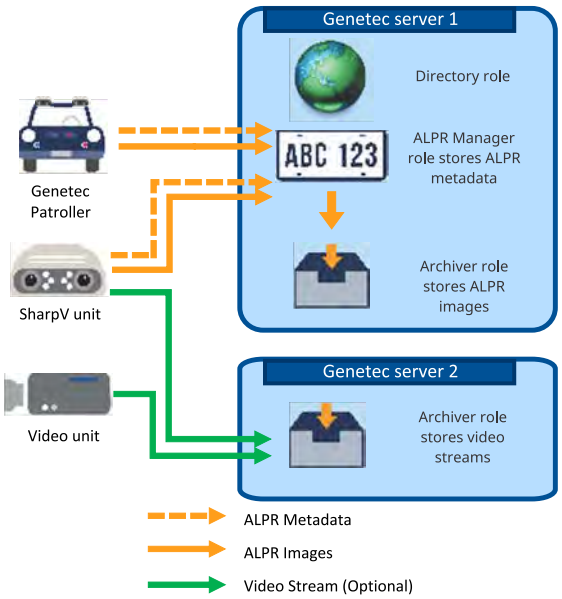
Small system server configuration



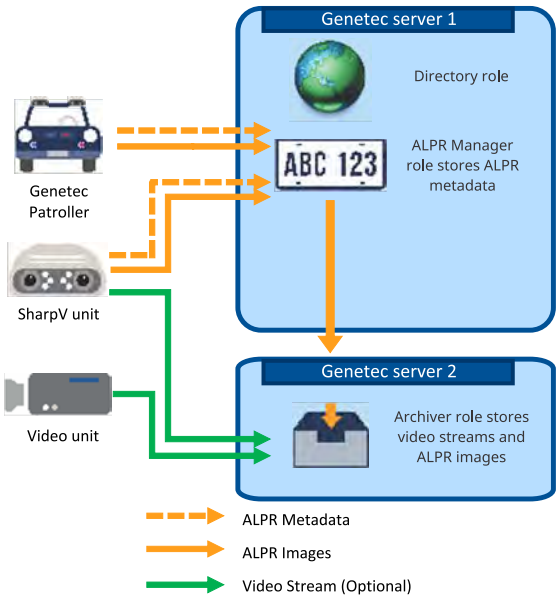
Multiple servers

In a multiple-server system, the Archiver role is installed on a separate server from the ALPR Manager and Directory roles. For better performance, you can configure separate Archiver roles for ALPR and video.

Recommended server configuration



Small system server configuration



Storage requirement for ALPR images

The images associated with the reads and hits are stored on disk in G64 files by an Archiver. You can estimate the disk space required to store these images if you know the average number of reads and hits processed by the ALPR Manager per day.

For every license plate read or hit processed by the ALPR Manager, the Archiver stores a set of four images:

- One context camera image (in either high resolution or low resolution)
- One ALPR camera image (cropped to show only the license plate)
- One context camera thumbnail image
- One ALPR camera thumbnail image

The size of the image set depends on the model of the Sharp camera and whether the context camera is configured to take images in high resolution or low resolution.

Use the following formula to estimate the disk space you need for the desired image retention periods.

```
Disk space = (ReadsPD x ImageSize x ReadIRP) + (HitsPD x ImageSize x HitIRP)
```

where:

- **ReadsPD:** Average number of reads per day.
- **ImageSize:** Estimated image size per read (depends on the Sharp model and configuration).
- **ReadIRP:** Read image retention period (see ALPR Manager's **Properties** tab).
- **HitsPD:** Average number of hits per day.
- **HitIRP:** Hit image retention period (see ALPR Manager's **Properties** tab).

If your patrol vehicles are equipped with wheel imaging cameras, double the number of hits per day in your formula (there is typically one wheel image per hit).

The following table gives you the rough estimates of the image size per read based on the Sharp model and configuration.

Type of image	Sharp VGA or XGA	SharpV	SharpZ3
High-resolution configuration			
Context camera image	~50 KB	~120 KB	~160 KB
ALPR camera image (cropped)	~3 KB	~3 KB	~2 KB
Context camera thumbnail image	~3 KB	~3 KB	~2 KB
ALPR camera thumbnail image	~1 KB	~1 KB	~1 KB
Total image size per read:	~57 KB	~127 KB	~165 KB
Low-resolution configuration			
Context camera image	~18 KB	-	-
ALPR camera image (cropped)	~3 KB	~3 KB	-
Context camera thumbnail image	~3 KB	~3 KB	-

Type of image	Sharp VGA or XGA	SharpV	SharpZ3
ALPR camera thumbnail image	~1 KB	~1 KB	-
Total image size per read:	~25 KB	-	-

NOTE: If a read or hit is protected and must be kept beyond its specified retention period, it will require more disk space for its associated images than what is calculated for a single event. Because the Archiver stores multiple ALPR images in a single G64 file, if one image in the file is protected, then all other images in the file are also protected. This uses up more disk space over time. However, an image whose corresponding read or hit has been deleted can no longer be read because the G64 files are encrypted.

If the Archiver is assigned to more than one ALPR Manager, add the numbers for all ALPR Manager roles together.

Supported ALPR contexts

ALPR contexts are created for specific regions in order to optimize ALPR for the license plates of that region.

NOTE: To help us improve the performance of regional contexts, click **Configuration** > **Connectivity** > **Product improvement** and register this camera to participate in the **Product improvement program**.

ALPR contexts are available for the following license plates:

Asia-Pacific

- Australia (optimized for New South Wales)
- Hong Kong
- India
- Japan
- Mongolia
- Northern territory (Australia)
- New Zealand
- Queensland (Australia)
- Singapore
- Sri Lanka[20]
- Turkmenistan
- Vietnam
- Western Australia

Caribbean and Latin America

- Argentina
- ArgentinaMulti[17]
- Bahamas
- Bermuda
- Brazil
- Cayman Islands
- Chile
- Colombia
- Costa Rica
- Dominican Republic
- Mexico
- Mexico Jalisco
- Paraguay
- Peru
- St-Maarten

Europe/Middle East/Africa

- Abu Dhabi
- Abu Dhabi WithPrefix[18]
- Algeria
- Arabic Peninsula[1]
- Azerbaijan
- Bahrain
- Belgium[9]
- BelgiumMulti[10]
- BelgiumMultiVanity[11]
- Denmark
- Dubai
- DubaiWithPrefix[18]
- Europe[2]
- Europe One and Two Lines[3]
- France
- Great Britain
- General European context
- Germany
- Iceland
- Ireland
- Italy
- Ivory Coast
- Jordan
- Kazakhstan
- Kuwait
- Lebanon
- Monaco
- Morocco
- Netherlands
- Norway
- Oman[4]
- Poland
- Portugal
- Qatar
- QatarMilitary[12]
- Romania
- Saudi Arabia
- Sharjah
- Sharjah WithPrefix[18]
- Slovakia
- South Africa
- Spain
- Sweden
- Switzerland
- Turkey
- TurkeyOnly[13]
- United Arab Emirates[5]
- United Arab Emirates WithPrefix[18]

North America

- Alabama
- Alberta
- Arizona
- British Columbia
- British Columbia Fixed[14]
- California
- Colorado
- Connecticut
- Delaware
- Florida
- General US context
- Georgia
- Georgia_3Chars[21]
- Hawaii
- Idaho
- Illinois
- Indiana
- Iowa
- Kansas
- Kentucky
- KentuckyIndiana
- Louisiana
- Maine
- Manitoba
- Maryland
- Massachusetts
- MassachusettsIR[15]
- Michigan
- Minnesota
- Mississippi
- Montana
- Nebraska
- Nevada
- New Brunswick
- Newfoundland
- New Hampshire
- New Jersey
- New Mexico
- New York
- New York City[16]
- North Carolina
- North Dakota
- Northeast states[6]
- Nova Scotia
- Ohio
- Oklahoma
- Ontario
- Oregon
- Pennsylvania
- PennsylvaniaDelaware[6]
- Prince Edward Island
- Quebec
- Rhode Island
- Saskatchewan
- South Carolina
- South Dakota
- Tennessee
- Texas
- Utah and Neighbors[8]
- Vermont
- Virginia
- Washington State[19]
- Wisconsin
- Wyoming
- Yukon

[1]Includes Saudi Arabia, Bahrain, Kuwait, and UAE.

[2]General European context for one-line plates.

[3]General European context for one-line and two-line plates.

[4]Only standard Omani plates are supported (wide-format, black-on-white, and black-on-yellow). License plates issued by neighboring countries are not supported.

[5]Includes Abu Dhabi, Dubai, and Sharjah plates.

[6]Includes Delaware, New York, Pennsylvania, and Vermont plates.

[7]Includes Pennsylvania, Delaware, Florida, Vermont, and New York plates.

[8]Includes Utah, Oregon, Montana, and North Dakota plates.

[9]Supports one-line plates with five or more characters.

[10]Supports one-line and two-line plates with five or more characters.

[11]Supports one-line and two-line plates with three or more characters. Note that this context can produce many false positive reads.

[12]Exposure settings are optimized for non-reflective military plates. Note that performance with standard plates might be reduced.

[13]Excludes the letters Q, W, and X. Note that foreign plates that contain these characters are not read correctly.

[14]Optimized for fixed installations.

[15]Optimized for SharpZ3 cameras with 850nm IR illuminators.

[16]Exposure settings are optimized for non-reflective taxi plates. Note that performance with standard plates might be reduced.

[17]Supports standard and motorcycle plates.

[18]*WithPrefix* includes characters that are present on the plate, but are separate from the license plate read.

[19]Specialized ALPR contexts available for ABMER (590 nm) and IR (850nm) illuminators.

[20]Supports Latin characters only.

[21]Supports plates with three or more characters. Note that using this context might increase the false positive count.

Supported plate origin recognition

In addition to reading the number on a license plate, the SharpZ3 can also read the state, province, or country. Plate origin recognition is performed on a best-effort basis, and is not necessarily available for the same plates that have a supported ALPR context.

Plate origin recognition is supported for the following plates:

Europe/Middle East/Africa

- Abu Dhabi (AD)
- Ajman (AJ)
- Bahrain (BRN)
- Belgium (B)
- Denmark (DK)
- Dubai (DUB)
- France (F)
- Fujairah (FUJ)
- Germany (D)
- Great Britain (GB)
- Italy (I)
- Kuwait (KWT)
- Netherlands (NL)
- Norway (N)
- Poland (PL)
- Portugal (P)
- Ras al Khaimah (RAK)
- Romania (RO)
- Saudi Arabia (KSA)
- Sharjah (SHJ)
- Slovakia (SK)
- Switzerland (CH)
- Spain (E)
- Umm al Qaiwain (UAQ)

North America

- Alabama (AL)
- Alberta (AB)
- Arizona (AZ)
- Arkansas (AR)
- British Columbia (BC)
- California (CA)
- Colorado (CO)
- Connecticut (CT)
- Delaware (DE)
- District of Columbia (DC)
- Florida (FL)
- Georgia (GA)
- Hawaii (HI)
- Idaho (ID)
- Illinois (IL)
- Indiana (IN)
- Iowa (IA)
- Kansas (KS)
- Kentucky (KY)
- Louisiana (LA)
- Maine (ME)
- Manitoba (MB)
- Maryland (MD)
- Massachusetts (MA)
- Michigan (MI)
- Minnesota (MN)
- Mississippi (MS)
- Missouri (MO)
- Montana (MT)
- Nebraska (NE)
- Nevada (NV)
- New Brunswick (NB)
- Newfoundland and Labrador (NL)
- New Hampshire (NH)
- New Jersey (NJ)
- New Mexico (NM)
- New York (NY)
- North Carolina (NC)
- North Dakota (ND)
- Nova Scotia (NS)
- Ohio (OH)
- Oklahoma (OK)
- Ontario (ON)
- Oregon (OR)
- Pennsylvania (PA)
- Price Edward Island (PEI)
- Rhode Island (RI)
- Quebec (QC)
- Saskatchewan (SK)
- South Carolina (SC)
- South Dakota (SD)
- Tennessee (TN)
- Texas (TX)
- US Government (GOV)
- Utah (UT)
- Vermont (VT)
- Virginia (VA)
- Washington (WA)
- West Virginia (WV)
- Wisconsin (WT)
- Wyoming (WY)
- Yukon (YT)

2

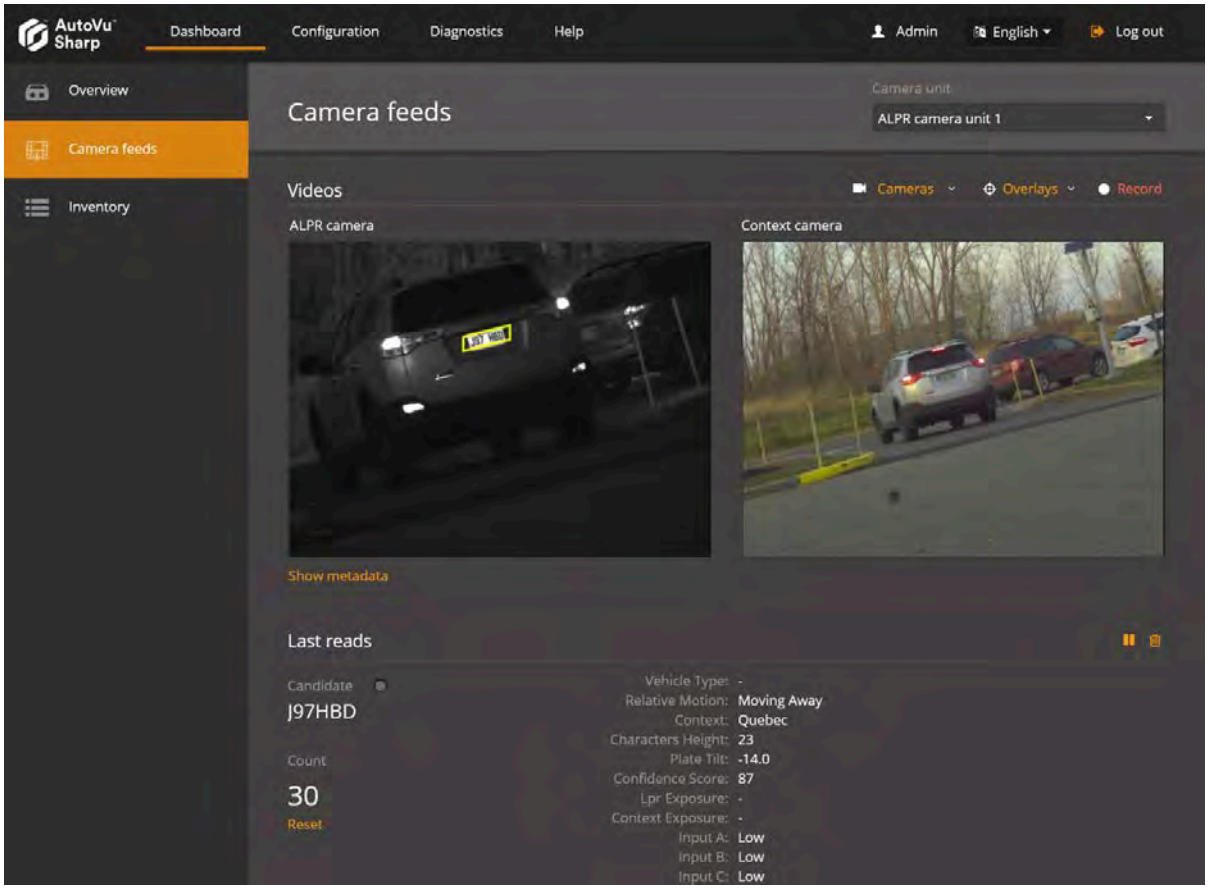
Introduction to the Sharp portal

This section includes the following topics:

- "About the Sharp Portal" on page 16
- "Logging on to the Sharp Portal" on page 17
- "Changing your logon password in the Sharp Portal" on page 21
- "Sharp Portal interface overview" on page 22
- "Viewing camera feeds" on page 24
- "SharpZ3 hardware inventory" on page 26
- "Rebooting the SharpZ3 ALPR module" on page 27
- "Synchronizing the SharpZ3 clock" on page 28
- "Configuring battery monitoring" on page 29

About the Sharp Portal

The Sharp Portal is a web-based administration tool used to configure Sharp cameras for AutoVu™ systems. From a web browser, you log on to a specific IP address (or the Sharp name in certain cases) that corresponds to the Sharp you want to configure. When you log on, you can configure options such as selecting the ALPR context (for example, Alabama, Oregon, Quebec), selecting the read strategy (for example, fast moving or slow moving vehicles), viewing the Sharp's live video feed, and more.



Benefits of the Sharp Portal

- **Open Sharp Portals in many tabs:** Web browsers use tab-based browsing, which provides you with a simple way to configure multiple SharpZ3 cameras. You can have many instances of the Sharp Portal open within the same Web browser.
- **Secure connection:** You can log on to the Sharp Portal securely using an HTTPS protocol with SSL encryption.
- **Use Favorites:** You can easily monitor and configure all the SharpZ3 units on your network. For example, if you have multiple SharpZ3 units on your network, you can add them all to your Web browser's Favorites folder, and then rename them (for example, SharpNorthParkingLot) for quick configuration and maintenance.

Logging on to the Sharp Portal

To configure SharpZ3 cameras, you must log on to the Sharp Portal.

Before you begin

- You need to know the IP address or name of the SharpZ3 camera you want to connect to:
  - **Fallback IP address:** The fallback IP address is `192.168.10.99`. The fallback IP address is only available if the camera is in DHCP mode (default). After camera startup, the camera searches for a DHCP server. If no DHCP server is present on the network after two minutes, the fallback IP address is made available.

What you should know

- You can access the Sharp Portal using the following browsers:
  - Microsoft Edge version 41 and later
  - Google Chrome version 46 and later
- To ensure that camera feeds are displayed correctly, only open one instance of the Sharp Portal at a time.

To log on to the Sharp Portal:

1 Open your Web browser, and go to `https://<SharpZ3 name or IP address>`.

A two-camera ALPR module is configured through one Sharp Portal; a four-camera ALPR module is configured through two Sharp Portals.

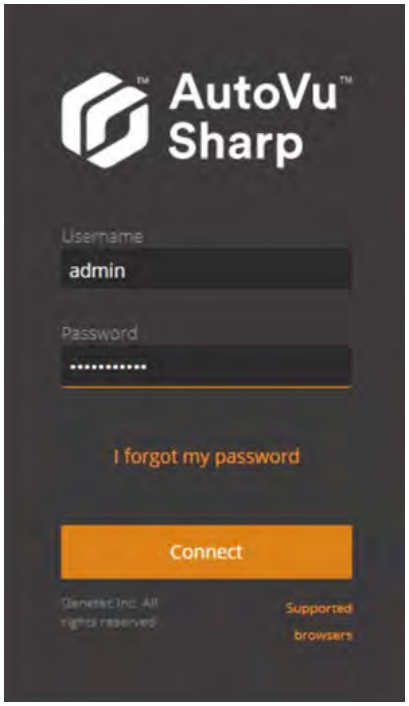
- **Sharp Portal 1 (camera ports 1 and 2):** http://192.168.10.1/
- **Sharp Portal 2 (camera ports 3 and 4):** http://192.168.10.2/



2 Enter the **Username** and **Password**.

- If you have already logged on and changed the default password, enter your **Username** and **Password** and click **Connect**.
- If this is the first time you are logging on to the Sharp Portal for this unit, enter the default credentials
  - **Username:** admin
  - **Password:** Genetec

3 Click **Connect**.



4 Select the power line frequency that corresponds to the installation location.

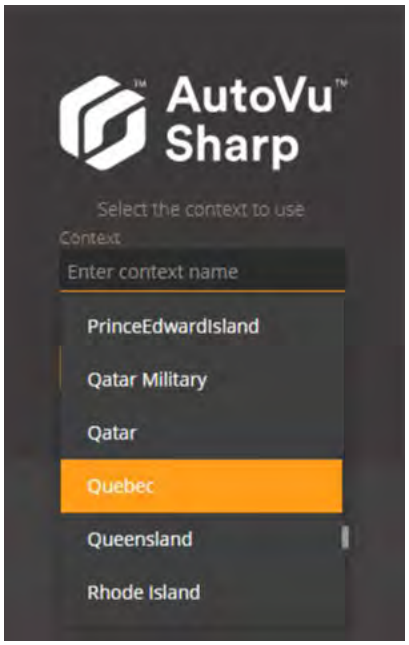


- **60 Hz:** Generally used in North America and South America
- **50 Hz:** Generally used in Africa, Australia, Asia, and Europe

NOTE: For more information on the power line frequency used in your installation location, click here.

5 Click **Enter context name** and select which regional context to use.

NOTE: You can change the regional context when you configure analytics for the SharpZ3.



6 Click **Next**.

7 Enter and confirm a new password.

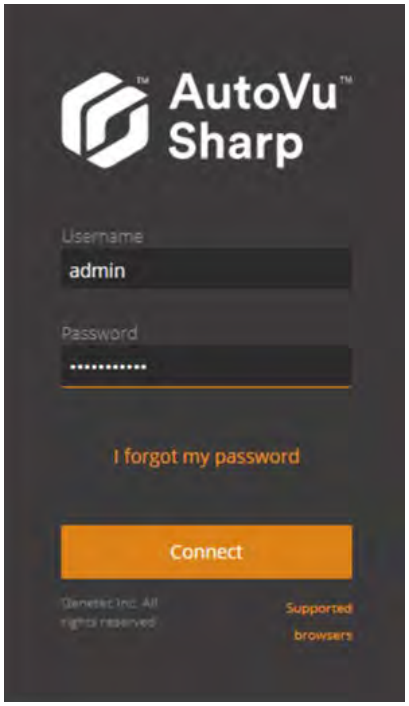


NOTE: You cannot modify the username.

8 Click **Next**.

9 You are redirected to the logon page. Enter the **Username** and new **Password**, then click **Connect**.

10 Click **Connect**.



After successfully logging on, the Sharp Portal opens to the **Overview** page of the **Dashboard** menu.

Changing your logon password in the Sharp Portal

For security reasons, you might need to change the logon password for the Sharp unit. You can do this in the Sharp Portal.

What you should know

A two-camera ALPR module is configured through one Sharp Portal; a four-camera ALPR module is configured through two Sharp Portals.

- **Sharp Portal 1 (camera ports 1 and 2):** http://192.168.10.1/
- **Sharp Portal 2 (camera ports 3 and 4):** http://192.168.10.2/

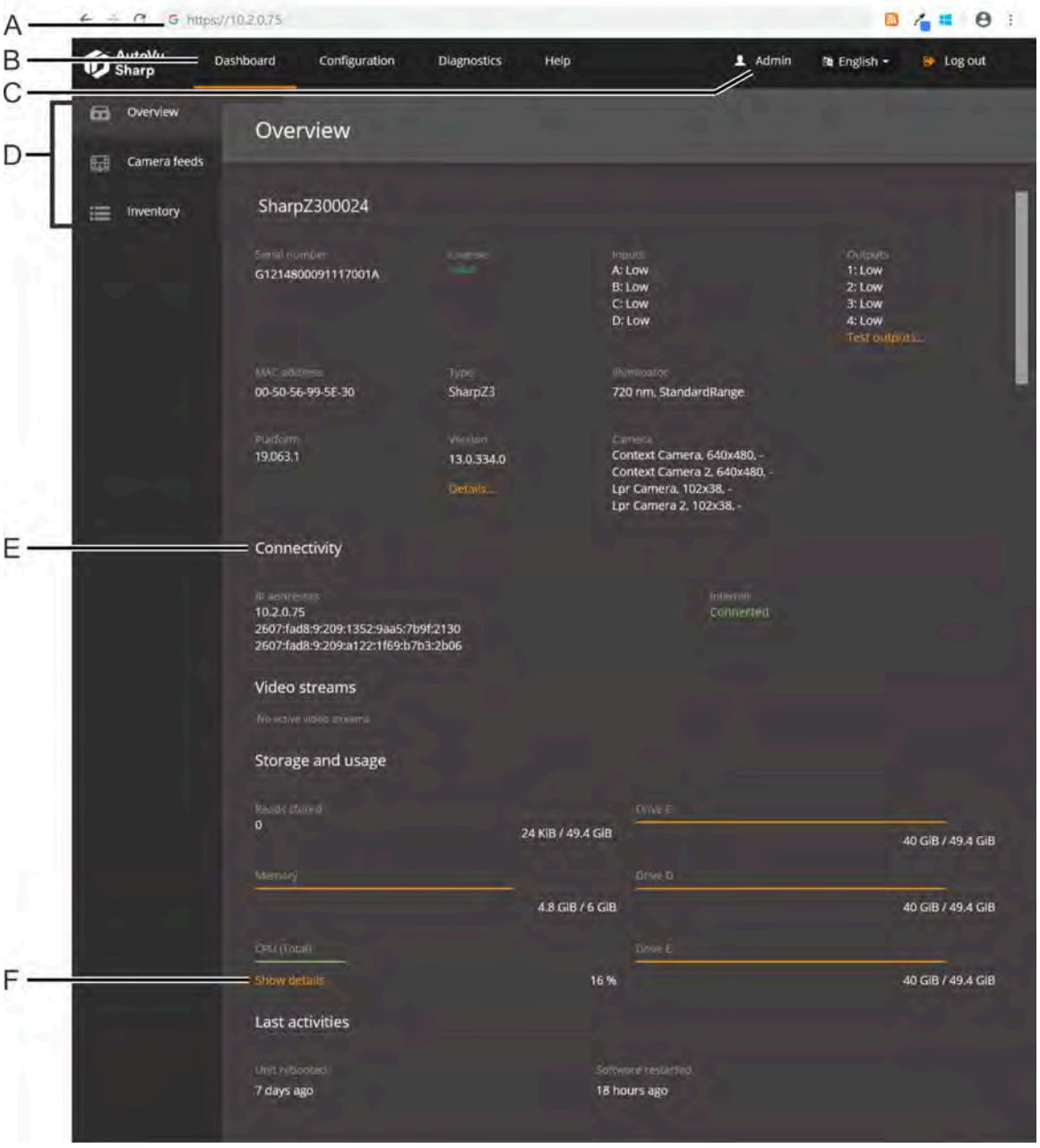


To change your password:

1. Log on to the Sharp Portal.
2. From the **Configuration** menu, select the **Security** page.
3. In the **Access** section, click **Modify password**.
4. Enter your old password, then enter and confirm your new password.
5. Click **Apply**.

Sharp Portal interface overview

To familiarize yourself with the Sharp Portal, you can take a tour of the main areas of the user interface.



A	Sharp Portal address	Type the SharpZ3 name or the IP address. The format is `https://Sharp12345` or `https://192.168.10.1`
B	Menu	Shows the main categories of the Sharp Portal.
C	Current user	Shows the current user, language selection, and log out command.
D	Pages	Shows the available pages for the selected portal menu.

E	Sections	Shows the available information, status, or settings for the selected portal page.
F	Additional information	Orange text indicates that the text is clickable. This can indicate a hyperlink, can trigger actions, or can display additional information.

Viewing camera feeds

You can use the camera feed to test and align Sharp cameras.

To view the Sharp unit camera feed:

1 Log on to the Sharp Portal.

2 From the **Dashboard** menu, select the *Camera feeds* page.

The *Camera feeds* page displays the feeds from the selected Sharp unit and recent license plate reads from the unit.

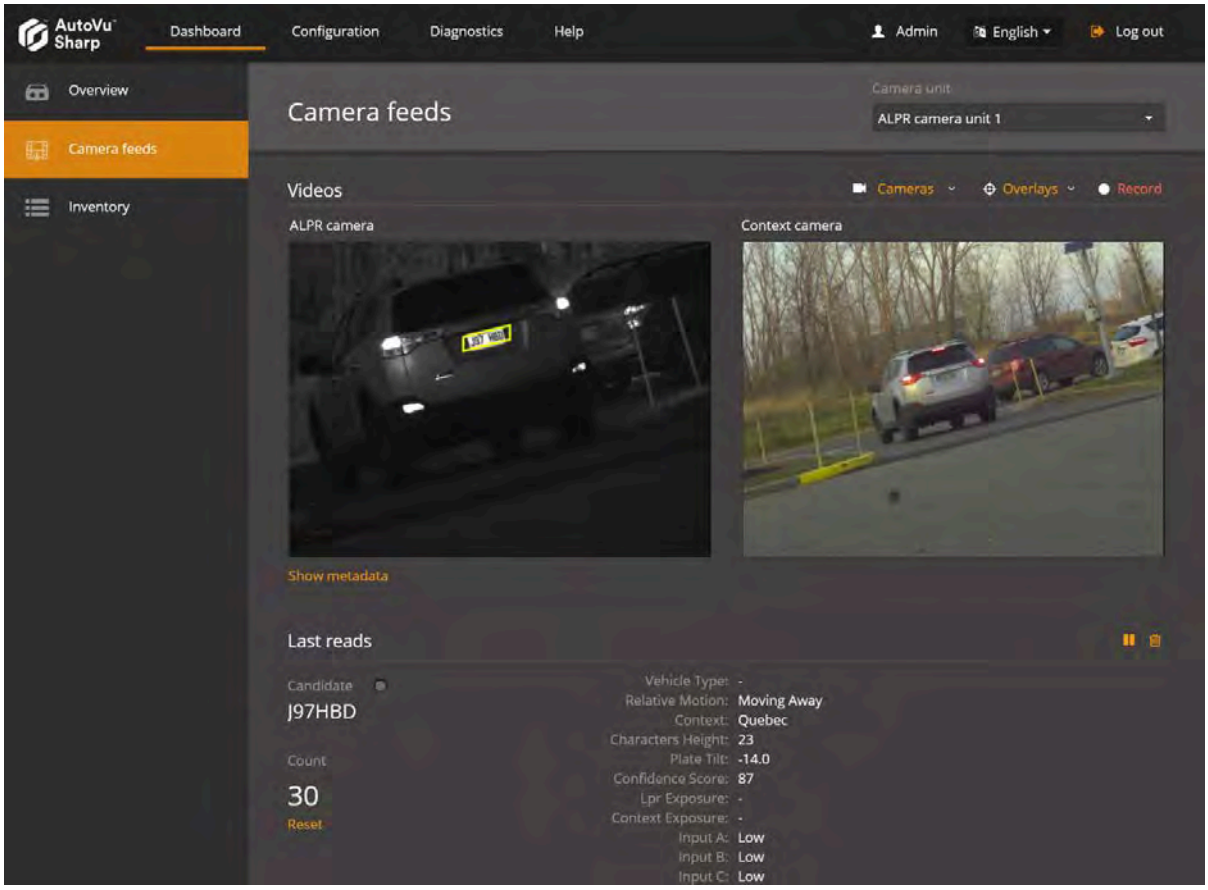
The following options are available in the *Camera feeds* page:

- **Camera unit:** Select which Sharp camera or auxiliary camera to view.
- **Cameras:** Displays the resolution and the lens focal range available for cameras connected to the SharpZ3 unit.
- **Overlays:**
  - **Crosshairs:** Select this option to display crosshairs in the ALPR or context camera window.
  - **Bounding box:** Select this option to display the yellow bounding box around detected plates in the ALPR camera window.
- **Record:** Click the **Record** button to capture a series of context and ALPR images directly from the *Camera feeds* window and save them to your computer as a .zip file for debugging purposes.

  NOTE:

  - Using the **Record** feature increases CPU usage.
  - To use this feature, you cannot use the camera's auto-generated certificate. You must install a self-signed certificate that includes the IP address of the camera.

3 From the **Camera unit** menu, select a camera group to view its live feeds.



After you finish

To reduce network bandwidth, after you have finished viewing the camera feeds, select **No camera** from the **Cameras** menu, or navigate to a different page of the Sharp Portal.

Related Topics

Camera alignment

SharpZ3 hardware inventory

The **Dashboard** > **Inventory** page in the Sharp Portal displays information on SharpZ3 system hardware.

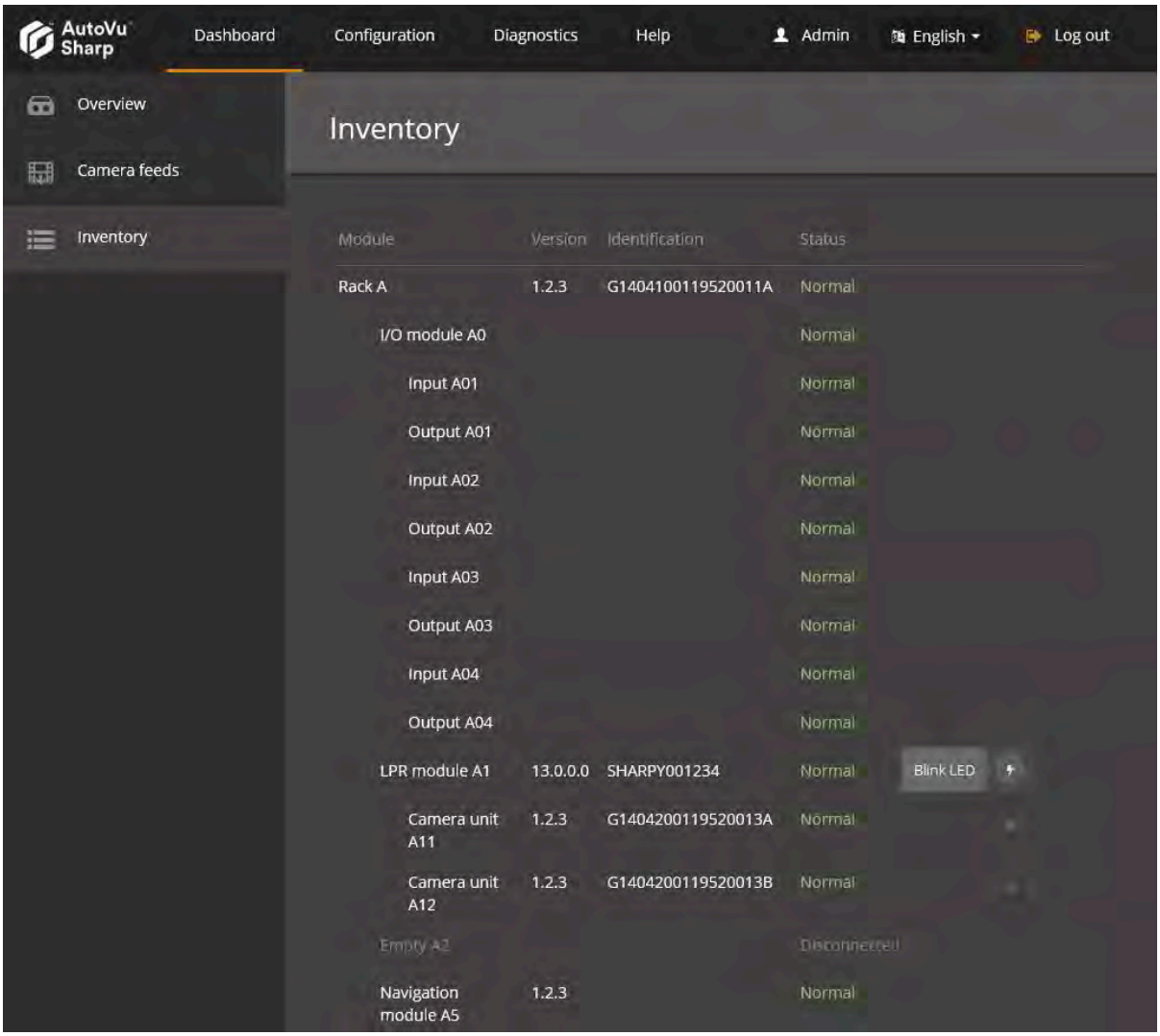
The *Inventory* page is available from the **Dashboard** menu. The page displays the status of the hardware components of the system and allows you to identify camera units by blinking their LEDs. You can see the installed expansion modules and available expansion module slots.

NOTE: To see the most recent information in the *Inventory* page, you must refresh the web page.

The *Inventory* page provides the following information:

- **Module:** Displays the name of the component.
- **Version:** Displays the component's firmware version.
- **Identification:** Displays a unique identifier of the component, such as its name or serial number.

  NOTE: The serial number is also printed on the component sticker.
- **Status:** Displays the health status of the component.
- **Blink LED:** Blinks the LED on SharpZ3 cameras or the SharpZ3 base unit.



Rebooting the SharpZ3 ALPR module

Certain configuration procedures require you to reboot the SharpZ3 ALPR module. You can do this from the Sharp Portal.

What you should know

- Following these steps will reboot the SharpZ3 base unit as well as the two camera ports associated with the Sharp Portal. To reboot the entire SharpZ3 system, you must power cycle the base unit.
- A two-camera ALPR module is configured through one Sharp Portal; a four-camera ALPR module is configured through two Sharp Portals.
  - **Sharp Portal 1 (camera ports 1 and 2):** http://192.168.10.1/
  - **Sharp Portal 2 (camera ports 3 and 4):** http://192.168.10.2/



To reboot the SharpZ3 system:

1 Log on to the Sharp Portal.
2 From the **Configuration** menu, select the *Maintenance* page.
3 Click the **Reboot unit** button.
The connection to the Sharp Portal is momentarily lost.
4 Wait approximately 2 minutes to allow the system to reboot and the Sharp Portal to restart.

Synchronizing the SharpZ3 clock

You can configure the SharpZ3 to synchronize time and date settings with the computer you are using to access the Sharp Portal, or with an NTP server.

What you should know

By default, the SharpZ3 synchronizes its time and date settings with the active extension defined in the **Configuration** > **Connectivity** > **Extension** page. Alternatively, you can manually configure the date and time selection in the **Configuration** > **General settings** > **Date and time** page.

To synchronize the SharpZ3 clock:

1 Log on to the Sharp Portal.

2 From the **Configuration** menu, select **General settings > Date and time**.

3 Select one of the following options:

- **NTP server:** The camera synchronizes with an NTP server that is typically either a foreign computer or a server within your organization that synchronizes itself with an external NTP server. The latter is recommended if synchronization is crucial to your organization. Click **Server** and enter the URL or IPv4 address of the machine running the NTP server. Click **Test connection** to tests the connection between the camera and the NTP server. The camera synchronizes with the NTP server every hour.
- **Active extension (Patroller):** If you select **Active extension (Patroller)**, the camera's date and time are synchronized with the Genetec Patroller™ server that the camera is connected to. The camera synchronizes with the server upon connection, then again every 10 minutes.

  NOTE: If you have not yet configured the active extension (see Configuring where the SharpZ3 sends its ALPR data on page 48), you can select **Active extension**, and it will be updated when you configure the extension.

  NOTE: The **Active extension** option displays whichever extension is currently selected for the camera in *Configuration* > *Extensions*, however, selecting this option has no effect if you are using an extension type other than Patroller (not valid for FTP, HTTP, and so on).

4 Click **Save**.

Configuring battery monitoring

By default, power to the SharpZ3 base unit and connected devices continues to be supplied for 60 seconds after the vehicle engine is turned off. You can configure how power is managed when the system shuts down.

What you should know

WARNING: Configuring incorrect battery monitoring settings can render the unit temporarily unusable or impair the battery.

To configure battery monitoring:

1 Log on to the Sharp Portal.
2 Click **Configuration** > **General settings** > **Power options**.
3 Click **Show Advanced**.
4 Configure **Battery Monitoring** settings.

- **Turn on voltage:** Input voltage threshold below which the unit does not turn on.
- **Ignition cut-off delay:** Grace period between ignition cut-off and trunk unit power-down.
- **Undervoltage:** Input undervoltage threshold that causes a unit shut-off if maintained for a certain time.

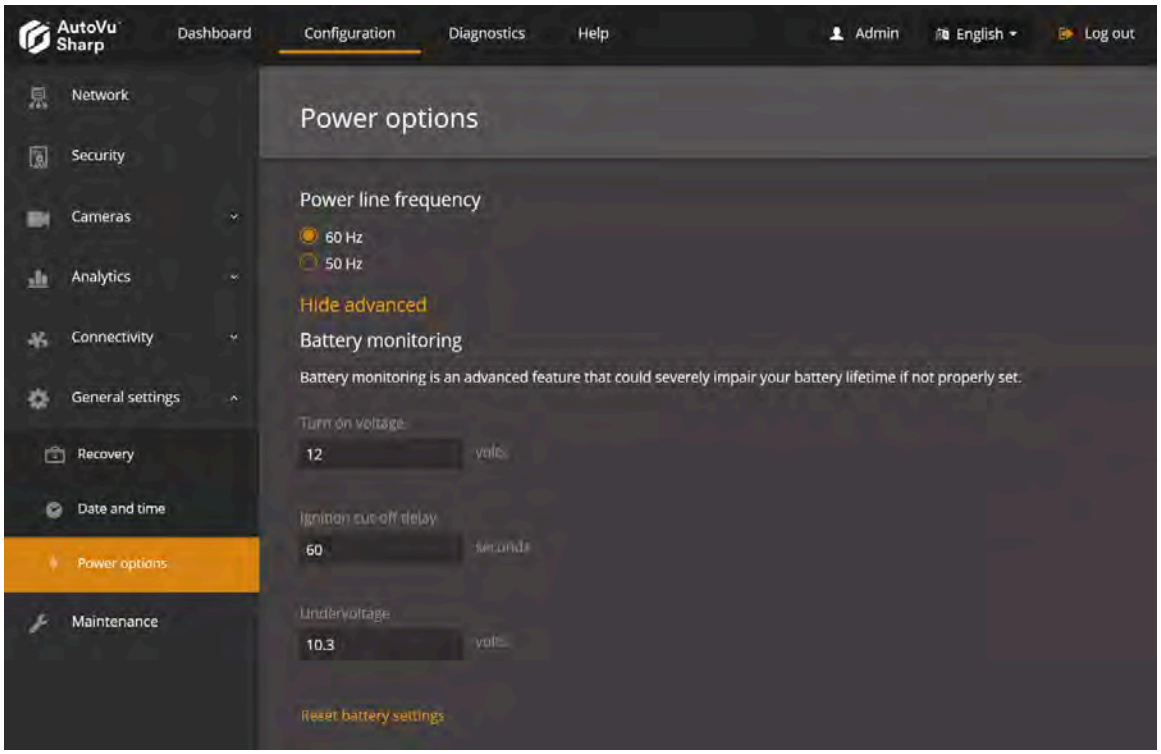
NOTE: The voltages in the following table are measured at the base unit power connector. Note that there is an approximate 0.5 - 0.7 V drop between the battery and the base unit power connector.

Parameter	Minimum	Maximum	Default
Turn on voltage	9.5 V	25.5 V	12 V

Parameter	Minimum	Maximum	Default
Ignition cut-off delay	10 seconds	30 minutes	60 seconds
Undervoltage	9 V	25.5 V	10.3 V

NOTE:

- The **Turn on voltage** and **Undervoltage** parameters have a precision of 0.1 V. For example, a voltage of 20.789456 V is rounded to 20.7 V.
- The **Ignition cut-off delay** parameter is rounded down to the nearest 10. For example, a cut-off time of 48 seconds is rounded to 40 seconds.



5 Click **Save**.

3

SharpZ3 camera configuration

This section includes the following topics:

- "Security configuration in the Sharp Portal" on page 32
- "About SharpZ3 exposure adjustment" on page 38
- "Configuring SharpZ3 position and location" on page 41
- "Associating wheel-imaging cameras with SharpZ3 camera units" on page 43
- "Configuring SharpZ3 analytics" on page 46
- "Configuring where the SharpZ3 sends its ALPR data" on page 48
- "About SharpZ3 network settings" on page 49
- "Configuring the SharpZ3 FTP extension" on page 53
- "Configuring the SharpZ3 HTTP/HTTPS extension" on page 56
- "Configuring Syslog for SharpZ3 log files" on page 60
- "Importing and exporting settings" on page 61

Security configuration in the Sharp Portal

SharpZ3 cameras must communicate using TLS encryption (HTTPS) using either the certificate that is auto-generated on the SharpZ3, a new self-signed certificate, or a signed certificate from your own public key infrastructure (PKI) or from a Certificate Authority such as VeriSign.

Consider the following:

- The first time you log on to the Sharp Portal, a self-signed certificate is generated and HTTPS is activated by default.
- You must install the certificate on all machines that communicate with the SharpZ3 camera. This includes the servers hosting the ALPR Manager, the Archiver, and all machines that connect to the Sharp Portal
- You can install multiple certificates and then select a certificate to activate.

  IMPORTANT: If the current certificate is a signed certificate, deleting the certificate signing request prevents the certificate from being reinstalled.
- To capture context and ALPR images directly from the SharpZ3 using the **Record** button on the *Camera feeds* window of the Sharp Portal, you cannot use the camera's auto-generated certificate. You must install a signed or self-signed certificate that includes the IP address of the camera as the *common name*.
- If the IP address of the SharpZ3 changes, you must regenerate and reinstall the signed or self-signed certificate.

Installing the SharpZ3 auto-generated certificate

If the SharpZ3 unit uses its auto-generated certificate for HTTPS communication, you must install the certificate on all machines that communicate with the Sharp unit.

Before you begin

Read about how the Sharp Portal must be encrypted.

What you should know

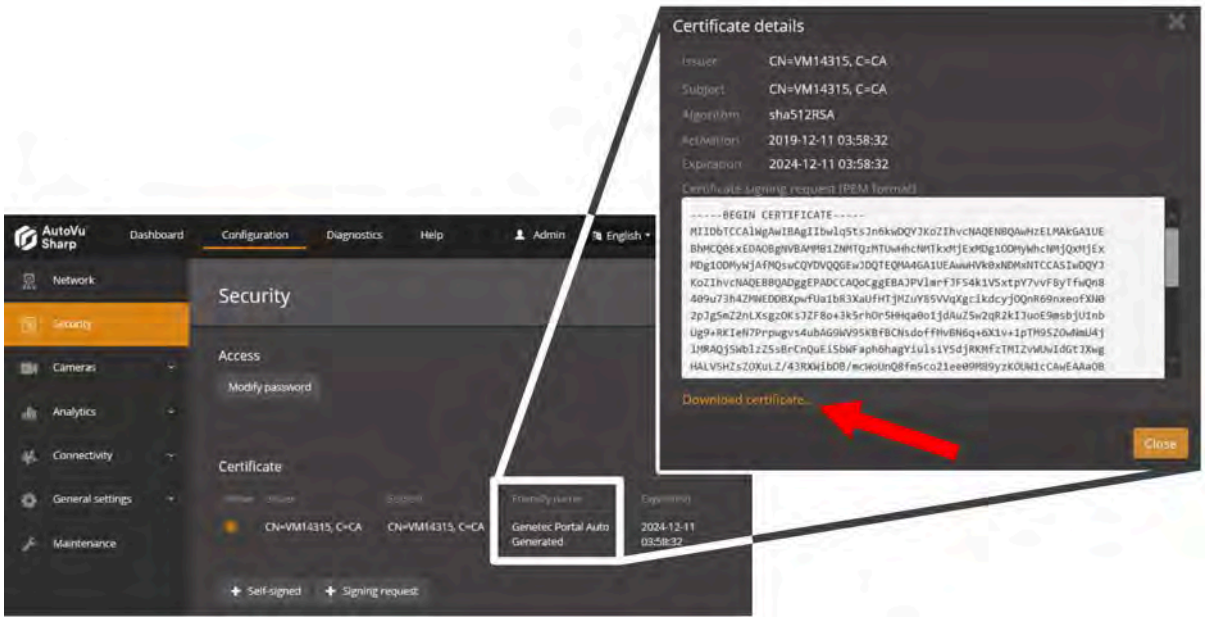
- To capture context and ALPR images directly from the SharpZ3 using the **Record** button on the *Camera feeds* window of the Sharp Portal, you cannot use the camera's auto-generated certificate. You must install a signed or self-signed certificate that includes the IP address of the camera as the *common name*.
- IPv6 static addresses are not supported.

To install the auto-generated certificate on a workstation:

1. On the machine where you want to register the certificate, log on as an Administrator.
2. Log on to the Sharp Portal.
3. From the **Configuration** menu, select the *Security* page.
4. Click the certificate with the **Friendly name**: *Genetec Portal Auto Generated*.

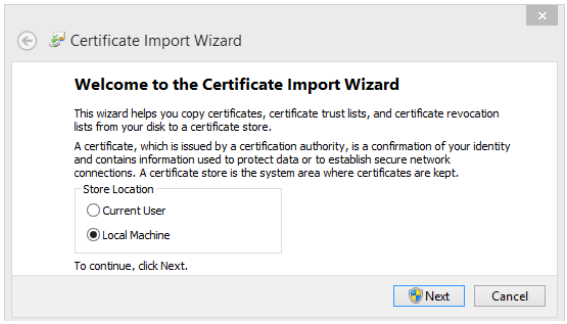
   The *Certificate details* are displayed.

5 Click **Download certificate** and save the certificate file as prompted by your browser.

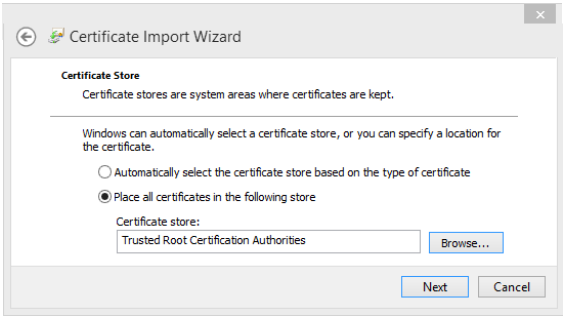


6 Double-click the *certificate.cer* file and click **Install Certificate**.

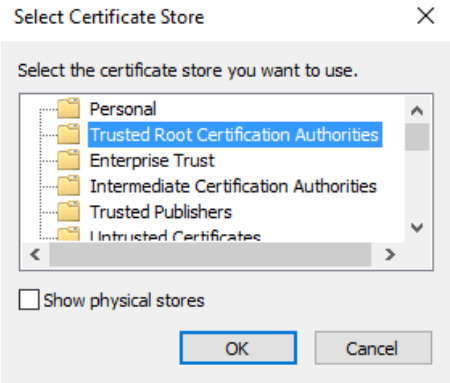
7 The *Certificate Import Wizard* prompts you to select a store location. Select **Local Machine** and click **Next**.



8 The wizard prompts you to select the certificate store you want to use. Select **Place all certificates in the following store** and click **Browse**.



9 From the **Select Certificate Store** window, select **Trusted root certification Authorities** and click **OK**.



10 Click **Next** to continue, and click **Finish** to close the wizard.

The system displays the message: *The import was successful*.

11 Close all web browsers and open the Windows Task Manager to ensure that no browser processes are running in the background.

12 Log on to the Sharp Portal. You are automatically logged on in HTTPS mode.

A lock icon ( ) in the browser's address bar indicates that you are now logged on to the SharpZ3 with a secure connection.

Installing a self-signed certificate

If the SharpZ3 unit uses a self-signed certificate for HTTPS communication, you must install the certificate on all machines that communicate with the Sharp unit.

Before you begin

Read about how the Sharp Portal must be encrypted.

What you should know

IPv6 static addresses are not supported.

To encrypt connection to the Sharp Portal using a self-signed certificate:

1 On the machine where you want to register the certificate, log on as an Administrator.

2 Log on to the Sharp Portal.

3 From the **Configuration** menu, select the *Security* page.

4 From the **Certificate** section, select **+ Self-signed**.

5 Enter the required information for the certificate and click **OK**.

- The **Country** field requires a two-letter country code.
- If you are also using the certificate to connect to the Archiver, the **Sharp's common name** (Sharp's IP address if connecting to the Archiver) defined in the certificate must be the Sharp unit's IP address, not the Sharp name.

The message *Operation succeeded* is displayed and the signing request is added to the certificate list.

6 Click the **Active** button for the certificate.

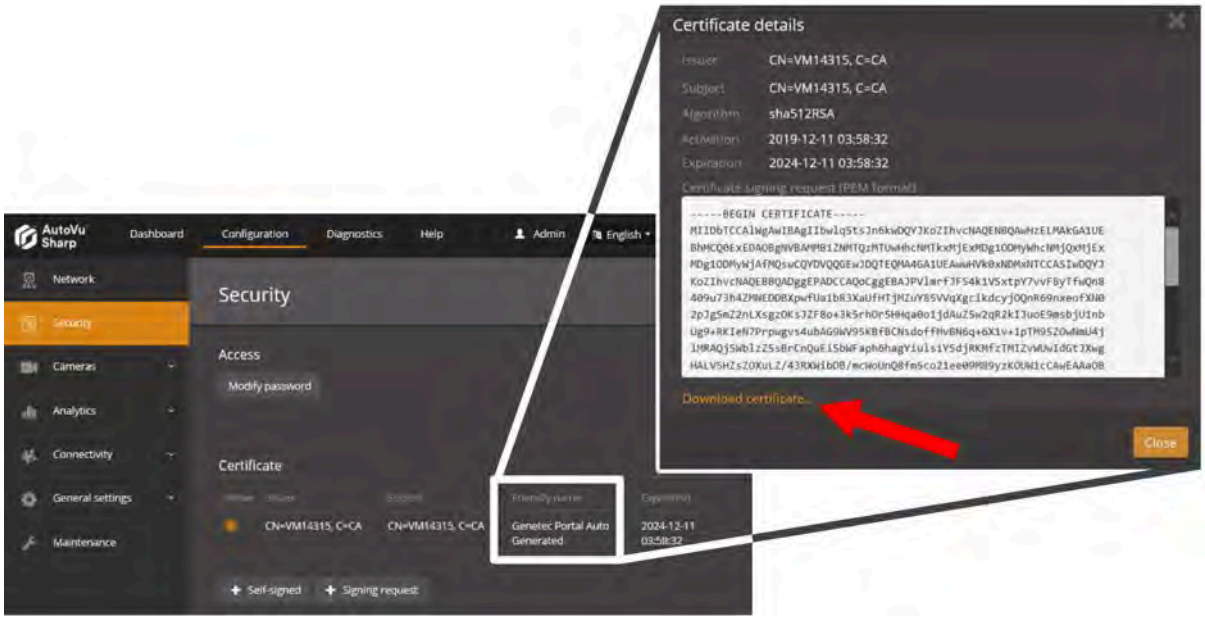
7 Click **Save and reboot** and click **OK** to confirm the reboot.

NOTE: Depending on the browser you are using, you might receive warnings because the certificate is not signed by a trusted certificate authority.

To install the certificate on a workstation:

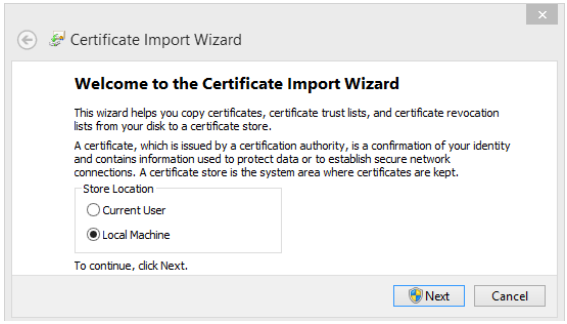
1 Click on the certificate to display the *Certificate details*.

2 Click **Download certificate** and save the certificate file as prompted by your browser.

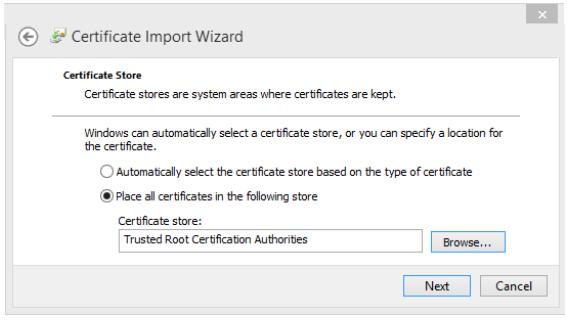


3 Double-click the *certificate.cer* file and click **Install Certificate**.

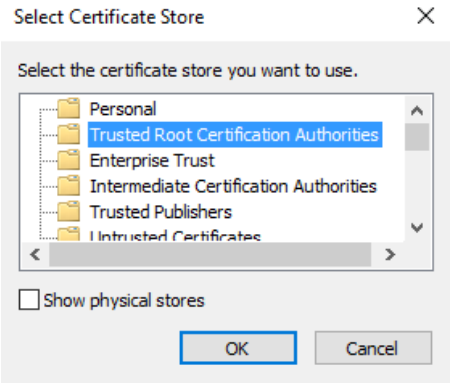
4 The *Certificate Import Wizard* prompts you to select a store location. Select **Local Machine** and click **Next**.



5 The wizard prompts you to select the certificate store you want to use. Select **Place all certificates in the following store** and click **Browse**.



6 From the **Select Certificate Store** window, select **Trusted root certification Authorities** and click **OK**.



7 Click **Next** to continue, and click **Finish** to close the wizard.
The system displays the message: *The import was successful*.
8 Close all web browsers and open the Windows Task Manager to ensure that no browser processes are running in the background.
9 Log on to the Sharp Portal. You are automatically logged on in HTTPS mode.
A lock icon ( ) in the browser's address bar indicates that you are now logged on to the SharpZ3 with a secure connection.

Installing a signed certificate

If the SharpZ3 unit uses a signed certificate from your own public key infrastructure (PKI) or from a Certificate Authority such as VeriSign, you must install the certificate on all machines that communicate with the SharpZ3 unit.

Before you begin

Read about how the Sharp Portal must be encrypted.

What you should know

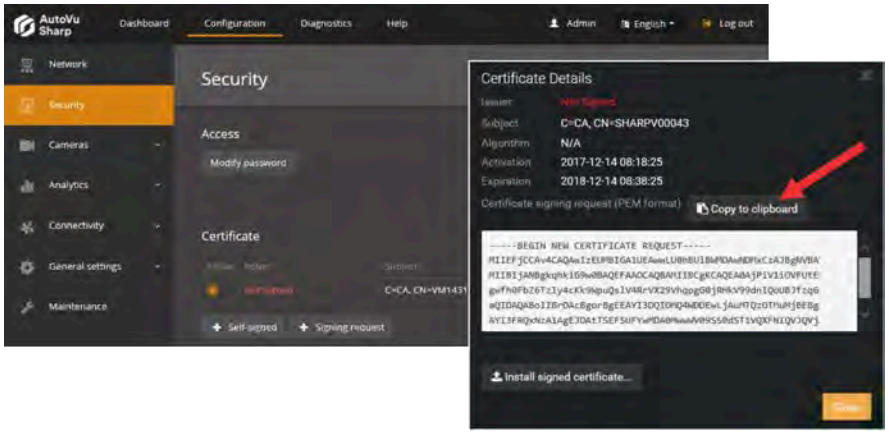
IPv6 static addresses are not supported.

To encrypt the connection to the Sharp Portal using a signed certificate:

1 On the machine where you want to register the certificate, log on as an Administrator.
2 Log on to the Sharp Portal.
3 From the **Configuration** menu, select the *Security* page.
4 Click **+ Signing request**.
5 Enter the required information for the certificate signing request and click **OK**.
NOTE:
- The **Country** field requires a two-letter country code.
- If you are also using the certificate to connect to the Archiver, the **Sharp's common name** (Sharp's IP address if connecting to the Archiver) defined in the certificate must be the Sharp unit's IP address, not the Sharp name.

The message *Operation succeeded* is displayed and the signing request is added to the certificate list with *not signed* displayed for the **Issuer**.
6 Click on the certificate to display the *Certificate details*.

7 Click **Copy to clipboard**.



8 Send the certificate signing request to a certificate authority.

IMPORTANT: Do not delete the signing request if it has been used to request a certificate.

You will receive an SSL certificate signed by the certificate authority.

9 In the *Certificate Details* window, click **Install signed certificate** then browse to the certificate location and click **Open**.

10 Click **Save**.

The system displays the message: *Installed signed certificate... successful*.

11 Refresh the browser (F5).

The certificate is displayed in the **Certificate** list.

12 Click the **Active** button for the certificate.

13 Click **Save and reboot** and click **OK** to confirm the reboot.

When the system comes back online, notice that the URL displays that you are in HTTPS mode. A lock icon (🔒) in the browser's address bar indicates that you are now logged on to the SharpZ3 with a secure connection.

About SharpZ3 exposure adjustment

We recommend that you keep the default SharpZ3 exposure settings. If you notice that license plates are often under-exposed (too dark) or over-exposed (too bright), you can adjust the exposure settings. However, there are many factors to consider in order to account for changing lighting conditions.

IMPORTANT: Modifying the SharpZ3 exposure settings can greatly impact ALPR performance. Vanity plates, or plates that are damaged or dirty can have different reflective properties. Improving the exposure using a stationary test plate can result in reduced ALPR performance on every-day traffic which includes plates with a wide range of reflective properties. You must test the system after modifying these settings.

Consider the following:

- In a correctly-exposed license plate image, the characters and the plate state are dark and well-defined, and the background is white or very bright.



- In the ALPR image, it is normal that the surroundings of the plate are under-exposed while the plate itself is correctly-exposed. Make sure that the plate is correctly exposed and ignore the quality of the surroundings.
- Modifying settings to improve read performance at night can have a negative impact on read performance during the day, and vice versa. Therefore, you must test the settings both at night and during the day (under sun illumination).
- If the SharpZ3 is expected to read both embossed and flat license plates, perform the day instructions with the flat plate and the night instructions with the embossed plate.

Setting custom SharpZ3 ALPR camera exposure levels

If the default exposure settings do not produce acceptable results, you can adjust the SharpZ3 ALPR camera exposure settings.

Before you begin

- Read about SharpZ3 exposure adjustment.
- Ensure that the lighting conditions match what is expected during normal camera operation.

To adjust the SharpZ3 ALPR camera exposure settings

1 Place a stationary license plate as close to the camera as possible while still being within range for the camera to capture plate reads.

2 Log on to the Sharp Portal.

3 From the **Configuration** menu, click **Cameras** > **Exposure**.

4 From the **Cameras** menu, click the **ALPR camera** you want to calibrate.

5 From the **Exposure** menu, click **Range (outdoor)**.

Gain and **Exposure time** settings are displayed.

NOTE: The ranges for the **Exposure time** and **Gain** settings must be large enough to allow good quality images in all lighting conditions, but you should reduce the range as much as possible. If the range is too large, it increases the risk of over-exposure or under-exposure. It is normal that the SharpZ3 constantly varies the exposure of the ALPR camera in order to get a correct exposure of a plate.

TIP: If you want to test using specific exposure settings rather than a range, use the **Fixed (indoor)** configuration from the **Exposure** menu. However, the setting should be set back to **Range (outdoor)** for normal operation so that the camera can adapt its exposure to varying lighting conditions.

6 With the plate close to the camera, set the **Gain** value to the minimum default value and adjust the **Exposure time** until you are satisfied with the plate image.
7 With the plate further from the camera, check to see that the plate is not too dark. If it is, increase the **Exposure time**.
8 (Optional) If you reach the maximum possible **Exposure time** and you are still not satisfied with your plate image, increase the **Gain**.
9 When you are satisfied with the appearance of the plate images in the video feed window, click **Save**.
The system displays the message *Configuration saved successfully*.

After you finish

Modifying the exposure settings can greatly impact ALPR performance. Test the system after modifying these settings.

Troubleshooting outdoor exposure issues for the SharpZ3 ALPR camera

You can resolve exposure adjustment issues that result in under-exposed or over-exposed license plate images in SharpZ3 installations.

If ALPR images (or some specific plate models) are always too dark at night:

1 Perform the exposure calibration at night.
2 Increase the maximum **Shutter time** value until you are satisfied with the ALPR images.
3 If you reach the maximum **Shutter time** level and the ALPR images are still too dark, increase the maximum **Gain** value.

If ALPR images are often too dark at night:

In this case, the exposure setting range might be too large, causing exposure to be too low. To reduce the range, start by increasing the minimum values. Because higher minimum values might lead to over-exposure for daytime reads, perform the adjustment during the day.

In this case, the exposure setting range might be too large, causing exposure to be too low. You can reduce the range by increasing the minimum values, but you should do this carefully because increasing the minimum values can cause over-exposure during the day. Therefore, this adjustment should be done during the day.

1 Make the adjustment under sun illumination.
2 Increase the minimum **Exposure time** value as much as possible without compromising image quality.
3 If the minimum **Exposure time** value reaches its maximum value, then you can increase the minimum **Gain** value. Test to make sure image quality is still satisfactory.

If ALPR images (or some specific plate models) are always too dark even under sunlight:

1 Increase the maximum **Exposure time** level as much as possible without over-exposing the plate.
2 If the maximum **Exposure time** reaches its maximum value and the plate is still under-exposed, increase the maximum **Gain** value one step at the time until you are satisfied with the images.

If ALPR images (or some specific plate models) are always too bright under sunlight:

1 Make the adjustment under sun illumination.
2 Decrease the minimum **Gain** value until you are satisfied with the plate images.

3 If you reach the minimum **Gain** level and the ALPR images are still too bright, decrease the minimum **Exposure time** value.

If ALPR images are often too bright under sunlight:

In this case, the **Exposure time** range might be too large, causing exposure to be too high. You can reduce the range by decreasing the maximum values, but you should do this carefully because decreasing the maximum values can cause under-exposure at night. Therefore, this adjustment should be done during the night.

1 Make the adjustment at night.
2 Decrease the maximum **Gain** value as much as possible without compromising image quality.
3 If the maximum **Gain** value reaches its minimum value, then you can decrease the maximum **Exposure time** value. Test to make sure image quality is still satisfactory.
4 If you reach the minimum **Exposure time** level and you are still not satisfied with the image quality, perform the complete day and night exposure adjustment again.

Troubleshooting outdoor exposure issues for the SharpZ3 context camera

You can resolve exposure adjustment issues that result in under-exposed or over-exposed context images in a SharpZ3 installation.

If context images are blurry on fast-moving vehicles:

1 Make the adjustment at night.
2 Decrease the maximum **Exposure time** value until the blur caused by vehicle motion is acceptable.

If context images are noisy during the night:

1 Make the adjustment at night.
2 (Optional) Select **Allow illuminator**. This allows the camera to turn on the IR illuminator under dark conditions, but removes color from the image as the light level diminishes.
3 Decrease the maximum **Gain** value. This prevents the camera from amplifying the noise, but it can result in darker images.
4 (Optional) Increase the maximum **Exposure** time. Note that this can increase the blur caused by vehicle motion.

If context images are too dark during the night:

1 Make the adjustment at night.
2 (Optional) Select **Allow illuminator**. This allows the camera to turn on the IR illuminator under dark conditions, but this progressively removes color from the image as the light level diminishes.
3 Increase the maximum **Exposure time** value until you are satisfied with the image quality. However, do not exceed the level that causes unacceptable motion blur on fast-moving vehicles.
4 If you reach the maximum **Exposure time** value and the image is still too dark, increase the maximum **Gain** value.

If context images are too bright during the day:

1 Make the adjustment under sun illumination.
2 Decrease the minimum **Gain** value until you are satisfied with the image quality.
3 If you reach the minimum **Gain** value and the image is still too bright, decrease the minimum **Exposure time** value.

Configuring SharpZ3 position and location

Based on the position of the patrol vehicle when a license plate is read, the SharpZ3 system can calculate the location of the target vehicle. To improve geocoding precision, you must define the exact location of the SharpZ3 cameras on the patrol vehicle roof.

What you should know

- To configure the camera orientation, you must measure the angle of the SharpZ3 cameras. For best results, use a digital level.
- The vehicle image on the *Camera position and orientation* page in the Sharp Portal dynamically updates to show the approximate position of the camera.

To configure the position of the SharpZ3 cameras:

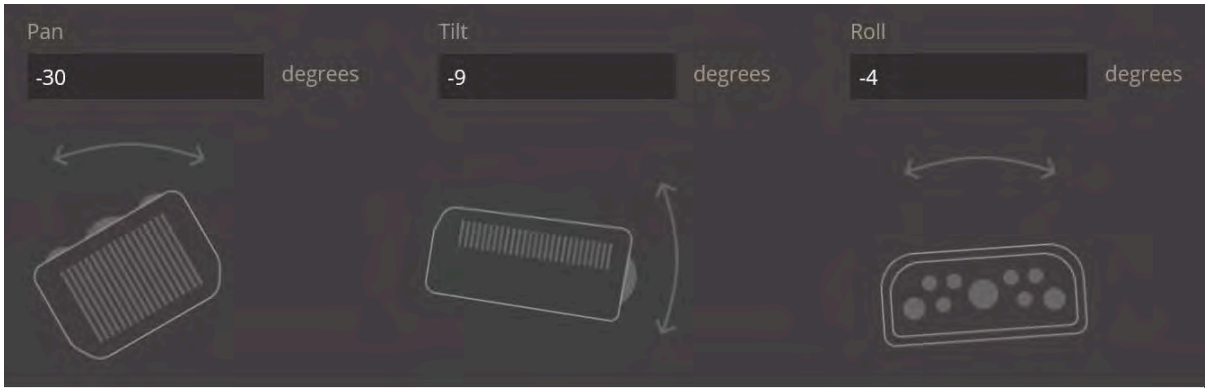
1 Log on to the Sharp Portal.
2 From the **Configuration** menu, click **Cameras** > **Position and orientation**.
3 From the **Cameras** menu, select the first SharpZ3 camera you want to configure.
4 Click **Enable** to turn on the feature for the camera.
5 Enter **Position** measurements in centimeters to indicate where the front of the camera is in respect to the GNSS antenna.

IMPORTANT: Take your measurements from the GNSS antenna to the front of the camera. Do not measure from the center of the vehicle.

As you enter positive or negative values, the camera moves on the vehicle image. This helps you to confirm that you have entered the correct positive or negative values.



6 Measure the camera's pan, tilt, and roll using a digital level and enter the **Orientation** values.



7 Click **Save**.

After you finish

Repeat these steps for the remaining SharpZ3 cameras.

Associating wheel-imaging cameras with SharpZ3 camera units

If the SharpZ3 system includes wheel-imaging cameras connected to an AUX PoE expansion module, then you must associate the right and left wheel-imaging cameras with their respective SharpZ3 camera units.

Before you begin

Connect wheel-imaging cameras to the AUX PoE expansion module.

What you should know

- On the *Auxiliary cameras* page, you can associate up to two wheel-imaging cameras with SharpZ3 cameras. Typically, left and right wheel-imaging cameras are associated with left and right SharpZ3 cameras, however, you can also associate one wheel-imaging camera with more than one SharpZ3 camera.
- If the wheel-imaging cameras are not connected to the AUX PoE expansion module ports, you can pre-associate the ports with the correct SharpZ3 camera units.

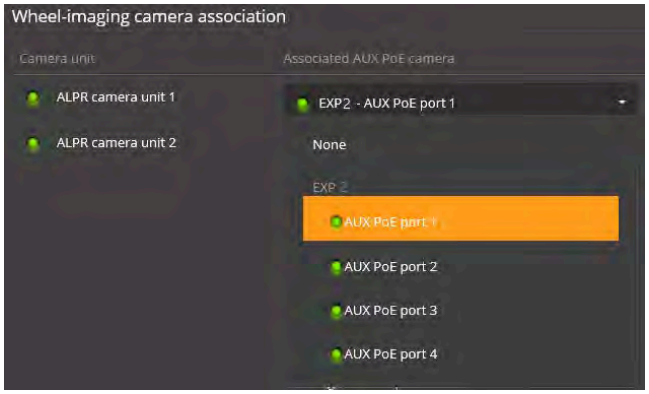
To associate wheel-imaging cameras with SharpZ3 cameras:

1 Log on to the Sharp Portal.

2 From the **Configuration** menu, click **Cameras** > **Auxiliary cameras**.

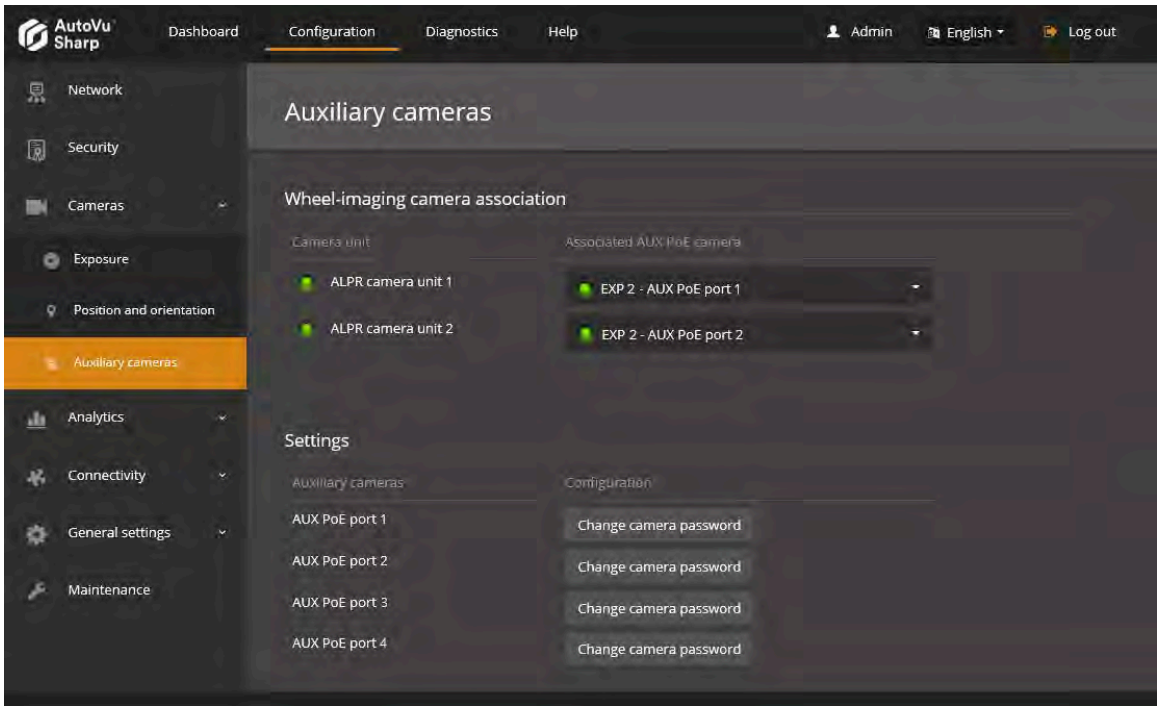
3 For each SharpZ3 **Camera unit** displayed in the *Wheel-imaging camera association* section, associate a wheel-imaging camera from the **Associated AUX PoE camera** menu.

The **Associated AUX PoE camera** menu displays the SharpZ3 base unit expansion slot (EXP) and port numbers for each of the installed AUX PoE expansion modules. If the light is green, the camera is connected and accessible.



TIP: If you are not sure which port a wheel-imaging camera is connected to, check the video feed for the auxiliary cameras in **Dashboard** > **Camera feeds**.

NOTE: The same wheel-imaging camera can be associated with more than one SharpZ3 camera, typically one per car side.



4 Click **Save**.

After you finish

1. If required by local regulations, click **Change camera password** and modify the password from the default Username: *admin* and Password: *1234*.

   NOTE: If you change the AUX PoE expansion module port connection after you change the password, you must reapply the password.

2. Configure wheel imaging settings in Genetec Patroller™. For more information, see the *Genetec Patroller™ Administrator Guide*.

Configuring SharpZ3 analytics

To ensure the highest license plate read accuracy, you must let the SharpZ3 system know what type of license plates to expect in the image. If required, you can also configure the system to extract additional information from the image, such as the license plate origin and the vehicle type.

To configure SharpZ3 analytics:

1 Log on to the Sharp Portal.

2 From the **Configuration** menu, click **Analytics** > **ALPR settings**.

3 From the **Context** menu, select which license plates will be most commonly read by the SharpZ3.

NOTE: For more information on the available regional contexts, see Supported ALPR contexts on page 11.

TIP: To help us improve the performance of regional contexts, click **Configuration** > **Connectivity** > **Product improvement** and register this camera to participate in the **Product improvement program**.

4 From the **Reading mode** menu, select one of the following reading modes:

- **Continuous:** Select this to capture plate reads continuously. This is the default setting.
- **Conditional:** Select this to capture plate reads continuously as long as the selected input signal meets the defined high or low condition.
- **Multiconditional:** Using this option, you can configure the system to generate reads from a specific camera only while an input's status meets the defined high or low condition. This option is required if using the AutoVu™ car camera switch.

5 From the **Read strategy** list, select a read strategy:

- **Slow moving vehicle:**
- **Fast moving vehicle:**

6 Under **Analytics**, select the contents of the plate you would like the SharpZ3 to attempt to read. You can select the following:

NOTE: You can add the state, vehicle make, and confidence score as annotation fields in Security Center to query for this information in Security Desk reports.

- **State:** Select this option if you want the SharpZ3 unit to attempt read the license plate origin. Depending on the region, this can refer to the issuing state, province, or country.

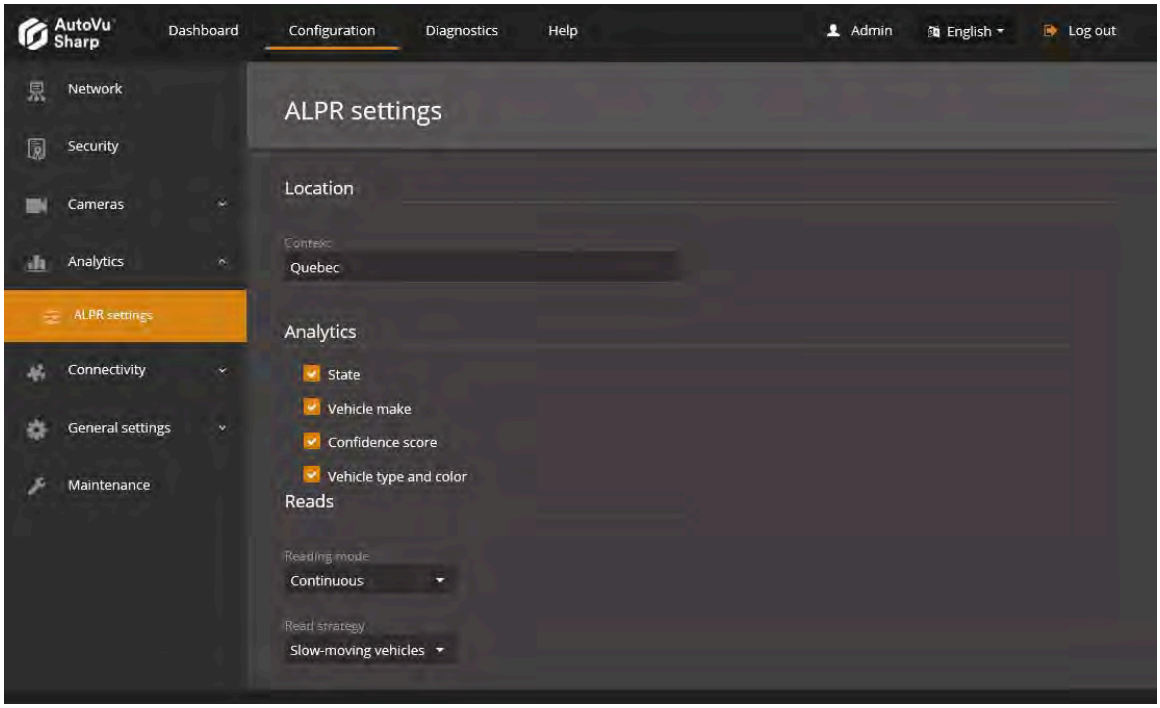
NOTE: For more information, see Supported plate origin recognition on page 14.

- **Vehicle make:** Select this option if you want the SharpZ3 unit to attempt to read the vehicle's make from the brand or logo (Honda, Toyota, and so on).

  NOTE: This setting is not recommended for MLPI installations.
- **Confidence score:** The SharpZ3 assigns a confidence score percentage to each license plate read. This value indicates how confident the SharpZ3 is in the accuracy of the read.

  NOTE: License plates that contain similar characters such as *8* and *B* are more difficult to read and generally produce reads with a lower confidence score.
- **Vehicle type and color:** Select this option if you want to include the vehicle type and vehicle color with plate reads. Based on the context image, the Sharp unit can detect if the vehicle is a bus, passenger vehicle, motorcycle, pickup, truck, work van, or an unknown vehicle type. In addition, the Sharp

unit can detect if the vehicle is black, white, blue, brown, green, gray, orange, red, or yellow. Colors excluding white and black are also assigned *light*, *neutral*, or *dark* according to the color analysis.



7 Click **Save**.

Configuring where the SharpZ3 sends its ALPR data

What you should know

- The default extension depends on the hardware you are installing. For example, if you log on to the Sharp Portal for a SharpZ3, the default extension is *Patroller*.
- For FTP and HTTP extensions, plate reads and images are automatically stored if the connection is lost, however, you can disable edge storage using the **Retain data when the connection is lost** setting in the extension configuration. To reduce cellular data usage, you can also configure whether the ALPR and context images are exported.

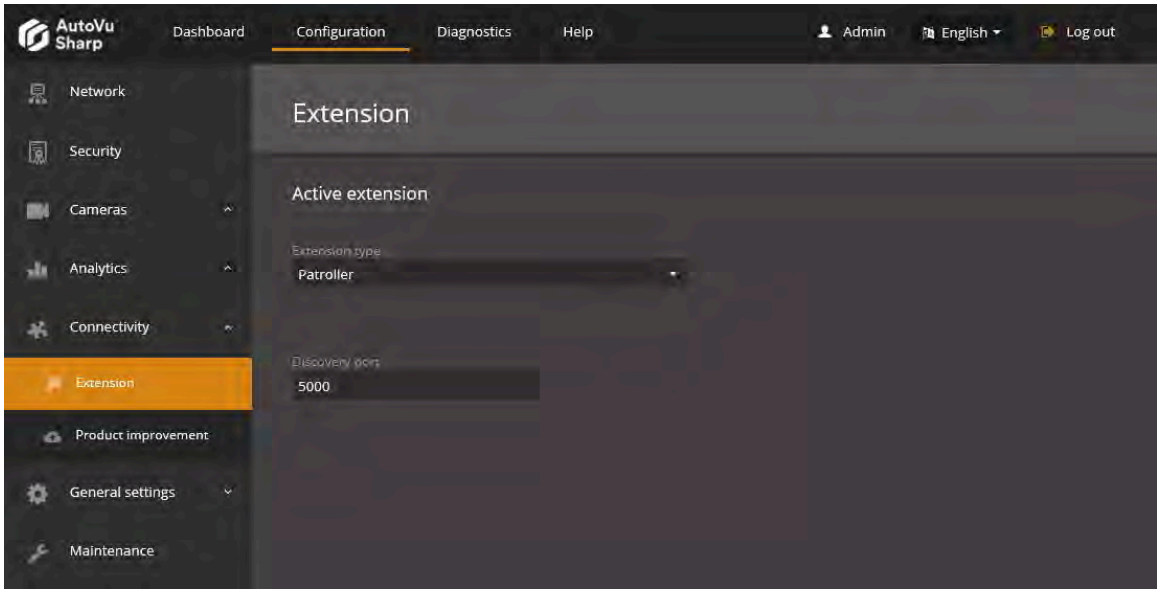
To configure the SharpZ3 extension:

1 Log on to the Sharp Portal.

2 From the **Configuration** menu, click **Connectivity** > **Extension**.

3 From the **Extension type** menu, select one of the following:

- **FTP:** Use this option to send ALPR data to an FTP server. You can configure the FTP XML template which can be integrated by third-party applications. For more information, see Configuring the SharpZ3 FTP extension on page 53.
- **HTTP/HTTPS:** Use this option to send ALPR data to an HTTP server. You can configure the system to send the data in XML or JSON format. For more information and examples of the exported XML and JSON files, see Configuring the SharpZ3 HTTP/HTTPS extension on page 56.



4 Click **Save**.

About SharpZ3 network settings

By default, the SharpZ3 base unit and modules communicate using their default static IP addresses and no configuration is required.

Static IP addresses

The following default static IP addresses are assigned to the SharpZ3 base unit, ALPR module, and expansion modules.

Module	Default static IP address
ALPR module ports 1 and 2	192.168.10.1
ALPR module ports 3 and 4	192.168.10.2
EXP 1	192.168.10.30
EXP 2	192.168.10.40
EXP 3	192.168.10.50

If there are no specific IP address range requirements for the installation, no configuration is required. If the system must use IP addresses within a specific range, you can assign them manually.

IMPORTANT:

- When assigning specific IP addresses, ensure the configuration stays compatible with the rest of the system, otherwise the base unit, expansion modules, or aux cameras might be unreachable. For example, it is important that all components be on the same subnet.
- If you change the static address of the ALPR module, it may invalidate its security certificate and could require replacement; communications might be blocked in the interim.
- You must use a fixed IP address if you want to stream video to the Security Center Archiver role. You can do this using a static IP address or a reserved IP address on the DHCP server.

DHCP

If the patrol vehicle uses a DHCP server, you can configure the SharpZ3 system for DHCP. Consider the following:

- When a SharpZ3 system is configured to use DHCP, the setting applies to the ALPR module, but does not apply to expansion modules. Expansion modules connected to the base unit always use static IP addresses that are defined on the *Network* page. For the expansion modules to work with the DHCP system, you must configure a compatible **Subnet mask** and **IP address** for each module.
- When a SharpZ3 is configured in DHCP and the DHCP server cannot be reached, the default fall-back IPv4 address is 192.168.10.99. On a four-camera ALPR module, the second group of two cameras has a default fall-back address of 192.168.10.99.

  NOTE: The default fallback takes at least two minutes to become effective when no DHCP server is detected at bootup.

Configuring the SharpZ3 system to use a specific IP address range

By default, the SharpZ3 base unit and modules communicate using their default static IP addresses and no configuration is necessary. If required, you can define new static IP addresses within a specific range.

Before you begin

Learn about SharpZ3 network settings.

What you should know

The IP address range that is assigned to the SharpZ3 system must account for the SharpZ3 base unit and all connected modules.

In an example using a 192.168.0.X range, the following addresses are required when all SharpZ3 expansion slots are in use:

Module	Default static IP addres
ALPR module ports 1 and 2	192.168.0.1
ALPR module ports 3 and 4	192.168.0.2
EXP 1: Navigation expansion module	192.168.0.30
EXP 2: AUX PoE expansion module 1	192.168.0.40 192.168.0.41 (Port 1) 192.168.0.42 (Port 2) 192.168.0.43 (Port 3) 192.168.0.44 (Port 4)
EXP 3: AUX PoE expansion module 2	192.168.0.50 192.168.0.51 (Port 1) 192.168.0.52 (Port 2) 192.168.0.53 (Port 3) 192.168.0.54 (Port 4)

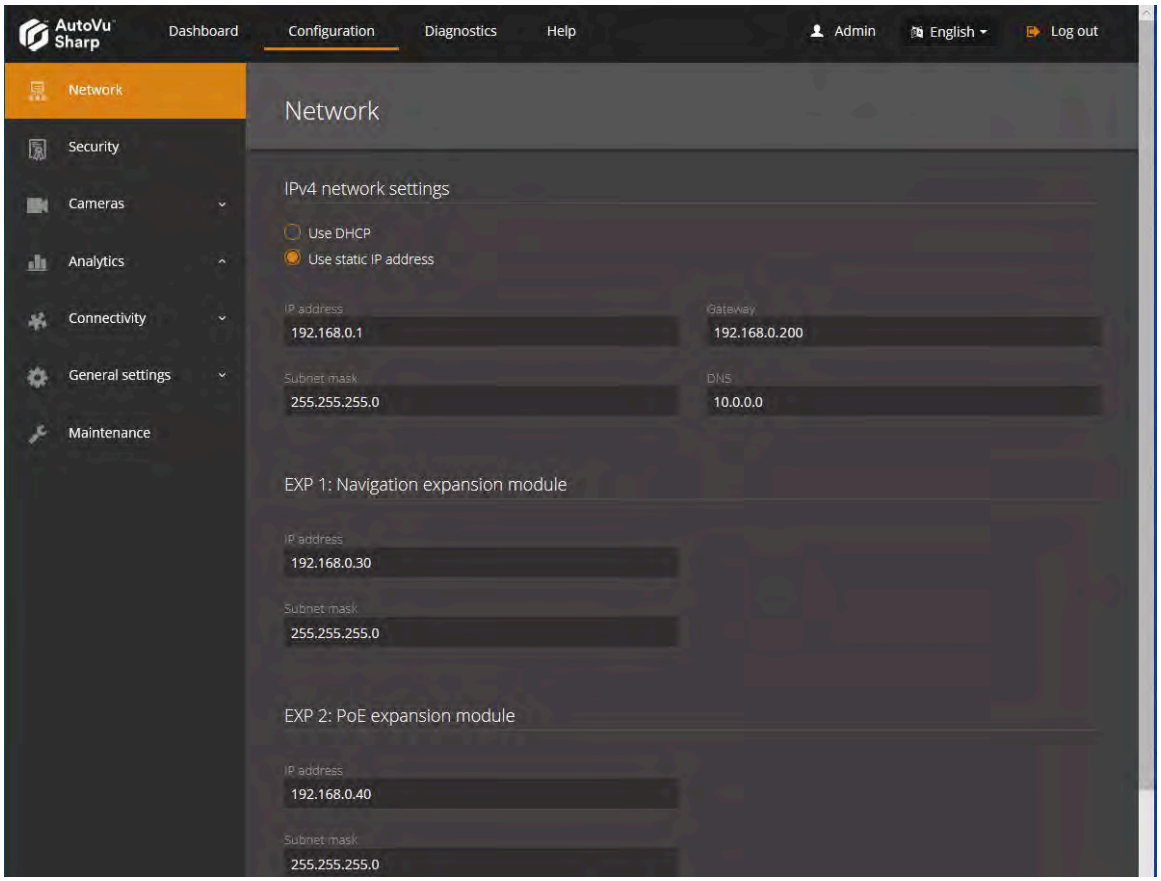
To configure the SharpZ3 system to use a specific IP address range:

1 Log on to the Sharp Portal.
2 From the **Configuration** menu, select the *Network* page.
3 Select **Use static IP address**.
The network settings are displayed for the ALPR module for each installed expansion module.
4 In the **IPv4 network settings** section, configure the ALPR module network settings, .
You can modify the following:

- **IP address:** Enter the new IP address you want to assign to the ALPR module. The default is 192.168.10.1 (port 1 and 2) and 192.168.10.2 (port 3 and 4).
- **Subnet mask:** Enter the new **Subnet mask** for the ALPR module, if applicable. The default is 255.255.255.0.

IMPORTANT: When assigning specific IP addresses, ensure the configuration stays compatible with the rest of the system, otherwise the base unit, expansion modules, or aux cameras might be unreachable. For example, it is important that all components be on the same subnet.

- **Gateway:** Enter the new **Gateway** for the ALPR module, if applicable. The default is 10.0.0.0.
- **DNS:** Enter the new **DNS** for the ALPR module, if applicable. The default is 10.0.0.0.



5 If the system includes a navigation expansion module, enter its new **IP address** and update the **Subnet mask** if required.

6 If the system includes AUX PoE expansion modules, enter their new **IP address** and update the **Subnet mask** if required.

The AUX PoE expansion modules automatically assigns compatible IP addresses to each PoE port on the same subnet. For example if you configure an AUX PoE expansion module to use the static IP address 192.168.0.40, then the first PoE port will be 192.168.0.41, second will be 192.168.0.42, and so on.

7 Click **Save**.

8 If the ALPR module includes four camera ports, log on to Sharp Portal 2 and enter the new static IP address for the second pair of camera ports.

A two-camera ALPR module is configured through one Sharp Portal; a four-camera ALPR module is configured through two Sharp Portals.

- **Sharp Portal 1 (camera ports 1 and 2):** http://192.168.10.1/
- **Sharp Portal 2 (camera ports 3 and 4):** http://192.168.10.2/



9 Click **Save**.

Configuring the SharpZ3 FTP extension

You can configure the SharpZ3 to send ALPR data to an FTP server instead of to Genetec Patroller™. ALPR data that is sent to an FTP server can then be processed by third-party applications.

What you should know

- The connection to the FTP server is made using passive mode. This means that the ports configured on the FTP server for that purpose must all be opened in the firewall and routers located between the Sharp units and the FTP server.
- You can only configure one extension for the SharpZ3 unit.

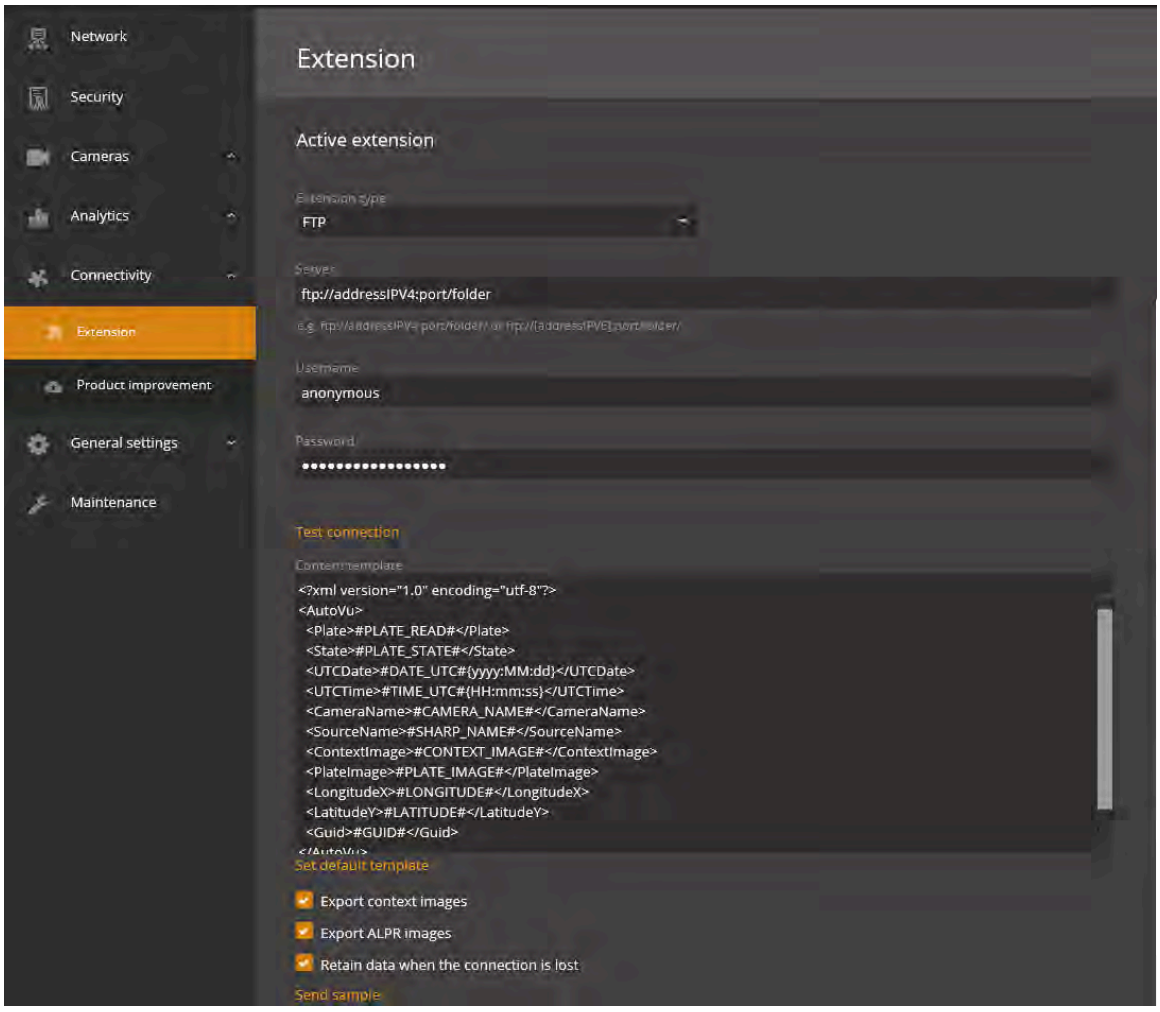
To configure the SharpZ3 for FTP:

1 Log on to the Sharp Portal.
2 From the **Configuration** menu, click **Connectivity** > **Extension**.
3 From the **Active extension** section, select **FTP** from the **Extension type** menu.
4 Configure the following:
   - **Server:** Enter the server name and location of the FTP server.

     NOTE: The appropriate rights on that location must be granted to the chosen user on the FTP server. The target directory must also be present and be writable by that user.
   - **Username:** Enter the username for the server.
   - **Password:** Enter the password for the username.
   - **Content Template:** ALPR data is sent in XML format, using the template shown. You can change certain elements if you choose.
   - **Export context images:** Export the context image (in JPEG format).
   - **Export ALPR images:** Export the plate image (in JPEG format).
   - **Retain data when the connection is lost:** Select this option for plate reads to be saved locally in the SharpZ3 database if the connection with the server is lost. The system attempts to reconnect with the server every 30 seconds. Stored reads are pushed to the server when the connection is reestablished.

     IMPORTANT: If there are any plate reads in the SharpZ3 database, clearing this check box and saving the configuration deletes the plate reads.
5 Click **Test connection** to verify that the server can be reached and that the credentials are valid.

6 Click **Send sample** to send a test plate to verify that the system can connect to the server using these settings.



7 Click **Save**.

Modifications you can make to the SharpZ3 FTP XML template

The XML code defines the structure of the XML files generated by the SharpZ3. You can re-sort or remove any of the fields. The XML file name consists of the SharpZ3 name and a unique identification number (for example, SHARP12345_6ee17b00-82c1-466b-9fd6-003417bc82c4_lpr.xml).

Template:

```
<?xml version="1.0" encoding="utf-8"?>
<AutoVu>
  <Plate>#PLATE_READ#</Plate>
  <State>#PLATE_STATE#</State>
  <UTCDate>#DATE_UTC#{yyyy:MM:dd}</UTCDate>
  <UTCTime>#TIME_UTC#{HH:mm:ss}</UTCTime>
  <CameraName>#CAMERA_NAME#</CameraName>
  <SourceName>#SHARP_NAME#</SourceName>
  <ContextImage>#CONTEXT_IMAGE#</ContextImage>
  <PlateImage>#PLATE_IMAGE#</PlateImage>
  <LongitudeX>#LONGITUDE#</LongitudeX>
  <LatitudeY>#LATITUDE#</LatitudeY>
  <Guid>#GUID#</Guid>
```

```
</AutoVu>
```

Note the following:

- Hotlist matching is not supported.
- `UTCDate` and `UTCTime` display the Windows date and time properties.
- `CameraName` displays the name of the camera, for example, `Context Camera`.
- `SourceName` is the SharpZ3 name (for example, Sharp12345).
- `ContextImage` and `PlateImage` images are encoded into JPEG and then converted to Base64 (text) for transport and storage in XML / JSON. To use them, you must transform them back into JPEG binary (Base64 -> array of bytes).
- `Guid` is the unique identification of the event read.
- You can add the following custom fields to the template:
  - **Confidence score:** The SharpZ3 assigns a confidence score percentage to each license plate read. This value indicates how confident the SharpZ3 is in the accuracy of the read. You can add the confidence score associated with the plate read to the XML using the following field:

    ```
    <ConfidenceScore>#CUSTOM_FIELDS#{Confidence Score}</ConfidenceScore>
    ```

    NOTE: License plates that contain similar characters such as *8* and *B* are more difficult to read and generally produce reads with a lower confidence score.
  - **Relative Motion:** When the SharpZ3 reads a plate, it detects and displays if the vehicle is approaching or moving away. To use this field, add the following line to the XML:

    ```
    <RelativeMotion>#CUSTOM_FIELDS#{Relative Motion}</RelativeMotion>.
    ```
  - **State Name:** The SharpZ3 attempts to read the plate's origin in addition to the plate number (some plates include the issuing state or province). This may not be possible for all types of license plates. To use this field, add `<State>#CUSTOM_FIELDS#{State Name}</State>` to the XML, and then select *State* on the *Analytics* page of the **Configuration** menu in the Sharp Portal.

    NOTE: The ALPR context you are using must support the state name feature.
  - **Vehicle Type:** Certain license plates include character symbols that identify specific vehicle types (for example, taxi, transport, and so on). If the SharpZ3 can read these symbols, it displays the vehicle type along with the other read and hit information. To use this field, add the following line to the XML:

    ```
    <VehicleType>#CUSTOM_FIELDS#{Vehicle Type}</VehicleType>.
    ```

Configuring the SharpZ3 HTTP/HTTPS extension

You can configure the SharpZ3 to send ALPR data to an HTTP server instead of to Genetec Patroller™. ALPR data that is sent to an HTTP/HTTPS server can then be integrated by third-party applications.

What you should know

You can only configure one extension for the SharpZ3 camera.

To configure the SharpZ3 for HTTP/HTTPS:

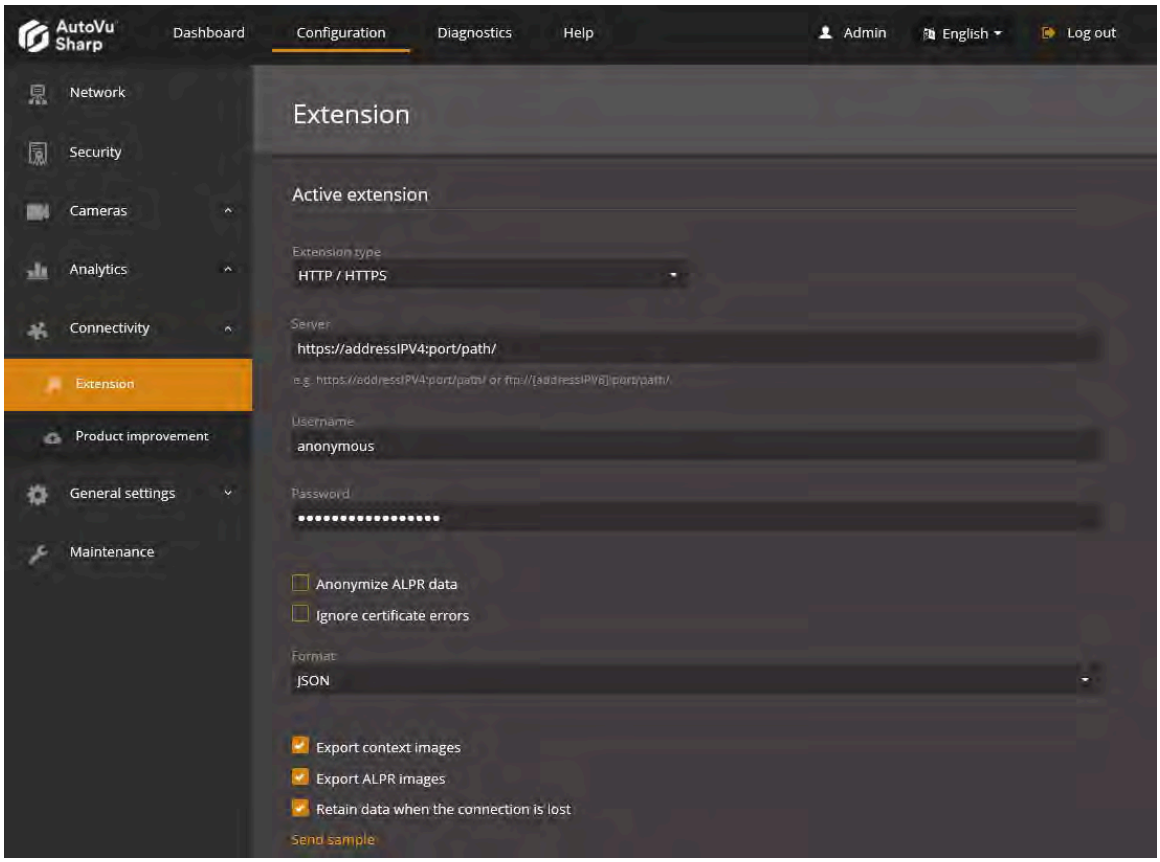
1 Log on to the Sharp Portal.
2 From the **Configuration** menu, click **Connectivity** > **Extension**.
3 From the **Active extension** section, select **HTTP/HTTPS** from the **Extension type** menu.
4 Configure the following:

- **Server:** Enter the server name and location of the third party receiving HTTP server.
- **Format:** Select the format you want to send the ALPR data in. You can select either **JSON** or **XML** format.
- **Username:** Enter the username for the server.
- **Password:** Enter the password for the username.
- **Export context images:** Export the context image (in JPEG format).
- **Export ALPR images:** Export the plate image (in JPEG format).
- **Retain data when the connection is lost:** Select this option for plate reads to be saved locally in the SharpZ3 database if the connection with the server is lost. The system attempts to reconnect with the server every 30 seconds. Stored reads are pushed to the server when the connection is reestablished.

  IMPORTANT: If there are any plate reads in the SharpZ3 database, clearing this check box and saving the configuration deletes the plate reads.
- **Anonymize ALPR data:** The camera *hashes* the license plate using the SHA-1 algorithm. When you add an alphanumeric *salt (cryptography)* to the license plate number, it increases the security of the hashed output. Adding the same salt on all of the cameras in a network means that the same license plate produces an identical hash on all cameras. This allows the external system to recognize the identical hashes as a the same vehicle while still maintaining privacy.

  IMPORTANT: If the salt is changed after it is set, it must also be changed on all other cameras. Changing the salt breaks the link between old reads and new reads.
- **Ignore certificate errors:** Select this option when sending ALPR data to an HTTPS server that does not have a trusted certificate. The SharpZ3 does not send the ALPR data to an HTTPS server that does not have a trusted certificate unless you select this option.

5 Click **Send sample** to send a test plate to verify that the system can connect to the server using these settings.



6 Click **Save**.

Examples of JSON and XML ALPR events for the SharpZ3 HTTP extension

When you send ALPR data to an HTTP server, you can configure the SharpZ3 system to send the data in XML or JSON format.

JSON format sample:

The following is an example of a license plate read event in JSON format.

NOTE: The binary image data has been removed from the example.

```
{ "ContextCameraName" : "Context Camera",
  "ContextImage" : "",
  "Id" : "32cf870a-46aa-4cfd-914b-00062d98e93a",
  "Latitude" : 0.0,
  "Longitude" : 0.0,
  "LprCameraName" : "LPR camera",
  "PlateAnalytics" : [ { "Key" : "State Name",
        "Score" : -1.0,
        "Value" : "-"
      },
      { "Key" : "Vehicle Type",
        "Score" : 1.0,
        "Value" : "-"
      },
      { "Key" : "Relative Motion",
        "Score" : -1.0,
```

```
        "Value" : "-"
      },
      { "Key" : "Context",
        "Score" : 1.0,
        "Value" : "US"
      },
      { "Key" : "Characters Height",
        "Score" : 1.0,
        "Value" : "70"
      }
    ],
  "PlateImage" : "",
  "PlateRead" : "AA7D2",
  "SourceUrl" : "SharpZ312345",
  "Timestamp" : "2020-03-12T08:42:45.797"
}
```


XML format sample:

The following is an example of a license plate read event in XML format.

NOTE: The binary image data has been removed from the example.


```
<Plate>
  <ContextCameraName>Context Camera</ContextCameraName>
  <ContextImage/>
  <Id>32cf870a-46aa-4cfd-914b-00062d98e93a</Id>
  <Latitude>0.0</Latitude>
  <Longitude>0.0</Longitude>
  <LprCameraName>LPR camera</LprCameraName>
  <PlateAnalytics>
    <PlateAnalytics>
      <Key>State Name</Key>
      <Score>-1.0</Score>
      <Value>-</Value>
    </PlateAnalytics>
    <PlateAnalytics>
      <Key>Confidence Score</Key>
      <Score>1</Score>
    <Value>100</Value>
    </PlateAnalytics>
  </PlateAnalytics>
  <PlateImage/>
  <PlateRead>AA7D2</PlateRead>
  <SourceUrl>SharpZ312345</SourceUrl>
  <Timestamp>2020-03-12T21:35:04.8627622+00:00</Timestamp>
</Plate>
```


Plate read event parameters

The following parameters are included in JSON and XML files that are exported to the HTTP server:

Parameter	Value type	Description
ContextCameraName	String	Name of the color context camera that generated the read event.
ContextImage	Binary	Color context image of the scene. Base64 encoded JPEG image.
Id	Guid	Unique identifier for the read event.
Latitude	Double	Decimal latitude of the SharpZ3 camera.
Longitude	Double	Decimal longitude of the SharpZ3 camera.

Parameter	Value type	Description
LprCameraName	String	Name of the license plate recognition camera that generated the read event.
PlateAnalytics	Array of analytics	Each analytic object is composed of a data triplet. This array is of variable size. The amount of analytic objects received depends on the SharpZ3 camera's configuration.
Key (analytic triplet)	String	Name of the analytic.
Score (analytic triplet)	Float (-1.0 or 1.0)	Indicates if the analytic value is reliable (1.0) or not (-1.0).
Value (analytic triplet)	String	Value of the analytic.
PlateImage	Binary	Black and white cropped license plate image. Base64 encoded JPEG image.
PlateRead	String	Detected license plate number.
SourceUrl	String	Unique name of the SharpZ3 camera.
Timestamp	DateTime	Date and time of the read event (UTC) in the following format: yyyy-MM-ddTHH:mm:ss:fff.

Configuring Syslog for SharpZ3 log files

For installations that include multiple SharpZ3 units, the *Syslog* feature allows you to configure a central repository for all SharpZ3 log entries.

Before you begin

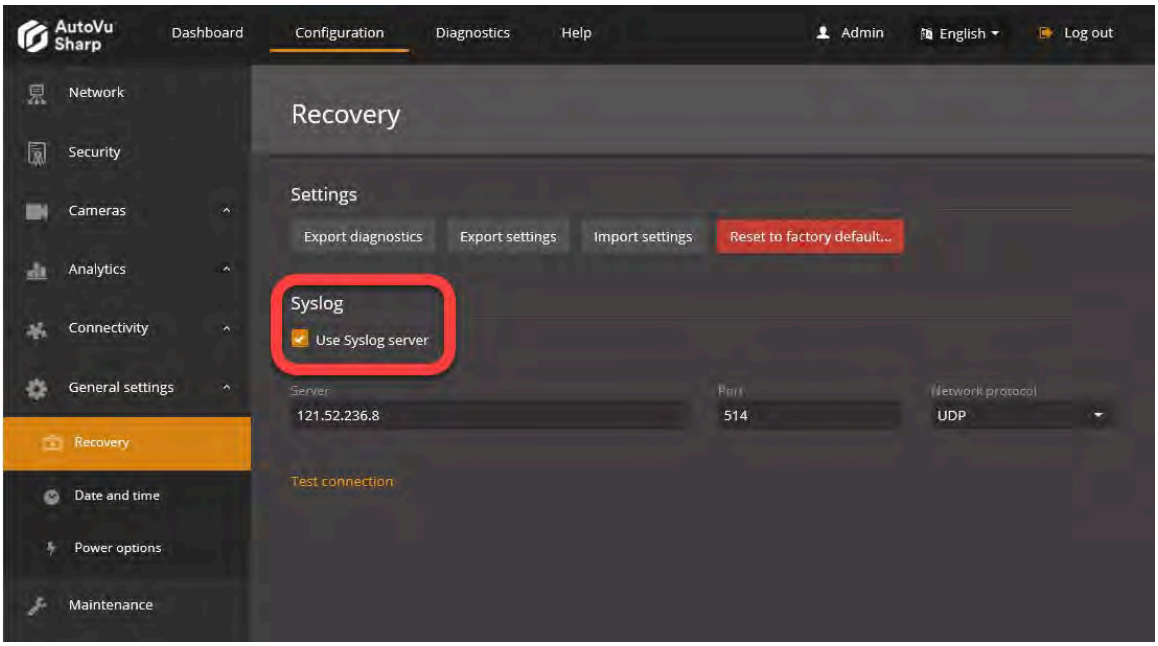
You must have a Syslog server that is accessible by the SharpZ3 unit.

What you should know

- The SharpZ3 syslog feature is compliant with the RFC 5424 protocol.
- Whether you use the syslog feature or not, SharpZ3 logs are available on Sharp Portal under **Diagnostics** > **Logs**.
- When you activate the Syslog server, logs are sent to that server, but are still recorded locally as usual.

To configure a syslog repository for SharpZ3 log files:

1 Log on to the Sharp Portal.
2 From the **Configuration** menu, click **General settings** > **Recovery**.
3 Select the **Use Syslog server** checkbox.
4 Configure the following:
   - **Use Syslog server:** Select this option to configure a central repository for all SharpZ3 log entries.
     - **Server:** Enter the IP address or name of the server.
       NOTE: Syslog server configurations do not support IPv6 addresses.
     - **Port:** Enter the port number of the syslog server.
     - **Network protocol:** Select UDP or TCP.
5 Click **Test connection** to verify that the server can be reached.



6 Click **Save**.

Importing and exporting settings

You can export SharpZ3 settings for use as diagnostic information if required by the AutoVu™ Support team. You can also use the exported settings file to restore the configuration of the SharpZ3 unit or to copy the configuration to another unit.

What you should know

- You can only import settings from the same Sharp model, for example, a SharpV can only import settings from another SharpV.
- You cannot export a configuration from a newer SharpOS version to an older SharpOS version.
- **WARNING:** When you import settings to a SharpZ3, the camera's current configuration is lost with some exceptions, including:
  - Sharp Portal password
  - Network static configuration
  - Certificates
  - Product improvement program registration
- Battery monitoring settings are unaffected by the import operation.

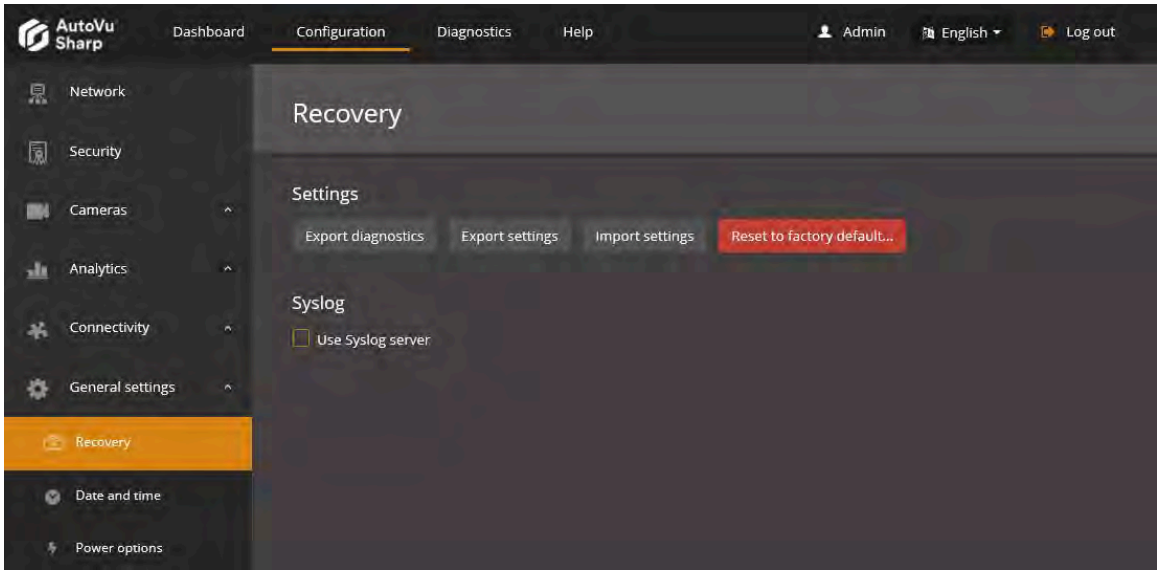
To export SharpZ3 settings:

1 Log on to the Sharp Portal of the SharpZ3 that you want to export settings from.

2 From the **Configuration** menu, click **General settings > Recovery**.

3 From the **Settings** section, select one of the following options:

- **Export diagnostics:** Export a file that includes SharpZ3 diagnostics and SharpZ3 settings.
- **Export settings:** Exports configuration and diagnostic settings as a .zip file. You can use the .zip file for technical support, or you can import the settings to another Sharp unit for quick configuration



The system prepares the files and displays the message "Download succeeded".

4 Save the diagnostics .zip file to a location that is accessible to the browser that is used to view the portal and to the Windows user that will be importing the file. The file is named with the date and time the file was created, for example, `Diagnostics-2020-02-25_12_49_36`.

To import SharpZ3 settings:

1 Log on to the Sharp Portal of the SharpZ3 that you want to import settings to.

2 From the **Configuration** menu, click **General settings > Recovery**.
3 From the **Settings** section, click **Import settings**.
4 Enter the path and filename, or browse to the ZIP file with the SharpZ3 settings you want to import and click **Yes, import**.
5 Follow the on-screen instructions and import the settings to the camera.

4

Troubleshooting for SharpZ3 installation

This section includes the following topics:

- "LED status on the SharpZ3 camera unit" on page 64
- "Resetting a lost password for the Sharp Portal" on page 67

LED status on the SharpZ3 camera unit

The status LEDs on the SharpZ3 camera unit, base unit, ALPR module, and expansion modules respond according to the status of the system.

SharpZ3 camera LED status



LED	State	Description
Off	Off	The unit is powered-off.
Off	Covert mode	SharpZ3 cameras are configured in covert mode. Following camera startup, their LEDs are deactivated.
Slow red blinking (0.5 seconds off – 0.5 seconds on)	Catastrophic failure	The unit is shut down due to a critical error, for example, an over-temperature alarm. In this state, you cannot connect to the cameras.
Three red blinks per second	Major failure	Internal services are down. You might be able to connect to the cameras and you might be able to see the logs.
One short red blink per second	Performance issues or minor failure	The system is running with important performance issues, for example, failure of the illuminator.
Five green blinks per second	System update	Internal services are down during the system update, but is expected to come back online after the update is complete.
Slow red and green alternating (0.5 seconds each)	Locate camera	After clicking **Blink LED** in the Sharp Portal, the LED blinks for 10 seconds.
Slow green blinking	Normal mode	The system is running normally.
One green blink per second	System startup	The system is booting up.

SharpZ3 base unit LED status



LED	OLED display	State	Description
Off		Off	The unit is powered-off.
Off	`CoverMode`	Covert mode	SharpZ3 cameras are configured in covert mode. Following camera startup, their LEDs are deactivated.
Slow red blinking (0.5 seconds off – 0.5 seconds on)	`C-fail`	Catastrophic failure	The unit is shut down due to a critical error, for example, an over-temperature alarm. In this state, you cannot connect to the cameras.
Three red blinks per second	`M-Fail`	Major failure	Internal services are down. You might be able to connect to the cameras and you might be able to see the logs.
One short red blink per second	`Perf Fail`	Performance issues or minor failure	The system is running with important performance issues, for example, failure of the illuminator.
Five green blinks per second	`Updating`	System update	Internal services are down during the system update, but is expected to come back online after the update is complete.
Solid green	`Normal`	Normal mode	The system is running normally.
One green blink per second	`Startup`	Camera startup	The system is booting up.

Navigation expansion module LED status



LED	State	Description
Off	Off	The unit is powered-off.
Slow green blinking	Normal mode	The module is running normally.
Slow red blinking	Error	The module is not receiving messages from GNSS chip.

AUX PoE expansion module LED status



LED	State	Description
Off	Off	The unit is powered-off.
Slow green blinking	Normal mode	The module is running normally.

Resetting a lost password for the Sharp Portal

If you forget your password to the Sharp Portal for a SharpZ3 system, you can reset the password using the **I forgot my password** button on the Sharp Portal logon screen.

What you should know

- To reset a lost password, you need the yellow *Important information* sticker that was shipped with the SharpZ3 unit. If you do not have the sticker, you must contact the AutoVu™ Support team.



- If you don't see the **I forgot my password** link on the Sharp Portal logon screen, it means the Sharp Portal has never been accessed and still uses the default **Username**: *admin* and **Password**: *Genetec*. You are prompted to change the default password when you access the Sharp Portal for the first time.

To reset a lost password for the Sharp Portal:

1 From the Sharp Portal logon screen, click **I forgot my password**.

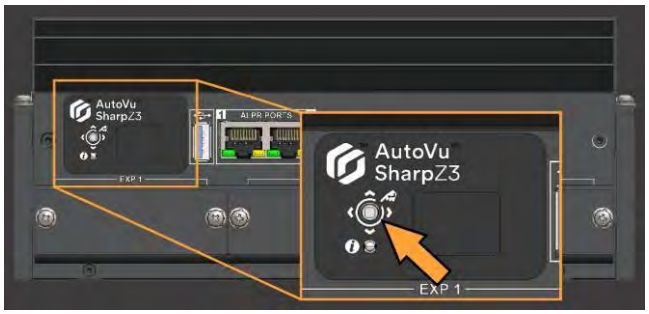
2 Enter the 32-character **Unit access code**.

You can find the code on the yellow sticker that was provided with the SharpZ3 unit.



3 Click **Next**.

4 Press and hold the joystick on the SharpZ3 base unit for two seconds.
This step ensures that the password cannot be reset remotely.



NOTE: If you do not press the joystick within two hours, the password recovery operation is canceled.

5 When prompted, enter and confirm the new Sharp Portal password.
6 Click **Apply**.
The message *The portal password has been changed* is displayed.
You are redirected to the logon page.
7 Log on to the Sharp Portal using your new password.
8 Store your password safely for future use.
9 Click **Connect**.

5

Updating the system

This section includes the following topics:

- "Updating a Sharp unit from the SharpOS 13 Sharp Portal" on page 70

Updating a Sharp unit from the SharpOS 13 Sharp Portal

To benefit from the most recent security improvements, it is recommended to upgrade the unit's SharpOS and platform software from the Sharp Portal.

Before you begin

If you are updating a SharpZ3 unit, ensure that all of the SharpZ3 cameras are connected to the ALPR module on the base unit.

What you should know

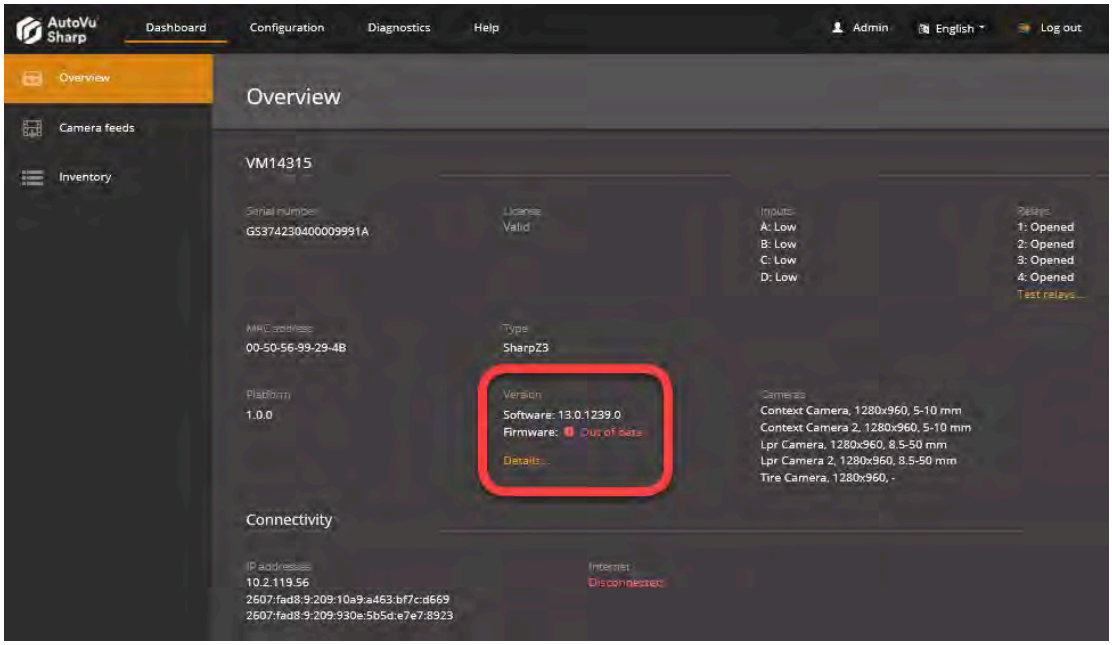
- You can update the Sharp unit's platform package or SharpOS package.
  - **Platform package:** Updates Windows 10 with the latest security patches.
  - **SharpOS package:** Updates the SharpOS installed on the Sharp.

    IMPORTANT: When the SharpOS is updated, any plate reads that are stored locally on the Sharp unit are deleted.
- **IMPORTANT:** If you need to update both the SharpOS software and the platform software, update the SharpOS first.
- On a SharpZ3 unit that includes a four-camera ALPR module, each set of two cameras is configured in a separate Sharp Portal which is available from a link on the *Maintenance* page. It is recommended that you update both portals with the same platform and SharpOS packages.

To update the unit's SharpOS or platform package:

1 Log on to the Sharp Portal.

2 To verify that the firmware needs to be updated, click **Dashboard** > **Overview**. If **Firmware** shows the message *Out of date*, continue with the update steps.



3 Download the update package from GTAP. Save the *.gpack* file on the local machine you are using to log on to the Sharp Portal.

4 From the **Configuration** menu, select **Maintenance**.

5 In the *Packages* section, click the **Update** button for the platform or SharpOS.

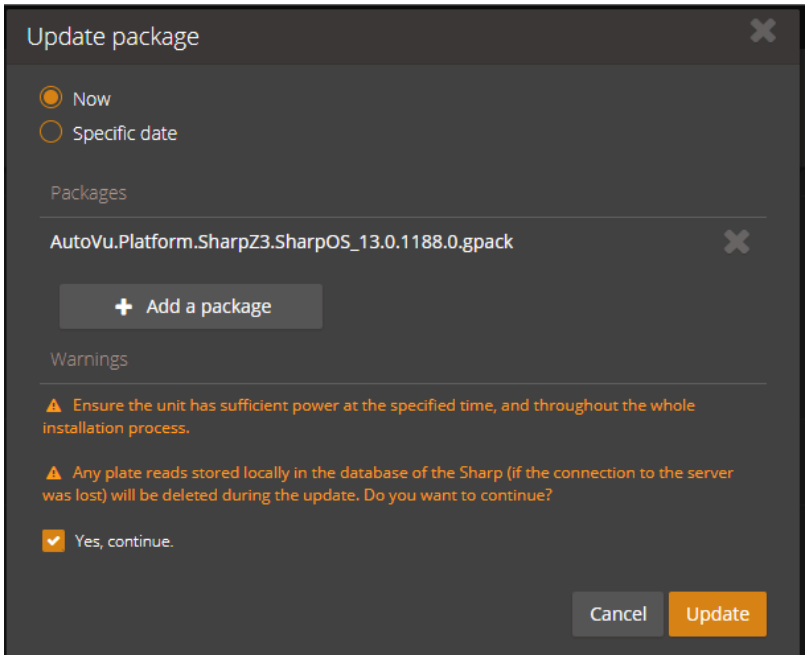
6 In the *Update package* dialog box, choose when to run the update.
   - Click **Now** to run the update immediately.
   - Click **Specific date** to schedule the update for off-peak hours.

7 Click **Add a package**, find the update *.gpack* file, and then click **Open**.

8 Acknowledge the warnings and click **Update** or click **Schedule** if you set a specific date for the update.

IMPORTANT:

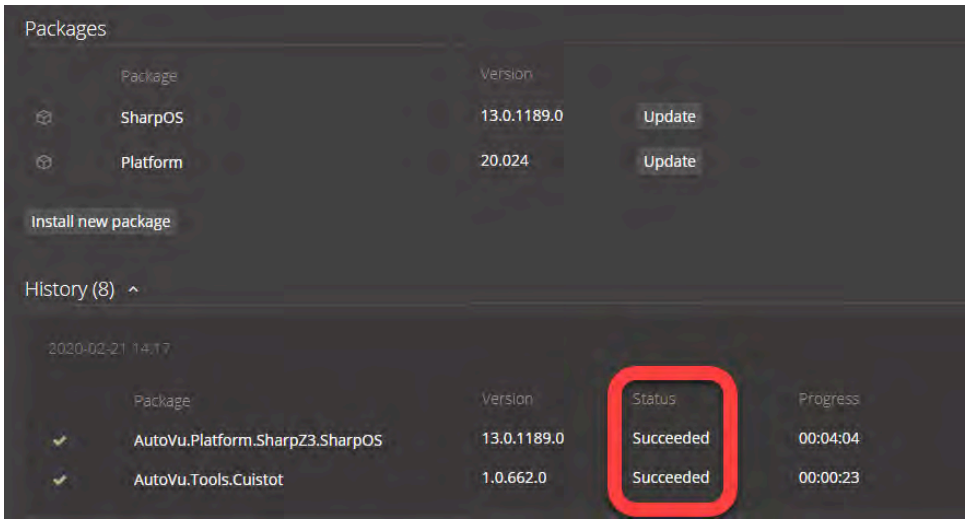
- Whether you configure the update for **Now** or for a **Specific date**, the package is transferred to the Sharp unit immediately. Do not close or navigate away from the browser page until the transfer is complete.



The files are transferred to the Sharp unit and the update process begins.

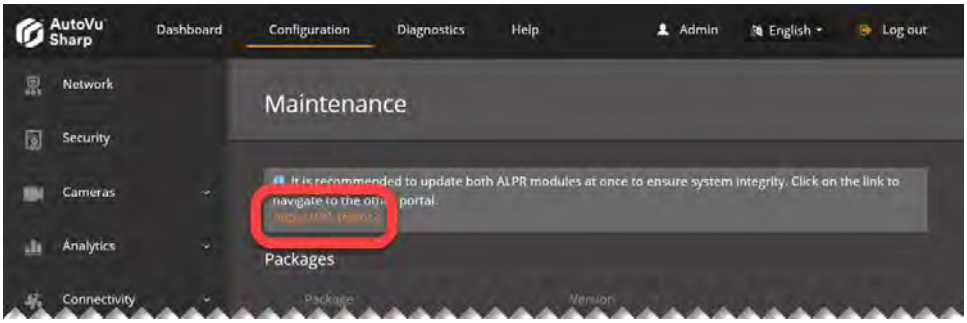
NOTE: At certain points in the update process, the progress bar might not move for several minutes. It can take up to 30 minutes to complete the update.

If the update is successful, the new platform version is displayed and the **History** displays that the update *Succeeded*.



After you finish

If you are updating a SharpZ3 system that includes a four-camera ALPR module, each group of two cameras is configured on a separate Sharp Portal. It is recommended that you update both portals at the same time. A link is provided at the top of the *Maintenance* page to direct you to the second Sharp Portal.



6

Sharp Portal reference

This section includes the following topics:

- "Sharp Portal - Overview page" on page 74
- "Sharp Portal - Camera feeds page" on page 76
- "Sharp Portal - Inventory page" on page 78
- "Sharp Portal - Network page" on page 79
- "Sharp Portal - Security page" on page 80
- "Sharp Portal - Exposure page" on page 82
- "Sharp Portal - Position and orientation page" on page 83
- "Sharp Portal - Auxiliary cameras page" on page 84
- "Sharp Portal - ALPR settings page" on page 85
- "Sharp Portal - Extension page" on page 86
- "Sharp Portal - Product improvement program page" on page 88
- "Sharp Portal - Recovery page" on page 89
- "Sharp Portal - Date and time page" on page 90
- "Sharp Portal - Power options page" on page 91
- "Sharp Portal - Maintenance page" on page 92
- "Sharp Portal - Logs page" on page 93
- "Sharp Portal - Log sources page" on page 94

Sharp Portal - Overview page

This section lists the settings found in the *Overview* page of the Sharp Portal and provides general information about the SharpZ3, such as serial number, license, IP address, input and relay status, and so on.

To navigate to the *Overview* page, click **Configuration** > **Overview**.

Camera info

The following information is displayed:

- **Serial number:** Displays the SharpZ3 hardware serial number.
- **License:** Displays whether the SharpZ3 license is valid, invalid, or missing.
- **Inputs:** Displays the inputs on the SharpZ3 and whether the input is in a **High** or **Low** state. A high-state input is indicative of a voltage of 5.75 V or higher. A low-state input is indicative of a voltage of 4.80 V or lower.
- **Relays:** Displays the SharpZ3 relays and whether the relay state is **Opened** or **Closed**. The SharpZ3 has two 0.25 A solid-state relays and two 8 A electromechanical relays.
- **Test relays:** Click to toggle your configured relay between **Opened** and **Closed** to validate the configuration.
- **Mac address:** Displays the MAC address of the SharpZ3. This information might be requested if you contact technical support.
- **Type:** Displays the type of Sharp unit.
- **Platform:** Displays the software image installed on the SharpZ3. If you contact technical support, you might be asked to provide this number.
- **Version:**
  - **Software:** Displays the SharpOS version currently installed.
  - **Firmware:** Displays the update status of the Sharp unit.
  - **Details:** Provides additional information about the versions of the files and components included in the package.

  Displays the SharpOS package version. You can use this information to confirm that your SharpZ3 is up to date.
- **Cameras:** Displays the resolution and the lens focal range available for cameras connected to the SharpZ3 unit.

Connectivity

The following information is displayed:

- **IP addresses:** Displays the IPv4 and IPv6 address of the SharpZ3.
- **Internet:** Displays whether the SharpZ3 is connected to the Internet.

Storage and usage

You can view information about reads stored on the SharpZ3, CPU usage, and memory usage. Indicator lines, usually green or orange, are provided so you can see the status. If an indicator line stays red for a prolonged period of time, it indicates either high CPU activity or that there is a problem.

- **Reads stored:** Indicates the reads stored in the database of the SharpZ3. The number of reads is also displayed.
- **Memory:** Displays information on the system's RAM memory.
- **CPU (Total):** Indicates the total CPU usage of the SharpZ3. Click **Show details** to see the usage for each CPU.

Last activities

- **Unit rebooted:** Indicates the last time the unit was restarted.
- **Software restarted:** Indicates the last time the PlateReader software was restarted.

Sharp Portal - Camera feeds page

This section lists the settings found in the *Camera feeds* page of the Sharp Portal. Use the *Camera feeds* page to view the live feeds of the context camera, ALPR camera, and auxiliary cameras.

NOTE: Some of the fields described in this section do not apply to auxiliary cameras.

To navigate to the *Camera feeds* page, click **Dashboard** > **Camera feeds**.

Camera feeds

The **Camera feeds** section displays the live video feeds for any two of the connected camera units or auxiliary cameras such as wheel-imaging cameras. You can also view information about the live video feed such as the **FPS**, **Resolution**, **Exposure time**, and so on.

Videos

- **Camera unit:** Select which Sharp camera or auxiliary camera to view.
- **Cameras:** Displays the resolution and the lens focal range available for cameras connected to the SharpZ3 unit.
- **Overlays:**
  - **Crosshairs:** Select this option to display crosshairs in the ALPR or context camera window.
  - **Bounding box:** Select this option to display the yellow bounding box around detected plates in the ALPR camera window.
- **Record:** Click the **Record** button to capture a series of context and ALPR images directly from the *Camera feeds* window and save them to your computer as a .zip file for debugging purposes.

  NOTE:

  - Using the **Record** feature increases CPU usage.
  - To use this feature, you cannot use the camera's auto-generated certificate. You must install a self-signed certificate that includes the IP address of the camera.

Metadata

- **FPS (actual/average):** Displays the FPS of the context camera. This is the framerate processed by the ALPR engine.
- **Resolution:** Displays the resolution of the camera's video feed.
- **Exposure time:** Displays the **Exposure** time of the video frame.
- **Gain:** Displays the **Gain** of the video frame.
- **Illuminator:** (Context camera only) Displays the intensity of light of the illuminator (as a percentage) on the Context camera.

Last reads

- **Candidate:** Every read detected is displayed in this field as a potential read candidate. The camera can read up to 30 frames (reads) per second. The **Read strategy** configured on the **Analytics** page determines which read candidate will be used as the final read.

NOTE:

- The list contains the reads that have been made in this portal session. Exiting the session resets the list.
- The list is of limited length and older reads are automatically removed.
- Clicking on an entry pauses the list. Clicking Play resumes the list refresh and adds new reads that were received while the list was paused.
- The **Count** field accounts for all incoming reads and does not distinguish between camera units.

Sharp Portal - Inventory page

This section lists the settings found in the *Inventory* page of the Sharp Portal. Use the *Inventory* page to view a list of hardware components along with their firmware versions and status.

To navigate to the *Inventory* page, click **Dashboard** > **Inventory**.

The following information is displayed:

NOTE: Additional functionality is available for certain hardware components, such as blinking the LED or connecting to a configuration portal.

- **Module:** Displays the name of the component.
- **Version:** Displays the component's firmware version.
- **Identification:** Displays a unique identifier of the component, such as its name or serial number.

  NOTE: The serial number is also printed on the component sticker.
- **Status:** Displays the health status of the component.

Sharp Portal - Network page

This section lists the settings found in the *Network* page of the Sharp Portal. Use the *Network* page to configure the SharpZ3 to use Dynamic Host Configuration Protocol (DHCP) or a static IP address.

IPv4 network settings

To navigate to the *Network* page, click **Configuration** > **Network**.

- **Use DHCP:** If the patrol vehicle uses a DHCP server, you can configure the SharpZ3 system for DHCP. Consider the following:
  - When a SharpZ3 system is configured to use DHCP, the setting applies to the ALPR module, but does not apply to expansion modules. Expansion modules connected to the base unit always use static IP addresses that are defined on the *Network* page. For the expansion modules to work with the DHCP system, you must configure a compatible **Subnet mask** and **IP address** for each module.
  - When a SharpZ3 is configured in DHCP and the DHCP server cannot be reached, the default fall-back IPv4 address is 192.168.10.99. On a four-camera ALPR module, the second group of two cameras has a default fall-back address of 192.168.10.99.
    NOTE: The default fallback takes at least two minutes to become effective when no DHCP server is detected at bootup.
- **Use static IP address:** If the SharpZ3 must use addresses withing a specific range, you can configure static addresses for the modules.

  IMPORTANT: When assigning specific IP addresses, ensure the configuration stays compatible with the rest of the system, otherwise the base unit, expansion modules, or aux cameras might be unreachable. For example, it is important that all components be on the same subnet.

  IMPORTANT: You must use a fixed IP address if you want to stream video to the Security Center Archiver role. You can do this using a static IP address or a reserved IP address on the DHCP server.
- **IP address:** Enter the new IP address you want to assign to the ALPR module. The default is 192.168.10.1 (port 1 and 2) and 192.168.10.2 (port 3 and 4).
- **Subnet mask:** Enter the new **Subnet mask** for the ALPR module, if applicable. The default is 255.255.255.0.

  IMPORTANT: When assigning specific IP addresses, ensure the configuration stays compatible with the rest of the system, otherwise the base unit, expansion modules, or aux cameras might be unreachable. For example, it is important that all components be on the same subnet.
- **Gateway:** Enter the new **Gateway** for the ALPR module, if applicable. The default is 10.0.0.0.
- **DNS:** Enter the new **DNS** for the ALPR module, if applicable. The default is 10.0.0.0.

EXP module settings

- **IP address:** Enter the new IP address you want to assign to the expansion module. The default IP address depends on which expansion slot the module is installed in.
- **Subnet mask:** Enter the new **Subnet mask** for the expansion module, if applicable. The default is 255.255.255.0.

Sharp Portal - Security page

This section lists the settings found in the *Security* page of the Sharp Portal. Use the *Security* page to change the password and to manage certificates and permissions.

To navigate to the *Security* page, click **Configuration** > **Security**.

Access

- **Modify password:** Click **Modify password** to change the password for the SharpZ3.

  NOTE: If you forget your password, you can reset it from the logon page.

Certificate

Displays the signed and self-signed certificates that have been installed in the trusted root store of the SharpZ3. You can install multiple certificates and select which certificate to activate.

To activate a certificate, select the **Active** button for the certificate and click **Save and reboot**.

To delete a certificate click **X** and click **Save**.

NOTE: You can delete certificates, but you must leave at least one certificate on the SharpZ3.

- **+ Self-signed:** Click to create a self-signed certificate. In the *Create a self-signed certificate* dialog box, you must enter a two-letter **Country** code, the **Common name** of the SharpZ3, one or more **IP addresses**, and you must define the **Validity (in years)**. The other fields are optional.

  NOTE:

  - If you use a self-signed certificate, you must also install the certificate on your client machine. For example, the machine used to log on to the Sharp Portal.
  - If a certificate signature is issued by a certificate authority that is not included in the list of Windows of third-party root certificate authorities (CA), or if your organization has its own public key infrastructure (PKI) which manages signatures, you must add the CA to the platform software running on the SharpZ3 so that the host can validate the chain of trust. For more information, see KBA-78971: Adding a certificate to a pre-12.8 SharpV from an unknown certificate authority on the Genetec™ TechDoc Hub.
- **+ Signing request:** Click to create a certificate signing request. A certificate signing request must be created for your server before you can order a signed certificate from a trusted Certificate Authority. You must enter a two letter **Country** code, the **Common name** of the SharpZ3, and the **IP address** in the *Create a certificate signing request* dialog box. The other fields are optional.

  IMPORTANT: If the SharpZ3 has been added to the Security Center Archiver and is being used to monitor video, you must enter the IP address of the SharpZ3 and not the SharpZ3 name.

  NOTE: The signing request is deleted when the certificate is signed.

Permissions

- **Accept remote reboot requests:** Select this option so that the SharpZ3 can be rebooted from Security Center.
- **Remote assistance:** Click **Enable for 1 hour** to grant remote access for technical support. The time and date when access expires is displayed.

  NOTE: After one hour, the remote assistance session ends. If the AutoVu™ Support team needs additional time to resolve the issue, you can extend the remote assistance session.

Unit

- **Run in covert mode:** Select this option to turn off the LED on the Sharp camera unit, making it less noticeable.

IMPORTANT: Selecting this option does not mean that the LED will never be illuminated. For example, if there is a serious error with the SharpZ3, the LED will blink to indicate that there is a problem.

Sharp Portal - Exposure page

This section lists the settings found in the *Exposure* page of the Sharp Portal. Use the *Exposure* page to adjust the exposure of the license plates in the ALPR image.

To navigate to the *Exposure* page, click **Configuration** > **Cameras** > **Exposure**.

The following information is displayed:

- **Select your camera:** Select the camera to configure.
- **Lighting type:** Select a lighting type from the menu:
  - **Auto (Default):** Select this option to have the SharpZ3 automatically adjust the lighting settings (white balance) according to the surroundings.
  - **Fixed (Sun):** Select this option if advised by the customer support team.
- **Exposure:** Choose from the following:
  - **Default:** Select this option to have the SharpZ3 automatically adjust the exposure settings.
  - **Fixed (indoor):** Select this option when constant lighting conditions are available. Use the sliders to adjust the **Gain** and **Exposure time**, until the overall brightness and clarity you want for the image is achieved.
  - **Range (outdoor):** Select this option for variable lighting conditions outdoors. Use the sliders to adjust the **Gain** and **Exposure time**, until the overall brightness and clarity you want for the image is achieved.
- **(Context camera only) Allow illuminator:** Select this to enable the IR illuminator in low light conditions. If **Exposure** is set to **Fixed (indoor)**, the IR illuminator is fixed to On or Off depending on **Allow illuminator** check box. If **Exposure** is set to **Range (outdoor)**, the illuminator is automatically turned On or Off depending on light conditions. However, the IR illuminator can be completely turned off by clearing the **Allow illuminator** check box.

Sharp Portal - Position and orientation page

This section lists the settings found in the *Position and orientation* page of the Sharp Portal. Use the *Position and orientation* page to define SharpZ3 camera positions on the patrol vehicle roof.

To navigate to the *Position and orientation* page, click **Configuration** > **Cameras** > **Position and orientation**.

The following information is displayed:

- **Enable:** When enabled, the system estimates the GNSS position of the license plate of the target vehicle.

Position

- **Left/right:** Define how far the camera is installed to the left (0 to -400 cm) or to the right (0 to 400 cm) of the GNSS antenna.
- **Rear/front:** Define how far the camera is installed to the rear (0 to -1000 cm) or to the front (0 to 1000 cm) of the GNSS antenna.
- **Below/above:** Define how far the camera is installed below (0 to -400 cm) or above (0 to 400 cm) the GNSS antenna.

Orientation

- **Pan:** Define how far the camera is panned to the left (-90°) or to the right (90°) from a straight forward view (0°).
- **Tilt:** Define how far the camera is tilted to the up (45°) or down (-45°) from a level installation (0°).
- **Roll:** Define how far the camera is rolled counter-clockwise (-45°) or clockwise (45°) from a level installation (0°).

Sharp Portal - Auxiliary cameras page

This section lists the settings found in the *Auxiliary cameras* page of the Sharp Portal. Use the *Auxiliary cameras* page to configure the ports of the SharpZ3 Aux PoE expansion module and to change PoE camera passwords.

To navigate to the *Auxiliary cameras* page, click **Configuration** > **Cameras** > **Auxiliary cameras**.

The following information is displayed:

Wheel-imaging camera association

- **Camera Unit:** Lists the installed SharpZ3 camera units.
- **Associated AUX PoE camera:** You must associate the right and left wheel-imaging cameras with their respective SharpZ3 camera units. Select the PoE expansion module port where the associated wheel-imaging camera is connected.

  TIP: If you are not sure which port a wheel-imaging camera is connected to, check the video feed for the auxiliary cameras in **Dashboard** > **Camera feeds**.

Settings

- **Change camera password:** AutoVu™ auxiliary PoE cameras use the default Username: *admin* and Password: *1234*. If required by local regulations, you can change the camera password from the Sharp Portal instead of using the camera's web portal.

  IMPORTANT: If you change the AUX PoE expansion module port connection after you change the password, you must reapply the password.

Sharp Portal - ALPR settings page

This section lists the settings found in the *ALPR settings* page of the Sharp Portal Use the *ALPR settings* page to configure the analytics used for the license plates read by the SharpZ3.

To navigate to the *ALPR settings* page, click **Configuration** > **Analytics** > **ALPR settings**.

The following information is displayed:

Location

- **Context:** Select which plate origin the SharpZ3 is reading.

Analytics:

- **State:** Select this option if you want the SharpZ3 unit to attempt read the license plate origin. Depending on the region, this can refer to the issuing state, province, or country.
- **Vehicle make:** Select this option if you want the SharpZ3 unit to attempt to read the vehicle's make from the brand or logo (Honda, Toyota, and so on).

  NOTE: This setting is not recommended for MLPI installations.
- **Confidence score:** The SharpZ3 assigns a confidence score percentage to each license plate read. This value indicates how confident the SharpZ3 is in the accuracy of the read.

  NOTE: License plates that contain similar characters such as *8* and *B* are more difficult to read and generally produce reads with a lower confidence score.
- **Vehicle type and color:** Select this option if you want to include the vehicle type and vehicle color with plate reads. Based on the context image, the Sharp unit can detect if the vehicle is a bus, passenger vehicle, motorcycle, pickup, truck, work van, or an unknown vehicle type. In addition, the Sharp unit can detect if the vehicle is black, white, blue, brown, green, gray, orange, red, or yellow. Colors excluding white and black are also assigned *light*, *neutral*, or *dark* according to the color analysis.

Reads

- **Reading mode:** Select one of the following reading modes:
  - **Continuous:** Select this for plates to be captured continuously. This is the default setting.
  - **Conditional:** When this option is selected, the SharpZ3 captures plate reads continuously as long as the selected input signal meets the condition defined (high/low). You must select an input and specify whether the state is high or low.
  - **Multiconditional:** Generates reads from a specific camera only while an input's status meets the defined high or low condition. This option is required if using the AutoVu™ car camera switch.

Read strategy

- **Slow moving vehicle:**
- **Fast moving vehicle:**

Sharp Portal - Extension page

This section lists the settings found in the *Extension* page of the Sharp Portal. Use the *Extension* page to configure where the SharpZ3 sends ALPR data.

To navigate to the *Extension* page, click **Configuration** > **Connectivity** > **Extension**.

The following information is displayed:

Extension type: None

- **None:** Plate reads are stored locally on the SharpZ3 and can only be retrieved using the Reads API which is an external application.

Extension type: FTP

Sends ALPR data to an FTP server. Configure the following:

- **Server:** Enter the server name and location of the FTP server.

  NOTE: The appropriate rights on that location must be granted to the chosen user on the FTP server. The target directory must also be present and be writable by that user.
- **Username:** Enter the username for the server.
- **Password:** Enter the password for the username.
- **Content Template:** ALPR data is sent in XML format, using the template shown. You can change certain elements if you choose.
- **Set default template:** Reverts to the default template values.
- **Export context images:** Export the context image (in JPEG format).
- **Export ALPR images:** Export the plate image (in JPEG format).
- **Retain data when the connection is lost:** Select this option for plate reads to be saved locally in the SharpZ3 database if the connection with the server is lost. The system attempts to reconnect with the server every 30 seconds. Stored reads are pushed to the server when the connection is reestablished.

  IMPORTANT: If there are any plate reads in the SharpZ3 database, clearing this check box and saving the configuration deletes the plate reads.
- **Send sample:** Verifies that the system can connect to the server and send a sample read file using the configured settings.

HTTP / HTTPS

- **Server:** Enter the server name and location of the FTP server.

  NOTE: The appropriate rights on that location must be granted to the chosen user on the FTP server. The target directory must also be present and be writable by that user.
- **Format:** Select the format you want to send the ALPR data in. You can select either **JSON** or **XML** format.
- **Username:** Enter the username for the server.
- **Password:** Enter the password for the username.
- **Anonymize ALPR data:** The camera *hashes* the license plate using the SHA-1 algorithm. When you add an alphanumeric *salt (cryptography)* to the license plate number, it increases the security of the hashed output. Adding the same salt on all of the cameras in a network means that the same license plate produces an identical hash on all cameras. This allows the external system to recognize the identical hashes as a the same vehicle while still maintaining privacy.

  IMPORTANT: If the salt is changed after it is set, it must also be changed on all other cameras. Changing the salt breaks the link between old reads and new reads.
- **Ignore certificate errors:** Select this option when sending ALPR data to an HTTPS server that does not have a trusted certificate. The SharpZ3 does not send the ALPR data to an HTTPS server that does not have a trusted certificate unless you select this option.

- **Export context images:** Export the context image (in JPEG format).
- **Export ALPR images:** Export the plate image (in JPEG format).
- **Retain data when the connection is lost:** Select this option for plate reads to be saved locally in the SharpZ3 database if the connection with the server is lost. The system attempts to reconnect with the server every 30 seconds. Stored reads are pushed to the server when the connection is reestablished.

  IMPORTANT: If there are any plate reads in the SharpZ3 database, clearing this check box and saving the configuration deletes the plate reads.

Patroller

Sends ALPR data to Genetec Patroller™. Configure the following:

- **Discovery port:** Port on which the SharpZ3 listens for discovery requests. This port number must match the discovery port entered on the Genetec Patroller™ Config Tool *Cameras* page.

Sharp Portal - Product improvement program page

This section lists the settings found in the *Product improvement program* page of the Sharp Portal. Use the *Product improvement program* page to configure the delay period to send images from SharpZ3 camera to servers at Genetec Inc.

To navigate to the *Product improvement program* page, click **Configuration** > **Connectivity** > **Product improvement**.

The following information is displayed:

Product improvement program

- **Activate program:** Select one of the following activation modes:
  - **Not Active:** Select this option if you are not participating in the program.
  - **Always activated (recommended):** Select this option if you are participating in the program. When this option is selected, the SharpZ3 camera sends images to Genetec Inc. cloud systems continuously as long as there is an established connection.
  - **Activated for:** Select this option if you want send images for a support case. You can choose a delay period from the menu.
    NOTE: When a delay period has been selected and the program is active, an expiration date and time is displayed.
  - **Support case number (optional):** If you activate the program for a support case, enter the support case number provided by Genetec™ Technical Support.
- **Agreement:** Select the check box to agree to terms and conditions of the product improvement program feature.

Sharp Portal - Recovery page

This section lists the settings found in the *Recovery* page of the Sharp Portal. Use the *Recovery* page to import or export settings and to configure a Syslog server.

To navigate to the *Recovery* page, click **Configuration** > **General settings** > **Recovery**.

The following information is displayed:

Settings

- **Export diagnostics:** Export a file that includes SharpZ3 diagnostics and SharpZ3 settings.
- **Export settings:** Exports configuration and diagnostic settings as a .zip file. You can use the .zip file for technical support, or you can import the settings to another Sharp unit for quick configuration
- **Import settings:** Imports configuration settings from a .zip file exported from another Sharp. You can use this .zip file to quickly configure your Sharp. After you import the settings, the Plate Reader service restarts automatically.

  IMPORTANT: You can only import settings from a similar Sharp (same model and SharpOS version).
- **Reset to factory default:** Click to reset the SharpZ3 to use the factory default settings. A message confirms the reset and offers to optionally clear the network settings as well. Note that some settings are never cleared, such as battery settings and certificates.

  NOTE: The passwords for auxiliary cameras are not reset during a factory reset. You must reenter the passwords in **Configuration** > **Cameras** > **Auxiliary cameras**

Syslog

- **Use Syslog server:** Select this option to configure a central repository for all SharpZ3 log entries.
  - **Server:** Enter the IP address or name of the server.
    NOTE: Syslog server configurations do not support IPv6 addresses.
  - **Port:** Enter the port number of the syslog server.
  - **Network protocol:** Select UDP or TCP.

Sharp Portal - Date and time page

This section lists the settings found in the *Date and time* page of the Sharp Portal. Use the *Date and time* page to configure how you want to configure the internal clock of the SharpZ3.

To navigate to the *Date and time* page, click **Configuration** > **General settings** > **Date and time**.

The following information is displayed:

- **Settings:** Select one of the following settings.
  - **NTP server:** The camera synchronizes with an NTP server that is typically either a foreign computer or a server within your organization that synchronizes itself with an external NTP server. The latter is recommended if synchronization is crucial to your organization. Click **Server** and enter the URL or IPv4 address of the machine running the NTP server. Click **Test connection** to tests the connection between the camera and the NTP server. The camera synchronizes with the NTP server every hour.
  - **Active extension (Patroller):** If you select **Active extension (Patroller)**, the camera's date and time are synchronized with the Genetec Patroller™ server that the camera is connected to. The camera synchronizes with the server upon connection, then again every 10 minutes.
    NOTE: If you have not yet configured the active extension (see Configuring where the SharpZ3 sends its ALPR data on page 48), you can select **Active extension**, and it will be updated when you configure the extension.
    NOTE: The **Active extension** option displays whichever extension is currently selected for the camera in *Configuration* > *Extensions*, however, selecting this option has no effect if you are using an extension type other than Patroller (not valid for FTP, HTTP, and so on).
- **Date and time format:** Select the date and time format to be used in the Sharp Portal.
  - **International:** Selecting the International option displays the date and time in the format: YYYY-MM-DD HH:MM:SS
  - **Imperial:** Selecting the Imperial option displays the date and time in the format: DD/MM/YYYY H:MM:SS AM/PM

Sharp Portal - Power options page

This section lists the settings found in the *Power options* page of the Sharp Portal. Use the *Power options* page to configure the camera based on the power grid of the installation location.

To navigate to the *Power options* page, click **Configuration** > **General settings** > **Power options**.

The following information is displayed:

- **Power line frequency:** Select the power line frequency that corresponds to the installation location.
  - **60 Hz:** Generally used in North America and South America
  - **50 Hz:** Generally used in Africa, Australia, Asia, and Europe

NOTE: For more information on the power line frequency used in your installation location, click here.

Advanced:

- **Turn on voltage:** Input voltage threshold below which the unit does not turn on.
- **Ignition cut-off delay:** Grace period between ignition cut-off and trunk unit power-down.
- **Undervoltage:** Input undervoltage threshold that causes a unit shut-off if maintained for a certain time.

Sharp Portal - Maintenance page

This section lists the settings found in the *Maintenance* page of the Sharp Portal. Use the *Maintenance* page to update software or reboot the unit.

To navigate to the *Maintenance* page, click **Configuration** > **Maintenance**.

The following information is displayed:

- **Update:** Update the SharpOS software or the platform OS with latest security updates.
- **Free up space:** Space is freed up by deleting log files, untransmitted reads, and clearing the update cache.
- **Reboot unit:** Click to restart the SharpZ3.

  NOTE: If you are rebooting a SharpZ3 system that includes a four-camera ALPR module, each group of two cameras is configured on a separate Sharp Portal. Rebooting the unit only reboots the stack associated with the current portal. To reboot the entire system, you must power cycle the base unit.
- **Blink LED:** Click to blink the LED on the SharpZ3 for about a minute. This is useful when you have multiple units and you want to physically identify the one you are configuring.

Sharp Portal - Logs page

This section lists the settings found in the *Logs* page of the Sharp Portal. Use the *Logs* page to run reports and generate logs about the status of the SharpZ3. You can filter by a specific source, message, and so on. Log reports can also be exported to a .zip file by selecting **Export settings** on the *Maintenance* page.

To navigate to the *Logs* page, click **Diagnostics** > **Logs**.

The following information is displayed:

- **Severity:** Click the icons to choose which severity types you want to include in the report query. You can choose from the following:
  - Error
  - Warning
  - Information
  - Debug
  - Performance
- **Source:** Select the source that you want to include in the report query.
- **Message:** Enter a message. Only logs containing the message string entered are displayed on the query.
- **Time:** Select a time range.
- **Search:** Click to run the query.
- **Pause:** Click to pause the auto-refresh on the query. This is useful when you want to stop new entries from coming in so you can focus on a particular entry. Click **Resume** to activate the auto-refresh on the query.
- **Download all logs in a text file:** Click to download in a text file.

  NOTE: The filters on this page apply only to the visual report. The log file always contains a full, unfiltered list of events.

Sharp Portal - Log sources page

This section lists the settings found in the *Log sources* page of the Sharp Portal. Use the *Log sources* page to activate sources and to specify the level of verbosity.

To navigate to the *Log sources* page, click **Diagnostics** > **Log sources**.

The following information is displayed:

- **Sources to log:** Select the sources from which to generate a log. For example, if you only want to generate log events related to Plate Reader, select **Plate Reader** from the list.

  NOTE:

  - A source that contains *Verbose* in its name might generate a lot of disk activity.
  - When a log entry contains an exception, a small box icon is displayed under the **Exception** column. Click on the box to see the exception details.

Glossary

action
An action is a user-programmable function that can be triggered as an automatic response to an event, such as door held open for too long or object left unattended, or that can be executed according to a specific time table.

area
An area entity represents a concept or a physical location (room, floor, building, site, and so on) used for grouping other entities in the system.

automatic enrollment
Automatic enrollment is when new IP units on a network are automatically discovered by and added to Security Center. The role that is responsible for the units *broadcasts* a discovery request on a specific port, and the units listening on that port respond with a message that contains the connection information about themselves. The role then uses the information to configure the connection to the unit and enable communication.

AutoVu™
The AutoVu™ automatic license plate recognition (ALPR) system automates license plate reading and identification, making it easier for law enforcement and for municipal and commercial organizations to locate vehicles of interest and enforce parking restrictions. Designed for both fixed and mobile installations, the AutoVu™ system is ideal for a variety of applications and entities, including law enforcement, municipal, and commercial organizations.

AutoVu MLC™
AutoVu MLC™ (Machine Learning Core) replaces traditional rule-based ALPR technology with machine learning-based algorithms to reduce common ALPR misreads and false positives. It is a proprietary technology of Genetec Inc. used in AutoVu™ Sharp hardware for license plate recognition.

capture rate
The capture rate measures the speed at which a license plate recognition system can take a photo of a passing vehicle and detect the license plate in the image.

certificate
Designates one of the following: (1) *digital certificate*; (2) *SDK certificate*.

Config Tool
Config Tool is the Security Center administrative application used to manage all Security Center users and to configure all Security Center entities such as areas, cameras, doors, schedules, cardholders, patrol vehicles, ALPR units, and hardware devices.

context camera
A context camera is a camera connected to an ALPR unit that produces a wider angle color image of the vehicle whose license plate was read by the ALPR camera.

contract permit parking	Contract permit parking is a parking scenario where only drivers with monthly permits can park in the parking zone. A whitelist is used to grant permit holders access to the parking zone.
Copy configuration tool	The Copy configuration tool helps you save configuration time by copying the settings of one entity to many others that partially share the same settings.
covert hit	A covert hit is a read (captured license plate) that is matched to a covert hotlist. Covert hits are not displayed on the Genetec Patroller™ screen, but can be displayed in Security Desk by a user with proper privileges.
covert hotlist	Covert hotlists allow you to ensure the discretion of an ongoing investigation or special operation. When a hit is identified, only the authorized officer at the Security Center station is notified, while the officer in the patrol vehicle is not alerted. This enables enforcement officials to assign multiple objectives to the vehicle and back-end systems, while not interrupting the priorities of officers on duty.
custom event	A custom event is an event added after the initial system installation. Events defined at system installation are called system events. Custom events can be user-defined or automatically added through plugin installations. Unlike system events, custom events can be renamed and deleted.
custom field	A custom field is a user-defined property that is associated with an entity type and is used to store additional information that is useful to your organization.
Daily usage per patroller entity	Daily usage per patroller entity is a type of investigation task that reports on the daily usage statistics of a selected patrol vehicle (operating time, longest stop, total number of stops, longest shutdown, and so on) for a given date range.
dashboard	A dashboard is one of the three panels that belong to the canvas in Security Desk. It contains the graphical commands (or widgets) pertaining to the entity displayed in the current tile.
database server	A database server is an application that manages databases and handles data requests made by client applications. Security Center uses Microsoft SQL Server as its database server.
Directory	The Directory role identifies a Security Center system. It manages all entity configurations and system-wide settings. Only a single instance of this role is permitted on your system. The server hosting the Directory role is called the *main server*, and must be set up first. All other servers you add in Security Center are called *expansion servers*, and must connect to the main server to be part of the same system.

Directory Manager	The Directory Manager role manages the Directory failover and load balancing in order to produce the high availability characteristics in Security Center.
Directory server	A Directory server is any one of the multiple servers simultaneously running the Directory role in a high availability configuration.
discovery port	A discovery port is a port used by certain Security Center roles (Access Manager, Archiver, ALPR Manager) to find the units they are responsible for on the LAN. No two discovery ports can be the same on one system.
district	A district is a type of parking regulation characterizing an overtime rule. A district is a geographical area within a city. A vehicle is in violation if it is seen within the boundaries of the district over a specified period of time.
enforce	To enforce is to take action following a confirmed hit. For example, a parking officer can enforce a scofflaw violation (unpaid parking tickets) by placing a wheel boot on the vehicle.
entity	Entities are the basic building blocks of Security Center. Everything that requires configuration is represented by an entity. An entity can represent a physical device, such as a camera or a door, or an abstract concept, such as an alarm, a schedule, a user, a role, a plugin, or an add-on.
entity tree	An entity tree is the graphical representation of Security Center entities in a tree structure, illustrating the hierarchical nature of their relationships.
event	An event indicates the occurrence of an activity or incident, such as access denied to a cardholder or motion detected on a camera. Events are automatically logged in Security Center. Every event has an entity as its main focus, called the event source.
event-to-action	An event-to-action links an action to an event. For example, you can configure Security Center to trigger an alarm when a door is forced open.
expansion server	An expansion server is any server machine in a Security Center system that does not host the Directory role. The purpose of the expansion server is to add to the processing power of the system.
failover	Failover is a backup operational mode in which a role (system function) is automatically transferred from its primary server to a secondary server that is on standby. This transfer between servers occurs only if the primary server becomes unavailable, either through failure or through scheduled downtime.

false positive read

False positive plate reads can occur when a license plate recognition system mistakes other objects in an image for license plates. For example, lettering on a vehicle or street signs can sometimes create false positive plate reads.

federated entity

A federated entity is any entity that is imported from an independent system through one of the Federation™ roles.

federated system

A federated system is a independent system (Omnicast™ or Security Center) that is unified under your local Security Center via a Federation™ role, so that the local users can view and control its entities, as if they belong to the local system.

Federation™

The Federation™ feature joins multiple, independent Genetec™ IP security systems into a single virtual system. With this feature, Security Center users can view and control entities that belong to remote systems, directly from their local Security Center system.

Fuzzy matching

Environmental factors such as dirt or snow can partially obstruct license plate characters and increase the likelihood of partial plate reads occurring. In addition, similarly shaped letters and numbers, like “2” and “Z” or, “8”, “B”, and “0”, can also reduce plate read accuracy. Fuzzy matching lets AutoVu™ compare reads not only to exact matches in hotlists, but also to potential or probable matches.

Genetec Patroller™

Genetec Patroller™ is the software application installed on an in-vehicle computer that analyzes license plate reads from AutoVu™ Sharp camera units. The application can be installed to operate in different modes to suit your specific enforcement needs and can be configured to notify the vehicle operator if immediate action is required.

Genetec™ Server

Genetec™ Server is the Windows service that is at the core of Security Center architecture, and that must be installed on every computer that is part of the Security Center's pool of servers. Every such server is a generic computing resource capable of taking on any role (set of functions) you assign to it.

geocoding

Geocoding is the process of finding associated geographic coordinates (latitude and longitude) from a street address.

georeferencing

Georeferencing is the process of using an object’s geographic coordinates (latitude and longitude) to determine its position on a map.

ghost patroller entity

A ghost patroller entity is automatically created by the ALPR Manager when the AutoVu™ license includes the XML Import module. In Security Center, all ALPR data must be associated to a Genetec Patroller™ entity or an ALPR unit corresponding to a fixed Sharp camera. When you import ALPR data from an external source via a specific ALPR Manager using the XML

	Import module, the system uses the ghost entity to represent the ALPR data source. You can formulate queries using the ghost entity as you would with a normal entity.
Geographic Information System	Geographic Information System (GIS) is a system that captures spatial geographical data. Map Manager can connect to third-party vendors that provide GIS services in order to bring maps and all types of geographically referenced data to Security Center.
Hardware inventory	Hardware inventory is a type of maintenance task that reports on the characteristics (unit model, firmware version, IP address, time zone, and so on) of access control, video, intrusion detection, and ALPR units in your system.
hash function	In cryptography, a hash function uses a mathematical algorithm to take input data and return a fixed-size alphanumeric string. A hash function is designed to be a one-way function, that is, a function which is infeasible to revert.
hit	A hit is a license plate read that matches a hit rule, such as a hotlist, overtime rule, permit, or permit restriction. A Genetec Patroller™ user can choose to reject or accept a hit. An accepted hit can subsequently be enforced.
hit rule	Hit rule is a type of ALPR rule used to identify vehicles of interest (called "hits") using license plate reads. The hit rules include the following types: hotlist, overtime rule, permit, and permit restriction.
Hits	Hits is a type of investigation task that reports on hits reported within a selected time range and geographic area.
hot action	A hot action is an action mapped to a PC keyboard function key (Ctrl+F1 through Ctrl+F12) in Security Desk for quick access.
hotlist	A hotlist is a list of wanted vehicles, where each vehicle is identified by a license plate number, the issuing state, and the reason why the vehicle is wanted (stolen, wanted felon, Amber alert, VIP, and so on). Optional vehicle information might include the model, the color, and the vehicle identification number (VIN).
Hotlist and permit editor	Hotlist and permit editor is a type of operation task used to edit an existing hotlist or permit list. A new list cannot be created with this task, but after an existing list has been added to Security Center, users can edit, add, or delete items from the list, and the original text file is updated with the changes.
illuminator	An illuminator is a light in the Sharp unit that illuminates the plate, thereby improving the accuracy of the images produced by the ALPR camera.

incident	An incident is an unexpected event reported by a Security Desk user. Incident reports can use formatted text and include events and entities as support material.
Incidents	Incidents is a type of investigation task that allows you to search, review, and modify incident reports.
Inventory report	Inventory report is a type of investigation task that allows you to view a specific inventory (vehicle location, vehicle length of stay, and so on) or compare two inventories of a selected parking facility (vehicles added, vehicles removed, and so on).
I/O linking	I/O (input/output) linking is controlling an output relay based on the combined state (normal, active, or trouble) of a group of monitored inputs. A standard application is to sound a buzzer (through an output relay) when any window on the ground floor of a building is shattered (assuming that each window is monitored by a "glass break" sensor connected to an input).
IPv4	IPv4 is the first generation Internet protocol using a 32-bit address space.
IPv6	IPv6 is a 128-bit Internet protocol that uses eight groups of four hexadecimal digits for address space.
Law Enforcement	Law Enforcement is a Genetec Patroller™ software installation that is configured for law enforcement: the matching of license plate reads against lists of wanted license plates (hotlists). The use of maps is optional.
license key	A license key is the software key used to unlock the Security Center software. The license key is specifically generated for each computer where the Directory role is installed. To obtain your license key, you need the *System ID* (which identifies your system) and the *Validation key* (which identifies your computer).
license plate inventory	A license plate inventory is a list of license plate numbers of vehicles found in a parking facility within a given time period, showing where each vehicle is parked (sector and row).
license plate read	A license plate read is a license plate number captured from a video image using ALPR technology.
license plate recognition	Automatic license plate recognition (ALPR) is an image processing technology used to read license plate numbers. ALPR converts license plate numbers cropped from camera images into a database searchable format.
live hit	A live hit is a hit matched by the Genetec Patroller™ and immediately sent to the Security Center over a wireless network.
live read	A live read is a license plate captured by the patrol vehicle and immediately sent to Security Center over a wireless network.

load balancing	Load balancing is the distribution of workload across multiple computers.
logical ID	Logical ID is a unique ID assigned to each entity in the system for ease of reference. Logical IDs are only unique within a particular entity type.
Logons per Patroller	Logons is a type of investigation task that reports on the logon records of a selected patrol vehicle.
long term	Long term is a type of parking regulation characterizing an overtime rule. The *long term* regulation uses the same principle as the *same position* regulation, but the parking period starts on one calendar date and ends on another calendar date. No more than one overtime rule can use the long term regulation in the entire system.
ALPR camera	An Automatic License Plate Recognition (ALPR) camera is a camera connected to an ALPR unit that produces high resolution close-up images of license plates.
ALPR context	An ALPR context is an ALPR optimization that improves license plate recognition performance for license plates from a specific region (for example, New York) or from a group of regions (for example, Northeast states).
ALPR Manager	The ALPR Manager role manages and controls the patrol vehicle software (Genetec Patroller™), Sharp cameras, and parking zones. The ALPR Manager stores the ALPR data (reads, hits, timestamps, GPS coordinates, and so on) collected by the devices.
SharpZ3 ALPR module	ALPR modules are available for the SharpZ3 trunk unit which can support either two or four SharpZ3 cameras.
ALPR rule	ALPR rule is a method used by Security Center and AutoVu™ for processing a license plate read. An ALPR rule can be a hit rule or a parking facility.
ALPR unit	An ALPR unit is a device that captures license plate numbers. An ALPR unit typically includes a context camera and at least one ALPR camera.
macro	A macro is a type of entity that encapsulates a C# program that adds custom functionalities to Security Center.
main server	The main server is the only server in a Security Center system hosting the Directory role. All other servers on the system must connect to the main server to be part of the same system. In a high availability configuration where multiple servers host the Directory role, it is the only server that can write to the Directory database.

manual capture	Manual capture is when license plate information is entered into the system by the user and not by the ALPR.
map link	A map link is a map object that brings you to another map with a single click.
map mode	Map mode is a Security Desk canvas operating mode that replaces tiles and controls with a geographical map showing all active, georeferenced events in your system. Switching to Map mode is a feature of AutoVu™ and Genetec Mission Control™, and requires a license for one of these products.
map object	Map objects are graphical representations of Security Center entities or geographical features, such as cities, highways, rivers, and so on, on your maps. With map objects, you can interact with your system without leaving your map.
map view	A map view is a defined section of a map.
Mobile Data Computer	Mobile Data Computer is a tablet computer or ruggedized laptop used in patrol vehicles to run the Genetec Patroller™ application. The MDC is typically equipped with a touch-screen with a minimum resolution of 800 x 600 pixels and wireless networking capability.
Mobile License Plate Inventory	Mobile License Plate Inventory (MLPI) is the Genetec Patroller™ software installation that is configured for collecting license plates and other vehicle information for creating and maintaining a license plate inventory for a large parking area or parking garage.
Mobile Admin	(Obsolete as of SC 5.8 GA) Mobile Admin is a web-based administration tool used to configure the Mobile Server.
Mobile Server	The Mobile Server role provides Security Center access on mobile devices.
Monitoring	The *Monitoring* task is a type of operation task that you can use to monitor and respond to real-time events that relate to selected entities. Using the *Monitoring* task, you can also monitor and respond to alarms.
network	The network entity is used to capture the characteristics of the networks used by your system so that proper stream routing decisions can be made.
network address translation	Network address translation is the process of modifying network address information in datagram (IP) packet headers while in transit across a traffic routing device, for the purpose of remapping one IP address space into another.

network view	The network view is a browser view that illustrates your network environment by showing each server under the network they belong to.
new wanted	A new wanted is a manually entered hotlist item in Genetec Patroller™. When you are looking for a plate that does not appear in the hotlists loaded in the Genetec Patroller™, you can enter the plate in order to raise a hit if the plate is captured.
notification tray	The notification tray contains icons that allow quick access to certain system features, and also displays indicators for system events and status information. The notification tray display settings are saved as part of your user profile and apply to both Security Desk and Config Tool.
OCR equivalence	OCR equivalence is the interpretation of OCR (Optical Character Recognition) equivalent characters performed during license plate recognition. OCR equivalent characters are visually similar, depending on the plate's font. For example, the letter "O" and the number "0", or the number "5" and the letter "S". There are several pre-defined OCR equivalent characters for different languages.
SharpZ3 expansion module	Up to three expansion modules can be added to the SharpZ3 base unit. The modules add additional functionality to the base system. For example, you can add modules for precise navigation, PoE ports for wheel imaging cameras, and so on.
output behavior	An output behavior is a type of entity that defines a custom output signal format, such as a pulse with a delay and duration.
overtime rule	An overtime rule is a type of entity that defines a parking time limit and the maximum number of violations enforceable within a single day. Overtime rules are used in city and university parking enforcement. For university parking, an overtime rule also defines the parking area where these restrictions apply.
Parking Enforcement Essential	Parking Enforcement Essential is a Genetec Patroller™ software installation configuration that is similar to the City Parking Enforcement configuration, but excludes features such as shared permits, zone auto-selection, Plate link, and wheel imaging. You can configure the system for either overtime enforcement or permit enforcement, but you cannot configure both enforcement types.
parking facility	A parking facility is a type of entity that defines a large parking area as a number of sectors and rows for the purpose of inventory tracking.
parking lot	A parking lot is a polygon that defines the location and shape of a parking area on a map. By defining the number of parking spaces inside the parking lot, Security Center can calculate its percentage of occupancy during a given time period.

parking zone — The parking zones that you define in Security Center represent off-street parking lots where the entrances and exits are monitored by Sharp cameras.

partition — A partition is a type of entity that defines a set of entities that are only visible to a specific group of users. For example, a partition could include all areas, doors, cameras, and zones in one building.

partition administrator — (Obsolete) Beginning in Security Center 5.7 GA, privileges that used to be exclusive to administrators can now be granted individually, making the concept of *partition administrator* obsolete.

patrol vehicle — A patrol vehicle monitors parking lots and city streets for parking violations or wanted vehicles. A patrol vehicle includes one or more Sharp automatic license plate recognition (ALPR) cameras and an in-vehicle computer running Genetec Patroller™ software.

patroller entity — A patroller entity in Security Center represents a patrol vehicle equipped with an in-vehicle computer running Genetec Patroller™ software.

Patroller Config Tool — Genetec Patroller™ Config Tool is the Genetec Patroller™ administrative application used to configure Patroller-specific settings, such as adding Sharp cameras to the in-vehicle LAN, enabling features such as Manual Capture or New Wanted, and specifying that a username and password are needed to log on to Genetec Patroller™.

Patrol vehicle tracking — Patrol vehicle tracking is a type of investigation task that allows you to replay the route followed by a patrol vehicle on a given date on a map, or view the current location of patrol vehicles on a map.

permit — A permit is a type of entity that defines a single parking permit holder list. Each permit holder is characterized by a category (permit zone), a license plate number, a license issuing state, and optionally, a permit validity range (effective date and expiry date). Permits are used in both city and university parking enforcement.

permit hit — A permit hit is a hit that is generated when a read (license plate number) does not match any entry in a permit or when it matches an invalid permit.

permit restriction — A permit restriction is a type of entity that applies time restrictions to a series of parking permits for a given parking area. Permit restrictions can be used by patrol vehicles configured for University Parking Enforcement and for systems that use the AutoVu™ Free-Flow feature.

Plate link	When a patrol vehicle that is registered with Plate link enters a parking zone, it downloads all recent plate reads and hits from other patrol vehicles that are registered with the same account. This data sharing ensures that the system catches parking violations that would otherwise be missed.
Plate Reader	Plate Reader is the software component of the Sharp unit that processes the images captured by the ALPR camera to produce license plate reads, and associates each license plate read with a context image captured by the context camera. The Plate Reader also handles the communications with the Genetec Patroller™ and the ALPR Manager. If an external wheel imaging camera is connected to the Sharp unit, the Plate Reader also captures wheel images from this camera.
plugin	A plugin (in lowercase) is a software component that adds a specific feature to an existing program. Depending on the context, plugin can refer either to the software component itself or to the software package used to install the software component.
plugin role	A plugin role adds optional features to Security Center. A plugin role is created by using the *Plugin* role template. By default, it is represented by an orange puzzle piece in the *Roles* view of the *System* task. Before you can create a plugin role, the software package specific to that role must be installed on your system.
primary server	Primary server is the default server chosen to perform a specific function (or role) in the system. To increase the system's fault-tolerance, the primary server can be protected by a secondary server on standby. When the primary server becomes unavailable, the secondary server automatically takes over.
private IP address	A private IP address is an IP address chosen from a range of addresses that are only valid for use on a LAN. The ranges for a private IP address are: 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.16.255.255, and 192.168.0.0 to 192.168.255.255. Routers on the Internet are normally configured to discard any traffic using private IP addresses.
private task	A private task is a saved task that is only visible to the user who created it.
privilege	Privileges define what users can do, such as arming zones, blocking cameras, and unlocking doors, over the part of the system they have access rights to.
public task	A public task is a saved task that can be shared and reused among multiple Security Center users.

read rate	The read rate measures the speed at which a license plate recognition system can correctly detect and read all of the characters in an image of a license plate.
Reads	Reads is a type of investigation task that reports on license plate reads performed within a selected time range and geographic area.
Reads/hits per day	Reads/hits per day is a type of investigation task that reports on license plate reads performed within a selected time range and geographic area.
Reads/hits per zone	Reads/hits per zone is a type of investigation task that reports on the number of reads and hits per parking area for a selected date range.
Report Manager	Report Manager is a type of role that automates report emailing and printing based on schedules.
report pane	Report pane is one of the panes found in the Security Desk task workspace. It displays query results or real-time events in a tabular form.
reverse geocoding	Reverse geocoding is an AutoVu™ feature that translates a pair of latitude and longitude into a readable street address.
role	A role is a software component that performs a specific job within Security Center. To execute a role, you must assign one or more servers to host it.
salt (cryptography)	In cryptography, a salt is data that is used as an additional input to the information you want to encrypt or protect with a hash function, so that the original information is nearly impossible to guess, even when the attacker knows what algorithm is being used.
same position	Same position is a type of parking regulation characterizing an overtime rule. A vehicle is in violation if it is seen parked at the exact same spot over a specified period of time. Genetec Patroller™ must be equipped with GPS capability in order to enforce this type of regulation.
schedule	A schedule is a type of entity that defines a set of time constraints that can be applied to a multitude of situations in the system. Each time constraint is defined by a date coverage (daily, weekly, ordinal, or specific) and a time coverage (all day, fixed range, daytime, and nighttime).
scheduled task	A scheduled task is a type of entity that defines an action that executes automatically on a specific date and time, or according to a recurring schedule.

Software Development Kit	The Software Development Kit (SDK) allows end-users to develop custom applications or custom application extensions for Security Center.
secondary server	A secondary server is any alternate server on standby intended to replace the primary server in the case the latter becomes unavailable.
Security Center	Security Center is a truly unified platform that blends IP video surveillance, access control, license plate recognition, intrusion detection, and communications within one intuitive and modular solution. By taking advantage of a unified approach to security, your organization becomes more efficient, makes better decisions, and responds to situations and threats with greater confidence.
Security Center Federation™	The Security Center Federation™ role connects a remote, independent Security Center system to your local Security Center. That way, the remote system's entities and events can be used in your local system.
Security Desk	Security Desk is the unified user interface of Security Center. It provides consistent operator flow across all of the Security Center main systems, Omnicast™, Synergis™, and AutoVu™. The unique task-based design of Security Desk lets operators efficiently control and monitor multiple security and public safety applications.
server	A server is a type of entity that represents a server machine on which the Genetec™ Server service is installed.
Server Admin	Server Admin is the web application running on every server machine in Security Center that allows you to configure the settings of Genetec Server. Server Admin also allows you to configure the Directory role on the main server.
SharpOS	SharpOS is the software component of a Sharp unit. SharpOS is responsible for everything related to plate capture, collection, processing, and analytics. For example, a SharpOS update can include new ALPR contexts, new firmware, Sharp Portal updates, and updates to the Sharp's Windows services (Plate Reader, HAL, and so on).
Sharp Portal	Sharp Portal is a web-based administration tool used to configure Sharp cameras for AutoVu™ systems. From a web browser, you log on to a specific IP address (or the Sharp name in certain cases) that corresponds to the Sharp you want to configure. When you log on, you can configure options such as selecting the ALPR context (for example, Alabama, Oregon, Quebec), selecting the read strategy (for example, fast moving or slow moving vehicles), viewing the Sharp's live video feed, and more.

Sharp unit	The Sharp unit is a proprietary ALPR unit of Genetec Inc. that integrates license plate capturing and processing components, as well as digital video processing functions, inside a ruggedized casing.
SharpZ3	SharpZ3 is a proprietary mobile ALPR system designed by Genetec Inc. that integrates license plate cameras and a trunk unit that is responsible for ALPR processing as well as communication with the Genetec Patroller™ software running on the in-vehicle computer.
SharpZ3 ALPR module	ALPR modules are available for the SharpZ3 trunk unit which can support either two or four SharpZ3 cameras.
SharpZ3 base unit	The SharpZ3 base unit is the processing component of the SharpZ3 system. The base unit includes the ALPR module and up to three expansion modules that are used to add features to the system such as precise navigation, PoE ports for wheel imaging cameras, and so on.
SharpZ3 expansion module	Up to three expansion modules can be added to the SharpZ3 base unit. The modules add additional functionality to the base system. For example, you can add modules for precise navigation, PoE ports for wheel imaging cameras, and so on.
standard schedule	A standard schedule is a type of schedule entity that may be used in all situations. Its only limitation is that it does not support daytime or nighttime coverage.
system event	A system event is a predefined event that indicates the occurrence of an activity or incident. System events are defined by the system and cannot be renamed or deleted.
System status	System status is a type of maintenance task that monitors the status of all entities of a given type in real time, and allows you to interact with them.
task	A task is the central concept on which the entire Security Center user interface is built. Each task corresponds to one aspect of your work as a security professional. For example, use a monitoring task to monitor system events in real-time, use an investigation task to discover suspicious activity patterns, or use an administration task to configure your system. All tasks can be customized and multiple tasks can be carried out simultaneously.
taskbar	A taskbar is a user interface element of the Security Center client application window, composed of the Home tab and the active task list. The taskbar can be configured to appear on any edge of the application window.
task workspace	A task workspace is an area in the Security Center client application window reserved for the current task. The

	workspace is typically divided into the following panes: canvas, report pane, controls, and area view.
tile	A tile is an individual window within the canvas, used to display a single entity. The entity displayed is typically the video from a camera, a map, or anything of a graphical nature. The look and feel of the tile depends on the displayed entity.
timeline	A timeline is a graphic illustration of a video sequence, showing where in time, motion, and bookmarks are found. Thumbnails can also be added to the timeline to help the user select the segment of interest.
transient parking	Transient parking is a parking scenario where the driver must purchase parking time as soon as the vehicle enters the parking lot.
unit	A unit is a hardware device that communicates over an IP network that can be directly controlled by a Security Center role. We distinguish four types of units in Security Center: • Access control units, managed by the Access Manager role • Video units, managed by the Archiver role • ALPR units, managed by the ALPR Manager role • Intrusion detection units, managed by the Intrusion Manager role
Unit replacement	Unit replacement is a tool that is used to replace a failed hardware device with a compatible one, while ensuring that the data associated to the old unit gets transferred to the new one. For an access control unit, the configuration of the old unit is copied to the new unit. For a video unit, the video archive associated to the old unit is now associated to the new unit, but the unit configuration is not copied.
University Parking Enforcement	University Parking Enforcement is a Genetec Patroller™ software installation that is configured for university parking enforcement: the enforcement of scheduled parking permits or overtime restrictions. The use of maps is mandatory. Hotlist functionality is also included.
unreconciled read	A unreconciled read is a MLPI license plate read that has not been committed to an inventory.
user	A user is a type of entity that identifies a person who uses Security Center applications and defines the rights and privileges that person has on the system. Users can be created manually or imported from an Active Directory.
user group	A user group is a type of entity that defines a group of users who share common properties and privileges. By becoming member of a group, a user automatically inherits all the

	properties of the group. A user can be a member of multiple user groups. User groups can also be nested.
user level	A user level is a numeric value assigned to users to restrict their ability to perform certain operations, such as controlling a camera PTZ, viewing the video feed from a camera, or staying logged on when a threat level is set. Level 1 is the highest user level, with the most privileges.
validation key	A validation key is a serial number uniquely identifying a computer that must be provided to obtain the license key.
vehicle identification number	A vehicle identification number (VIN) is an identification number that a manufacturer assigns to vehicles. This is usually visible from outside the vehicle as a small plate on the dashboard. A VIN can be included as additional information with license plate entries in a hotlist or permit list, to further validate a hit and ensure that it is the correct vehicle.
wheel imaging	Wheel imaging is a virtual tire-chalking technology that takes images of the wheels of vehicles to prove whether they have moved between two license plate reads.
whitelist	A whitelist is a hotlist that is created for the purpose of granting a group of license plates access to a parking lot. A whitelist can be compared to an access rule where the secured area is the parking lot. Instead of listing the cardholders, the whitelist applies to license plate credentials.
widget	A widget is a component of the graphical user interface (GUI) with which the user interacts.
Zone occupancy	Zone occupancy is a type of investigation task that reports on the number of vehicles parked in a selected parking area, and the percentage of occupancy.

Where to find product information

You can find our product documentation in the following locations:

- **Genetec™ TechDoc Hub:** The latest documentation is available on the TechDoc Hub. To access the TechDoc Hub, log on to Genetec™ Portal and click TechDoc Hub. Can't find what you're looking for? Contact documentation@genetec.com.
- **Installation package:** The Installation Guide and Release Notes are available in the Documentation folder of the installation package. These documents also have a direct download link to the latest version of the document.
- **Help:** Security Center client and web-based applications include help, which explains how the product works and provide instructions on how to use the product features. To access the help, click **Help**, press F1, or tap the **?** (question mark) in the different client applications.

Technical support

Genetec™ Technical Assistance Center (GTAC) is committed to providing its worldwide clientele with the best technical support services available. As a customer of Genetec Inc., you have access to TechDoc Hub, where you can find information and search for answers to your product questions.

- **Genetec™ TechDoc Hub:** Find articles, manuals, and videos that answer your questions or help you solve technical issues.

  Before contacting GTAC or opening a support case, it is recommended to search TechDoc Hub for potential fixes, workarounds, or known issues.

  To access the TechDoc Hub, log on to Genetec™ Portal and click TechDoc Hub. Can't find what you're looking for? Contact documentation@genetec.com.
- **Genetec™ Technical Assistance Center (GTAC):** Contacting GTAC is described in the Genetec™ Lifecycle Management (GLM) documents: Genetec™ Assurance Description and Genetec™ Advantage Description.

Additional resources

If you require additional resources other than the Genetec™ Technical Assistance Center, the following is available to you:

- **Forum:** The Forum is an easy-to-use message board that allows clients and employees of Genetec Inc. to communicate with each other and discuss many topics, ranging from technical questions to technology tips. You can log on or sign up at https://gtapforum.genetec.com.
- **Technical training:** In a professional classroom environment or from the convenience of your own office, our qualified trainers can guide you through system design, installation, operation, and troubleshooting. Technical training services are offered for all products and for customers with a varied level of technical experience, and can be customized to meet your specific needs and objectives. For more information, go to http://www.genetec.com/support/training/training-calendar.

Licensing

- For license activations or resets, please contact GTAC at https://gtap.genetec.com.
- For issues with license content or part numbers, or concerns about an order, please contact Genetec™ Customer Service at customerservice@genetec.com, or call 1-866-684-8006 (option #3).
- If you require a demo license or have questions regarding pricing, please contact Genetec™ Sales at sales@genetec.com, or call 1-866-684-8006 (option #2).

Hardware product issues and defects

Please contact GTAC at https://gtap.genetec.com to address any issue regarding Genetec™ appliances or any hardware purchased through Genetec Inc.

Next

Bid

REKOR
AI DRIVEN DECISIONS

SUBMITTED BY:

Rekor Recognition Systems
7172 Columbia Gateway Dr. Suite 400
Columbia, MD 21046
www.rekor.ai info@rekor.ai 410.762.0800

November 5, 2020

Request For Bid | RFB# 10493

License Plate Readers



SUBMITTED TO:

San Diego County Sheriff's Department
5560 Overland Avenue, Suite 270
San Diego, CA 92123-1204

Table of Contents

Transmittal Letter 5

A. Required Documents 7

A.1 Cover Page (PC 600 Form) 8
A.2 Representations and Certifications Form 9
A.3 Nondisclosure Indemnification Agreement 10

B. Pricing Schedule 11

C. Statement of Work / Technical Response 15

C.1 Background Information 15
C.1.1 The San Diego County (County) has a requirement for the purchase of Automatic License Plate Reader (LPR) camera systems 15
Our Company 16
Our Vision 16
Our Core Competencies 17
Our Experience and Expertise 18
Our Core Values 19
The Sectors We Serve 22
C.2 Specifications 28
C.2.1 Security 31
C.2.2 LPR Cameras 35
C.2.3 LPR Processor 51
C.2.4 LPR Software -- Watchman Software Application and Back Office 52
Overview 52
Hotlist Integration 54
Cloud Hosting 55
Dashboard 55
Searches 55
Reports 56
Ability to Integrate with Other Third-Party ALPR Systems 57
C.3 Demonstration or Sample 64
C.3.1 County reserves the right to request an on-site demonstration of the LPR camera system being bid or a sample be sent to determine if it meets the requirements stated. All specifications listed in the General Requirements shall be confirmed. All travel, demonstration supplies and/or shipping expenses shall be at the contractor's expense. 64
C.4 Installation 64
C.4.1 Contractor shall provide the option to purchase systems as a "kit" that includes all hardware, wiring and software for standard installations 64
C.4.2 Contractor shall provide installation and warranty repair options on vehicles within San Diego County ... 64
C.4.3 Contractor shall provide a technician or representative to visit customer site for system start-up, configuration and commissioning of LPR system 64
C.4.4 System Installation and Lead Times (SOW Section 9) 65
C.5 Customer Support 67
C.5.1 The Contractor shall provide technical advice and sales support within 72 business hours. 67
C.6 Training 68
C.6.1 The County reserves the right to request up to eight (8) hours of training at a San Diego County Sheriff's Department facility within 30 days of delivery at no additional charge. This is in addition to the requirement set forth in 4.3 68
C.7 Data Sharing 68
C.8 System Scalability and Flexibility 69
C.8.1 System Scalability 69
C.8.2 Full Video Edge Processing for Speed and Scalability 70
C.8.3 System Flexibility 70

C.9 Remote Monitoring of Equipment 71
C.10 Maintenance and Support 73
C.10.1 Equipment Maintenance 73
C.10.2 Equipment Reliability 73
C.10.3 24/7 Support 73
C.11 Rekor Current Reference Projects 74
C.11.1 City of Lauderhill, FL Police Department 74
C.11.2 Town of Mount Juliet, TN Police Department 74
C.12 Project Team 75
C.12.1 Project Team Bios 76
C.12.2 Rekor Management Team Bios 77
D. Offer of Value-Added Products and/or Services 79
D.1 Rekor Smartphone Mobile Application 79
D.2 Rekor One – Multipurpose Solution 79
E. Appendix 81
E.1 Rekor Edge 300 Specifications Sheet 81
E.2 Rekor Finder In-Vehicle Specification Sheet 83
E.3 Mobile ALPR Speed Trailer Camera 85

List of Figures

Figure 1 *Revolutionary intelligence for smarter, quicker, cost-competitive public safety solutions.* *16*
Figure 2 *AI based vehicle intelligent solutions that help make cities smarter, people safer and commerce more efficient.* *17*
Figure 3 *Rekor has proven success delivering industry-leading vehicle recognition technology across the globe.* *17*
Figure 4 *Law enforcement deserves cutting-edge ALPR technology.* *18*
Figure 5 *Our Chief Science Officer developed the OpenALPR technology and continues to improve it.* *18*
Figure 6 *Our commitment to integrity is reflected in our longstanding relationships, testimonials and referrals.* *19*
Figure 7 *Rekor's community focus.* *20*
Figure 8 *167 cameras in 73 locations covering 260+ lanes.* *21*
Figure 9 *Find out more about vehicle recognition software.* *22*
Figure 10 *Providing actionable, real-time insights for commercial and government clients.* *23*
Figure 11 *A single source for multiple purposes.* *24*
Figure 12 *An effective and efficient solution for safer and smarter communities.* *25*
Figure 13 *Advanced, real-time vehicle intelligence-based actionable data from a broad network.* *25*
Figure 14 *Accurate, affordable license plate recognition.* *26*
Figure 15 *Creating value through improved infrastructure, increased safety and generating revenue* *26*
Figure 16 *As more cameras are added to a network, its effectiveness and value increase* *27*
Figure 17 *Rekor's differentiators provide agencies with unparalleled performance and massive system flexibility.* *37*
Figure 18 *One Rekor camera can capture vehicle reads over multiple lanes of travel.* *38*
Figure 19 *167 cameras in 73 locations covering 260+ lanes.* *39*
Figure 20 *See how one Edge camera captures license plates across multiple lanes.* *39*
Figure 21 *Edge 300 camera.* *40*
Figure 22 *Example of two ALPR cameras located above the mirror and not obstructing any occupant's view.* *43*
Figure 23 *See our in-vehicle camera in action.* *45*
Figure 24 *Unique interior mount provides a "stealth" element and protects equipment from damage* *46*
Figure 25 *Domed ALPR camera mounted under the solar panel.* *47*
Figure 26 *Rekor's ALPR solution can accurately capture license plate data in some of the most extreme conditions.* *53*
Figure 27 *Rekor's AI-driven technology is unmatched in terms of accuracy, data control and client support.* *54*
Figure 28 *Watchman user interface showing dashboard features, read details and recent alerts. Inset image shows still image extraction.* *55*
Figure 29 *Locate vehicles of interest using Watchman's advanced search functionality.* *56*
Figure 30 *Security is paramount at Rekor.* *59*
Figure 31 *Forward-looking in-vehicle cameras* *67*
Figure 32 *Through its state-of-the-art remote monitoring and round-the-clock support, Rekor offers clients proactive management of the sensor network to ensure up-time is maximized.* *71*
Figure 33 *Rekor monitors and receives alerts on key performance indicators to more efficiently address issues or service needs.* *72*
Figure 34 *Click on the above image and see how Rekor is creating a safer community in Mt. Juliet.* *75*
Figure 35 *Rekor's ALPR Program Team, showing key functional leadership.* *76*
Figure 36 *Example of Rekor Go finding a hotlist match.* *79*
Figure 37 *Creating value through improved infrastructure, increased safety and generating revenue* *80*

Transmittal Letter

November 5, 2020

San Diego County Sheriff's Department
5560 Overland Avenue, Suite 270
San Diego, CA 92123-1204

To whom it may concern:

It is my pleasure to transmit to the San Diego County Sheriff's Department ("Sheriff's Department") this response to your Request for Bids ("RFB") #10493, for License Plate Readers, including Addendums Nos. 1, 2, 3 and 4.

Rekor Recognition Systems, Inc. ("Rekor") is a Maryland-based company that provides real-time roadway intelligence through AI-driven decisions. We are a leading technology provider of public safety solutions, including our advanced AI-based vehicle recognition system. Our innovative approach to affordable turnkey subscription-based vehicle recognition and ALPR services has been a game changer for government clients.

Rekor provides vehicle recognition systems powered by our innovative machine learning Watchman (aka OpenALPR) software, which dramatically improves the accuracy of license plate reads and also identifies the make, model, color, and body type of vehicles. Rekor's solutions include artificial intelligence software that upgrades nearly any Internet Protocol ("IP") security camera to a license plate reader, as well as highly accurate mobile and fixed vehicle recognition systems that are continuously improving with machine learning techniques. Additionally, this drive to continuously improve includes regularly added feature releases. Rekor's applications and solutions are intelligent, flexible, and leading the next generation of vehicle recognition.

Rekor acknowledges the instructions and terms of the Request for Bids and agrees to comply with them. This proposal is firm for 90 days from the submittal date and may be extended upon mutual agreement if the Sheriff's Department requests so in writing. I am the primary person authorized to answer any questions and make representations for Rekor and my contact information is below.

Rekor's experienced team stands ready to provide the Sheriff's Department with a modern solution that not only dramatically outperforms current-day OCR-based legacy products, but also offers a long-term horizon for software-based technology improvements as they become available. These benefits include capabilities that go beyond just ALPR or vehicle recognition, thus leveraging the Sheriff's Department investment to support future roadway intelligence initiatives.

As your team evaluates the product options available, it is important to point out that capabilities and performance in a law enforcement environment represent a key differentiator for Rekor's technology. Our Edge 300 roadside product offers full video streaming plate capture with edge processing, and it is designed for highway speeds. Certain competitor products are designed for low speed residential applications and others use outdated OCR technology with cameras that cover one lane of traffic. In most law enforcement implementations, the vast majority of locations require coverage of up to three lanes at highway speeds and these locations are best served by state-of-the art equipment which is becoming more affordable to a greater number of law enforcement agencies.

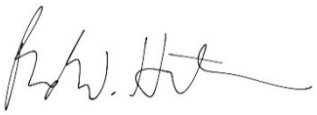
In reviewing the RFB, it seems evident that there is an expectation of performance that is based on perceptions of older technology offerings. Rekor does not make empty promises or claims, thus we would be glad to provide an extended on-site demonstration of the technology, directly against any other competitor of your choosing. Our detection systems utilize best-in-class components driven by incredibly reliable and accurate AI-based vehicle recognition software, capturing not just the plate number and state, but also vehicle attributes such as make, model, type, color, and direction of travel.

Rekor believes in transparency and clear communication. Within the body of this proposal you will gain an understanding of how Rekor's technology can provide vehicle recognition technology benefits to the Sheriff's Department, not just to meet current needs, but to support future needs without relying on antiquated or obsolete equipment and software. We are proposing our proven law enforcement solutions for fixed/portable, trailer, and mobile environments. While our mobile solution may not perfectly adhere to every requirement within the RFB, we urge you to consider what is a revolutionary 2-camera solution that captures up to 5 lanes of traffic with cameras mounted inside the windshield of the vehicle. We will soon be releasing a 4-camera external IR solution (Q1 2021) that leverages this same technology, and will be a game changer in the law enforcement mobile arena.

The combination of Rekor's advanced technology with our commitment to extreme customer satisfaction will position the San Diego County Sheriff's Department as a leader with respect to effective and ethical ALPR deployment.

We are prepared to provide any additional information requested and appreciate the opportunity to share our solution with the Sheriff's Department.

Sincerely,



Rodney Hillman, Chief Operating Officer
rhillman@rekor.ai; Office (410) 762-0800 x301 ; Cell 443-615-1548

A. Required Documents

Checklist

Failure to submit the following items may result in your Bid being declared non- responsive.

- [X] Cover Page (PC 600 Form)
- [X] Representations and Certifications Form
- [X] Indemnification Agreement

A.1 Cover Page (PC 600 Form)

COUNTY OF SAN DIEGO - REQUEST FOR BIDS (RFB # **10493**)
SHERIFF'S DEPARTMENT
LICENSE PLATE READERS
SECTION A: COVER PAGE (P&C 600 FORM)

COUNTY OF SAN DIEGO
SECTION A-P&C 600 FORM
This is not an order

Issued: October 22, 2020

MAIL OR DELIVER TO:
COUNTY OF SAN DIEGO, RFB NO. 10493
DEPARTMENT OF PURCHASING & CONTRACTING
5560 OVERLAND AVE., SUITE 270
SAN DIEGO, CA 92123

AWARD WILL BE MADE TO THE LOWEST RESPONSIVE, RESPONSIBLE BIDDER BASED ON
[ ] ALL OR NONE
[ ] EACH LOT
[X] TOTAL PRICE
[ ] OTHER (SEE PRICING SCHEDULE)

UNSPSC commodity code: **461716.0000**

FOR INFORMATION, PLEASE CONTACT:
PUNNITA DINMUONG, ASSISTANT PROCUREMENT SPECIALIST
PUNNITA.DINMUONG@SDCOUNTY.CA.GOV

BID OPENING DATE: NOVEMBER 5, 2020
BIDS MUST BE RECEIVED AT THE ABOVE ADDRESS PRIOR TO 11:00 A.M. ON DATE OF BID OPENING.

PLEASE STATE YOUR LOWEST PRICE F.O.B. DESTINATION AND BRAND NAME OR TRADE NAME IF APPLICABLE.
(Please use typewriter or black ink)
YOUR ENVELOPE MUST INCLUDE RFB NO. 10493

DESCRIPTION

THE COUNTY OF SAN DIEGO (COUNTY), SHERIFF'S DEPARTMENT HAS A REQUIREMENT FOR LICENSE PLATE READERS IN ACCORDANCE WITH THE TERMS & CONDITIONS AND THE STATEMENT OF WORK REFLECTED HEREIN.

INITIAL TERM: DATE OF AWARD – OCTOBER 31, 2021
1ST OPTION YEAR: NOVEMBER 1, 2021 – OCTOBER 31 2022
2ND OPTION YEAR: NOVEMBER 1, 2022 – OCTOBER 31, 2023

PRICING SUBMITTED IS TO REMAIN FIRM FIXED FOR THE TERM PERIOD IDENTIFIED ABOVE. ALL ITEMS WITHIN EACH TERM PERIOD MUST BE PRICED TO BE CONSIDERED RESPONSIVE. AWARD WILL BE MADE TO THE LOWEST RESPONSIVE, RESPONSIBLE OFFEROR BASED ON THE TOTAL PRICE. OFFEROR WHO SUBMITS THE LOW BID WILL BE DEEMED RESPONSIBLE BASED ON THE RESULTS OF THE PRE-AWARD SURVEY.

ARE YOU ABLE TO COMPLY WITH ALL ITEMS SPECIFIED WITHIN THE SCOPE OF WORK? YES_X_ OR__NO

As noted in the Compliance Matrix and response.

BIDDER ACKNOWLEDGES ADDENDUM NO. 1 [X] 2 [X] 3 [X] 4 [X] 5 [ ]

SUBJECT TO ACCEPTANCE WITHIN **90** DAYS

NAME AND ADDRESS OF BIDDER
Rekor Recognition Systems, Inc.
STREET, CITY, STATE, ZIP
7172 Columbia Gateway Drive, Suite 400
Columbia, Maryland 21046
TELEPHONE: NUMBER (410) 762-0800
FAX TELEPHONE: ( )
E-MAIL: RHillman@rekor.ai

PAYMENT TERMS NET **30** DAYS OR % DAY

NAME AND TITLE OF PERSON AUTHORIZED TO SIGN OFFER:
SIGNATURE — OFFEROR DATE: 11/05/2020
PRINTED NAME: Rod Hillman
PRINTED TITLE: Chief Operating Officer

NOTIFICATION OF AWARD

ACCEPTANCE AS TO ITEM(S) NUMBERED:
(VC NO.)
TOTAL AMOUNT
AWARD NO.

(THIS SECTION FOR COUNTY USE ONLY)
COUNTY OF SAN DIEGO
BY: _____ DATE: _____
JOHN M. PELLEGRINO, DIRECTOR
DEPT OF PURCHASING & CONTRACTING
NAME AND TITLE OF CONTRACTING OFFICER

P&C 600 Form

A.2 Representations and Certifications Form

County of San Diego
Department of Purchasing and Contracting

REPRESENTATIONS AND CERTIFICATIONS

The following representations and certifications are to be completed, signed and returned with the offer (the term "offer" includes a bid, proposal, quote, statement of qualifications, or any other submission to provide goods and/or services).

1. **BUSINESS TYPE**
   ■ For-profit ☐ Non-profit ☐ Government
2. **INTERLOCKING DIRECTORATE**
   In accordance with Board of Supervisors Policy A-79, if Offeror is a non-profit and will be subcontracting with a related for-profit entity where an interlocking directorate, management or ownership relationship exists, Offeror must list all such entity(ies) on an attached separate sheet, and authorization must be sought from Board of Supervisors. If Offeror is a non-profit and does not submit such a list, Offeror certifies it has not entered into a subcontract relationship with a related for-profit entity.
   List Attached? Yes ☐
3. **BUSINESS REPRESENTATION**
   Offeror represents as a part of this offer the following information regarding the ownership, operation, and control of its business:
   - **3.1.** Are you a local business with a physical address within the County of San Diego? ☐ Yes ■ No
   - **3.2.** Are you certified by the State of California as a:
     ☐ Disabled Veteran Business Enterprise(DVBE)
     Certification #: _____
     ☐ Small Business Enterprise (SBE)
     Certification #: _____
   - **3.3.** Are you certified by the U.S. Dept Of Veterans' Affairs as:
     ☐ Veteran Owned Small Business (VOSB)
     Certification # _____
     ☐ Service Disabled Veteran Owned Small Business (SDVOSB)
     Certification # _____
   - **3.4.** Estimated percentage of work in this offer to be performed or fulfilled locally (within the geographic boundaries of the County of San Diego): 100% %
4. **DEBARMENT, SUSPENSION, AND RELATED MATTERS**
   - **4.1.** Offeror certifies to the best of its knowledge that neither it nor any of its officers:
     - **4.1.1.** Are presently debarred, suspended, declared ineligible, or voluntarily excluded from covered transactions by any state, local, or federal department or agency.
     - **4.1.2.** Have within a three (3) year period preceding this agreement been convicted of or had a civil judgment rendered against them for commission of fraud or criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or contract under a public transaction; violation of federal or state antitrust statutes; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;
   - **4.2.** Except as allowed for in Section 4.2.5, Offeror hereby certifies to the best of its knowledge that neither it nor any of its officers:
     - **4.2.1** Are presently indicted for or otherwise criminally or civilly charged by a government entity (federal, state, or local) with the commission of any of the offenses enumerated in paragraph 4.1.2 of this certification;
     - **4.2.2** Have within a three (3) year period preceding this agreement had one or more public transactions (federal, state or local) terminated for cause or default;
     - **4.2.3** Are presently the target or subject of any investigation, accusation or charges by any federal, state or local agency or law enforcement, licensing, certification, ethics, or compliance body;
     - **4.2.4** Are proposed for debarment by any state, local, or federal department or agency.
     - **4.2.5** If Offeror is unable to certify Sections 4.2.1, 4.2.2, 4.2.3, or 4.2.4, it certifies that it has disclosed and attached to this Representations and Certifications the reason(s) it cannot do so. The disclosure must include the Section(s), specific relevant facts including dates, contracts, individuals involved, status of actions, and any other relevant information that prevent it from making the requested certification(s). The County reserves the right to disqualify an Offeror based upon information disclosed.
       Disclosure Attached? Yes ☐ N/A
5. **RELATED WORK**
   Offeror certifies to the best of its knowledge that, other than as disclosed in an attached separate sheet, it and its proposed subcontractors, agents, and consultants have not previously contracted with the County to perform work on or related to this project (e.g. preparing related studies or recommendations, components of the statement of work, or plans and specifications).
   Disclosure Attached? Yes ☐ N/A
6. **CURRENT COST OR PRICING**
   Offeror certifies to the best of its knowledge that cost and/or pricing data submitted with this offer, or specifically identified by reference if actual submission of the data is impracticable, are accurate, complete, and current as of the date signed below.
7. **INDEPENDENT PRICING**
   Offeror certifies that in relation to this offer:
   - **7.1.** The prices in this offer have been arrived at independently, without consultation, communication, or agreement, for the purpose of restricting competition, as to any matter relating to such prices with other offerors, with any competitors, or with any County employee(s) or consultant(s) involved in this or related procurements;
   - **7.2.** Unless otherwise required by law, the prices that have been quoted in this offer have not been knowingly disclosed by the Offeror and will not knowingly be disclosed by the Offeror prior to opening, in the case of a bid, or prior to award, in the case of a proposal, directly or indirectly to any other Offeror or to any competitor or with any County employee(s) or consultant(s) involved in this or related procurements; and
   - **7.3.** No attempt has been made or will be made by the Offeror to induce any other person or firm to submit or not to submit an offer for the purpose of restricting competition.
8. **ADDITIONAL DISCLOSURES**
   Offeror shall report in writing to the County Department of Purchasing and Contracting within five business days of discovering or having any reason to suspect any change in status as certified in the preceding paragraphs. Upon County's request, Offeror shall provide additional information supporting Offeror's Representations and Certifications. Offeror's obligations under this Section 8 shall continue until Offeror is no longer under consideration for award of a contract, or until termination or expiration of any resulting contract(s).

CERTIFICATION

The information furnished in Paragraphs 1 through 8 and in the accompanying offer is certified to be factual and correct as of the date submitted and this certification is made under penalty of perjury under the laws of the State of California.

Name: Rod Hillman Signature: [signature]

Title: Chief Operating Officer Date: 11/05/2020

Company/Organization: Rekor Systems, Inc.

SUBMIT THIS FORM AS DIRECTED IN THE REQUEST FOR SOLICITATION DOCUMENTS OR WITH THE OFFER

Revised 05-02-17

A.3 Nondisclosure Indemnification Agreement

COUNTY OF SAN DIEGO
NONDISCLOSURE INDEMNIFICATION AGREEMENT

IF OFFEROR SUBMITS EXHIBIT CONFIDENTIAL/PROPRIETARY, THE FOLLOWING NONDISCLOSURE INDEMNIFICATION AGREEMENT MUST BE COMPLETED, SIGNED AND RETURNED WITH THE OFFER

This indemnification agreement ("Agreement") is made and entered into by and between the County of San Diego ("County") and Offeror Company/Organization Name: _Rekor Recognition Systems, Inc.
("Offeror") with reference to the following facts: _____

WHEREAS the County may receive a request for disclosure of Offeror's submission under the California Public Records Act, Government Code Section 6250, et seq.; and

WHEREAS, Offeror has included in its submission an exhibit entitled "*EXHIBIT – CONFIDENTIAL/PROPRIETARY*" containing records that Offeror has determined to constitute trade secrets or other proprietary information exempt from disclosure under the California Public Records Act; and

WHEREAS the County requires defense and indemnity from Offeror for the County's ongoing non-disclosure of Offeror's *EXHIBIT-CONFIDENTIAL/PROPRIETARY*;

NOW, THEREFORE, for good and valuable consideration and the mutual promises contained herein, the parties agree to the following:

1. The above recitals are incorporated herein by this reference.
2. Except as otherwise provided herein, the County will not release Offeror's *EXHIBIT-CONFIDENTIAL/PROPRIETARY* based on Offeror's representation that the records contained therein are proprietary and exempt from disclosure under the California Public Records Act and/or are trade secrets as that term is defined in Government Code Section 6250, et seq. Notwithstanding the foregoing, however, the County may release Offeror's *EXHIBIT-CONFIDENTIAL/PROPRIETARY* in the event of any of the following:
   a. Offeror fails to comply with the terms and conditions of this Agreement; or
   b. Offeror provides the County with written notice that some or all of the records may be released; or
   c. A court of competent jurisdiction orders the County to release the records and the County has exhausted or waived its appeal rights.
3. To the fullest extent allowed by law, the County shall not be liable for, and Offeror shall defend and indemnify County and its Board of Supervisors, officers, directors, employees and agents of County (collectively "County Parties"), against any and all claims, demands, liability, judgments, awards, fines, mechanics' liens or other liens, labor disputes, losses, damages, expenses, charges or costs of any kind or character, including attorneys' fees (whether incurred by County attorneys or attorneys employed by County) and court costs (hereinafter collectively referred to as "Claims"), related to Offeror's *EXHIBIT-CONFIDENTIAL/PROPRIETARY*.
4. Offeror waives any and all claims in law or equity and hereby releases the County Parties from any and all claims, deductibles, self-insured retentions, demands, liability, judgments, awards, fines, mechanics' liens or other liens, labor disputes, losses, damages, expenses, charges or costs of any kind or character, including attorneys' fees and court costs, which arise out of or are in any way connected to Offeror's *EXHIBIT-CONFIDENTIAL/PROPRIETARY*.

TO BE COMPLETED BY AN AUTHORIZED REPRESENTATIVE OF THE OFFEROR	
Offeror Company/Organization Name:	Rekor Recognition Systems, Inc.
Authorized Representative Name:	Rodney Hillman
Authorized Representative Title:	Chief Operating Officer
Signature:	Date: 11/05/2020

B. Pricing Schedule

BASE YEAR
DATE OF AWARD – OCTOBER 31, 2021

DESCRIPTION	MFG & MODEL	ESTIMATED QUANTITY	UNIT PRICE	TOTAL
Mobile In-Vehicle LPR 4-camera system for license plate capture and a color overview image of the vehicle (Available Q1 2021)	Rekor Finder-4	1	$ 8,950.00	$ 8,950.00
Portable LPR 1 camera system, dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle	Rekor Edge 300	10	$ 6,950.00	$ 69,500.00
LPR Camera Mounting Brackets for Light Bar	Included with Finder-4	4	$ -	$ -
LPR Mounting for Portable system	Included with Edge	10	$ -	$ -
LPR Processor	Included with systems	14	$ -	$ -
Modem	Included with systems	14	$ -	$ -
LPR Software	Watchman License (1yr)	14	$ 588.00	$ 8,232.00
LPR Speed Trailer complete package with one camera	Speed Trailer	1	$ 39,000.00	$ 39,000.00
Start-up, configuration, and commissioning of LPR Systems at Sheriff's facility to include all expenses such as travel		14	$ -	$ -
Installation		14	$ 500.00	$ 7,000.00
Covert Installation in vehicle		1	$ -	$ -
Installation "Kit", Includes all hardware, wiring and software for "do it yourself" standard installations (on poles & trailers)	Included with systems	5	$ -	$ -
Training per hour		8	$ 150.00	$ 1,200.00
Shipping				$
			BASE YEAR SUBTOTAL:	$ 133,882.00

**Quantities are estimates only and not guaranteed

Additional System Options

DESCRIPTION	MFG & MODEL	ESTIMATED QUANTITY	UNIT PRICE	TOTAL
Rekor Finder-2 (Available Now)	2-Camera System	1	$ 6,950.00	$ 6,950.00
Rekor Edge 300x2 (Available Now)	2-Camera System	1	$ 7,950.00	$ 7,950.00
Solar Kit (Available Now)	Solar Panel and supplies for renewable power source	1	$ 4,500.00	$ 4,500.00
Trailer Camera Only (Available Now)		1	$ 6,950.00	$ 6,950.00

OPTION YEAR 1

NOVEMBER 1, 2021 – OCTOBER 31, 2022

(Base Year Unit Prices will be honored for new equipment purchased in Option Year 1
and are not displayed here because new purchases would require adjusting the Estimated Quantity))

DESCRIPTION	MFG & MODEL	ESTIMATED QUANTITY	UNIT PRICE	TOTAL
Mobile In-Vehicle LPR 4-camera system for license plate capture and a color overview image of the vehicle (Available Q1 2021)		4	$ -	$ -
Portable LPR 1 camera system, dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle		10	$ -	$ -
LPR Camera Mounting Brackets for Light Bar		4	$ -	$ -
LPR Mounting for Portable system		10	$ -	$ -
LPR Processor		14	$ -	$ -
Modem		14	$ -	$ -
LPR Software	Watchman License (1yr)	14	$ 588.00	$ 8,232.00
LPR Speed Trailer complete package	Watchman License (1yr)	1	$ 588.00	$ 588.00
Start-up, configuration and commissioning of LPR Systems at Sheriff's facility to include all expenses such as travel		14	$ -	$ -
Installation		14	$ -	$ -
Covert Installation		1	$ -	$ -
Installation "Kit", Includes all hardware, wiring and software for do it yourself standard installations (on poles & trailers)		5	$ -	$ -
Training per hour		8	$ 150.00	$ 1,200.00
Shipping				$ -
			OPTION YEAR 1 SUBTOTAL:	$ 10,020.00

**Quantities are estimates only and not guaranteed

OPTION YEAR 2

NOVEMBER 1, 2022 – OCTOBER 31, 2023

(Base Year Unit Prices will be honored for new equipment purchased in Option Year 2
and are not displayed here because new purchases would require adjusting the Estimated Quantity))

DESCRIPTION	MFG & MODEL	ESTIMATED QUANTITY	UNIT PRICE	TOTAL
Mobile In-Vehicle LPR 4-camera system for license plate capture and a color overview image of the vehicle (Available Q1 2021)		4	$ -	$ -
Portable LPR 1 camera system, dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle		10	$ -	$ -
LPR Camera Mounting Brackets for Light Bar		4	$ -	$ -
LPR Mounting for Portable system		10	$ -	$ -
LPR Processor		14	$ -	$ -
Modem		14	$ -	$ -
LPR Software	Watchman License (1yr)	14	$ 588.00	$ 8,232.00
LPR Speed Trailer complete package	Watchman License (1yr)	1	$ 588.00	$ 588.00
Start-up, configuration and commissioning of LPR Systems at Sheriff's facility to include all expenses such as travel		14	$ -	$ -
Installation		14	$ -	$ -
Covert Installation		1	$ -	$ -
Installation "Kit", Includes all hardware, wiring and software for do it yourself standard installations (on poles & trailers)		5	$ -	$ -
Training per hour		8	$ 150.00	$ 1,200.00
Shipping				$ -
			OPTION YEAR 2 SUBTOTAL:	$ 10,020.00

**Quantities are estimates only and not guaranteed

GRAND TOTAL (BASIS OF AWARD) :	$ 153,922.00

COUNTY OF SAN DIEGO - REQUEST FOR BIDS (RFB# **10493**)
SHERIFF'S DEPARTMENT
LICENSE PLATE READERS
SECTION C: EXHIBIT C PRICING SCHEDULE

1. PRICING

1.1. Enter unit prices for each line item, Base Term Period, 1st Option Period, and 2nd Option Period tabs for each line item on the appropriate tab.

1.2. These worksheets have built-in formulas that will calculate the extended prices for each line item and each term period. The aggregate total for each term period will be automatically transferred to the Grand Total (Extended Price) where your total will be calculated.

1.3. The worksheets are locked/protected. The format and the contents of the worksheets should not be tampered with or altered in any way.

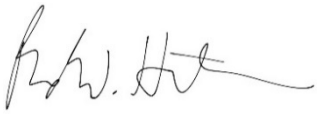
1.4. Bids must meet specifications provided.

1.5. All items must be priced to be considered responsive.

2. GENERAL REQUIREMENTS

2.1 A specifications sheet with pictures and operations manual for the product shall be submitted with the bid.

COMPANY:	Rekor Recognition System, Inc.
REPRESENTATIVE NAME:	Rodney Hillman, COO
REPRESENTATIVE EMAIL:	rhillman@rekor.ai
REPRESENTATIVE PHONE:	Office (410) 762-0800, extension #301



Page **32** of **46**

C. Statement of Work / Technical Response

C.1 Background Information

C.1.1 The San Diego County (County) has a requirement for the purchase of Automatic License Plate Reader (LPR) camera systems

Rekor understands that the San Diego County ("County") currently uses LPR technology from vendors that is OCR-based and thus not state-of-the-art with respect to camera performance in accurately reading license plates consistently with high confidence in varying lighting and weather. Furthermore, older technology tends to use cameras that are limited to covering one lane of traffic.

We note in Addendum No. 2, that the County indicated "If there are new cameras that can be placed inside a vehicle with the windows up, then we would like a demonstration to test the accuracy and reliability of the system." ***Rekor does have LPR cameras (Rekor "Finder") that can be placed inside a vehicle with the windows up, and we welcome the opportunity to demonstrate to the County our Finder camera's accuracy and reliability.*** When combined with our fixed/portable and trailer solutions, this represents an LPR ecosystem that is unmatched with respect to high performance and reliability.

Our Finder cameras are in use by law enforcement agencies who have recognized the systems' superior performance in almost all conditions outweighs certain limitations in absolute darkness due to lack of infrared ("IR") illumination. In very low light conditions, provided by headlights, streetlights, or moonlight, the systems perform quite well in comparison to IR-based technology. While we can't publicly disclose the name of a California-based law enforcement group that effectively uses Finder due to the nature of their operations, with your permission, we can ask them if they would be willing to contact your offices directly. In addition, law enforcement agencies at Cal State Fullerton, Vacaville and Suisan City are some California users of our Watchman ALPR software and the Stanislaus County Sheriff's Office uses our pole-mounted "Edge 300" camera and Finder cameras.

Beyond law enforcement in California, other state and local agencies that use our Watchman ALPR software include the California Air Resources Board, the San Diego County Air Pollution Control and the California Bureau of Automotive Repair. The first two agencies also use our Forensic Plate Finder servers that allow agency personnel to post-process videos for license plate and vehicle data. Because this RFP does not request a service like the Forensic Plate Finder, we will not address it at this time and would certainly respond to any questions on this capability, if the Sheriff's Department has further interest.

We hope that you will find the following information about how Rekor can enhance the Sheriff's Department informative, interesting and warranting a deeper review.

Our Company

We provide real-time roadway intelligence through AI-driven decisions. The company initially operated as Brekford, Inc. but changed its name to Brekford Traffic Safety, Inc. to better reflect its growing portfolio of core public safety technology solutions delivered to state, local, and federal customers. We continued to expand our footprint with government clients, and in 2019 we acquired OpenALPR, our vehicle and license plate recognition technology platform that now powers solutions such as Watchman. At the time of the acquisition, we rebranded to Rekor Recognition Systems, Inc. to signify our focus on AI-driven image and video recognition analytical solutions.

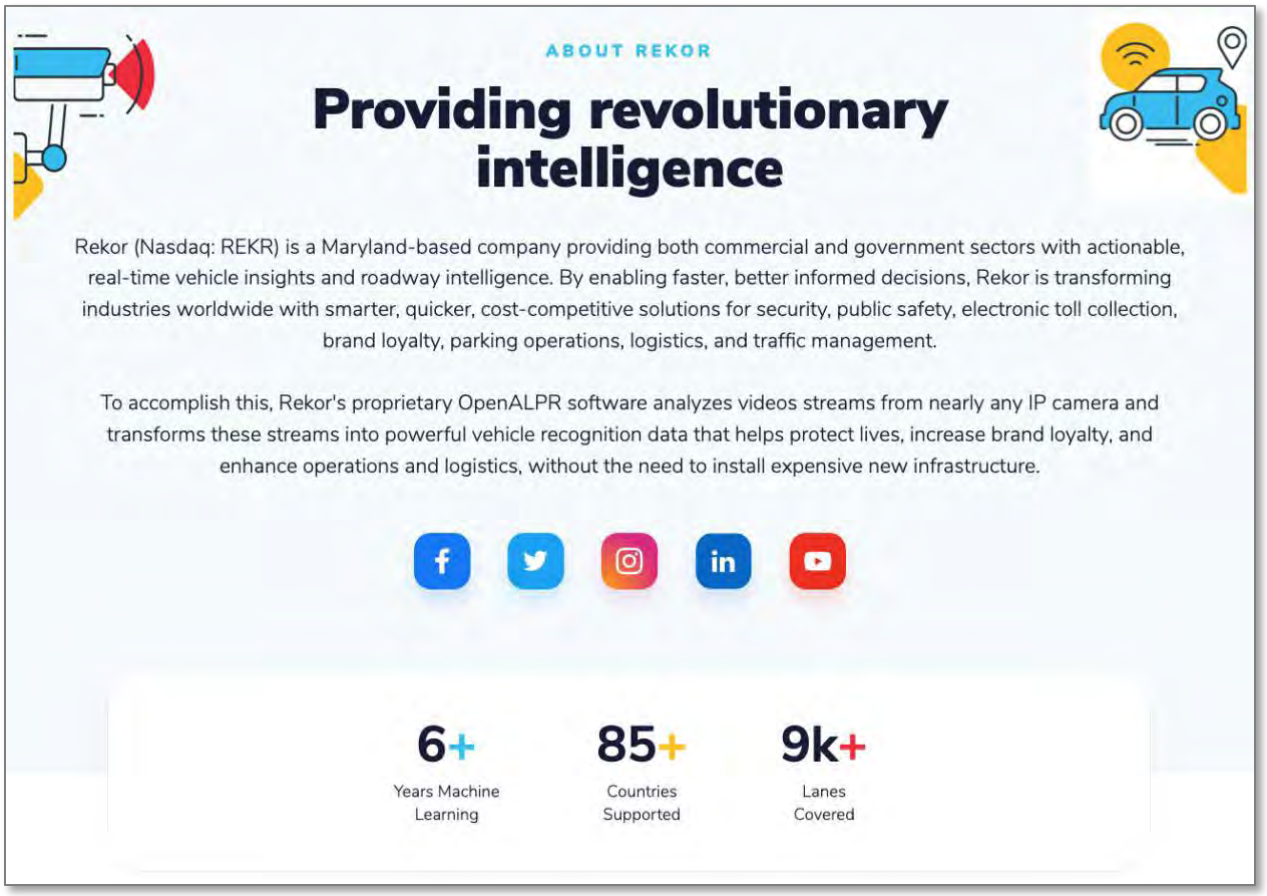


Figure 1 Revolutionary intelligence for smarter, quicker, cost-competitive public safety solutions.

Our Vision

Rekor's vision is to enable organizations and agencies to make "AI Driven Decisions" to solve complex real-world roadway and vehicle challenges. We harness the power of machine vision data and analytics to deliver solutions which help make governments more efficient, communities safer and organizations solve business challenges.

The video Rekor - AI Driven Decisions in the image below provides a brief summary of Rekor.

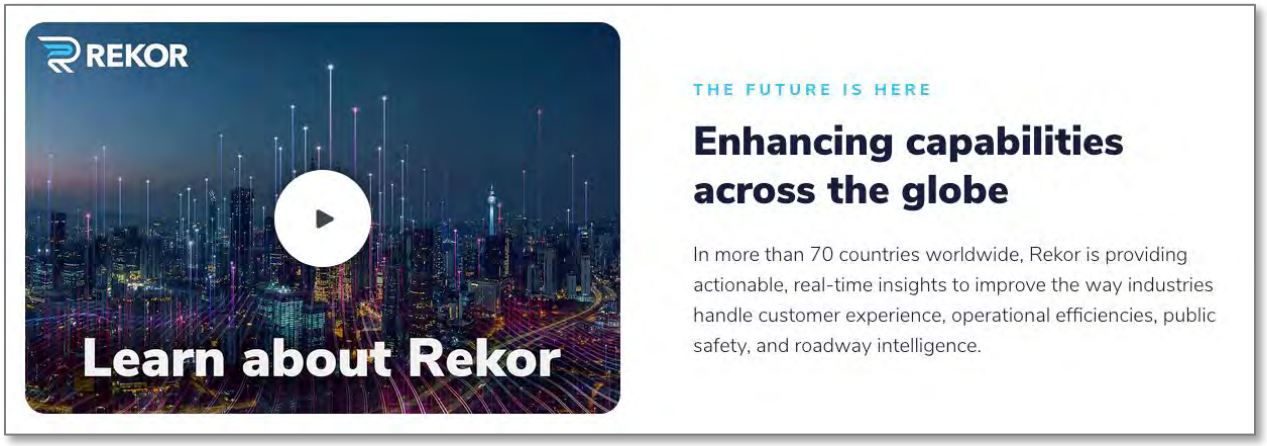


Figure 2 AI based vehicle intelligent solutions that help make cities smarter, people safer and commerce more efficient.

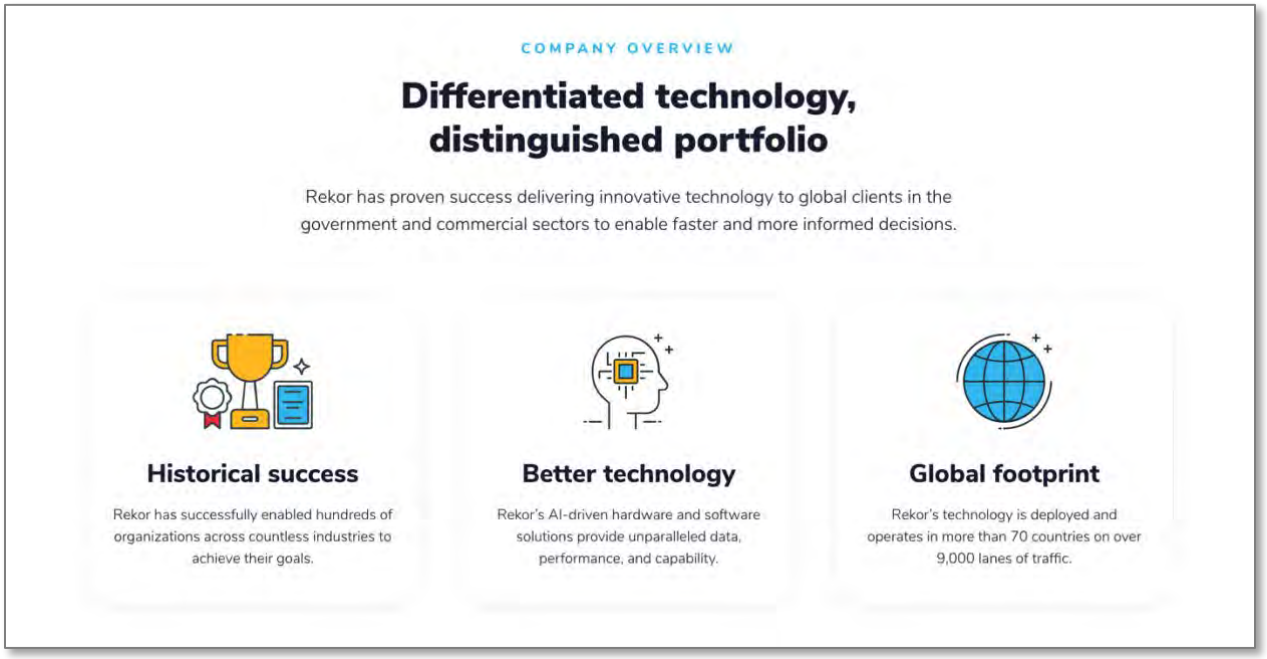


Figure 3 Rekor has proven success delivering industry-leading vehicle recognition technology across the globe.

Our Core Competencies

At its core, Rekor's technology centers around image processing and analytics, which is quite simply the ability to take video or still images, analyze them and provide valuable insights related thereto. Rekor employs both machine learning and machine vision in its software algorithms, two features of AI that result in more accurate results. Rekor's software is camera agnostic, and therefore can be deployed on nearly any IP surveillance or security camera. In

situations where the camera infrastructure is not optimized for Rekor's software, Rekor is able to complement its software with industry leading cameras to produce highly accurate results.

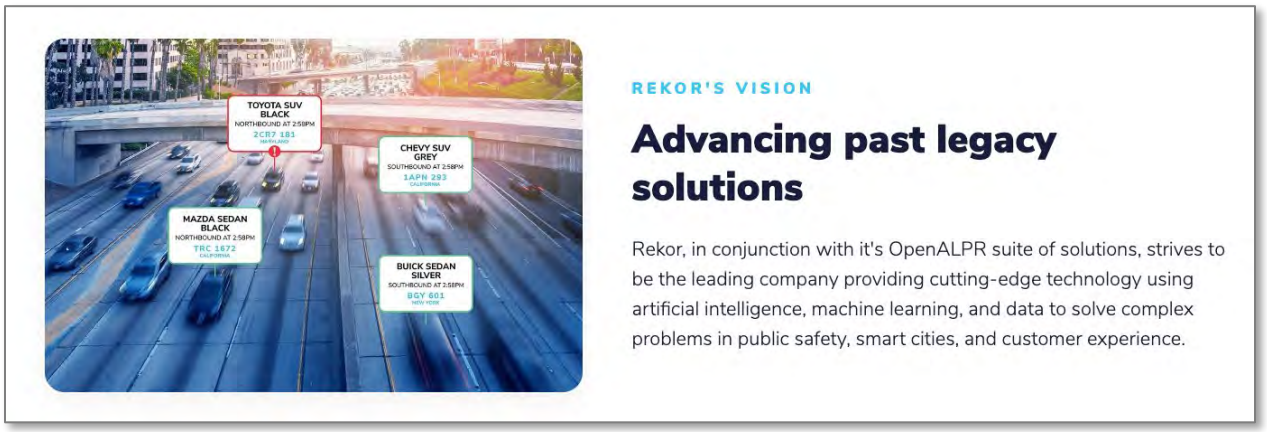


Figure 4 Law enforcement deserves cutting-edge ALPR technology.

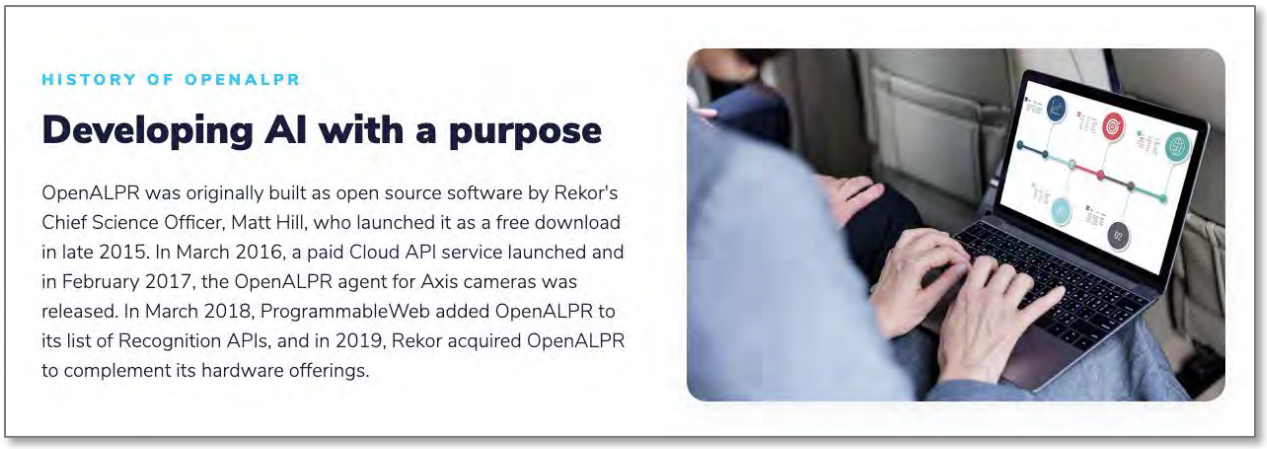


Figure 5 Our Chief Science Officer developed the OpenALPR technology and continues to improve it.

Our Experience and Expertise

Rekor has provided modern ALPR solutions for five years for both commercial and law enforcement customers worldwide. These solutions typically include hardware and software configuration and installation, testing, quality assurance, training, documentation, program management, maintenance, and customer service.

Rekor's leadership team brings decades of innovation, experience, strategic vision and exceptional results across commercial and public sectors.

- Members of our executive team have built and led teams at companies such as L3 Communications, Axon Enterprise, Motorola Solutions, and LexisNexis.

- Our Chief Science Officer developed the core technology that is employed in our vehicle and license plate recognition solutions and he remains integral in the algorithmic evolution that continues to provide our clients with expanded capabilities in their technology deployments.
- Two exceptional leaders from our original traffic safety and enforcement business currently serve as officers of the company.

Rekor has over 1,000 clients, representing 70 countries, using our ALPR software and over 70 public safety agencies use our ALPR systems. In addition, our ALPR cameras are used to cover over 9,000 lanes, for public safety and commercial purposes.

Our Core Values

Rekor maintains company core values that guide both our external and internal relationships.

Integrity

Rekor is a trusted partner of individual clients, companies, and government agencies of all sizes. We also partner with a broad range of technology vendors to help achieve greater outcomes by combining our solutions. Our technology was built on the principal of “openness” and transparency, and we maintain those principles in the way we communicate and work with our clients, our employees and our technology partners.



Figure 6 Our commitment to integrity is reflected in our longstanding relationships, testimonials and referrals.

Customer Centric

We believe in listening to the "voice of the customer" and allow it to drive our innovation. We seek to understand the needs and challenges of our clients and collaborate with them to develop solutions that best fit their needs and help them achieve in their missions.

- Video: Rekor's Law Enforcement Donation Program (or https://www.openalpr.com/donation)



Figure 7 Rekor's community focus.

Determined to Deliver

Rekor is driven to exceed customer expectations in the way we innovate, in the products we deliver and the service we provide. We do not allow external forces to hold us back from delighting our customers and we are motivated to overcome adversity and challenges. For example, amid the COVID-19 pandemic, we stood by our commitment to install one of the largest camera deployments to-date and stayed ahead of schedule, despite the significant challenges the pandemic presented. Helping fulfil the client's mission drives all facets of our business.

- Video: Installation at Lauderhill, Florida

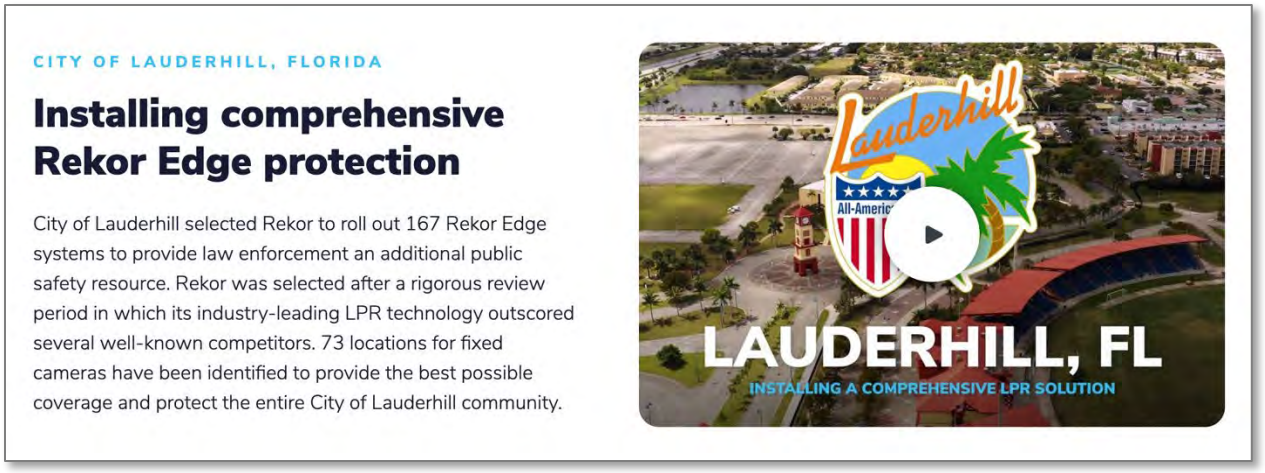


Figure 8 167 cameras in 73 locations covering 260+ lanes.

Commitment to Sharing Best Practices with Public Safety Agencies

Rekor regularly hosts "lunch and learn" sessions for public safety agencies, which involve members of the Rekor team presenting to law enforcement personnel on best practices related to vehicle and license plate recognition technology. Recently, due to COVID-19 restrictions on travel, we have hosted online events, such as two webinars related to law enforcement's use of vehicle and license plate recognition technology.

- Webinar: Improving Your Crime Reduction Strategy with LPR, June 4, 2020
- Webinar: Navigating Community Concerns about Your LPR Program, July 23, 2020

Members of our executive team have also been contributing members to public sector technology task forces, such as the IJIS/IACP Law Enforcement Imaging Task Force and IACP In-Car Video Task Force.

Currently, Rekor manages a robust discussion forum for users of our OpenALPR software suite. The blog has over 220 discussion topics, over 1,400 posts with over 380 active users.

Finally, we recently launched Rekor Academy, a series of videos intended to enhance client's and potential client's understanding of our technology and its features. The Academy currently hosts 15 videos and access to the Academy is offered at no-cost. Below is an example of one of the videos.

- Rekor Academy: What is Vehicle Recognition Software?

What is vehicle recognition software?

Vehicle recognition is no longer just license plate recognition. With Rekor's powerful suite of vehicle recognition tools, users are now able to identify a multitude of vehicle characteristics and behaviors. These variables include vehicle make, model, body type, color, direction of travel, and more. Additionally, these technological breakthroughs allow Rekor to surpass overly expensive and outdated ALPR systems that utilize optical character recognition, and provide real-time actionable insights for customers.

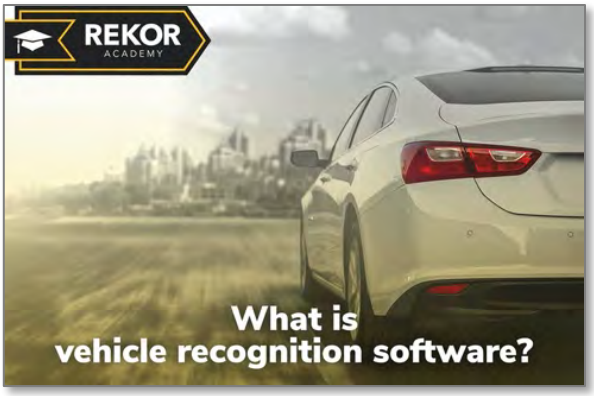


Figure 9 Find out more about vehicle recognition software.

The Sectors We Serve

Rekor provides both commercial and government customers with actionable, real-time vehicle recognition data to enable informed decisions to be made faster and with greater outcomes. Through its innovative image and video analytics technology, Rekor is transforming industries in the public and commercial sectors in more than 70 countries across the globe with smarter, quicker, cost-competitive vehicle recognition solutions. Applications for these solutions include security, revenue discovery and recovery, public safety, electronic toll collection, brand loyalty, frictionless restaurant and retail transactions, parking operations, logistics, and traffic management. To learn more please visit our website: https://rekor.ai.



Figure 10 Providing actionable, real-time insights for commercial and government clients.

Rekor has delivered ALPR technology, in both software and hardware form, to law enforcement and municipal agencies over the past decade. As a result, Rekor has gained excellent insight into the challenges of these agencies and how the technology must continue to evolve to help overcome these challenges. Rekor is a trusted partner of these agencies not only for the quality of the technology it provides, but also for the customer service which is offered prior to, during and after the client's purchase. As Rekor has developed these meaningful agency relationships, it has helped inform our technology development roadmap. A recent evolution in that roadmap includes Rekor One:



Figure 11 A single source for multiple purposes.

Rekor One is Rekor's AI-driven technology platform which serves as single source of roadway intelligence for government entities. Cities, counties and state agencies can derive actionable vehicle insights from the Rekor One platform to enable their agencies to more efficiently and effectively fulfill their missions. With Rekor One, governments can fractionalize costs by leveraging and expanding their sensor infrastructure and maximize their intelligence to maintain a safe and smart roadway network.

Roadway and Community Safety

Rekor One is the company's platform that improves citizens' safety by detecting and alerting to unsafe roadway conditions. Whether a vehicle is driving the wrong way, traveling erratically or at a dangerous speed, or encounters an obstruction, Rekor One delivers real-time alerting to allow for efficient action and correction, thus minimizing the risk of accidents and injury.



Figure 12 An effective and efficient solution for safer and smarter communities.

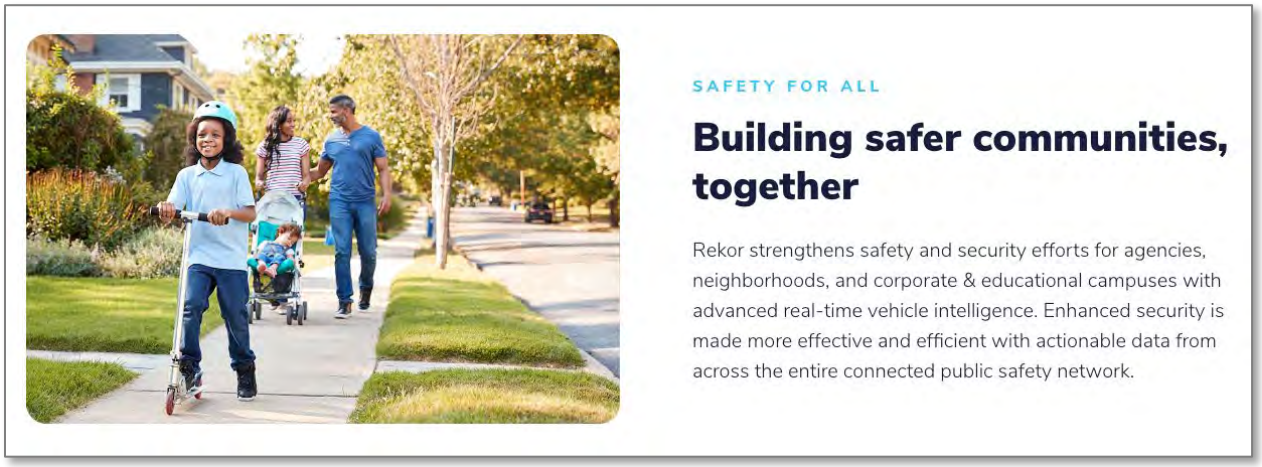


Figure 13 Advanced, real-time vehicle intelligence-based actionable data from a broad network.

Enhanced Policing

Additionally, Rekor One makes policing more effective and efficient. Officers can access the law enforcement module on the Rekor One platform to leverage actionable license plate and vehicle recognition data captured from fixed, mobile and handheld sensors across the Rekor One network. Critical alerts based on the license plate, vehicle make, model, color and type of vehicle help accelerate investigations, the apprehension of criminals, and the recovery of AMBER and Silver alerts.

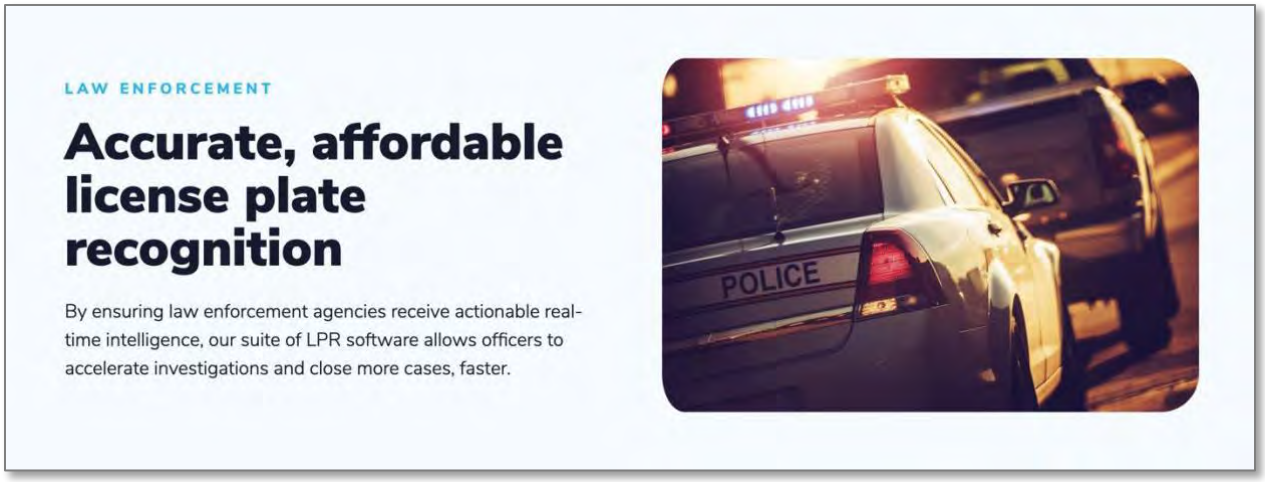


Figure 14 Accurate, affordable license plate recognition.

Traffic Monitoring and Management

Rekor One provides transportation agencies with extensive traffic monitoring capabilities. Traffic flow is improved by the ability to count vehicle totals, analyze congestion patterns, and generate detailed traffic reports. Insights regarding historical volume counts, vehicle class and type, and tonnage calculations can further infrastructure planning and budgeting efforts. Rekor One can also provide electronic vehicle counts and related data for emissions calculations.



Figure 15 Creating value through improved infrastructure, increased safety and generating revenue.

The Rekor One platform is representative of our commitment to create a safer future for everyone by enabling AI-driven decisions for the betterment of states, cities, and communities.



Figure 16 As more cameras are added to a network, its effectiveness and value increase.

C.2 Specifications

Compliance Matrix

Specification Reference	Specification	Compliance
C.2.1.1	Must be compliant with California Senate Bill 34 (SB34)	Comply
C.2.1.2	Single Sign-On (SSO) implementation options	Comply
C.2.1.2.1	Security Assertion Markup Language (SAML) 2.0 compliance	Comply
C.2.1.2.2	Other SSO methods, such as Active Directory and Office 365	Comply
C.2.1.3	User and Entity Based Behavioral Analytics (UEBA)	Would require additional requirements discussion
C.2.1.4	Distributed Denial of Service (DDoS) protection	Comply
C.2.1.5	Data sanitization and anti-malware prevention. Minimizing attack vectors throughout the LPR solution using a multi-layered approach	Comply
C.2.1.5.1	Anti-malware scanning and threat prevention with up to date signatures	Comply
C.2.1.5.2	Alerts and notifications	Comply
C.2.1.5.3	Input sanitization: All data coming into the system from users or application programming interfaces (APIs)	Comply
C.2.1.5.4	White list of file types for attaching/uploading for all purposes	Comply
C.2.1.5.5	File Contents Disarm and Reconstruction (CDR)	Comply
C.2.1.6	Disaster Recovery	Comply
C.2.1.6.1	Data protection, backup, and recovery strategy	Comply
C.2.1.6.2	Disaster recovery liability in case of catastrophic event	Comply
C.2.1.7	California Consumer Privacy Act (CCPA) compliance	Comply
C.2.1.8	Contractor shall provide a secure, database encrypted and web-based system that provides real-time access to uploaded data	Comply
C.2.1.9	Contractor shall allow authorized users access to LPR data in a number of LPR-specific dashboards	Comply
C.2.1.10	Dashboard will show LPR vehicle scans in an easy to read graphical format	Comply
C.2.1.11	LPR dashboard will show vehicle location, images captured and provide the ability to search using the license plate	Comply
C.2.1.12	Contractor shall provide an option to purge data at specified intervals or dates	Comply
C.2.1.12.1	Will have a notification process to assure compliance	Would require additional requirements discussion
C.2.1.12.1.1	Provide notification of purge date	Would require additional requirements discussion

Specification Reference	Specification	Compliance
C.2.1.12.1.2	Provide confirmation and notification that specified data was purged	Would require additional requirements discussion
C.2.1.13	Data uploaded will only be shared at the discretion of an administrator designated by the San Diego County Sheriff's Department	Comply
C.2.2.1	Contractor shall have LPR systems capable of being installed on a fixed object (i.e. light pole), marked patrol vehicles, covert vehicles and speed	Comply
C.2.2.2	Marked patrol vehicle camera mounting brackets must be compatible with Whelen, Code3, TOMAR, Federal Signal, Arjent S2 light bars	Alternative Solution
C.2.2.3	Cameras shall be self-illuminating Infrared (IR) for effective license plate image capture in a variety of weather and lighting conditions	Alternative Solution
C.2.2.4	LPR cameras shall be water-resistance with few moving parts that can be damaged	Comply
C.2.2.5	LPR cameras shall have the ability to automatically capture all variations of California license plates, to include California dealer issued plates (paper plates)LPR cameras shall have the ability to automatically capture all variations of California license plates, to include California dealer issued plates (paper plates)	Comply
C.2.2.6	Cameras shall have a dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle for verification purposes	Alternative Solution
C.2.2.7	Cameras shall be sealed to NEMA 6 (IP67) standards	Comply
C.2.2.8	Dual lens cameras shall be capable of capturing up to 60 frames per second	Comply
C.2.2.9	Cameras shall have the ability to adjust shutter, brightness, and gain settings to ensure a high-quality image regardless of weather or lighting conditions	Comply
C.2.2.10	The cameras shall be able to have a fixed focal point or target distance from the camera to the vehicle's license plate from 9 ½ feet to 30 feet	Comply
C.2.2.11	The camera shall be capable of various configurations to capture plates in any of the following modes depending on the configuration	Comply
C.2.2.11.1	An adjacent lane on either side of the vehicle while driving through traffic and/or parking lots	Comply

Note: RFB Section C.2.2 LPR Cameras referred to subsections as 2.7.X and the above table conforms the Section number to 2.2.X format.

Specification Reference	Specification	Compliance
C.2.2.11.2	Traffic in an adjacent lane while parked on the side of the shoulder of a roadway	Comply
C.2.2.11.3	Parked vehicles in parking lots	Comply
C.2.3.1	Processor shall have a “self-trigger” mode to detect the presence of correctly mounted vehicle license plates in the camera's field of view for image capture from the camera	Comply
C.2.3.2	Processor's installed in vehicles shall be equipped with an intelligent Power Supply Unit (PSU) that provides for a safe start and shut-down each time the vehicle's ignition is turned on and turned off	Comply
C.2.3.3	Processor controls the power supplied to the cameras and provides video connection points for simplified system wiring	Comply
C.2.3.4	Processor shall have at least four (4) LPR camera connections and multiple USB ports	Alternative Solution
C.2.3.5	Vehicle mounted processors shall meet the environmental conditions associated with being mounted in a trunk	Alternative Solution
C.2.4.1	Application software shall be capable of running on a Windows based mobile computer	Comply
C.2.4.2	There shall be no Java programming or Java derivatives	Comply
C.2.4.3	LPR system shall have real time alerting and the ability to program custom hotlist	Comply
C.2.4.4	There shall be a secure login and password function on the LPR software; The user's access shall be controlled by an administrator designated by the San Diego County Sheriff's Department	Comply
C.2.4.4.1	API capable of integrating user defined active directory	Comply
C.2.4.5	The software shall provide live, simultaneous display of all the following data:	Comply
C.2.4.6	Software shall capture GPS coordinates for every recorded license reads	Comply
C.2.4.7	Software shall have the ability to GPS stamp all the reads	Comply
C.2.4.8	Software will give a unique audible and visible alert when a wanted license plate is discovered	Comply
C.2.4.9	The Alert Screen remains displayed until acknowledged by the user, and, while displayed, the system continues to process license plate data in the background	Comply

Specification Reference	Specification	Compliance
C.3.1	County reserves the right to request an on-site demonstration of the LPR camera system being bid or a sample be sent to determine if it meets the requirements stated. All specifications listed in the General Requirements shall be confirmed. All travel, demonstration supplies and/or shipping expenses shall be at the contractor's expense.	Will Comply If County Requests
C.4.1	Contractor shall provide the option to purchase systems as a "kit" that includes all hardware, wiring and software for standard installations	Comply
C.4.2	Contractor shall provide installation and warranty repair options on vehicles within San Diego County	Comply
C.4.3	Contractor shall provide a technician or representative to visit customer site for system start-up, configuration and commissioning of LPR system	Comply
C.4.4	System Installation and Lead Times (SOW Section 9)	Comply
C.5.1	The Contractor shall provide technical advice and sales support within 72 business hours.	Comply
C.6.1	The County reserves the right to request up to eight (8) hours of training at a San Diego County Sheriff's Department facility within 30 days of delivery at no additional charge. This is in addition to the requirement set forth in 4.3.	Comply

Note: RFB Section C.2.2 LPR Cameras referred to subsections as 2.7.X and the above table conforms the Section number to 2.2.X format.

C.2.1 Security

C.2.1.1 Must be compliant with California Senate Bill 34 (SB34)

Rekor places a high priority on privacy, security and ethics. Our system will allow the Sheriff's Department to set retention policies, log all activity and secure the content in order to be compliant with state and local standards such as California Senate Bill SB34. We are also aware of the Automated Regional Justice Information System (ARJIS) *Acceptable Use Policy for the Regional License Plate Reader System*.

Through our work with ALPR data and other law enforcement agencies, we are well versed in ensuring that our systems are fully compliant with state and local requirements. As we mentioned above, we do work with law enforcement elsewhere in California.



C.2.1.2 Single Sign-On (SSO) implementation options

C.2.1.2.1 *Security Assertion Markup Language (SAML) 2.0 compliance*

Rekor supports secured communications required to enable cross application web authentication using languages such as SAML (v2.0) and others.

C.2.1.2.2 *Other SSO methods, such as Active Directory and Office 365*

Our system also supports integration with an agency's Active Directory system (and thus Office 365) so as to streamline account management and system authorization.

C.2.1.3 User and Entity Based Behavioral Analytics (UEBA)

Rekor's current software contains certain UEBA analytics that are required for CJIS Security Policy compliance including geo-location of user logins with historical comparisons and repeated failed login attempts. Additional, broader UEBA analytics are not on our current product roadmap at this time, as there is not a current demand from our collective customer base. If the Sheriff's Department desires additional specific analytics to be provided within the software, Rekor would be pleased to assess those requirements in detail and provide a quote for the additional services.

C.2.1.4 Distributed Denial of Service (DDoS) protection

All standard threats, such as DDoS, are addressed within our Watchman back-office. We leverage static threshold DDoS protection, including always-on network flow monitoring, which inspects incoming traffic and its source, and apply a combination of traffic signatures, anomaly algorithms, as well as other analysis techniques, to detect malicious traffic in real-time.

Our Watchman back-office protects against common, frequently occurring infrastructure attacks. Automatic mitigations are applied inline and in real-time for added protection so that there is no latency impact. Rekor also uses techniques including deterministic packet filtering, and priority-based traffic shaping to automatically mitigate basic network layer attacks.

C.2.1.5 Data sanitization and anti-malware prevention. Minimizing attack vectors throughout the LPR solution using a multi-layered approach

C.2.1.5.1 *Anti-malware scanning and threat prevention with up to date signatures*

Rekor protects our servers and applications through a multi-layered approach with advanced security controls, such as an intrusion prevention system ("IPS"), integrity monitoring, machine learning, and application control. We can detect and block threats in real-time, and can detect



and block unauthorized software execution with multiplatform application controls and anti-malware scanning.

C.2.1.5.2 *Alerts and notifications*

Part of our security offering includes security alerts and notifications of potential concerns. Beyond just sending alerts, our system triggers proactive prevention upon the detection of suspicious or malicious activity.

C.2.1.5.3 *Input sanitization: All data coming into the system from users or application programming interfaces (API's)*

Rekor uses defined, controlled and versioned APIs which ensure all data coming into the system conforms to specifications.

C.2.1.5.4 *White list of file types for attaching/uploading for all purposes*

All APIs which accept file inputs only accept our defined whitelist of data types and file formats.

C.2.1.5.5 *File Contents Disarm and Reconstruction (CDR)*

Rekor places a high priority on data security and has the ability to filter, restrict and remove portions of potentially malicious file types (CDR).

C.2.1.6 Disaster Recovery

C.2.1.6.1 *Data protection, backup, and recovery strategy*

Our system contains standard backup and recovery processes and procedures allowing for point-in-time recovery, in the event of a disaster.

C.2.1.6.2 *Disaster recovery liability in case of catastrophic event*

The service maintains catastrophic loss insurance.

C.2.1.7 California Consumer Privacy Act (CCPA) compliance

Rekor places a high priority on privacy, security and ethics. Our system allows our clients to set retention policies, and logs all activity and secures content (in order to be in accordance with privacy regulations, such as the CCPA). Rekor does not sell or disclose any personal data collected to third parties. Having other California clients, Rekor understands the unique data privacy requirements the must be followed.



C.2.1.8 Contractor shall provide a secure, database encrypted and web-based system that provides real-time access to uploaded data

Our system provides encrypted and secure, real time, access through a web interface where all agency data is encrypted at rest and in-transit for security.

C.2.1.9 Contractor shall allow authorized users access to LPR data in a number of LPR-specific dashboards

Our system provides secure, real time, access through a web interface and several LPR-specific dashboards that are tailored for the specific mission.

C.2.1.10 Dashboard will show LPR vehicle scans in an easy to read graphical format

Our system provides secure, real time, access through a web interface and several LPR-specific dashboards that are tailored for the specific mission. User access to the web interface is controlled by a Sheriff's Department administrator empowering the Department to control who can assess the application.

C.2.1.11 LPR dashboard will show vehicle location, images captured and provide the ability to search using the license plate

The provided dashboards provide an easy to read graphical presentation of the data including license plate read, vehicle and location information, as well as accompanying images. Data is searchable by a number of metrics including license plate number, vehicle characteristics, location, date/time, etc.

Additional information about Rekor's Watchman dashboard is provided in Section C.2.4.

C.2.1.12 Contractor shall provide an option to purge data at specified intervals or dates

Our Watchman back-office is easily configured to automatically purge data after specified retention periods or intervals. Purging data on specific dates is a manual process and automating such a feature would require additional discussions with the Sheriff's Department, since typical protocol is to define a retention time period that then triggers automatic purging.

C.2.1.12.1 *Will have a notification process to assure compliance*

C.2.1.12.1.1 Provide notification of purge date

Our system allows the Sheriff's Department to set retention policies. The system currently is not configured to provide automatic purge notices since the administrator would likely receive

daily emails as data is purged. If this is a feature that the Sheriff's Department requires, Watchman could be set up to do this. Upon setup, data retention policies are all logged and reported.

C.2.1.12.1.2 Provide confirmation and notification that specified data was purged

All activities, including purging, are tracked and logged, and reporting is provided to document these activities, however, automatic notification is not provided. As mentioned above, if the Sheriff's Department requires automatic notification, such a feature would require additional discussions with the Sheriff's Department.

C.2.1.13 Data uploaded will only be shared at the discretion of an administrator designated by the San Diego County Sheriff's Department

All accounts, including Administrative, can be defined and restricted, as needed by the Sheriff's Department.

C.2.2 LPR Cameras

C.2.2.1 Contractor shall have LPR systems capable of being installed on a fixed object (i.e. light pole), marked patrol vehicles, covert vehicles and speed

C.2.2.1.1 *Types of ALPR Cameras*

Rekor's ALPR System is comprehensive and includes cameras and all associated hardware, as well as storage and management software, installation as needed, training, maintenance, and support and warranty of products provided. It is our understanding that the Sheriff's Department would like three types of cameras:

1. **Portable –** are camera systems that will be stationary. These are slightly different than "fixed" systems that are generally seen as a more permanent installations that are hard-wired and not easily moved. Any ALPR camera that operates off of AC power will require a connection to an electrical source. Our AC-powered ALPR cameras can be installed in one hour, if AC power is available at the supporting structure, and they can be removed in about 45 minutes. Alternatively, our solar-powered ALPR cameras are also easy to install and because two pieces of equipment (ALPR camera unit and solar panel) need to be mounted to the supporting structure, we can install a solar-powered unit on a supporting structure in about 1.5 hours, and the removal time is about one hour. If the Sheriff's Department intends on temporarily installing an ALPR camera, our solar-powered ALPR units can operate for about five days without connecting the solar panel. The unit's battery pack could be easily replaced, if the Sheriff's Department wanted the ALPR camera to be in place longer without a solar panel. Our portable systems are easily



moveable and can be deployed for single events. Should we mention a "fixed" camera in any of our graphics or videos, please consider this to be in reference to a "portable" camera solution.

2. **Mobile** – are camera systems that can be installed either in a vehicle or a trailer. We will refer to **"in-vehicle"** systems and **"trailer-mounted"** systems to distinguish between mobile systems.

Rekor believes our system will provide significant advantages compared to the Sheriff Department's existing system and those of competitors. For example, we believe that Rekor's key system features, as listed below, would provide significant differentiators over the Sheriff Department's system and that of competitors:

- Superior read performance and accuracy provided by our Watchman software
- Full video edge processing for superior ALPR read speed and scalability
- Robust remote supportability
- Smartphone mobile application

These and other features are described in more detail below.

Rekor understands the law enforcement objectives that should be supported by a robust ALPR System, such as the ability to be an affordable force multiplier that integrates with multiple law enforcement hotlist databases and/or ALPR sources, provides fast and efficient license plate reads often in challenging light and weather conditions across multiple lanes of traffic, and providing easy-to-use search capabilities that quickly provide results across multiple databases to aid in finding vehicles of interest to combat crime, including drug and human trafficking.

C.2.2.1.2 *Technology Overview*

Rekor's ALPR technology platform consists of a finely tuned ecosystem of portable and mobile (trailer and in-vehicle) cameras that operate with full edge processing, and integrate seamlessly with our back-office application. Our Edge (portable and trailer) and Finder (mobile) camera solutions are driven and managed by our AI-based machine learning Watchman software, enabling a comprehensive approach to any ALPR program. **All cameras provide color overview images for vehicle identification, as well as video clips for enhanced verification,** and all cameras except our in-vehicle mobile cameras are supported by IR illumination. Each of our camera solutions and our software platform are described in more detail below.



Figure 17 Rekor's differentiators provide agencies with unparalleled performance and massive system flexibility.

While Rekor is not aware of current ALPR camera locations used by the Sheriff's Department, we do believe given the variety of roadways in San Diego County that there could be many locations requiring coverage over multiple lanes of traffic. Typical legacy systems provided by our competitors require a single camera to provide maximum effectiveness for each lane, thus requiring multiple cameras for each direction monitored for multiple lanes. Rekor understands that this can be problematic as systems that do not cover more than one or two lanes require greater infrastructure build-out, power consideration, and can unnecessarily increase costs.

Our system, regardless of the hardware model, captures and reads a license plate regardless of its position in the field of view. Thus, we can achieve the client's vision for installation and operation on a more economical basis. We have systems that capture multiple lanes (up to three or four depending on model), using a single camera—regardless of the vehicle's position. Furthermore, our application has a broader range of distance and positioning options with the capability to read information at extreme viewing angles.



Figure 18 One Rekor camera can capture vehicle reads over multiple lanes of travel.

A significant advantage of Rekor's Watchman software is that it can accept video streams from nearly any IP camera making it **hardware agnostic**. Unlike legacy OCR-based systems with costly purpose-built cameras, Rekor is able to leverage continuously evolving hardware technology. By fusing the power of machine learning and artificial intelligence, parallel processing capabilities, and best-in-class hardware, our solution captures license plate data and vehicle characteristics at extremely high vehicle speeds with a high degree of accuracy, even in unusually difficult conditions, such as low lighting, poor weather, extreme camera viewing angles, and obstructions.

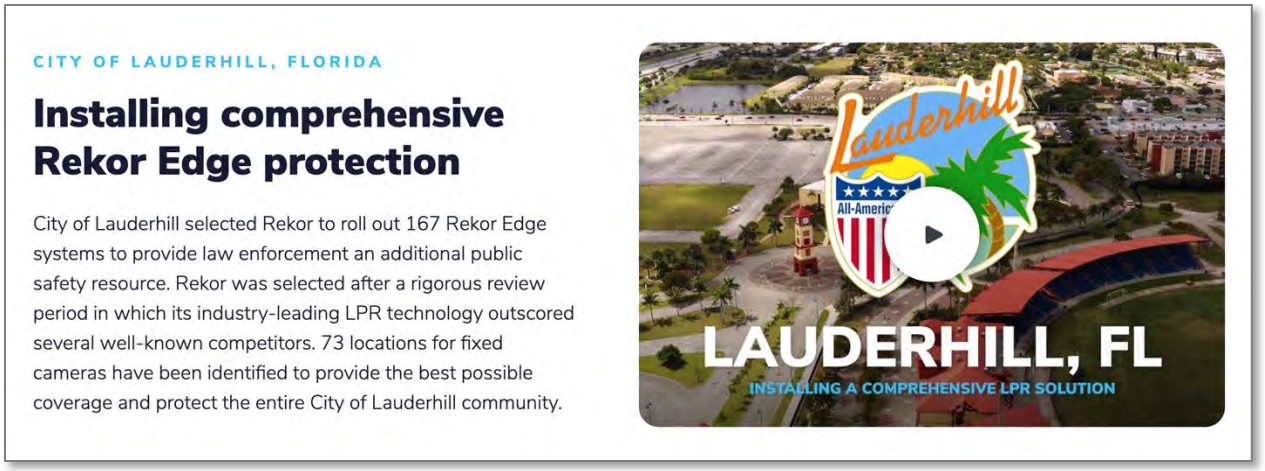


Figure 19 167 cameras in 73 locations covering 260+ lanes.

C.2.2.1.3 *Portable Cameras*

Rekor's camera systems have been able to successfully reduce crime, while our installations have had minimal impact on traffic flow during easy and fast installation to existing structures. We offer in this proposal cameras that can achieve the desired capture results without requiring additional physical infrastructure. We can provide cameras that work on your infrastructure, or if necessary, we can provide a fully off-grid solution that includes solar power. Due to our proprietary compression techniques, we can operate seamlessly via 3G or 4G wireless communication protocols.

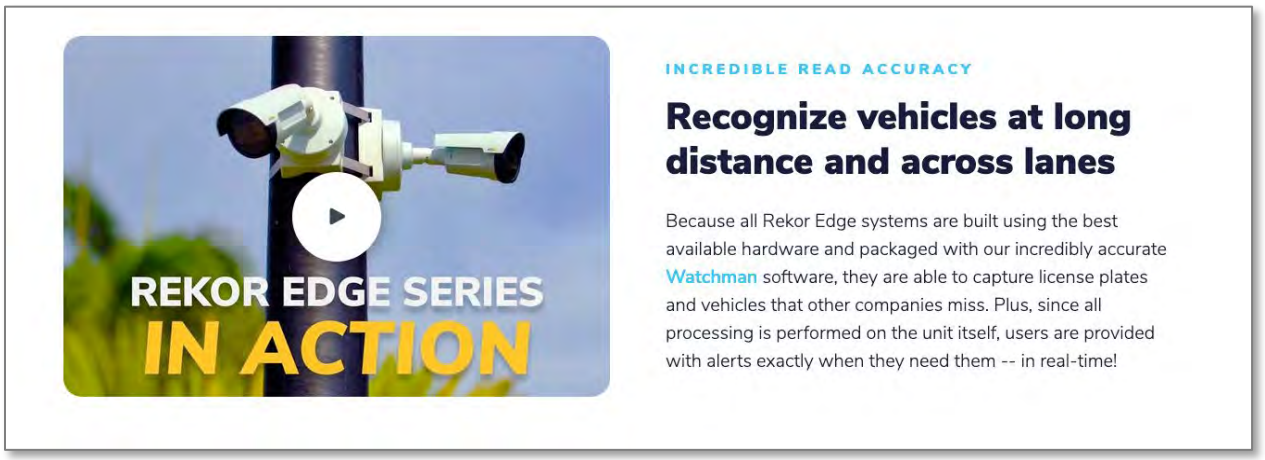


Figure 20 See how one Edge camera captures license plates across multiple lanes.

For portable camera locations, Rekor offers real-time edge processing based on ALPR program needs with respect to lane coverage, power availability and mounting options. Our Edge 300 camera, which is recommended for both residential areas and highways and speeds up to 120 miles per hour, covers up to four lanes at 300 feet. We also offer an Edge 300x2 which includes two cameras on a single system, for up to five lanes of coverage (same travel direction) or bi-directional coverage (opposite travel directions).

When evaluating the product options available from Rekor versus others, it is important to point out that capabilities and performance in a law enforcement environment represent a key differentiator for Rekor's technology. Our Edge 300 roadside product offers full video streaming plate capture with real-time edge processing, which is not interrupted when communications are down. When viewing an ALPR "hit", the user can access the video clip to look for additional evidence about the vehicle of interest. Certain competitors offer a residential product performing low-speed image capture with full-cloud processing, which dramatically extends the alert time and is inoperable when communications are interrupted. Other legacy competitors offer purpose-built cameras that perform only one lane of coverage, thus requiring multiple cameras for multiple lanes. In most law enforcement implementations, the vast majority of locations require coverage of up to three lanes at highway speeds, so a "residential" or "one-lane" system would not suffice.



Figure 21 Edge 300 camera.

All of our portable and trailer-mounted camera solutions include IR for excellent night and poor weather capture, with near 100% capture rates on the lane counts specified for each model. Read accuracy exceeds 99% in benchmark testing, and greater than 95% in live environments. In addition, our cameras read license plates from all 50 states and U.S. Territories, the District of Columbia, Canada, Mexico and over 85 countries, including vanity plates, and half-height characters. **In addition to the plate, each read contains make, model, color, direction of travel, and body type of the vehicle, identified natively in real time by the software, as opposed to using a motor vehicle registration database lookup like many ALPR vendors**. Our native determination of these critical vehicle attributes is superior in all situations, especially where nefarious actors swap license plates to different vehicles in furtherance of the commission of a crime. Additionally, our cameras have high read accuracy at night and in dim lighting situations, with no additional external lighting required other than lighting that is integrated within the hardware.

Rekor combines the best-of-breed cameras and ALPR-related peripherals into our single, comprehensive, turnkey solution. As such, we bring to the Sheriff's Department a hardened application with the peace of mind that comes from the combined expertise of market leaders for each component. All proposed cameras are seamlessly integrated, controlled and managed through our proprietary ALPR application and back-office Watchman software application.

Because our software is hardware agnostic, we are not restricted to utilizing proprietary equipment and peripherals which often are quickly outdated. Rather, Rekor remains on the cutting-edge by integrating our ALPR engine into best-in-class commercially available equipment that exceeds resolution, processing, communications, and environmental requirements. This allows us to offer to our customers the perpetual "latest and greatest" component mixture. Our solution to the Sheriff's Department brings together Axis Communications video cameras, Nvidia GPU graphics processors, and Sierra Wireless modems, all representing best-in-class components in the industry for their respective function. We work with leading engineering firms to design integrated circuit boards and other peripherals that optimize the interaction between these commercial components to provide the highest quality equipment for our clients. We don't rest on our laurels and continue to work with hardware manufacturers to improve on our products based on experience with law enforcement agencies that want better solutions than those that they have had to accept over the past decade and to keep our prices affordable for cash-strapped municipalities.

A critical added benefit to our solution is that security and surveillance features (e.g. video monitoring and recording) are NOT disabled when used for ALPR purposes. **With an included SD card, we provide 30 days of continuously recorded video at each camera, enabling historical review of environmental video feeds, based on reported incidents within the view of the cameras.**

Performance Measure	Rekor Capabilities for Fixed and Trailer-Mounted Cameras
Cameras' ability to read all readable license plates, including digitally printed plates, from all fifty (50) states including vanity plates, multiple plates and half-height characters, in both daylight and darkness	All portable and trailer-mounted cameras read all types of license plates (digitally printed, vanity, multiple and half-height characters plates) from all 50 states, the District of Columbia and U.S. Territories, and over 85 countries, including Canada and Mexico, in both daylight and darkness
Speed at which the camera captures readable license plates	Up to 120 MPH
Accuracy at which the camera captures readable license plates	99% in controlled test environments and 95% in typical field trials
Performance under varying (dim or bright) light conditions	Excellent
Performance under varying weather conditions.	Excellent
Range capabilities	300 feet daytime; 150 feet nighttime

Detailed specifications for the Rekor Edge 300 camera system are provided in our product sheet in Appendix E.1.

C.2.2.1.4 *Mobile In-Vehicle Cameras*

Our vehicle mobile cameras are mounted inside of vehicles and provide a "stealth" mode that does not signal to others that license plate and vehicle data are being recorded. These cameras rely on ambient light illumination from other vehicles, streetlights and even the moon. Because IR illuminators cannot transmit their signal through glass, our vehicle mobile cameras can experience a degradation of read accuracy in extremely dark conditions – a tradeoff with stealth that many law enforcement agencies have welcomed. The agencies that we have worked with saw the advantages of our system over having the ability to read a license plate in absolute darkness.

While the RPF specified self-luminating IR cameras, which we have for our portable and trailer solutions, **Rekor has a differentiated vehicle-mounted ALPR that has its ALPR cameras mounted inside the vehicle**. Most law enforcement agencies are accustomed to seeing trunk-mounted or light bar-mounted ALPRs that scream "We are reading your license tag", take longer to install, are subject to weather, and may have challenges going through a car wash. These systems are equipped with IR cameras that provide a good read when there is absolutely no ambient light. Because our Finder cameras are mounted inside of vehicles, they provide a "stealth" element that keeps an unmarked vehicle looking much more like a civilian vehicle. An inside-vehicle mount also keeps the camera out of the elements. Since IR illumination does not work through glass, our Finder ALPR systems include high-quality color cameras that provide superior, multi-lane coverage during daylight and rely on ambient light for nighttime ALPR

captures. Ambient light can come from the vehicle's headlights, other vehicle headlights, street lighting and moonlight. The main situation when a pure IR-illuminated vehicle system performs better is when a vehicle is sitting on the side of the road with all of its lights off on a completely dark road. Please ask yourself how often that's a situation in which your Sheriffs will want to read license plates. Our interactions with law enforcement indicate that they prefer a higher performing solution and are not concerned with the narrow use case when IR illumination works well. We have plenty of law enforcement and federal agencies that have found our in-vehicle ALPR cameras to provide a better overall solution to those vendors that mount their ALPR cameras on trunks or light bars.

Our mobile in-vehicle camera installation has two (2) cameras which operate independently and simultaneously. The two cameras are mounted between the rear-view mirror and the front windshield and in such a way that an individual's field of view is not obstructed. A failure of one (1) camera will not prevent normal operation of the other camera.



Figure 22 Example of two ALPR cameras located above the mirror and not obstructing any occupant's view.

The mobile in-vehicle camera system is capable of capturing license plates in any of the following scenarios:

- An adjacent lane on either side of the patrol vehicle while driving through traffic and/or parking lots;
- Traffic in an adjacent lane while parked on the side or shoulder of a roadway;

- Any parking application from parallel to perpendicular parked car orientation with respect to the movement of the patrol vehicle, and

Performance Measure	Rekor Capabilities for In-Vehicle Cameras
Cameras' ability to read all readable license plates, including digitally printed plates, from all fifty (50) states including vanity plates, multiple plates and half-height characters, in both daylight and darkness	In-vehicle cameras read all types of license plates (digitally printed, vanity, multiple and half-height characters plates) from all 50 states, the District of Columbia and U.S. Territories, and over 85 countries, including Canada and Mexico, in both daylight and darkness
Speed at which the camera captures readable license plates	Up to 120 MPH closing speed
Accuracy at which the camera captures readable license plates	99% in controlled test environments and 95% in typical field trials
Performance under varying (dim or bright) light conditions	Variable dependent on ambient light
Performance under varying weather conditions.	Excellent
Range capabilities	40-50 feet, adjacent two lanes on either side of the patrol vehicle

The chart below provides an overview of the Rekor solution in comparison to more traditional in-vehicle ALPRs:

Feature	Rekor Mobile ALPR	Traditional ALPR Systems
Portable ALPR Operability	• Portable system can be hard-wired or plugged into vehicle's 12-volt outlet for immediate installation or removal • Embedded wireless communication eliminates need to use vehicle's WiFi or cellular connection	• Portable product not available • Installed cameras only
Integration	• Rekor provided tablet • Portable solution requires NO additional install	• Does not provide option for external tablet
Configurations	• Two-camera configuration • Portable or fully installed in vehicle • Parallel (bidirectional) or perpendicular enforcement • Easy setup • Uses ambient lighting	• Limited lighting and configuration options
Weather Consideration	• Unit installed INSIDE the vehicle, which provides full protection from elements • Inside position systems offer the most optimal image resolution	• Systems affected by external conditions
Installation	• No special installation required	• Requires 2 to 8 hours installation per vehicle
Maintenance & repair	• Immediate unit replacement option results in no downtime	• Vehicle needs to be removed from service for repair



Figure 23 See our in-vehicle camera in action.

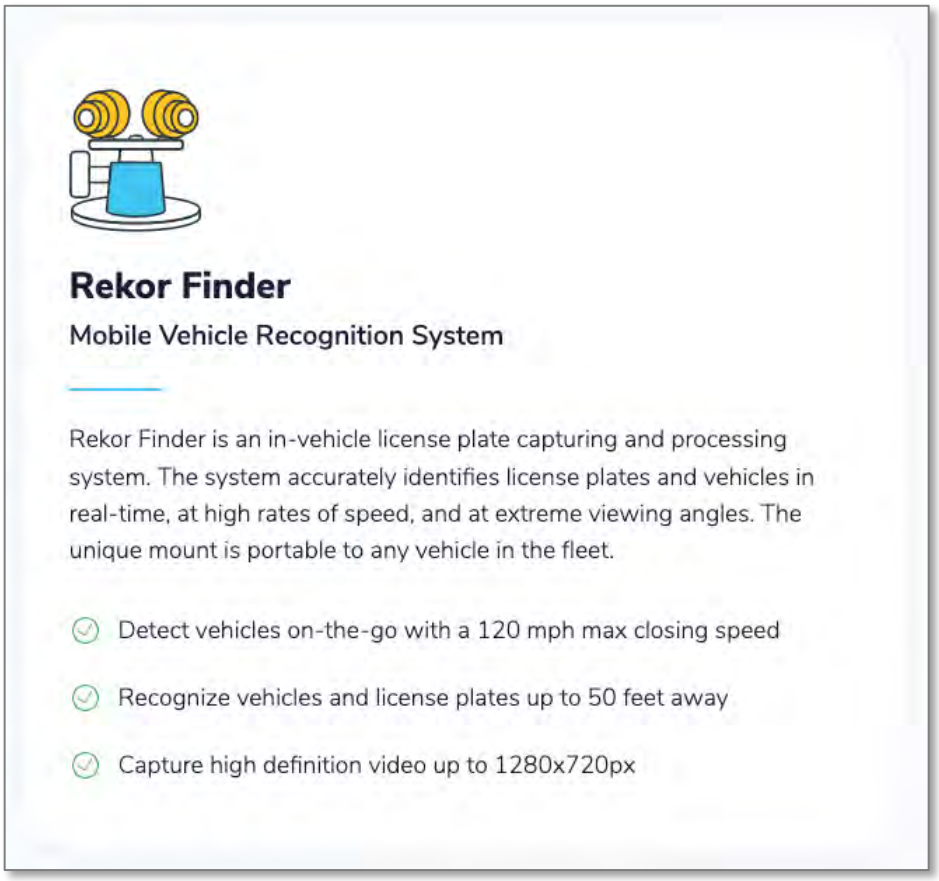


Figure 24 Unique interior mount provides a "stealth" element and protects equipment from damage.

Detailed specifications for the Rekor Finder in-vehicle cameras are provided in our product sheets in Appendix E.2.

C.2.2.1.5 *Mobile ALPR Speed Trailer Camera*

Rekor's mobile trailer-mounted ALPR camera is integrated into a traditional speed warning sign trailer to provide an element of stealth. The dome camera is the equivalent of the Edge 300 fixed-pole camera and has an optical zoom capability.

The trailer features a large portable speed awareness sign and can be strategically placed in dangerous, high-risk areas to improve motorist and pedestrian safety. The ALPR camera can help law enforcement to cover major city or localized access points for wanted vehicles, receive AMBER and Silver alerts, and accelerate investigations.

Designed to withstand the rigors of a small trailer bouncing, the dome camera is equipped with an easy-to-adjust manual slewing capability to set the camera for optimal lane coverage,

irrespective of the trailer's orientation to the roadway. While competitor dome cameras may require removing the dome to adjust the camera slew angle, our camera is can be adjusted without removing the dome cover.

The trailer is US Department of Transportation approved and equipped with IP67-rated, lockable enclosures that protect equipment from the elements and theft or tampering. Well suited for highway and residential use, the trailer's compact design is easily portable and can be set up in five (5) minutes. As an added feature, the trailer's see-through design keeps pedestrians and road workers in view.

The FCC/CE compliant radar captures vehicle speeds up to 120 miles per hour. The integrated GPS ensures all ALPR read locations are accurately documented and the 3G/4G wireless modem is FirstNet-ready.

The 300-watt solar array provides plenty of power to run the system and charge batteries that can provide up to 15-day backup. Furthermore, our trailers are equipped with AGM (absorbed glass-mat) batteries that are designed to be more effective when the temperature drops. These heavier batteries help to lower the trailer's center of gravity for better stationary and moving stability. When operating in warmer climates, cooling fans protect equipment from overheating. Our trailer weighs approximately 870 pounds and can be towed by a small vehicle and easily maneuvered into operating positions.



Figure 25 Domed ALPR camera mounted under the solar panel.

While our standard trailer-mounted ALPR system includes one camera, we do offer the option to mount a second camera to capture the rear license plates on vehicles traveling in both directions relative to the trailer. In addition, the Sheriff's Department has the option of adding one or two of our ALPR cameras to existing trailers in its inventory.

Detailed specifications for the Rekor trailer-mounted cameras are provided in our product sheets in Appendix E.3.

C.2.2.2 Marked patrol vehicle camera mounting brackets must be compatible with Whelen, Code3, TOMAR, Federal Signal, Arjent S2 light bars

As discussed above, Rekor's current in-vehicle ALPR systems are mounted within the vehicle and as such do not require light bar mounting. In our effort to provide more flexibility to our

customers, Rekor's next generation vehicle-mounted ALPR camera system (expected release in Q1 2021) is being designed to be placed on the exterior of a vehicle and will not require mounting to the lightbar or trunk. Since Rekor spent many years in the law enforcement vehicle upfitting business, we are very familiar with light bar manufacturers including Whelen, Code3, TOMAR, Federal Signal, and Arjent S2, and should the County want to have our next-generation ALPR cameras on a light bar, we will be able to do so, but we believe that law enforcement agencies will welcome a more streamlined external ALPR camera.

C.2.2.3 Cameras shall be self-illuminating Infrared (IR) for effective license plate image capture in a variety of weather and lighting conditions

The Rekor portable and trailer-mounted ALPR cameras are self-illuminating for superior night operating and the mobile systems operate effectively in many low light conditions without the need for IR illumination. They have excellent read capability in a variety of weather conditions. As we discussed above, we invite the County to test our equipment.

C.2.2.4 LPR cameras shall be water-resistance with few moving parts that can be damaged

Al Rekor ALPR cameras that are not located inside of a vehicle are rated for water resistance and contain few moving parts that can be damaged. Our mobile systems, which operate from within the vehicle, are naturally protected from wet weather by the vehicle.

C.2.2.5 LPR cameras shall have the ability to automatically capture all variations of California license plates, to include California dealer issued plates (paper plates)

All Rekor ALPR camera systems can read all variations of California license plates, including the dealer issued (paper) plates. Our systems also can read all types of license plates (digitally printed, vanity, multiple and half-height characters plates) from all other 49 states, the District of Columbia and U.S. Territories, and over 85 countries, including Canada and Mexico, in both daylight and darkness. Since all ALPR reads are not 100% accurate, Rekor provides a bonus for its clients by providing a video clip along with each ALPR license plate hit. **Our system also captures a video of each ALPR read, thereby providing additional visual evidence should it be necessary for more detailed investigation.**

C.2.2.6 Cameras shall have a dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle for verification purposes

The Rekor portable and trailer-mounted cameras provide complete capability to capture the IR image for night LPR plate reading as well as the color overview image (during the day) without



the need for a dual lens configuration. The mobile systems operate effectively in many low light conditions without the need for a dual lens configuration (they also capture the color overview image of the target vehicle).

We hope that the Sheriff's Department will be open to ALPR solutions that achieve its ALPR goals without unnecessarily requiring a dual-lens configuration. ALPR state-of-the-art solutions have advanced beyond dual-lens solutions.

Unlike most ALPR vendors, Rekor delivers true "vehicle recognition" software, not simply license plate recognition capabilities**. Reads include, but are not limited to, the vehicle's make, model, type, color, state, and direction of travel**. By fusing the power of machine learning, parallel processing capabilities and best-in-class hardware, our solution captures license plate data and vehicle characteristics at extremely high vehicle speeds with an exceptional degree of accuracy, even in unusually difficult conditions, such as low lighting, poor weather, extreme camera viewing angles, and obstructions. **Why would a law enforcement agency not want to have this capability? Wouldn't your Sheriffs and investigators like to search for a vehicle based on make, model, color, exclusive of license plate?**

C.2.2.7 Cameras shall be sealed to NEMA 6 (IP67) standards

The Rekor portable and trailer-mounted ALPR cameras are IP67-rated and the in-vehicle mobile systems operate from within the vehicle and as such the vehicle itself provides water protection.

C.2.2.8 Dual lens cameras shall be capable of capturing up to 60 frames per second

Rekor's cameras are capable of operating at 60 frames per second for superior high-speed capture. Please note that our cameras are capable of reading license plates of vehicles travelling up to 120 miles per hour. The speed of a vehicle may be an easier metric to evaluate when testing an ALPR systems' capabilities.

C.2.2.9 Cameras shall have the ability to adjust shutter, brightness, and gain settings to ensure a high-quality image regardless of weather or lighting conditions

Rekor cameras have the ability to adjust all critical image capture metrics (e.g. shutter, brightness, gain, etc.) to ensure superior image quality in a broad range of environmental conditions. These characteristics can be monitored and adjusted remotely.

C.2.2.10 The cameras shall be able to have a fixed focal point or target distance from the camera to the vehicle's license plate from 9 ½ feet to 30 feet

Rekor's mobile in-vehicle cameras can support short-range operation as low as 9.5 feet as well target distances well beyond 30 feet. In order to give our clients the flexibility to place cameras in convenient locations, our fixed and portable ALPR cameras can capture license plates at distances up to 300 feet. In addition, our ALPR solutions can cover multiple lanes with one camera. Thus, the Sheriff's Department can cover more lanes of traffic at a lower overall cost when considering that many competitor systems have cameras that are limited to one lane of coverage.

C.2.2.11 The camera shall be capable of various configurations to capture plates in any of the following modes depending on the configuration:

As introduced above, all of Rekor's ALPR solutions can support the specifications listed below.

C.2.2.11.1 *An adjacent lane on either side of the vehicle while driving through traffic and/or parking lots*

Our in-vehicle cameras can support reading license plates in the adjacent lanes on either side of the vehicle while driving through traffic as well as all expected parking environments.

C.2.2.11.2 *Traffic in an adjacent lane while parked on the side of the shoulder of a roadway*

Our in-vehicle mobile cameras read license plates in adjacent lanes (left or right) while parked on the side of the shoulder of a roadway.

C.2.2.11.3 *Parked vehicles in parking lots*

Rekor's in-vehicle mobile cameras can support reading license plates of parked vehicles in parking lots and in all expected parking environments.

In addition, with our next generation 4-camera IR external system (expected release Q1 2021) the rear-facing cameras will read the rear license plates of vehicles traveling in the opposite direction in an adjacent lane, as well as the front license plate (if there is one) of a vehicle passing the law enforcement vehicle.

C.2.3 LPR Processor

C.2.3.1 Processor shall have a "self-trigger" mode to detect the presence of correctly mounted vehicle license plates in the camera's field of view for image capture from the camera

Rekor cameras monitor their field of view on a continuous basis and our software is designed to recognize license plates and identify using AI and machine learning. Our system does not just take one picture per license plate seen. Instead, it takes a series of images and retains the one that the system determines to be the highest quality read. As mentioned above, our systems also retain a video clip of the license plate "hit" in order to provide addition information or evidence.

In addition to the license plate, each read contains make, model, color, direction of travel, and body type of the vehicle, identified natively in real time by the software, as opposed to using a motor vehicle registration database lookup like many ALPR vendors. Our native determination of these critical vehicle attributes is superior in all situations, especially where nefarious actors swap license plates to different vehicles in furtherance of the commission of a crime.

C.2.3.2 Processor's installed in vehicles shall be equipped with an intelligent Power Supply Unit (PSU) that provides for a safe start and shut-down each time the vehicle's ignition is turned on and turned off

The Rekor mobile systems are configured to robustly and safely support the expected on/off conditions from the vehicles ignition circuit. Our Finder is equipped with a power conditioning box between the CPU and the ignition circuit to handle power surges at on/off.

C.2.3.3 Processor controls the power supplied to the cameras and provides video connection points for simplified system wiring

Rekor system processors provide power to cameras via a POE power distribution, and a central wiring point is provided for simplified installation.

C.2.3.4 Processor shall have at least four (4) LPR camera connections and multiple USB ports

Our next generation 4-camera external IR camera system will support four camera connections and multiple USB ports.

C.2.3.5 Vehicle mounted processors shall meet the environmental conditions associated with being mounted in a trunk

The current version of our in-vehicle ALPR solution does not require equipment to be mounted in a trunk. All components are mounted within the passenger compartment and are designed to withstand normal passenger compartment environmental conditions. Our next-generation of the Finder, which will be fully upfitted within the vehicle, will certainly be capable of withstanding a trunk's environmental conditions.

C.2.4 LPR Software -- Watchman Software Application and Back Office

Overview

Watchman is full-featured AI-based software package the reads live video and provides real-time license plate and vehicle recognition results. By running on existing IP, traffic, and security cameras, Watchman provides a comprehensive ALPR solution that can be deployed in the Cloud without the need for costly proprietary server hardware. Once installed, the Watchman agent recognizes vehicles and license plates with the results being searchable in our highly secure AWS GovCloud environment that is currently operational for other California customers. Watchman also integrates and operates seamlessly with all Rekor manufactured hardware products.

A key feature of Watchman that differentiates Rekor from our competitors are the fact that it is true "vehicle recognition" software and not just a license plate reader. Reads include but are not limited to the vehicle's make, model, type, color, state, and direction of travel. By fusing the power of machine learning, parallel processing capabilities and best-in-class hardware, our solution captures license plate data and vehicle characteristics at extremely high vehicle speeds with an exceptional degree of accuracy, even in unusually difficult conditions, such as low lighting, poor weather, extreme camera viewing angles, and obstructions.

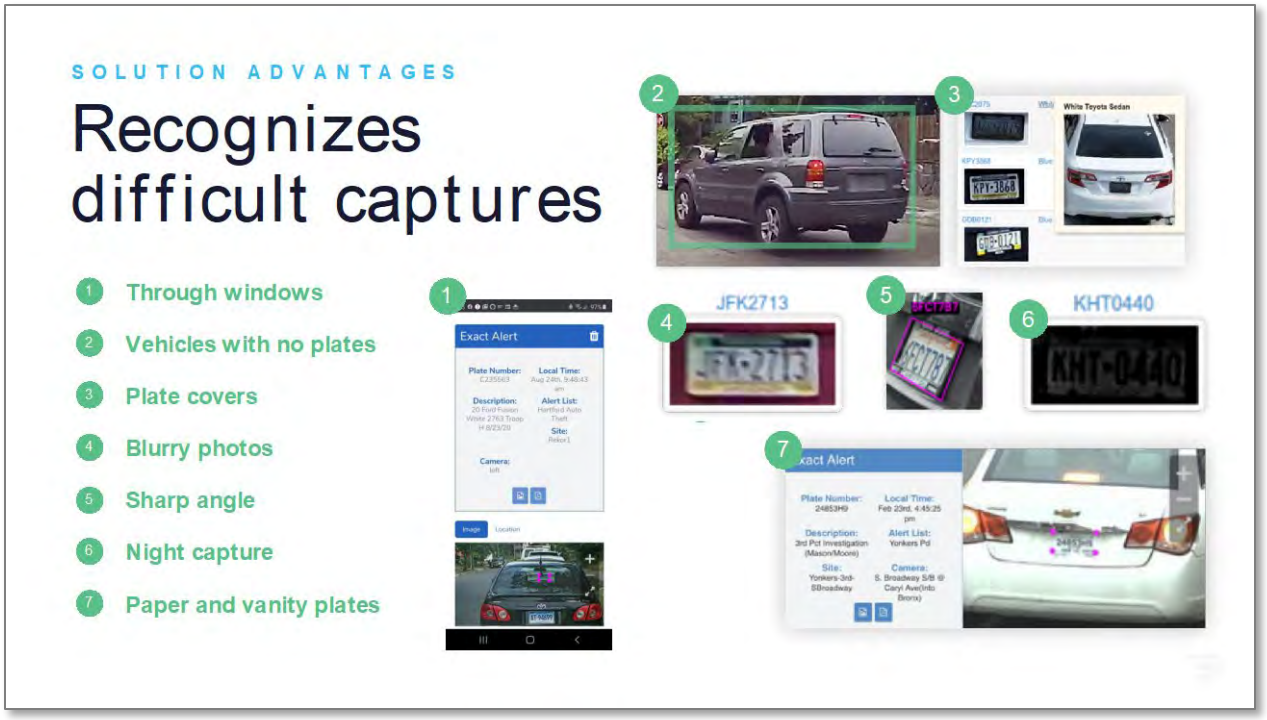


Figure 26 Rekor's ALPR solution can accurately capture license plate data in some of the most extreme conditions.

Our system also captures a video of each ALPR read, thereby providing additional visual evidence should it be necessary for more detailed investigation. This video link would be available for ALPR program users.

SOLUTION ADVANTAGES

Surpassing the competition

	REKOR	Competition
Lanes of traffic covered from a single camera	Up to 3 lanes (options out to 5 lanes)	Max 2 lanes
Camera range	300 feet (day), 100 feet (night)	60-70 feet
Retention policy on data	Flexible / Automated; defined by the agency	Rigid; limited to 30 days
Data control	Agency	Vendor
Time from read to alert	< 10 seconds	30-60 seconds
Video attached to read records	✓	✗
Remote support of devices	✓	✗
Suitable for extreme environmental conditions	✓	✗
Mobile ALPR app	✓	✗

Figure 27 Rekor's AI-driven technology is unmatched in terms of accuracy, data control and client support.

Hotlist Integration

With Rekor's system, the Sheriff's Department can import law enforcement "hotlist" databases to provide real-time alerts for vehicles of interest and maintain historical vehicle recognition information for investigatory purposes. Our in-house engineers and CJIS specialists work in tandem with the client's law enforcement team to simultaneously commence integration activities with hotlist download authorization, as well as inter-agency agreements, if necessary. All approvals and transmission testing for each installed ALPR camera are completed in parallel to prevent any downtime beyond site construction. ALPR reads will be processed in real time at the source, followed by transmission of cropped images and data for hotlist matching or exporting to tracking databases. This all occurs within 1-2 seconds.

Plate reads are transmitted to our hosted CJIS-ready AWS GovCloud server where alerts are generated from the NCIC or state hotlists, or even from supplementary (optional) local hotlists created by your agency (e.g. vehicles of interest that may not necessarily be in state or national databases). Our machine learning Watchman software operates with a benchmark 99% accuracy on plate reads, and also captures state, make, color, and vehicle type in real time. Alerts can be configured for viewing within the backend software, or via text or email forwarding to specified authorized personnel.

Cloud Hosting

Part of our implementation plan will include configuration of the Sheriff's Department secure AWS GovCloud environment, with customizable data retention periods that are policy-driven. Before the system goes live, users can be seamlessly added, according to Sheriff's Department policy and authorization. All data access is via web browser, so users will not require downloadable software to reside on their laptop or desktop.

Dashboard

Watchman's easy-to-use and intuitive dashboard provides the central control point for end users. It allows end users to view ALPR camera read activity in list form (as shown below) or in a map-centric display. The dashboard supports the ability to comprehensively search for wanted plates in several functional modes.

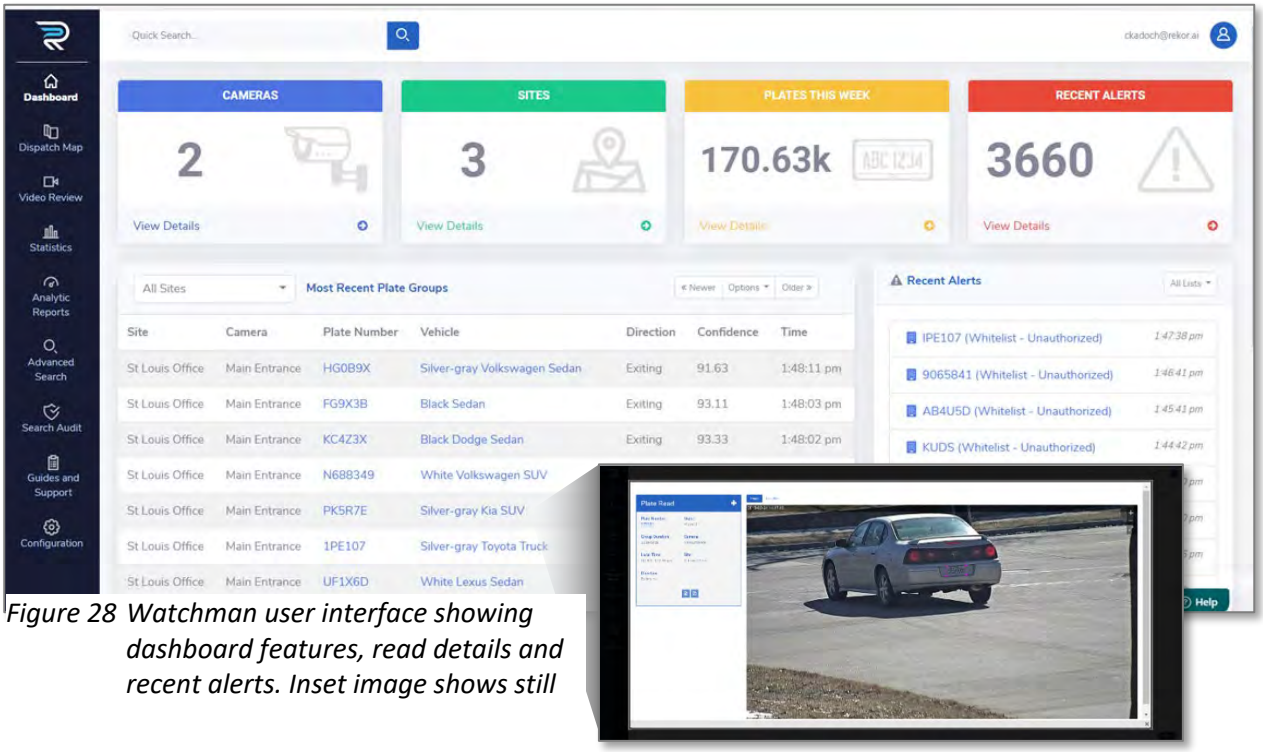


Figure 28 Watchman user interface showing dashboard features, read details and recent alerts. Inset image shows still

Searches

Watchman's search capabilities are extensive and allow for searching ALPR camera hits based on:

- License tag characters, using an exact or "fuzzy" search
- License tag state

- Vehicle make
- Vehicle body type
- Vehicle color
- Vehicle travel direction

Searches can also be filtered by camera geographic location, and date and time ranges.

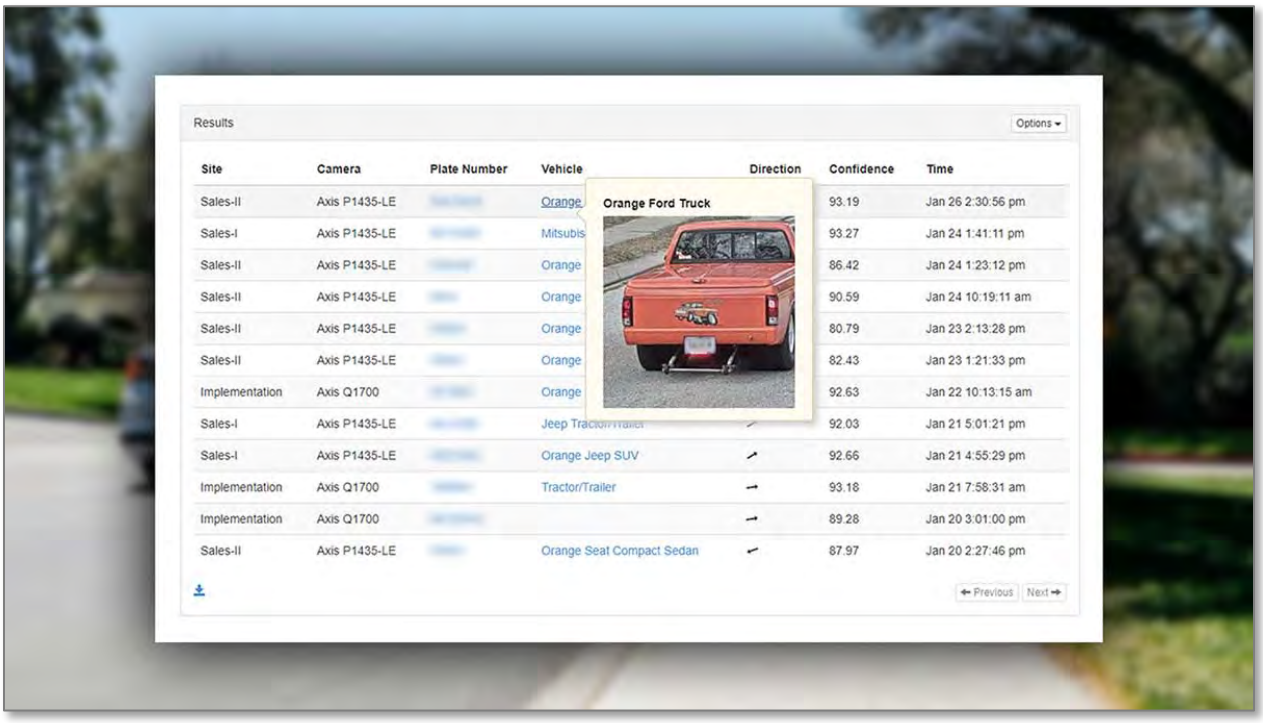


Figure 29 Locate vehicles of interest using Watchman's advanced search functionality.

Rekor has also defined and automated several common investigative search analytics including the following:

- Interdiction -- vehicles traveling on a defined path.
- Convoy Analysis -- vehicles commonly associated with each other.
- Common Vehicle Analysis -- vehicles associated with one or more locations of interest such as a crime location a certain day and/or time.
- Bulk Search Analysis -- vehicles associated with a defined list.
- Vehicle Speed Analysis -- speed estimated by time between two know locations.

Reports

Rekor will provide a system capable of producing a variety of mutually agreed upon standard and customized reports operational reports for the System as a whole and each of its functionalities, as well as the consumption of all consumables for all System hardware as



described in this proposal. The reports will include at minimum: Hits; license plate images and associated data; and license plate searches performed by the officer indicating the date and time the search was conducted.

Access to, and delivery of, all reports will meet the following minimum requirements:

- Sheriff's Department designated personnel will have the ability to access all reports from a centralized location.
- Rekor will work with the Sheriff's Department to replicate reports currently utilized by the Sheriff's Department.
- The Sheriff's Department will have the ability to create customized reports based on parameters determined by the Sheriff's Department.
- Sheriff's Department designated personnel will have the ability to perform real-time ad-hoc reports through Sheriff's Department-approved tools with Sheriff's Department-designated personnel having access to only those data fields permitted based on their roles/security classes.
- Reports and results of queries will be downloadable in multiple formats, including tab-delimited, Microsoft Excel, Microsoft Word, and PDF.
- The System will be capable of sending all reports to paper, screen, or file (i.e., Print, View, Save as).
- Rekor will collaborate with the Sheriff's Department to establish the scheduling parameters and retention periods for reporting. Scheduling parameters and retention periods for reporting must be approved in writing by the Sheriff's Department prior to implementation.

Ability to Integrate with Other Third-Party ALPR Systems

Rekor routinely integrates with third-party vendors and their databases, and we can seamlessly provide customized solutions and move quickly to integrate with other authorized databases or to migrate authorized data. The biggest risk with any third-party integration is ensuring full cooperation in a timely manner from the third-party.

C.2.4.1 Application software shall be capable of running on a Windows based mobile computer

Rekor's in-vehicle mobile ALPR system can integrate with any standard Windows-based mobile computer. In addition, since our back-office Watchman software is cloud-based, it can be run from any authorized computer with internet connectivity.

C.2.4.2 There shall be no Java programming or Java derivatives

Rekor's systems do not use any Java programming or Java derivatives.

C.2.4.3 LPR system shall have real time alerting and the ability to program custom hotlist

Rekor's system allows for a hotlist hit to be optionally triggered on an "exact" or "fuzzy" match against a hotlist as a Sheriff's Department definable setting. Rather than a limited (N-1 or N-2) mismatch, an ALPR industry standard, our Watchman system matches against a definable number of closely matched license plates based on their relative recognition confidence values. This assures that the alert is against the holistically closest values rather than a simplistic one- or two-character mismatch.

Hotlists can be custom defined and created and enabled within the Watchman back-office. Select lists are pushed to mobile systems for tailored enforcement.

C.2.4.4 There shall be a secure login and password function on the LPR software; The user's access shall be controlled by an administrator designated by the San Diego County Sheriff's Department

Rekor's Watchman software provides for secure login and password functions and user access is controlled by a designated administrator within the Sheriff's Department.

Logging into Rekor's applications requires users to have a unique username and password. Configurable polices require the user to have a complex password and password exhaustion schedule. Optionally, two-factor authentication can be enabled for additional security. Highly configurable user management capabilities allow for an administrator to grant and revoke access to the application. The administrator can have fine-grained controls over the application modules to which a user has access.

All customer data is logically separated from other clients' data to ensure that a single customer can only see their data.

All users are required to have unique user accounts with a complex password. Password polices are in place to enforce password complexity, rotation, and prevent reuse of previous passwords. Where desired multi-factor authentication is implemented to add additional protection from unauthorized access.

User permissions are granted based on a principle of least privilege, meaning that a user is only granted access to the system resources necessary to do their job. If a user's role changes, access permissions will be adjusted to fit their new role.

Timestamped audit logs are maintained for Rekor's network environment and applications. Logs can be retained to meet compliance or customer requirements. Log entries are protected

from unauthorized access and from deletion or modification. Designated Rekor staff will review logs for abnormalities.

We understand that while supporting the Sheriff's Department ALPR program we will have access to, process, store and/or transmit sensitive data including, but not limited to:

- Vehicle plate and location information;
- Infrastructure information (camera locations, etc.); and
- Information relating to the Sheriff's Department computers to vendor software and other state systems.

Through our services provided to the Sheriff's Department, we provide ALPR systems that enable CJIS compliance that can be fully integrated and compliant for hotlist processing.

Security is paramount when constructing all of our products and services. Rekor offers end-to-end encryption, using an industry standard AES-256 encryption algorithm to encrypt data at rest (inactive data that is stored physically in any digital form). We also use SSL/TLS for encryption during transport. Data is only used to provide our services and we do not share personally identifiable information.

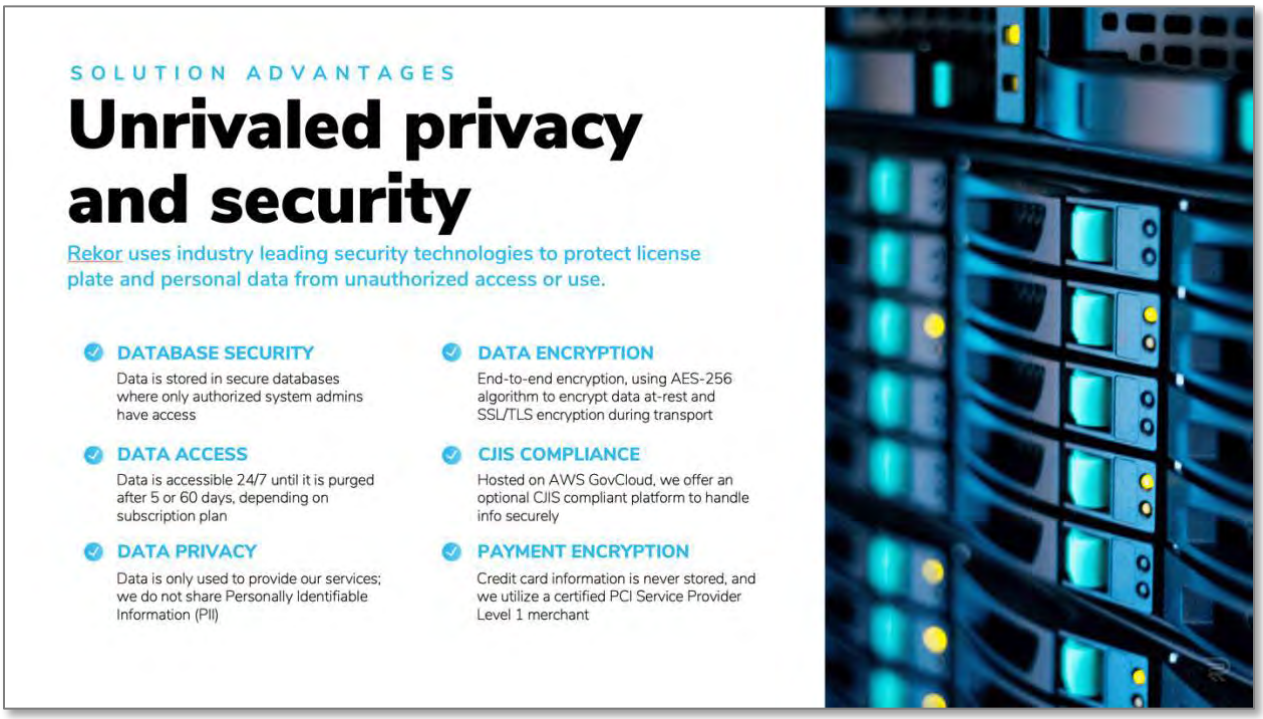


Figure 30 Security is paramount at Rekor.

Because we work with law enforcement agencies and are a publicly-traded, Nasdaq-listed company, the Rekor team is accustomed to working with sensitive information and treating

customer non-public data and personal data from unauthorized dissemination and use with a high degree of care. For further information, our Privacy Policy is located here.

Our systems are hosted in highly secure environments (AWS GovCloud and Nlets) that have been accepted by law enforcement agencies throughout the United States. Our ALPR systems and software comply with CJIS policy as a prerequisite to operating law enforcement ALPR programs.

Rekor requires that all personnel who maintain, have physical access to, or the responsibility to configure computer systems and network devices that provide ALPR access within Rekor, must have their identification, state of residency and national fingerprint-based record checked within 30 days upon initial employment. “Authorized personnel” are those persons who have passed a state and national fingerprint-based record check and have been granted access. Support personnel, contractors, and custodial workers who access computer terminal areas shall be subject to a state of residency and national fingerprint-based record check, unless these individuals are escorted by authorized personnel at all times. As an added measure, Rekor recently increased its security protocols and requires all employees to have their identification, state of residency and national fingerprint-based record checked.

In addition, all required Rekor staff complete Level IV CJIS Security Awareness Training after hire in accordance with the FBI CJIS Security Policy version 5.9. Identified Rekor staff review and sign a CJIS Security Addendum with the expectation this the agreement is applicable to all Rekor clients that create, store, or transmit data identified as criminal justice information with Rekor.

As mentioned above, Rekor employs technical specialists who focus on protocols and compliance measures with respect to CJIS. Although commercial vendors are not technically required to comply with CJIS policy, we believe it is important to ensure the utmost security standards with respect to all data where we are the custodian on behalf of a law enforcement agency or municipal government. We recently conducted a rigorous audit process to identify all areas of CJIS policy that apply to our business. Although much of it is tangential, we have adopted a policy to meet or exceed all CJIS policy requirements with respect to our overall business operations.

All hardware provided by Rekor will be of current design and technology, and none of the camera systems (hardware and software) are prohibited by Federal or state law, policy, or regulation. Furthermore, all the camera systems are Trade Agreement Act (“TAA”) Compliant.

Rekor’s ALPR System provides for system administrator-defined data retention periods that ensure data and records are stored in accordance with federal and state laws, rules, and regulations.

Physical Security

To protect customer data, Rekor uses the highly secure data centers of Amazon Web Services ("AWS") and the Nova hosting solution from Nlets. When hosting information that is deemed Criminal Justice Information ("CJI"), as defined by the FBI's CJIS Security Policy, Rekor will utilize Nova or AWS GovCloud. These hosting environments have been optimized to comply with the CJIS Policy requirements. Both datacenter offerings are equipped with redundant power and internet, environmental controls, and security staff and systems for 24/7 monitoring.

Network Security

Rekor's web applications are deployed in a three-tiered architecture. Web, application, and persistence tiers are separated by highly restrictive firewall rules. Only necessary ports and protocols are allowed through the firewall.

Secure Network Connections

All access to Rekor's web applications take place over HTTPS to protect customer data while in transit. Connections to the application terminates in Rekor's secure server environment to prevent man-in-the-middle attacks.

All remote system access by Rekor's system administrators takes place over encrypted tunnels and flow through a controlled access point for monitoring.

Data Protection

Rekor encrypts all customer data. Customer data in transit is secured by industry standard SSL/TLS encryption. Data at rest is protected by drive encryption using 256-bit AES encryption. Rekor works to ensure that all cryptographic algorithms in use meet all compliance requirements.

Scheduled backups are in place to be able to protect customer data. Controls are in place to be able to protect customer backups. Rekor's backup and restore procedures are periodically tested.

Antivirus and Malware Protection

All Rekor servers and workstations are deployed with advanced, real-time antivirus and malicious code protection deployed. These tools are set to automatically keep threat definitions up-to-date. Rekor uses of scheduled and real-time scanning to protect against malware.

Vulnerability Management

Real-time tools, as well as scheduled external vulnerability scans, are in place throughout the Rekor network to assess for network and application vulnerabilities. When vulnerabilities are discovered, they are assessed by Rekor's security team and assigned to the appropriate team for remediation.

Patch Management

Rekor has necessary patch management processes and procedures in place to ensure that security patches are implemented in a timely manner.

Change Management

Rekor follows a change management process for all changes that take place in the production environment. This process ensures that all proposed changes to the environment are reviewed, approved, and monitored.

C.2.4.4.1 *API capable of integrating user defined active directory*

Rekor's software can support integration with an agency's Active Directory system so as to streamline password management.

C.2.4.5 The software shall provide live, simultaneous display of all the following data:

As described above, our Watchman software provides a full complement of information to identify hotlist "hits", supporting information, and live, simultaneous display for all of the specifications listed below.

- The IR license plate image
- The license plate interpretation or system read
- A corresponding color overview of the vehicle displaying the captured IR license plate
- The date and time stamp
- Identification of the camera capturing the image

Rekor's derived read record contains an image of the license plate for verification. In addition, our system provides a daytime color image from all Rekor cameras and a night-time IR (portable and trailer mounted) black and white (in-vehicle mobile) image of the vehicle and a video clip of the vehicle of interest to provide additional information or evidence.



C.2.4.6 Software shall capture GPS coordinates for every recorded license reads

All Rekor ALPR cameras capture the GPS location for every recorded license plate read and this data is recorded in the Watchman software.

C.2.4.7 Software shall have the ability to GPS stamp all the reads

All GPS location information related to a license plate read is recorded in the Watchman software.

C.2.4.8 Software will give a unique audible and visible alert when a wanted license plate is discovered

Our system provides a unique audio and visual alert when a vehicle of interest licence plate is identified by the Watchman system. When the system identifies a hotlist match, it displays a hit "Alert" screen and generates an audio alert to que the user to the presence of the vehicle of interest. The Alert screen contains all the information necessary to allow the user to validate the hit including the following:

- License plate number and state
- Hotlist that triggered the alert
- Vehicle make, model, color, body style
- Date and time
- Location
- Direction of travel
- Image of the license plate
- Color overview image of the vehicle

The User is thereby queued to confirm the hit or dismiss. A video clip of the vehicle is also available for user review.

C.2.4.9 The Alert Screen remains displayed until acknowledged by the user, and, while displayed, the system continues to process license plate data in the background

When the Rekor system detects a vehicle associated with a defined watchlist, the Watchman system alerts the operator and the alert remains displayed until acknowledged. The system remains operational and continues reading all license plate without interruption during the alert time.

C.3 Demonstration or Sample

C.3.1 County reserves the right to request an on-site demonstration of the LPR camera system being bid or a sample be sent to determine if it meets the requirements stated. All specifications listed in the General Requirements shall be confirmed. All travel, demonstration supplies and/or shipping expenses shall be at the contractor's expense.

As referenced above, based on Addenda No. 2 and 3, Rekor understands that the Sheriff's Department may not be aware of alternative state-of-the-art ALPR capabilities beyond its experience with its current ALPR systems. If the County wants to ensure that it is getting an ALPR system that will provide it with useful features that provide a force multiplier and high performance, Rekor would be honored to provide an on-site demonstration of our ALPR cameras, at no cost to the Sheriff's Department. We understand that the Sheriff's Department would like to move quickly, and we will do all that we can to accommodate the Department's schedule.

C.4 Installation

C.4.1 Contractor shall provide the option to purchase systems as a "kit" that includes all hardware, wiring and software for standard installations

All Rekor ALPR systems are provided with all hardware, wiring, software, and instructions for standard installation.

C.4.2 Contractor shall provide installation and warranty repair options on vehicles within San Diego County

As described previously, installation of the in-vehicle mobile ALPR systems is a straight-forward process. We would initially have our personnel install the equipment and depending on the number of units desired by the Sheriff's Department, we may coordinate with one of our partners in San Diego to further support installations within the Department's schedules.

C.4.3 Contractor shall provide a technician or representative to visit customer site for system start-up, configuration and commissioning of LPR system

As stated immediately above, Rekor personnel will be involved with system start-up, configuration and commissioning of ALPR systems. Our team is well versed in large scale commissioning projects with federal, state and municipal-level agencies.

C.4.4 System Installation and Lead Times (SOW Section 9)

We have internal and subcontractor teams that are experienced with large-scale ALPR rollouts of fixed-pole cameras and equipment. Because of our previous experience running a large regional upfitting operation that served federal, state and local law enforcement agencies around the Washington, DC metropolitan area, we have deep and broad technical experience in how to install ALPR equipment in law enforcement vehicles. All equipment provided to the Sheriff's Department will be new and unused. Summaries for the installation procedures for portable, in-vehicle and trailer-mounted systems are provided below.

As part of the overall rollout, Rekor will work with the Sheriff's Department to determine Watchman software roles, rights, reporting, data integration, testing and user training.

The Rekor Watchman ALPR application is an installed turnkey solution. The system will come completely integrated with a Rekor Edge camera system, that can be fully installed by our highly skilled technicians. We will be responsible for all integration and processes necessary to be fully operational.

C.4.4.1 Portable ALPR Camera Installation

Extreme accuracy, attention to detail, and rapid installation are hallmarks of our implementation projects. As such, Rekor and our partners always anticipate that time will be of the essence with regard to final implementation. We take all critical steps to avoid scheduling delays and unexpected supply-chain issues. Rekor places pre-order holds on an inventory of systems necessary to complete installs for awarded projects. Upon notification of award, Rekor will quickly complete the notification of the order to our suppliers and be able to get all the equipment in a matter of weeks.

For Rekor's portable-camera installations, we offer several options for installation. Whether on existing customer infrastructure, or mounted in a manner comingled with other existing utility infrastructure, we accommodate a wide variety of installation options, including AC or solar-powered alternatives. We can provide, where necessary, a completely "off-grid" solution powered by solar and wireless 3G/4G transmission. Where feasible, from a time and cost standpoint, we will use AC power (generally, when the source is within 20 feet of the pole and within the jurisdictional easement).

All systems offered by Rekor have the ability for their sole power source to be solar, further reducing overall operating costs. Using "green" technology systems, Rekor has turned to a more responsible and energy efficient solar-based solution.

Where power infrastructure is available, we can accomplish full installations in an extremely short timeframe due to flexible pole placement and less burden with respect to permitting and power or communication pulls. It is important to keep in mind that these can be, at times, major factors affecting most vendors' ability to move rapidly toward full implementation.

Our Watchman application provides the end-user with the capability to configure each camera manually (by editing its configuration files) or remotely from the Watchman back-office. We provide step-by-step instructions to assist customers with configuring their applications to fit their specific needs.

All work will be conducted to provide the least possible interference to the activities of the responsible parties, commercial traffic, and public use of roadways. We will supply the appropriate traffic signage and gain all required permissions for access to adjacent properties, as required, to maintain safe, continuous vehicular and pedestrian traffic through all installation areas. All work will be conducted within the public right-of-way. We will protect adjacent public and private property from damage. Where damage occurs, we will restore the damaged area to a condition equivalent to the pre-construction condition before continuing to the next installation location. All ALPR equipment will be installed in the right-of-way with no encroachments onto private properties.

To ensure maximum installation efficiency and accuracy, Rekor employs a systematic and well documented approach to executing implementation projects. Our engineering and contractor teams and our internal personnel adhere to the execution plan in order to complete the installation on time and on budget.

C.4.4.2 Mobile In-Vehicle ALPR Camera Installation

Rekor offers a completely portable in-vehicle mounted, mobile ALPR solution that can be optionally fully vehicle-integrated (embedded) in the vehicle at the customer's request. Through our many years of servicing police departments and installing other available ALPR systems, we have listened to their concerns and have developed, tested and implemented a portable camera solution that addresses the many draw-backs experienced by agencies using mobile ALPR cameras mounted on the exterior of the vehicle. We have created an innovative two (2) camera solution that features our state-of-the-art Watchman AI mobile application while accentuating portability and ease-of-use.

Due to its portability, "installation" of the Rekor Finder is virtually unnecessary. Installation requires a mere attachment of two (2) camera sensors to the interior of the front and plugging the power cord into the vehicle's 12-volt outlet. Wiring is tucked neatly inside the vehicle's 'A' and 'C' pillars as the control units are affixed under the rear deck in the trunk. At the client's option, we can also permanently mount Finder units within any vehicle.



Figure 31 Forward-looking in-vehicle cameras

Rekor will provide all cables, mounting components, and hardware required for Installation. If applicable, all System equipment shall be shipped to the Sheriff's Department at no additional charge.

C.4.4.3 Mobile Trailer-Mounted ALPR Camera Installation

Our trailers are manufactured on an OEM-basis by nationally recognized and DOT certified trailer manufacturer and will be shipped to directly to the Sheriff's Department. They will then be configured by Rekor personnel or an approved local contractor depending on timing and purchase volume, in full coordination with the Sheriff's Department. While we typically have trailers in inventory, our manufacturer currently has a six-week lead time, which can vary based upon demand.

C.5 Customer Support

C.5.1 The Contractor shall provide technical advice and sales support within 72 business hours.

In addition to providing maintenance and support services located in the United States, our customer support center will be available during normal weekday business hours of 8 a.m. to 6 p.m. Eastern Time, excluding holidays. We also provide 24/7 monitoring and support to address

the needs of our West Coast customers, any critical problems that may arise outside of business hours.

C.6 Training

C.6.1 The County reserves the right to request up to eight (8) hours of training at a San Diego County Sheriff's Department facility within 30 days of delivery at no additional charge. This is in addition to the requirement set forth in 4.3.

Rekor will provide initial and ongoing training for our products and services, including all hardware, peripherals, and Watchman software. The initial training sessions can be held at either the Sheriff's Department facility or by video conference, at the Sheriff's Department's sole discretion. The initial training sessions combine classroom instruction with hands-on application, equipping trainees with practical knowledge and real-world experience.

Rekor offers various training types, including system administrator, equipment operation, web-portal navigation, web-portal operation, managing hotlist, and reporting. Ongoing training can be provided on a monthly, scheduled basis or as needed. Each training level will be tailored to the specific audience, specific job duties, and cover each component of the overall system. Training levels shall include but not be limited to: System Administrator; Account Administrator; Train the Trainer; and End-User Training.

Training sessions are typically 4-hour classes, however, Administrative training is typically comprised of two 4-hour classes.

C.7 Data Sharing

We do not facilitate or provide any sharing of customer data without express written permission. Rekor fully understands and commits to the ALPR program requirement that data obtained by the ALPR program is not to be shared externally without written authorization. Rekor adheres to the highest possible security protocols relative to safeguarding of customer data.

To supplement the cameras that we will install throughout San Diego County, we also have the ability to enhance the ALPR program in two additional ways:

1. Our "open architecture" system design described above is capable of ingesting ALPR reads from other third-party platforms, if the hosting agency is willing to share their data with the ALPR program. Thus, with Sheriff's Department's approval, we could

contact law enforcement agencies that have ALPR cameras, and ask if they would be willing to share their data, thereby increasing the number of vehicle reads. We are currently implementing this feature in two major projects in Collierville, Tennessee and Lauderhill, Florida. This option would apply to any agency regardless of which vendor operates the system, and assumes vendor compliance with the agency's request to share the data.

2. We are currently undergoing a wide-scale national expansion in our law enforcement channel and have established relationships with law enforcement agencies nationwide. All agencies we add with new Rekor cameras, or software on their current cameras, will be eligible and encouraged to opt into sharing data with the ALPR program, as the overall system cost could be fractionalized based on multi-agency participation.

C.8 System Scalability and Flexibility

C.8.1 System Scalability

Rekor provides an ALPR system that is infinitely scalable. Our system has this capability because of:

- **Edge-Based Processing** -- Our cameras are edge-based, meaning that video processing takes place at the ALPR camera, thereby reducing the need to transfer massive amounts of data.
- **Cellular Data Transfer** -- We use cellular communications and don't rely on the need to run hardwired data communications cables. All cameras store data locally for later transmission should communications be interrupted.
- **Remote Control** – Our cameras are remotely controlled and configured, thereby allowing for rapid configuration and firmware updates.
- **Automatic Monitoring** -- Our cameras are automatically monitored by a system that is designed to identify potential problems before they result in an equipment failure.
- **Easy and fast installation** – Our portable cameras typically take about 1-2 hours to install and configure.
- **Solar Powered** – We can power any of our portable cameras by solar power (all trailer-mounted cameras are solar powered), thereby eliminating the need for costly and time-consuming power infrastructure.

Our ALPR System is also configurable and its open design allows for customizable architecture designed to allow incremental changes in capacity and functionality.



C.8.2 Full Video Edge Processing for Speed and Scalability

Rather than being dependent on communications infrastructure, which can result in lost data in adverse conditions and/or limit expansion, Rekor processes data collected via the sensor network on the "edge" (at the camera) for a robust infinitely scalable solution and near real-time alerting. Certain competitors' systems that are entirely dependent on cloud computing are unable to create or retain ALPR reads, and thus lose a tremendous amount of critical data when communications are interrupted. Rekor's Edge systems do not miss any reads during a communications outage, and are automatically synced to the back-office once communication is restored.

Rekor understands that the Sheriff's Department will provide network resources used by the ALPR System. Because all of our cameras us full video edge processing, the data transmitted via cellular communications or over the Sheriff Office's infrastructure is negligible and would not negatively impact other Sheriff's Department systems.

C.8.3 System Flexibility

Rekor's system is flexible in its ability to work with and integrate data from other ALPR systems and to migrate. As more thoroughly discussed above, our Watchman system is an easy-to-use system that gives the user the ability to run a variety of reports and our staff is available to develop custom features needed by the Sheriff's Department.

Because our Watchman software is capable of operating on nearly any IP camera, the Sheriff's Department will have significant flexibility for expansion by leveraging existing camera infrastructure, and simply purchasing and deploying software licenses for those cameras.

C.9 Remote Monitoring of Equipment

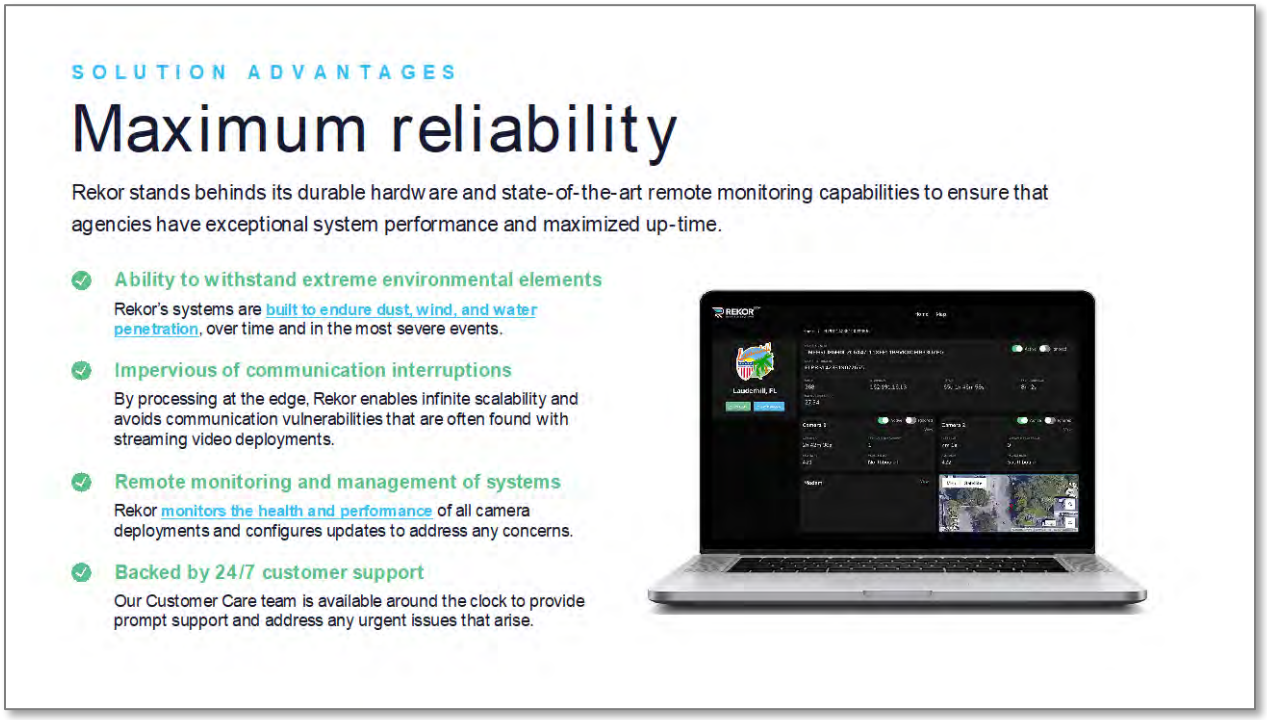


Figure 32 Through its state-of-the-art remote monitoring and round-the-clock support, Rekor offers clients proactive management of the sensor network to ensure up-time is maximized.

Rekor believes operational oversite and monitoring of our deployed equipment and systems is critical to ensuring ALPR systems meets our client's mission-critical objectives. With this in mind, we developed Rekor Vision. This continuous monitoring application leverages AWS GovCloud to send and receive MQTT messages (MQTT is an extremely lightweight publish/subscribe messaging transport that is ideal for connecting remote devices with a small code footprint and minimal network bandwidth) through web socket tunnels directly to our edge-based ALPR cameras. This bi-directional communication allows for receiving live operation data from every ALPR camera as well as pushing updates and configurations to ALPR cameras.

Rekor Vision allows our team to control all ALPR camera configurations remotely via groups that makes sense for our clients. From defining small groups to test updates, to single-click fleet-wide updates, we handle all stages of software deployment, firmware updates and configuration management.

Rekor Vision also allows technical support and maintenance personnel to detect any read anomalies or system issues (low battery, communication outage) and receive alerts in real time whenever a device is not operating efficiently or inactive. Through this monitoring and alerting, technicians can proactively address any issues to ensure system performance optimization.

The video link below provides a 3.5-minute user experience of the Ops Vision dashboard detailing how we monitor the status and health of all deployed devices. Some of the dashboard data include:

- Uptime
- battery voltage
- “heartbeat”
- last ALPR read
- number of reads in the last hour
- Communications information
- A real-time camera view
- CPU fan RPM
- CPU temperature
- Battery current
- Panel voltage
- CPU utilization
- Current load.
- Video: Rekor’s Remote Monitoring

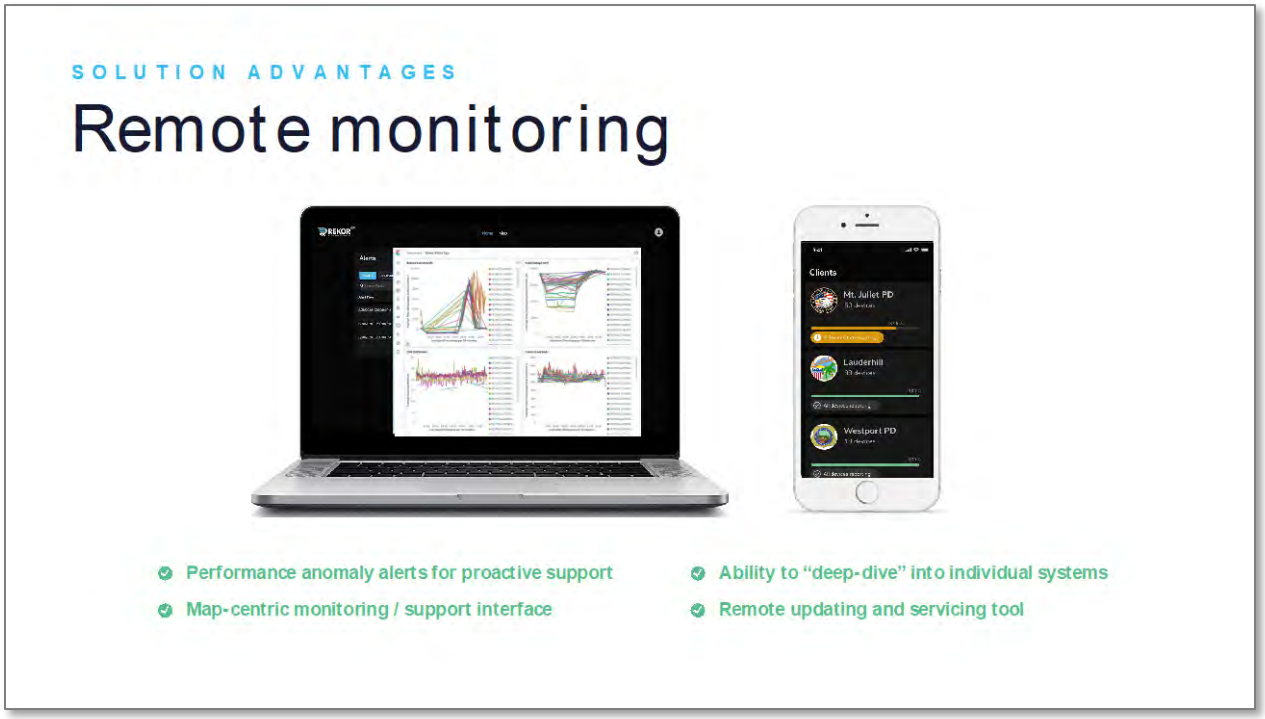


Figure 33 Rekor monitors and receives alerts on key performance indicators to more efficiently address issues or service needs.

C.10 Maintenance and Support

C.10.1 Equipment Maintenance

Due to the limited downtime, efficient operation, and remote maintenance capabilities of our systems, technical and maintenance support requires minimal resources. Nonetheless, we also will deploy support whenever needed. Our attention to equipment uptime, using our comprehensive Rekor Vision monitoring application (further described in Section C.9), is a key differentiator versus our competitors.

Rekor's systems are all modular and specifically designed for rapid, easy in-field servicing. Additionally, we only use best-in-class manufactured hardware and peripherals, so each component is readily available. We maintain sufficient spare parts inventory locally to ensure timely support; however, the consistency and reliability of our Edge systems translates to minimal on-site maintenance or repair.

C.10.2 Equipment Reliability

All proposed equipment supplied by Rekor is optimized to meet the demands for reliable high-definition surveillance cameras with best-in-class hardware and software components for peak performance. To further safeguard system uptime, the products offered by Rekor can include a full turnkey program management package, where Rekor literally installs, monitors, maintains, and optimizes all software and in-field hardware on behalf of the client.

C.10.3 24/7 Support

In addition to providing maintenance and support services located in the United States, our customer support center will be available during normal weekday business hours of 8 a.m. to 6 p.m. Eastern Time, excluding holidays. We also provide 24/7 monitoring and support to address any critical problems that may arise outside of business hours.

C.11 Rekor Current Reference Projects

C.11.1 City of Lauderhill, FL Police Department

Client	City of Lauderhill, FL Police Department
Project Name	Lauderhill ALPR Program
Description/Scope of Work	Supply, install, maintain and warranty solar-powered ALPR systems to include poles, processors, telecommunications, storage and backend application. Assist with hotlist and other external connections, programming and systems training.
Completion Date	95% complete; "Live" system has already been handed over to Lauderhill. Expected final completion in November 2020
Number of Locations	73 locations; 101 Edge systems; 160 cameras;
Contact Name and Title	Doug Downs, City Director IT
Phone	954-730-3099
Email	ddowns@lauderhill-fl.gov

C.11.2 Town of Mount Juliet, TN Police Department

Client	Town of Mount Juliet, TN Police Department
Project Name	Mount Juliet ALPR Program
Description/Scope of Work	Supply, install, maintain and warranty AC and solar-powered ALPR systems to include poles, processors, telecommunications, storage and backend application. Assist with hotlist and other external connections, programming and systems training.
Completion Date	Completed October 23, 2020.
Number of Locations	39 locations
Contact Name and Title	Captain Tyler Chandler
Phone	615-754-2550
Email	tchandler@mtjuliet-tn.gov

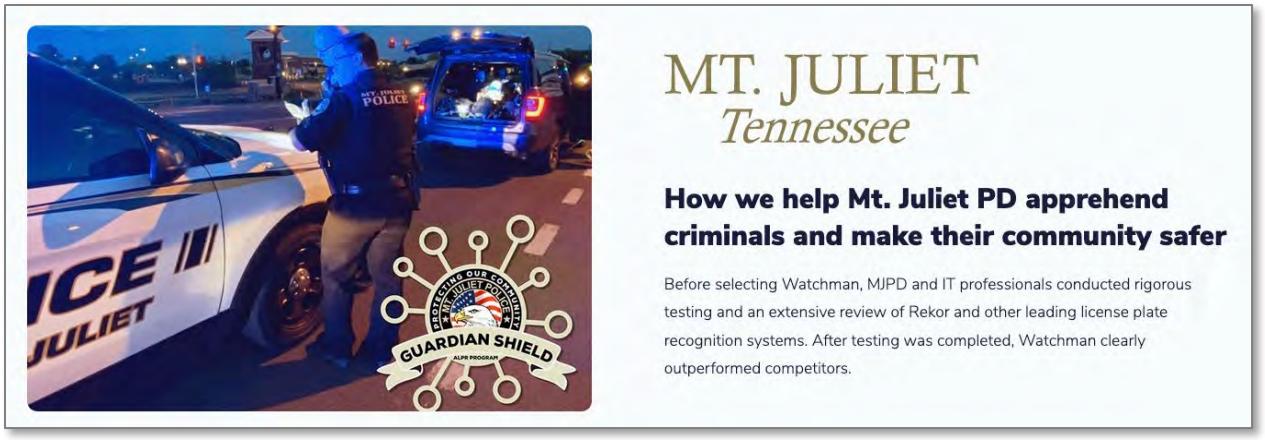


Figure 34 Click on the above image and see how Rekor is creating a safer community in Mt. Juliet.

> ***"Our number one priority is maintaining the safety of our community, and we are always looking for robust tools and technologies that can help us to do so. Rekor's Edge and Watchman vehicle recognition technology provided better results than its competition during our trial period."***
>
> ***Chief James Hambrick, MJPD***

C.12 Project Team

Rekor is organized on a functional basis to provide key expertise and leadership within each of our major areas of operation. For each of our implementations, we identify a dedicated implementation manager along with key individuals from each functional area to provide direct support to the implementation manager. These individuals have ultimate accountability to the implementation manager in relation to the specific programs to which they are assigned.

The San Diego County Sheriff's Department ALPR implementation would be managed by David Tindall, our Rekor's VP of Implementation, who brings 15 years of ALPR program implementation experience. He will be the primary contact for all aspects of the ALPR program, including business rules, implementation, engineering, field support, configuration management, quality control, customer service, maintenance, and accounting. Mr. Tindall will have full authority on behalf of Rekor for all decisions related to program implementation and support.

Although we prefer to designate a single point of contact for simplicity and accountability, we offer direct access as requested by our clients to program support personnel as well as management personnel, including our officers.

Issue escalation beyond the program manager, although rarely required, will involve the following management personnel:

- VP of Operations – Brad Schaeffer
- VP of Program Development – Maurice Nelson
- Chief Technology Officer – Chris Kadoch
- Chief Operating Officer – Rod Hillman

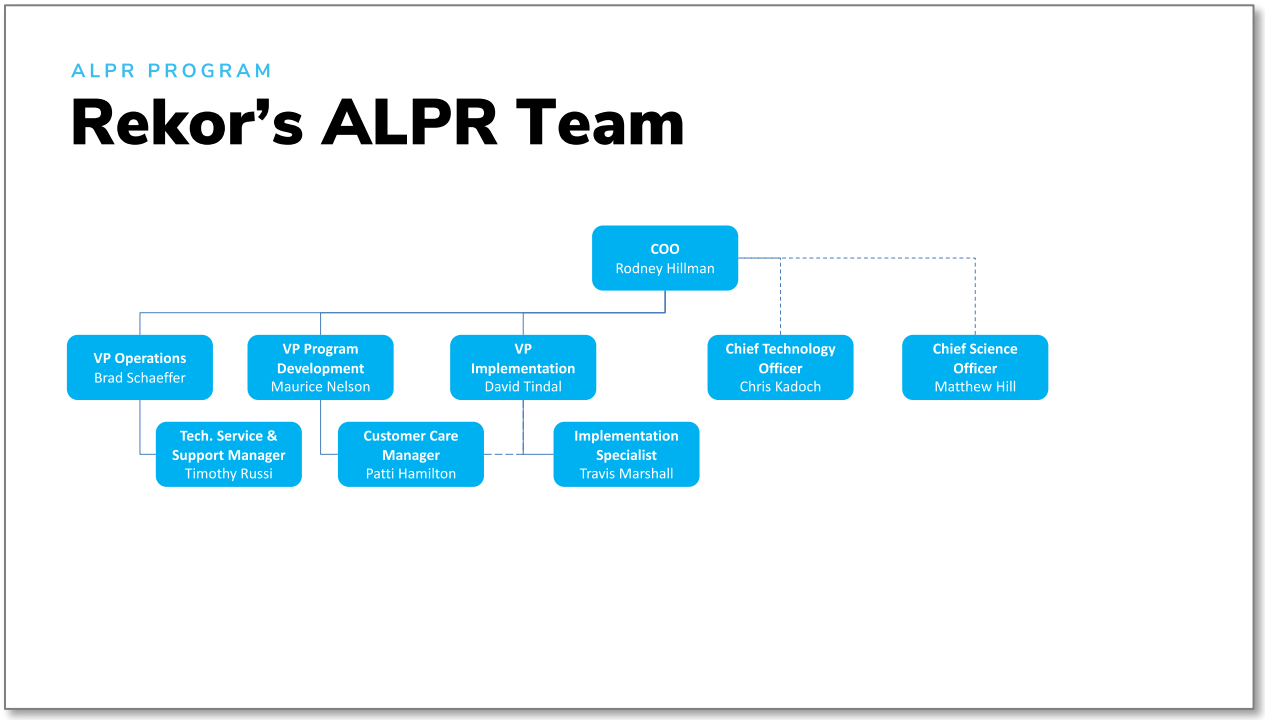


Figure 35 Rekor's ALPR Program Team, showing key functional leadership.

Brief biographies of management and operational personnel that will support the ALPR program are presented below.

C.12.1 Project Team Bios

C.12.1.1 Program Management – David Tindall, VP Implementation

Mr. Tindall is a proven leader with more than 15 years of experience in public safety, pre-sales engineering, and project management. He has extensive experience working with AI and video camera technologies, including his previous role at AnyVision and prior roles with WatchGuard Video and L-3 Communications, where he managed and executed millions of dollars' worth of public safety projects. Mr. Tindall has a Bachelor of Arts in Radio/Television from the University of Central Florida.



C.12.1.2 Operations – Brad Schaeffer, VP of Operations

Mr. Schaeffer has been with Rekor since 2012 and serves as our VP of Operations. He oversees all aspects of program implementation and operations including field support, citation/notification processing, customer service, collections, and adjudication support. Mr. Schaeffer has personally managed multiple speed enforcement programs and he was instrumental in implementing one of the largest ALPR programs in Mexico. Mr. Schaeffer holds a Bachelor of Science in Business Administration from York College of Pennsylvania and is working towards his MBA from the University of Maryland.

C.12.1.3 Program Management – Patti Hamilton, Customer Care Manager

Ms. Hamilton manages Rekor's ALPR programs. She has extensive experience in both implementation and ongoing program oversight and is able to draw upon internal resources, both technical and administrative, to accomplish complete client satisfaction. She has over 20 years' experience in training, implementing, supervising, and managing citation processing and permit management back-office operations, vendors, and customer service centers for city, county and state highway administration programs.

C.12.1.4 Technical Support & Maintenance – Timothy Russi, Technical Service & Support Manager

Mr. Russi is one of our customer service and technical support professionals responsible for providing hardware and cloud products support and building and managing support teams for our clients. In this role, he responsible for managing all field work orders, ensuring timely resolution and SLA compliance. Mr. Russi has over 30 years of technical customer support experience. He holds a Master of Arts in Communications from the New York Institute of Technology and Bachelor of Science in Media Studies / Communications from Sacred Heart University.

C.12.2 Rekor Management Team Bios

C.12.2.1 Chris Kadoch, Chief Technology Officer

Mr. Kadoch has served as our Chief Technology Officer since February 2020. Prior to joining Rekor, he served for 12 years as Vice President and Chief Scientist at L3 Communications and was CTO of an APAC AI/video analytics company. Most recently Mr. Kadoch provided strategic guidance to Axon Enterprises. Mr. Kadoch holds Bachelor of Science degrees in physics and mathematics from San Jose State University and pursued graduate studies in optics and physics at Michigan Technology University, Georgia Institute of Technology and San Jose State University. He also holds several patents, two of which are related ALPR and high-speed communications.

C.12.2.2 Rodney Hillman, Chief Operating Officer

Mr. Hillman has served as our Chief Operating Officer since May 2019. From December 2013 to May 2019, Mr. Hillman served as President and Chief Operating Officer of Rekor Recognition Systems. Prior to joining Rekor, Mr. Hillman served in various executive level capacities in other companies and industries. From 2003-2012 he held the positions of Chief Operating Officer and Chief Financial Officer at Game Trading Technologies, Inc. (GTTI), a publicly traded company that he co-founded. Prior to his tenure at GTTI, Mr. Hillman was Vice President of Product Development at InterAct Accessories, Inc. and held various management positions at both Baltimore Gas & Electric and Constellation Energy Group. Mr. Hillman holds a Master of Science in Finance from Loyola College in Baltimore, Maryland, an MBA from the University of Baltimore, and a Bachelor of Science in Electrical and Computer Engineering from The Johns Hopkins University.

D. Offer of Value-Added Products and/or Services

D.1 Rekor Smartphone Mobile Application

Rekor recently announced Rekor Go, a revolutionary new mobile application that will bring the power of accurate ALPR to a broader group of users. ***The app will enable a cell phone camera to be used as a handheld ALPR tool, capturing images and recognizing license plates and vehicles on the edge using the cell phone's processing capabilities.*** The app processes both still photos and streaming video and permits both stationary users and users in motion to capture and identify plates.



Figure 36 Example of Rekor Go finding a hotlist match.

Unlike some other cell phone-based ALPR applications, Rekor Go is the first in the world to offer full processing on the edge (enabling instant responsivity and operability in low/no connected environments), using the same technology and advantages of our Edge and Finder systems.

As a value-added service, Rekor offers to integrate Rekor Go with the Sheriff's Department's ALPR program system for law enforcement use with their mobile devices (one Rekor Go license issued for each every five (5) Watchman licenses or hardware systems purchased) as a supplemental and flexible means to read additional license plates. Potential law enforcement use cases include parking lot patrol, event management, and crime scene scanning.

D.2 Rekor One – Multipurpose Solution

The Rekor One platform, as described above in The Sectors We Serve, is representative of our commitment to create a safer future for everyone by enabling AI-driven decisions for the betterment of states, cities, and communities.

Rekor has developed meaningful agency relationships which have helped to inform our technology development roadmap and Rekor One as single source of roadway intelligence for government entities that can fractionalize costs by leveraging and expanding sensor infrastructure to maintain a safe and smart roadway network. ALPR cameras are not limited to law enforcement applications, and can also serve useful purposes to a variety of state agencies beyond law enforcement including the Department of Transportation, the Department of Revenue, and the Department of Commerce and Insurance.

In addition to enhancing roadway and community safety, policing, and traffic monitoring and management, Rekor One, also includes the ability to automatically enforce motor vehicle insurance laws by identifying vehicles being operated without insurance and offering their owners to enter into a “diversion” program that reduces potential punitive action, if the owner pays a lesser fee and maintains insurance going forward. The added benefits of such a diversion program are that it can reduce the number of uninsured vehicles on the road, reduce insurance premiums, increase state taxes from insurance premiums, and generate revenue for states.

Because our system can evolve with hardware technology improvements and is not dependent on hardware that becomes obsolete, it has the capability to provide long-term and new solutions for clients.

If the Sheriff’s Department is interested in evaluating any features of Rekor One, we can make them available for testing as a pre-release beta.



Figure 37 Creating value through improved infrastructure, increased safety and generating revenue.

E. Appendix

E.1 Rekor Edge 300 Specifications Sheet

REKOR
AI DRIVEN DECISIONS

Rekor Edge 300

FIXED VEHICLE & LICENSE PLATE RECOGNITION

Rekor Edge is a complete vehicle recognition solution that seamlessly captures and processes vehicle data. Designed in a sleek, durable enclosure, Rekor Edge can be easily mounted to a building or pole and includes a full repair/replace warranty with no additional service fee.



FEATURES AND FUNCTIONS

- Edge recognition includes plate read, vehicle characteristics, direction of travel, vehicle count, and traffic density
- 3 lanes, 300 ft max range*
- 120 mph max capture speed*
- Accurate in day/night and all weather conditions
- Outdoor rated, IP67, NEMA4
- 4G LTE, Wi-Fi, Ethernet ready
- User dashboard available in the cloud or on-premise
- Optional solar power

*Solutions available for extreme ranges and lane coverage

Rekor Edge 300 | Fixed Vehicle & License Plate Recognition

rekor.ai

REKOR EDGE SPECIFICATIONS

Recommended usage	
Rekor Edge 300:	Highways, Primary Roads

Coverage*	
Lane coverage:	3 - 4 lanes max
Distance:	300 ft max
Speed:	120 mph max

Camera specifications	
Camera resolution:	1920 x 1080 HDTV 1080p
Image compression:	JPEG
Video streaming:	H.264
Network security:	Password, IP address filtering
IR illumination:	Optimized IR w/power efficient, long-life 850 nm IR LED's
Plate search:	Automated; Records, Edge, Account, and Hotlist Ingestion & Management

Communications	
Communications:	Ethernet, Cellular Modem
Cellular modem:	3G, 4G LTE MIMO
Cellular service:	Not included
GPS:	Included
Security:	SSL over websockets & HTTPs

Mount & power	
Mounting style:	Surface, Pole
Mounting pole:	Optional
Input voltage range:	9 VDC - 48 VDC
Power consumption:	Average: 18W, Max: 22W
Solar power:	Optional

Environmental specifications	
Enclosure:	Diecast aluminum, IP67
Operational temperature:	-22°F to 131°F
Storage temperature:	-40°F to 149°F
Warranty:	Full repair/replace

*Coverage up to. Actual performance may vary.



REKOR™
AI DRIVEN DECISIONS

Ready to get started?
Contact sales@rekor.ai

Rekor Systems

7172 Columbia Gateway Dr. Suite 400
Columbia, MD 21046

www.rekor.ai
info@rekor.ai
410.762.0800

E.2 Rekor Finder In-Vehicle Specification Sheet

REKOR
AI DRIVEN DECISIONS

Rekor Finder



MOBILE LICENSE PLATE & VEHICLE RECOGNITION

Rekor Finder accurately identifies license plates and vehicles in real-time at high rates of speed and extreme viewing angles. The unique interior mount design is portable to any vehicle in the fleet, allowing for full-featured LPR wherever it is needed.

FEATURES AND FUNCTIONS

- 1280x720 HD Video at 25/30 FPS
- 50 ft capture distance @ 1MP resolution
- Closing speed of up to 120 mph
- 512 GB of M.2 SSD storage
- 1.5 Teraflop NVIDIA GPU
- 4G LTE, Wi-Fi, and GPS network connectivity
- Low-profile, two camera interior mount
- Rekor Watchman software included
- Full repair/replace warranty

Rekor Finder | Mobile License Plate & Vehicle Recognition

rekor.ai

REKOR FINDER SPECIFICATIONS

Technical specifications

ALPR image capture range:	50 feet
Closing speed:	Up to 120 mph
Video resolution:	720p HD Video
Video capture rate:	25/30 FPS
Video compression format:	MPEG-4, H.264
Memory storage capacity:	512GB M.2 SSD
GPU:	1.5 teraflop NVIDIA

Electrical specifications

Input voltage range:	10 - 15 V DC
Power consumption:	20W
Operation duration:	Continuous charge

External components

Network connectivity:	4G LTE, Wi-Fi, GPS
Data comm. components:	USB3, Ethernet Ports

Mechanical specifications

Length:	9.5 inches
Width:	4 inches
Height:	2.5 inches
Weight:	3.4 pounds
Enclosure:	Anodized aluminum

Environmental specifications

Operational temperature:	-20°C to 60°C
Portability:	Mobile unit (5 min. setup)
Durability:	Impact resistant



REKOR™
AI DRIVEN DECISIONS

Ready to get started?
Contact sales@rekor.ai

Rekor Systems

7172 Columbia Gateway Dr. Suite 400
Columbia, MD 21046

www.rekor.ai
info@rekor.ai
410.762.0800

E.3 Mobile ALPR Speed Trailer Camera

REKOR
AI DRIVEN DECISIONS

Rekor ALPR Speed Trailer



PORTABLE ALPR AND SPEED DETECTION

Combine the power of Rekor's automated vehicle and license plate recognition (ALPR) technology with radar-speed detection in Rekor's ALPR Speed Trailer. The trailer features one of the largest portable speed sign available today. With standard speed display and customizable alerts and notifications, the trailer allows you to strategically place the sign in dangerous, high-risk areas to improve motorist and pedestrian safety. By adding ALPR technology, you can cover major city or localized access points for wanted vehicles, receive AMBER and Silver alerts, and accelerate investigations.

FEATURES AND FUNCTIONS

INTEGRATED WITH ACCURATE ALPR

- Integrated Rekor AI-driven ALPR technology
- Advanced vehicle recognition with plate, make, type, color
- Accurate in day/night and all-weather conditions
- Up to 120 mph capture speed

HIGH QUALITY AND EXTREMELY PORTABLE

- DOT approved
- Heavy duty security locks
- Highway and residential use
- Compact, easily portable with a 5-minute setup

FLEXIBLE COMMUNICATIONS AND POWER OPTIONS

- FCC/CE compliant Radar captures speeds up to 120mph
- 3G/4G FirstNet ready wireless modem
- Integrated GPS
- 300w solar array and up to 15-day battery backup

Rekor ALPR Speed Trailer | Portable ALPR and Speed Detection

rekor.ai

QUICK AND FLEXIBLE SETUP

- Portable system is easy to transport and deploy
- Changeable speed numbers
- Customizable speed limit setting and flashing excessive-speed message
- Localization options for speed units, mph or kmh
- Heavy-duty hand-winch with safety brake raises regulatory sign for deployment
- Locking device holds signs frame in place while operating and during transport

OPERATION READY

- Extra-large electronic speed display with full matrix of LEDs and up to three digits
- Lenses and shades over LEDs produce superior visibility
- Display flashes when a vehicle exceeds speed limit
- Radar unit is CE compliant, FCC approved
- See-through design puts pedestrians and road workers in view

DURABLE DESIGN

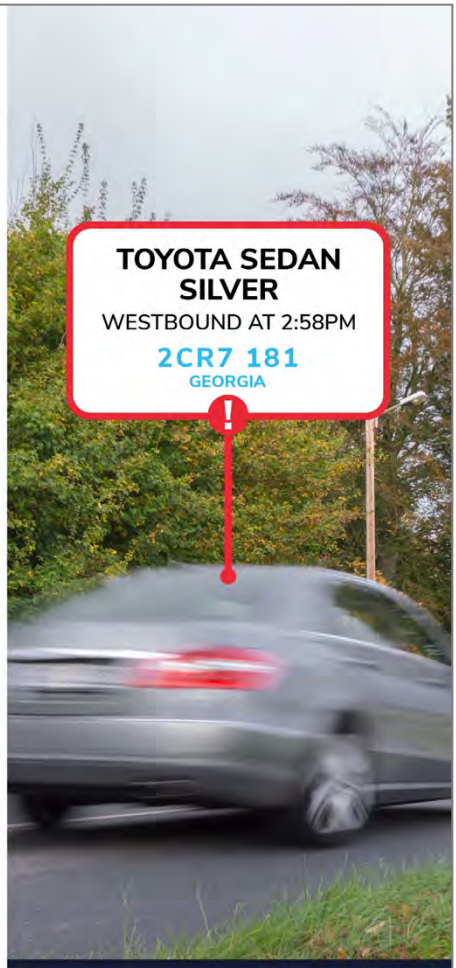
- DOT approved materials and design
- Durable powder-coat finish
- Heavy-duty fenders
- IP67-rated lockable control box

POWER SYSTEM

- Energy-efficient operation for extended run times
- Battery powered with solar or commercial charging
- Automatic charging system shuts down when batteries are fully charged, preventing damage
- Cooling fan protects battery charger from overheating
- Battery box can be locked to prevent unauthorized access

Compact Trailer	
Deployed footprint (LxW):	106x61 in (268x154 cm)
Operating height:	123 in (312 cm)
Travel height:	91 in (231 cm)
Display cabinet size (WxH*):	26x38 in (91x95 cm)
Speed display font size:	26 in (66 cm)
Speed limit sign size (WxH):	24x30 in (61x76 cm)
Weight, approx:	870 lb (395 kg)
Power:	Batteries with solar or commercial recharging

*Height includes Your Speed sign



REKOR
AI DRIVEN DECISIONS

Ready to get started?
Contact sales@rekor.ai

Rekor Systems

7172 Columbia Gateway Dr. Suite 400
Columbia, MD 21046

www.rekor.ai
info@rekor.ai
410.762.0800



REKOR™
AI DRIVEN DECISIONS

Rekor Recognition Systems
7172 Columbia Gateway Dr. Suite 400
Columbia, MD 21046
www.rekor.ai info@rekor.ai 410.762.0800

Next

Bid

UTILITY

REQUEST FOR BIDS

RFB No. 10493

Sheriff's Department License Plate Readers

ORIGINAL SUBMITTAL
One (1) Electronic Copy Original submitted via email to:
cosd_procurement@sdcounty.ca.gov

Closing Date and Time:
November 5, 2020 at 11:00 A.M. PT

County of San Diego
Department of Purchasing and Contracting
5560 Overland Avenue, Suite 270
San Diego, CA 92123-1204

ATTN: Punnita Dinmuong, Assistant Procurement Specialist
Punnita.dinmuong@sdcounty.ca.gov
(858) 505-6367

Utility Associates, Inc.

County of San Diego, California
Request for Bids (RFB) # 10493 for Sheriff's Department License Plate Readers

Submittal: *One (1) Electronic Copy Original submitted via email to cosd_procurement@sdcounty.ca.gov*

Table of Contents

Before Section 1: Cover Letter

Section 1: Required Forms

- Cover Page
- Representations and Certifications Page
- Section C; Exhibit C Pricing Schedule
- Non-Disclosure Indemnification Form - *Not Included, Not Applicable*
- W-9 Form for Utility Associates, Inc.

Section 2: Company Qualifications and Experience

- Company Profile and Experience
- *Flyer – Utility Named Innovation Challenge Award Winner by AWS (2016-2019)*
- Project Team for San Diego County Sheriff's Department

Section 3: Approach to Technology

- Summary of the Technical Approach Narrative of the RocketIoT™ ALPR Solution
- Table of Responses to Specifications Section C: Exhibit A Statement of Work
- *Flyer - Five ALPR 'Must Haves'*
- Product Data Sheet for the RocketIoT™ ALPR Solution
- AVaiLWeb™ Digital Evidence Management Platform, and SMART REDACTION™
- *Flyer – Features of RocketIoT ALPR Paired with the RocketIoT™ In-Car Camera*
- Product Data Sheet for the RocketIoT™ In-Car Camera System

Section 4: Appendix - Procurement Information

- Installation Operations Guide for RocketIoT-XLE ALPR
- Summary: Warranties, Terms & Conditions, Software as a Service (SaaS) Agreement
- Summary Sheet: Data Security Documentation
- Summary Sheet: Utility CJIS Compliance, and CJIS Compliance in the Cloud

UTILITY

Punnita Dinmuong, Assistant Procurement Specialist
County of San Diego
Department of Purchasing and Contracting
5560 Overland Avenue, Suite 270
San Diego, CA 92123-1204
punnita.dinmuong@sdcounty.ca.gov
(858) 505-6367

November 4, 2020

Subject: Request for Bids (RFB #10493) for Sheriff's Department License Plate Readers

On behalf of Utility Associates, Inc., thank you for the opportunity to present our RocketIoT Advanced LPR license plate reader camera system technology to the County of San Diego and the San Diego County Sheriff's Department. Utility's RocketIoT ALPR™ technology is a partnership with Sony Corporation, and is installed in fixed stationary applications and in-vehicle applications for customers across the US. Utility is an Amazon Web Services (AWS) City on a Cloud Innovation Challenge award winner (2016-2019), and our Smart RocketIoT ALPR™ is the most advanced license plate reader solution in the industry.

Utility's technology model is not reliant upon the Vigilant Learn cloud platform, and instead drives LPR using Artificial Intelligence (AI) at-the-edge, and real-time connectivity to Hot Lists from State, local and Federal data sources. The RocketIoT ALPR™ features highly sophisticated optical technology and machine learning algorithms to improve accuracy and efficiency.

The RocketIoT ALPR™ provides unique benefits to the San Diego County Sheriff's Department:

- **Intelligent.** Unlike traditional LPR systems, Utility's RocketIoT ALPR™ is powered by artificial intelligence (AI) and a new ability to read license plates at high speeds and through windshields - all while comparing data at-the-edge. In both fixed stationary and in-vehicle applications, Smart ALPR runs passively the background throughout an officer's patrol shift allowing **unknown threats to become known in real-time**.

- **Force Multiplier.** ALPR provides greater efficiency for the patrol officer which translates to increased productivity for your agency. ALPR allows officers to focus on their job functions while patrolling as it leverages AI and the total system to maximize the officer's effectiveness, safety and situational awareness.

Because the technology does not depend upon legacy proprietary platforms, it is designed to be cost-effective, allowing Departments to extend LPR to more fixed stationary applications, and to more vehicles, for greater coverage and officer safety in performance of their duties. Beyond its cost-effective aspects, RocketIoT ALPR™ technology model is designed to focus advanced AI capabilities to promote officer safety and real-time connectivity in these ways:

- **Connected.** RocketIoT ALPR™ and AVaiLWeb™ provide officers with **total system connectivity** directly to the AWS GovCloud for real-time access to Federal, State and local databases for purposes of automatically searching for hotlisted vehicles.

- **Alerts.** Policing our communities today has become more increasingly dangerous for our officers on patrol and as a result, increased officer safety measures are

paramount. **ALPR Alerts** are automated and connected to the Department by Utility's AVaiLWeb™ ecosystem. Dispatch, supervisors and nearby officers can receive real-time alerts when a patrol officer receives an ALPR Alert of a hotlisted vehicle.

- **Automatic Updates.** As a smart device, Utility's RocketIoT ALPR™ has policy-based Smart Recording for automated and independent operation, asynchronous, over-the-air (OTA) updates occur in the background, without effort by the Department, all the while updating the same device.
- **Pathway to Future Integrations.** Utility's RocketIoT ALPR™ is capable of integrating with RMS and CAD , where it can create an Action Zone for High Priority Calls, and can make them visible on the AVaiLWeb™ video management system live map. The RocketIoT ALPR™ can ingest other digital data, and is compatible and interoperable with the entire ecosystem of Utility's automatic, policy based mobile video recording systems, including our RocketIoT™ in-vehicle DVR/router (a FirstNet Certified device) and our interview room camera system. This enables officers to focus on policing instead of video equipment.

Utility's RocketIoT ALPR™ with AVaiLWeb™ is provided as a System as a Service (SaaS) subscription. The solution does not require user licenses, and an active SaaS subscription allows access by authorized personnel of the San Diego County Sheriff's Department, including prosecutors, and automatically supports unlimited concurrent logins.

The RocketIoT ALPR™ is CJIS-compliant, Made in the USA, and includes 24/7/365 support from Utility's headquarters in Decatur, Georgia in Metropolitan Atlanta, and the Sony Corporation in Southern California.

Taken together, Utility's mobile license plate reader, digital evidence management, and video capture solutions are the most advanced technology for law enforcement today. Utility's RocketIoT ALPR™ allows today's efficiency-focused law enforcement leaders to use this new technology to leverage their budgeted resources to increase safety and LPR coverage.

We look forward to working with the County of San Diego, and the San Diego County Sheriff's Department to make your License Plate Readers project a resounding success!

Sincerely,

Michael Nark, President and Chief Executive Officer,
Utility Associates, Inc.
mnark@utility.com
404-816-0300 office, or 800-597-4707 toll free

COUNTY OF SAN DIEGO - REQUEST FOR BIDS (RFB # 10493)
SHERIFF'S DEPARTMENT
LICENSE PLATE READERS
SECTION A: COVER PAGE (P&C 600 FORM)

COUNTY OF SAN DIEGO
SECTION A-P&C 600 FORM
This is not an order

Issued: October 22, 2020

MAIL OR DELIVER TO:
COUNTY OF SAN DIEGO, RFB NO. 10493
DEPARTMENT OF PURCHASING & CONTRACTING
5560 OVERLAND AVE., SUITE 270
SAN DIEGO, CA 92123

AWARD WILL BE MADE TO THE LOWEST RESPONSIVE, RESPONSIBLE BIDDER BASED ON
[ ] ALL OR NONE
[ ] EACH LOT
[X] TOTAL PRICE
[ ] OTHER (SEE PRICING SCHEDULE)

UNSPSC commodity code: 461716.0000

FOR INFORMATION, PLEASE CONTACT:
PUNNITA DINMUONG, ASSISTANT PROCUREMENT SPECIALIST
PUNNITA.DINMUONG@SDCOUNTY.CA.GOV

BID OPENING DATE: NOVEMBER 5, 2020
BIDS MUST BE RECEIVED AT THE ABOVE ADDRESS PRIOR TO 11:00 A.M. ON DATE OF BID OPENING.

PLEASE STATE YOUR LOWEST PRICE F.O.B. DESTINATION AND BRAND NAME OR TRADE NAME IF APPLICABLE.
(Please use typewriter or black ink)
YOUR ENVELOPE MUST INCLUDE RFB NO. 10493

DESCRIPTION

THE COUNTY OF SAN DIEGO (COUNTY), SHERIFF'S DEPARTMENT HAS A REQUIREMENT FOR LICENSE PLATE READERS IN ACCORDANCE WITH THE TERMS & CONDITIONS AND THE STATEMENT OF WORK REFLECTED HEREIN.

INITIAL TERM: DATE OF AWARD – OCTOBER 31, 2021
1ST OPTION YEAR: NOVEMBER 1, 2021 – OCTOBER 31 2022
2ND OPTION YEAR: NOVEMBER 1, 2022 – OCTOBER 31, 2023

(NOTE: Dates for Inital Term Base Year, 1st Option Year, and 2nd Option Year were Modified by Addendum #3)

PRICING SUBMITTED IS TO REMAIN FIRM FIXED FOR THE TERM PERIOD IDENTIFIED ABOVE. ALL ITEMS WITHIN EACH TERM PERIOD MUST BE PRICED TO BE CONSIDERED RESPONSIVE. AWARD WILL BE MADE TO THE LOWEST RESPONSIVE, RESPONSIBLE OFFEROR BASED ON THE TOTAL PRICE. OFFEROR WHO SUBMITS THE LOW BID WILL BE DEEMED RESPONSIBLE BASED ON THE RESULTS OF THE PRE-AWARD SURVEY.

ARE YOU ABLE TO COMPLY WITH ALL ITEMS SPECIFIED WITHIN THE SCOPE OF WORK? YES X OR __NO

BIDDER ACKNOWLEDGES ADDENDUM NO. 1 X 2 X 3 X 4 X 5 [ ]

SUBJECT TO ACCEPTANCE WITHIN **90** DAYS

NAME AND ADDRESS OF BIDDER
Utility Associates, Inc.
STREET, CITY, STATE, ZIP
250 E. Ponce de Leon Avenue, Suite 700
Decatur, GA 30030
TELEPHONE: NUMBER (800) 597-4707 Toll Free, or 404-816-0300
FAX TELEPHONE: (404) 795-0525

E-MAIL: mnark@utility.com or proposals@utility.com

PAYMENT TERMS NET **30** DAYS OR ____ % ____ DAY

NAME AND TITLE OF PERSON AUTHORIZED TO SIGN OFFER:

11-4-2020
SIGNATURE OFFEROR DATE

PRINTED NAME: Michael Nark

PRINTED TITLE: President and CEO

NOTIFICATION OF AWARD

ACCEPTANCE AS TO ITEM(S) NUMBERED:

(VC NO.)

(THIS SECTION FOR COUNTY USE ONLY)
COUNTY OF SAN DIEGO
BY: _____ DATE: _____
JOHN M. PELLEGRINO, DIRECTOR
DEPT OF PURCHASING & CONTRACTING

TOTAL AMOUNT AWARD NO.
NAME AND TITLE OF CONTRACTING OFFICER

P&C 600 Form

REPRESENTATIONS AND CERTIFICATIONS

The following representations and certifications are to be completed, signed and returned with the offer (the term "offer" includes a bid, proposal, quote, statement of qualifications, or any other submission to provide goods and/or services).

1. BUSINESS TYPE

☒ For-profit ☐ Non-profit ☐ Government

2. INTERLOCKING DIRECTORATE

In accordance with Board of Supervisors Policy A-79, if Offeror is a non-profit and will be subcontracting with a related for-profit entity where an interlocking directorate, management or ownership relationship exists, Offeror must list all such entity(ies) on an attached separate sheet, and authorization must be sought from Board of Supervisors. If Offeror is a non-profit and does not submit such a list, Offeror certifies it has not entered into a subcontract relationship with a related for-profit entity.

List Attached? Yes ☐

3. BUSINESS REPRESENTATION

Offeror represents as a part of this offer the following information regarding the ownership, operation, and control of its business:

3.1. Are you a local business with a physical address within the County of San Diego? ☐ Yes ☒ No

3.2. Are you certified by the State of California as a:

☐ Disabled Veteran Business Enterprise(DVBE)
Certification #: _____

☐ Small Business Enterprise (SBE)
Certification #: _____

3.3. Are you certified by the U.S. Dept Of Veterans' Affairs as:

☐ Veteran Owned Small Business (VOSB)
Certification # _____

☐ Service Disabled Veteran Owned Small Business (SDVOSB)
Certification # _____

3.4. Estimated percentage of work in this offer to be performed or fulfilled locally (within the geographic boundaries of the County of San Diego): installation and training only, less than 10% %

4. DEBARMENT, SUSPENSION, AND RELATED MATTERS

4.1. Offeror certifies to the best of its knowledge that neither it nor any of its officers:

4.1.1. Are presently debarred, suspended, declared ineligible, or voluntarily excluded from covered transactions by any state, local, or federal department or agency.

4.1.2. Have within a three (3) year period preceding this agreement been convicted of or had a civil judgment rendered against them for commission of fraud or criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or contract under a public transaction; violation of federal or state antitrust statutes; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;

4.2. Except as allowed for in Section 4.2.5, Offeror hereby certifies to the best of its knowledge that neither it nor any of its officers:

4.2.1 Are presently indicted for or otherwise criminally or civilly charged by a government entity (federal, state, or local) with the commission of any of the offenses enumerated in paragraph 4.1.2 of this certification;

4.2.2 Have within a three (3) year period preceding this agreement had one or more public transactions (federal, state or local) terminated for cause or default;

4.2.3 Are presently the target or subject of any investigation, accusation or charges by any federal, state or local agency or law enforcement, licensing, certification, ethics, or compliance body;

4.2.4 Are proposed for debarment by any state, local, or federal department or agency.

4.2.5 If Offeror is unable to certify Sections 4.2.1, 4.2.2, 4.2.3, or 4.2.4, it certifies that it has disclosed and attached to this Representations and Certifications the reason(s) it cannot do so. The disclosure must include the Section(s), specific relevant facts including dates, contracts, individuals involved, status of actions, and any other relevant information that prevent it from making the requested certification(s). The County reserves the right to disqualify an Offeror based upon information disclosed.

Disclosure Attached? Yes ☐

5. RELATED WORK

Offeror certifies to the best of its knowledge that, other than as disclosed in an attached separate sheet, it and its proposed subcontractors, agents, and consultants have not previously contracted with the County to perform work on or related to this project (e.g. preparing related studies or recommendations, components of the statement of work, or plans and specifications).

Disclosure Attached? Yes ☐

6. CURRENT COST OR PRICING

Offeror certifies to the best of its knowledge that cost and/or pricing data submitted with this offer, or specifically identified by reference if actual submission of the data is impracticable, are accurate, complete, and current as of the date signed below.

7. INDEPENDENT PRICING

Offeror certifies that in relation to this offer:

7.1. The prices in this offer have been arrived at independently, without consultation, communication, or agreement, for the purpose of restricting competition, as to any matter relating to such prices with other offerors, with any competitors, or with any County employee(s) or consultant(s) involved in this or related procurements;

7.2. Unless otherwise required by law, the prices that have been quoted in this offer have not been knowingly disclosed by the Offeror and will not knowingly be disclosed by the Offeror prior to opening, in the case of a bid, or prior to award, in the case of a proposal, directly or indirectly to any other Offeror or to any competitor or with any County employee(s) or consultant(s) involved in this or related procurements; and

7.3. No attempt has been made or will be made by the Offeror to induce any other person or firm to submit or not to submit an offer for the purpose of restricting competition.

8. ADDITIONAL DISCLOSURES

Offeror shall report in writing to the County Department of Purchasing and Contracting within five business days of discovering or having any reason to suspect any change in status as certified in the preceding paragraphs. Upon County's request, Offeror shall provide additional information supporting Offeror's Representations and Certifications. Offeror's obligations under this Section 8 shall continue until Offeror is no longer under consideration for award of a contract, or until termination or expiration of any resulting contract(s).

CERTIFICATION

The information furnished in Paragraphs 1 through 8 and in the accompanying offer is certified to be factual and correct as of the date submitted and this certification is made under penalty of perjury under the laws of the State of California.

Name: Michael Nark Signature: _____

Title: President and CEO Date: 11-4-2020

Company/Organization: Utility Associates, Inc.

SUBMIT THIS FORM AS DIRECTED IN THE REQUEST FOR SOLICITATION DOCUMENTS OR WITH THE OFFER

Revised 05-02-17

BASE YEAR
DATE OF AWARD – OCTOBER 31, 2021

* NOTE: Revised by Addendum #2 to 'Base Year Date of Award - November 30, 2021'

DESCRIPTION	MFG & MODEL	ESTIMATED QUANTITY	UNIT PRICE	TOTAL
Mobile LPR 1 camera system, dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle	ALPR-H-4001-Mobile (4 Camera System)	4	$ 8,000.00	$ 32,000.00
Portable LPR 1 camera system, dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle	ALPR-H-4001-Port	10	$ 6,500.00	$ 65,000.00
LPR Camera Mounting Brackets for Light Bar	Included in ALPR-H-4001-Mobile	4	$ 0.00	$ 0.00
LPR Mounting for Portable system	Included in ALPR-H-4001-Port	10	$ 0.00	$ 0.00
LPR Processor	Included in ALPR	14	$ 0.00	$ 0.00
Modem	Included in ALPR	14	0.00	0.00
LPR Software	ALPR-S-4001	14	$ 2,500.00	$ 35,000.00
LPR Speed Trailer complete package	ALPR-H-4001-Trail	1	$ 13,000	$ 13,000.00
Start-up, configuration, and commissioning of LPR Systems at Sheriff's facility to include all expenses such as travel	ALPR-H-4001-SVCS Included in ALPR	14	$ 0.00	$ 0.00
Installation	ALPR-H-4001-INSTALL	14	$ 2,500.00	$ 35,000.00
Covert Installation in vehicle	ALPR-H-4001-COVERT	1	$ 600.00	$ 600.00
Installation "Kit", Includes all hardware, wiring and software for "do it yourself" standard installations (on poles & trailers)	ALPR-H-4001-KIT	5	$ 5,000.00	$ 25,000.00
Training	Included in ALPR	8	$ 0.00	$ 0.00
Shipping	Included in ALPR		0.00	$ 0.00
			BASE YEAR SUBTOTAL:	$ 205,600.00

**Quantities are estimates only and not guaranteed

OPTION YEAR 1
NOVEMBER 1, 2021 – OCTOBER 31, 2022

* NOTE: Revised by Addendum #2 to 'Option Year 1 December 1, 2021 - November 30, 2022'

DESCRIPTION	MFG & MODEL	ESTIMATED QUANTITY	UNIT PRICE	TOTAL
Mobile LPR 1 camera system, dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle	ALPR-H-4001-Mobile (4 Camera System) WARRANTY	4	$ 400.00	$ 1,600.00
Portable LPR 1 camera system, dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle	ALPR-H-4001-Port WARRANTY	10	$ 325.00	$ 3,250.00
LPR Camera Mounting Brackets for Light Bar		4	$	$
LPR Mounting for Portable system		10	$	$
LPR Processor		14	$	$
Modem		14	$	$
LPR Software	ALPR-S-4001	14	$ 2,500.00	$ 35,000.00
LPR Speed Trailer complete package	ALPR-H-4001-Trail WARRANTY	1	$ 650.00	$ 650.00
Start-up, configuration and commissioning of LPR Systems at Sheriff's facility to include all expenses such as travel		14	$	$
Installation		14	$	$
Covert Installation		1	$	$
Installation "Kit", Includes all hardware, wiring and software for do it yourself standard installations (on poles & trailers)		5	$	$
Training per hour	TRAIN	8	$ 80.00	$ 640.00
Shipping				$
			OPTION YEAR 1 SUBTOTAL:	$ 41,140.00

**Quantities are estimates only and not guaranteed

OPTION YEAR 2
NOVEMBER 1, 2022 – OCTOBER 31, 2023

* NOTE: Revised by Addendum #2 to 'Option Year 2 December 1, 2022 - November 30, 2023'

DESCRIPTION	MFG & MODEL	ESTIMATED QUANTITY	UNIT PRICE	TOTAL
Mobile LPR 1 camera system, dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle	ALPR-H-4001-Mobile (4 Camera System) WARRANTY	4	$ 400.00	$ 1,600.00
Portable LPR 1 camera system, dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle	ALPR-H-4001-Port WARRANTY	10	$ 325.00	$ 3,250.00
LPR Camera Mounting Brackets for Light Bar		4	$	$
LPR Mounting for Portable system		10	$	$
LPR Processor			$	$
Modem		14	$	$
LPR Software	ALPR-S-4001	14	$ 2,500.00	$ 35,000.00
LPR Speed Trailer complete package	ALPR-H-4001-Trail WARRANTY	14 1	$ 650.00	$ 650.00
Start-up, configuration and commissioning of LPR Systems at Sheriff's facility to include all expenses such as travel		14	$	$
Installation			$	$
Covert Installation		14	$	$
Installation "Kit", Includes all hardware, wiring and software for do it yourself standard installations (on poles & trailers)		1 5	$	$
Training per hour	TRAIN		$ 80.00	$ 640.00
Shipping		8		$
			OPTION YEAR 2 SUBTOTAL:	$ 41,140.00

**Quantities are estimates only and not guaranteed

GRAND TOTAL (BASIS OF AWARD) :	$ 287,880.00

1. PRICING

1.1. Enter unit prices for each line item, Base Term Period, 1st Option Period, and 2nd Option Period tabs for each line item on the appropriate tab.

1.2. These worksheets have built-in formulas that will calculate the extended prices for each line item and each term period. The aggregate total for each term period will be automatically transferred to the Grand Total (Extended Price) where your total will be calculated.

1.3. The worksheets are locked/protected. The format and the contents of the worksheets should not be tampered with or altered in any way.

1.4. Bids must meet specifications provided.

1.5. All items must be priced to be considered responsive.

2. GENERAL REQUIREMENTS

2.1 A specifications sheet with pictures and operations manual for the product shall be submitted with the bid.

COMPANY:	Utility Associates, Inc.
REPRESENTATIVE NAME:	Michael Nark, President & CEO
REPRESENTATIVE EMAIL:	mnark@utility.com or proposals@utility.com
REPRESENTATIVE PHONE:	800-597-4707 Toll Free or 404-816-0300

Form **W-9**
(Rev. October 2018)
Department of the Treasury
Internal Revenue Service

Request for Taxpayer Identification Number and Certification

▶ **Go to *www.irs.gov/FormW9* for instructions and the latest information.**

Give Form to the requester. Do not send to the IRS.

Print or type. See Specific Instructions on page 3.

1 Name (as shown on your income tax return). Name is required on this line; do not leave this line blank.
Utility Associates, Inc.

2 Business name/disregarded entity name, if different from above

3 Check appropriate box for federal tax classification of the person whose name is entered on line 1. Check only **one** of the following seven boxes.

☐ Individual/sole proprietor or single-member LLC ☑ C Corporation ☐ S Corporation ☐ Partnership ☐ Trust/estate

☐ Limited liability company. Enter the tax classification (C=C corporation, S=S corporation, P=Partnership) ▶ _____

Note: Check the appropriate box in the line above for the tax classification of the single-member owner. Do not check LLC if the LLC is classified as a single-member LLC that is disregarded from the owner unless the owner of the LLC is another LLC that is **not** disregarded from the owner for U.S. federal tax purposes. Otherwise, a single-member LLC that is disregarded from the owner should check the appropriate box for the tax classification of its owner.

☐ Other (see instructions) ▶

4 Exemptions (codes apply only to certain entities, not individuals; see instructions on page 3):

Exempt payee code (if any) _____

Exemption from FATCA reporting code (if any) _____

(Applies to accounts maintained outside the U.S.)

5 Address (number, street, and apt. or suite no.) See instructions.
250 E. Ponce de Leon Avenue, Suite 700

Requester's name and address (optional)

6 City, state, and ZIP code
Decatur, Georgia 30030

7 List account number(s) here (optional)

Part I Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. The TIN provided must match the name given on line 1 to avoid backup withholding. For individuals, this is generally your social security number (SSN). However, for a resident alien, sole proprietor, or disregarded entity, see the instructions for Part I, later. For other entities, it is your employer identification number (EIN). If you do not have a number, see *How to get a TIN*, later.

Note: If the account is in more than one name, see the instructions for line 1. Also see *What Name and Number To Give the Requester* for guidelines on whose number to enter.

Social security number
[ ][ ][ ] - [ ][ ] - [ ][ ][ ][ ]

or

Employer identification number
5 8 - 2 5 7 4 3 1 8

Part II Certification

Under penalties of perjury, I certify that:

1. The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me); and
2. I am not subject to backup withholding because: (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding; and
3. I am a U.S. citizen or other U.S. person (defined below); and
4. The FATCA code(s) entered on this form (if any) indicating that I am exempt from FATCA reporting is correct.

Certification instructions. You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and generally, payments other than interest and dividends, you are not required to sign the certification, but you must provide your correct TIN. See the instructions for Part II, later.

Sign Here Signature of U.S. person ▶ Amanda [illegible] Date ▶ 12/6/19

General Instructions

Section references are to the Internal Revenue Code unless otherwise noted.

Future developments. For the latest information about developments related to Form W-9 and its instructions, such as legislation enacted after they were published, go to *www.irs.gov/FormW9*.

Purpose of Form

An individual or entity (Form W-9 requester) who is required to file an information return with the IRS must obtain your correct taxpayer identification number (TIN) which may be your social security number (SSN), individual taxpayer identification number (ITIN), adoption taxpayer identification number (ATIN), or employer identification number (EIN), to report on an information return the amount paid to you, or other amount reportable on an information return. Examples of information returns include, but are not limited to, the following.

- Form 1099-INT (interest earned or paid)
- Form 1099-DIV (dividends, including those from stocks or mutual funds)
- Form 1099-MISC (various types of income, prizes, awards, or gross proceeds)
- Form 1099-B (stock or mutual fund sales and certain other transactions by brokers)
- Form 1099-S (proceeds from real estate transactions)
- Form 1099-K (merchant card and third party network transactions)
- Form 1098 (home mortgage interest), 1098-E (student loan interest), 1098-T (tuition)
- Form 1099-C (canceled debt)
- Form 1099-A (acquisition or abandonment of secured property)

Use Form W-9 only if you are a U.S. person (including a resident alien), to provide your correct TIN.

If you do not return Form W-9 to the requester with a TIN, you might be subject to backup withholding. See What is backup withholding, *later.*

Company Qualifications and Experience

Utility Associates, Inc. is a vertically integrated US manufacturer and supplier of software solutions, digital in-vehicle cameras, advanced license plate readers, mobile routers, mobile digital multi-media evidence management systems, body worn cameras, and situational awareness software solutions for the law enforcement community, transportation agencies, and utilities. With over 50,000 devices deployed, Utility has worked with many progressive first responders, transit agencies and utilities to incorporate industry best practices to help solve critical legal evidence capture and field situational awareness management challenges. We support a base of over 200+ client agencies spanning small 5-unit installations to multi-precinct fleets with hundreds of vehicles and hundreds of officers.

Company Location and Contact Information:

Utility is a Delaware Corporation incorporated in 2001 with Headquarters in Decatur, Georgia, in Metropolitan Atlanta.

Utility Associates, Inc. Global Headquarters:
250 East Ponce De Leon Avenue, Suite 700
Decatur, Georgia 30030
404-816-0300 general office 404-795-0525 fax
www.utility.com www.bodyworn.com

Primary Representatives:

Contract Approval: Michael Nark, President and CEO, mnark@utility.com 404-816-0300

Business Manager: Clay Campbell, Retired Sworn Officer, Business Manager ccampbell@utility.com, 832-953-9849

Support Manager: Dahlia Blake, Customer Support Specialist dblake@utility.com

Repair and Maintenance: Samson Aberra, Support Manager saberra@utility.com

Utility hardware and software is designed, developed, manufactured, packaged, and shipped at our state-of the-art Headquarters location in Decatur, Georgia, within Metropolitan Atlanta. Utility has more than 80 employees, based in the US in all time zones dedicated to our evidence capture and digital evidence management solutions.

Company Qualifications and Experience

Utility's digital recording software is the proven result of 10+ years of development and deployment in thousands of patrol car video recording systems around the US.

Utility solutions are US FBI CJIS compliant, and Utility maintains state-of-the-art security.

Utility owns key US Patents for video recording systems, including:

- 6,831,556 – Composite Mobile Digital Information System
- 7,768,548 – Mobile Digital Video Recording System
- 8,781,475 – System for Switching between Cellular Networks
- 9,246,898 – Method for Securely Distributing Legal Evidence
- 9,282,495 – Method and Device for Switching between Cellular Networks

Many vendors outsource engineering, software development and support, and/or manufacturing offshore. By contrast, Utility's control of the design, development, manufacturing and customer support experience through our in-house team of professionals allows us to provide a secure, reliable solution, and eliminate an 8,000 miles supply chain, while rapidly innovating and responding to our customer's needs.

Utility solutions are Country of Origin USA, manufactured in the USA.

- Utility is committed to supporting the USA through the Buy American Act and the American Recovery Reinvestment Act, to which all Utility solutions are Compliant.



Amazon Web Services (AWS) City on a Cloud Innovation Challenge Winner

2016, 2017, 2018, 2019

Utility, Inc. has been recognized the past four years by Amazon as a winner of the Amazon Web Services (AWS) City on a Cloud Innovation Challenge for its innovative use of Amazon cloud storage.

Recently in 2019, Utility won the Powered by AWS Award. In a case of a school shooting, police and school administrators need to know immediately when a gunshot happens, where the gun was fired, and what type of gun was fired. Active Shooter Response Technology (ASRT) provides real-time alerts of the location of gunshots to central dispatch, nearby police and resource officers, and school administrators. ASRT ultrasound analysis distinguishes gunshot ultrasounds from other loud noises. Because ultrasounds do not penetrate hard surfaces, the specific gunshot location can be known and reported immediately. The AWS Cloud and ASRT ultrasound waveform artificial intelligence (AI) processing can further identify gunshot signature metadata such as gun type (shotgun, rifle, pistol) and caliber. Police and school administrators can immediately respond. Just as importantly, having ASRT may deter a shooter from assaulting a school.

In 2018, Utility was awarded the Partners in Innovation Award for it's cutting-edge police technology. Utility's BodyWorn and In-Car Video systems integrate audio, video, and tactile A.I. to automate video recording policy rules. Gunshot audio recognition automatically triggers recording and smart saves pre-event audio and video whenever a gunshot happens close to an officer. Smart Holsters automatically start recording when a weapon has been pulled. In-Car Video AI automatically captures license plate numbers to support immediate analysis.

Utility's partner agency, Lawrence Police Department (IN) was awarded the Best Practices Award in 2017. Aiming to improve public safety, reduce crime, and build public trust between police and the citizens they serve, the Lawrence Police Department partnered with BodyWorn by Utility to provide Body Worn Camera technology. The project used AWS for big data storage and analytics. Video and audio recording collected by police officers is instantly, effortlessly uploaded in a safe, encrypted storage environment.

In the previous year, 2016, Utility was presented the Partners in Innovation Award for its BodyWorn camera and AVaiLWeb evidence management Solutions.

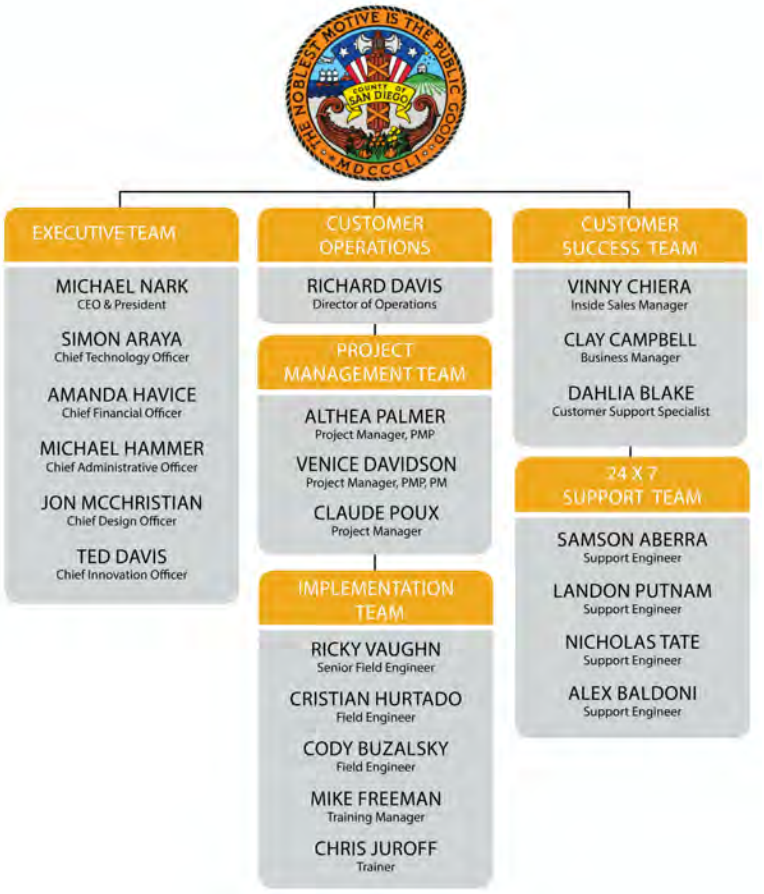
Robert McKeeman, Vice President of Utility said, "Being named as a winner by Amazon Web Services for our innovative solutions to solve a government challenge solidifies our work to meet our mission to make police officers' jobs safer, while protecting Privacy for Police Officers and Citizens, and enabling Police Accountability and Transparency. Through our partnership with Amazon Web Services, we provide our customers with a very reliable and cost effective video management and redaction solution."



Utility's customers can choose to access to Amazon AWS-based e-discovery, e-citation, secure image management, mobile forensics, crime forecasting, major risk event management, public records management, backup, archival and disaster recovery tools on the Amazon AWS Cloud.

Project Team for San Diego County Sheriff's Department

Project Customer Success Team



A successful and seamless implementation is vital for Utility to build lasting customer partnerships. The San Diego County Sheriff's Department relationship will be managed by the **Customer Success Team,** and led by Utility's Clay Campbell (retired officer, Harris County TX Sheriff's Office), who will guide the focus of other key personnel to ensure that your needs will be our team's top priority. Clay Campbell will have direct contact and interaction on this project to ensure the system is meeting expectations.

Customer Operations and Project Management Teams

System implementation will be led by **Customer Operations, by the Project Management Team, and Implementation Team,** which will be solely dedicated, from start to finish, to the success of the deployment of the mobile video system for the San Diego County Sheriff's Department. We propose Claude Poux as our designated **Project Manager** for this project. A resume for Claude Poux is provided below. Claude Poux has more than eight years of experience in project and program management, analysis and information security. He will be responsible for adhering to scheduling deadlines and overall management of the project, with experience on recent projects similar to this project. His background demonstrates his ability to keenly manage and solve applied technology problems.

Claude R. Poux

| Duluth, Georgia 30096
T: 770.895.8161 E: cpoux325@gmail.com

Professional Profile

Highly knowledgeable and dedicated project management professional with extensive experience in a variety of project focused activities and coordination in both corporate and business administration. Eager to apply creativity and client relational skills and improve organization effectiveness with a vision that promotes success.

Skills

- Project Planning & Management
- Tradeshow Marketing & Sales
- Drafting & Analyzing Reports
- Training Material Composition
- Metrics Execution
- Compliance Analysis
- Material Take off estimator
- Small Business Operations

Technical Proficiencies

Software Programs:

- MS Office Suite: Word, Excel, PowerPoint, Outlook, Access, Publisher, FrontPage
- Internet Explorer, Mozilla Firefox, Apple Safari, Google Chrome
- Provide Information Platform, Oracle 11i & R12, Infolease, Salesforce, and SAGE

Experience

Body Worn by Utility (Elite Technical) | Decatur, GA — **09/2019 – Present**
Project Manager

Manage and coordinate all stakeholders and parts required to successfully complete full-scale deployments for Law Enforcement agencies.

Develop and manage project plans, schedules and resources using an agile or adaptive approach to ensure optimal quality.

Initiate and lead conference, video calls and meetings for Sales handoffs, kick off calls, and closeouts meetings with stakeholders.

Oversee project procurement management while tracking and managing incoming documents from vendors, purchasing, logistics and engineers providing field service.

Manage project knowledge and communication for all team members and stakeholders

Develop, maintain and enforce scope of work to ensure project follows agreed upon guidelines and action items to ensure that milestones, timelines and schedule compliance are met.

Caterpillar Switchgear (Rose International, Inc.) | Alpharetta, GA — **09/2018 – Present**
Project Manager

Ammacore | Roswell, GA — **09/2017 – 05/2018**
Project Manager

Nichiha USA | Johns Creek, GA — **03/2016 – 07/2017**
Project Coordinator

Coca-Cola/Randstad | Alpharetta, GA — **08/2014 – 02/2016**
Project Install Coordinator (Contract)

Education

University of Florida, College of Journalism & Communications
Bachelor of Science in Public Relations

Utility's **Senior Field Engineer** Ricky Vaugh will lead the **Implementation Team**, which is responsible for the initial configuration and project setup. The team leader is a Certified Dell Systems Expert, a Certified Microsoft Expert (Network Administrator, Windows XP, Server, Messaging) with more than 25 years of experience. This team will initially work with both your sworn and technology staff to ensure proper configuration and then will direct the training sessions with officers and support staff.

Training for this project will be led by Michael Freeman. Michael has a mastery of formal classroom instructor training, with relevant experience with the software and hardware. He possesses a thorough knowledge of the equipment and the AVaiLWeb™ digital evidence management system. He has mastery of the subject material, training process, system documentation tools, and training aids. Michael is highly competent, and able to work independently of outside support to accomplish the San Diego County Sheriff's Department goals and objectives.

The **Customer Success Team, Customer Operations Team**, and **Implementation Team,** will work with appointed staff from the Sheriff's Department in an integrated, streamlined process for a seamless and efficient delivery of services.

The RocketIoT™ ALPR implementations are all-inclusive. They include technical support and assistance devices, networking equipment, video uploading, charging, connectivity, system software and upgrades, and data and video retrieval software and procedures.

The technical system functionality is fully managed by our software engineers to ensure that it will always be up to date for all of our customers on our Cloud-based platform.
All system upgrades are all done over-the-air (OTA), without requiring officer effort.

UTILITY

Technical Approach of Utility's RocketIoT ALPR™, and AVaiLWeb™ Digital Evidence Management System (DEMS)

The Ultimate Ecosystem

Mission Critical Mobile Intelligence.

Protect What's Important:
Accurate Detection, Connectivity and Officer Safety

ROCKETIOT™

Capture high-quality license plate images with our AI on-the-edge ALPR system. Upload ALPR recordings instantly to the cloud via LTE cellular

AVAILWEB™

Utility's Virtual Command Center – a comprehensive user-friendly online platform allows the user to store, manage and retrieve digital data at the click of a button.



Download CCIC/NCIC data directly (by Department's credential) to the RocketIoT ALPR™ 'box', without human review. Data is only used to look up license plates that are read 'on the street'.



All ALPR data collected 'on the street' by Utility is encrypted and securely stored in the cloud.

Share captured data within Utility's Virtual Command Center using our state-of-the-art digital evidence management system.

UTILITY

The RocketIoT ALPR™ License Plate Reader Camera System (RocketIoT ALPR™) is an all-inclusive, turnkey, cloud-based solution. The RocketIoT ALPR™ and AVaiLWeb™ DEMS are provided as a System as a Service (SaaS) subscription. The SaaS subscription provides complete end-to-end security from the time data is captured and recorded until it is purged at the end of the retention classification. Utility provides unlimited storage at no additional cost to the Department.



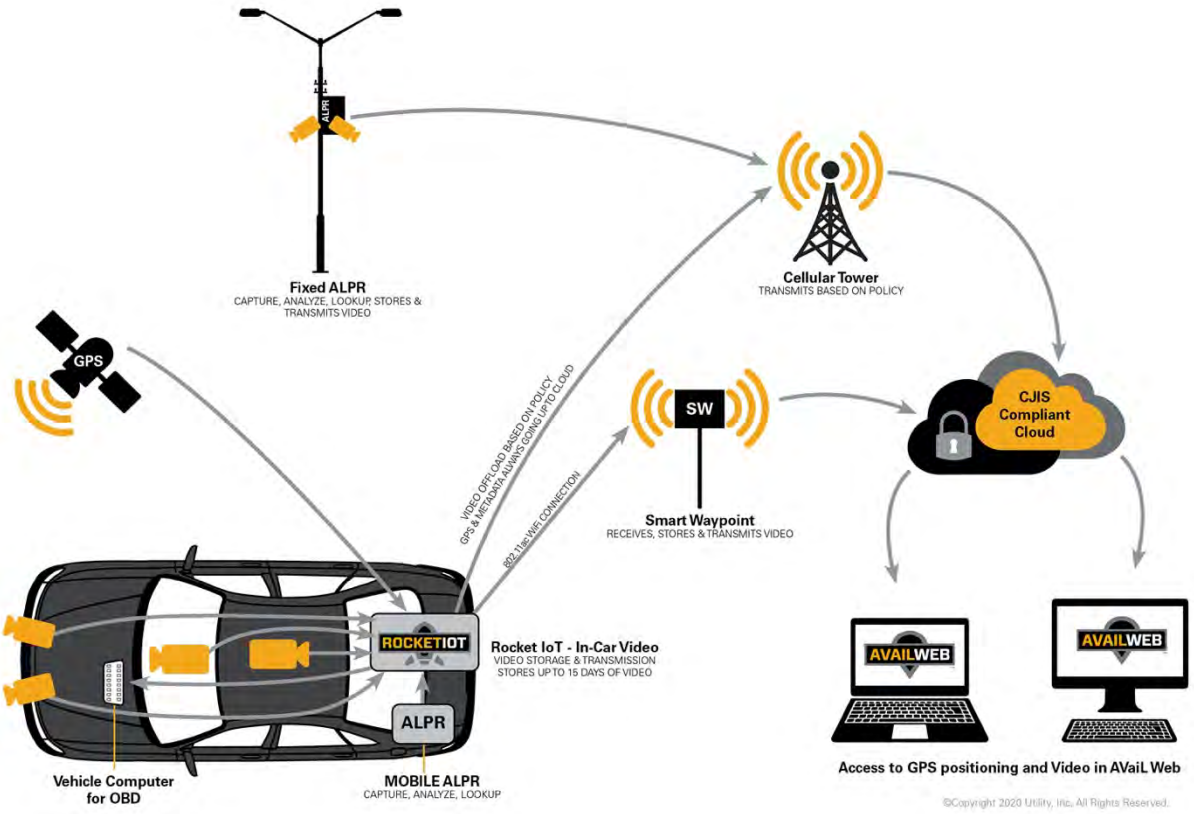
Utility's technology model is not reliant upon the Vigilant Learn cloud platform, and instead drives LPR using Artificial Intelligence (AI) at-the-edge, and real-time connectivity to Hot Lists from State, local and Federal data sources. The RocketIoT ALPR™ features highly sophisticated optical technology and machine learning algorithms to improve accuracy and efficiency.

Utility's RocketIoT ALPR™ allows today's efficiency-focused law enforcement leaders to use AI enhanced technology to accurately capture and manage digital data. This provides officers a Smart ALPR tool to help protect their community and themselves from mobile threats.

This combination of features and capabilities is unmatched by any other solution, and is designed to serve as a Force Multiplier, promote a Connected department, and offer a Pathway to Future Integrations, such as CAD, RMS, and mobile video camera systems.

Utility's ALPR™ technology is a partnership with Sony Corporation, and is installed in fixed stationary applications and in-vehicle applications for customers across the US.

This narrative describes a system overview of technical features, capabilities, and design considerations that are included in the RocketIoT ALPR™ Ecosystem, beginning with a description of RocketIoT ALPR™, and AVaiLWeb™.



(*The Exhibit above also details the optional integration of Utility's FirstNet Certified RocketIoT™ in-car DVR/Router, part of the RocketIoT ALPR™ technology Ecosystem).*

Utility is a video communications industry-leader. As such, we provide the following link to video presentation of the RocketIoT ALPR™ system:

http://bodyworn-4053552.hs-sites.com/en/knowledge/smart-alpr

The RocketIoT ALPR™ is a smart license plate reader device that utilizes real-time 4G-LTE cellular communications provided by its own LTE connection. The device has capability for a variety of sensors and configurable operating software for autonomous processing. This combination of software and communications driven technology provides Smart ALPR recording control, automatic safety reporting (such as “ALERT” bulletins), and when used in combination with the RocketIoT™ in-car DVR/Router can enable geo-fence zone awareness.



RocketIoT ALPR™ also offers the ability to receive messages and take actions based upon configuration rules processed by software that can be updated at any time.

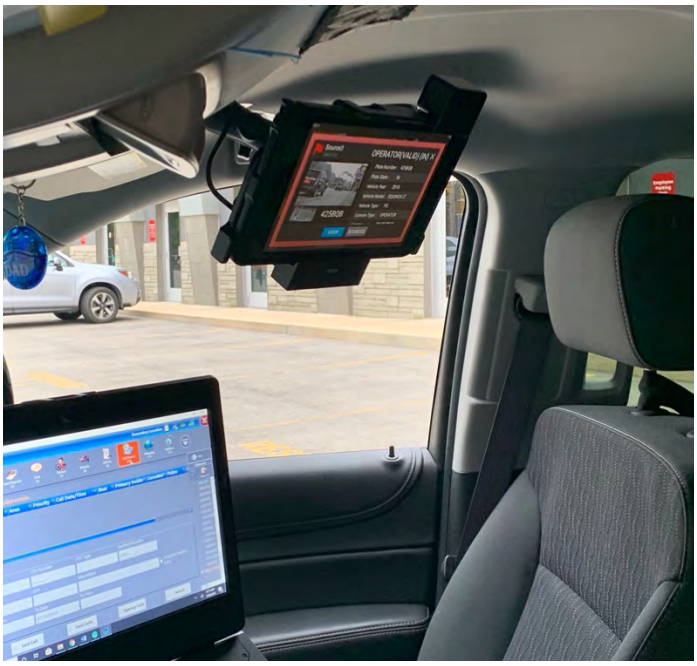
RocketIoT ALPR™ Camera Mounting Options

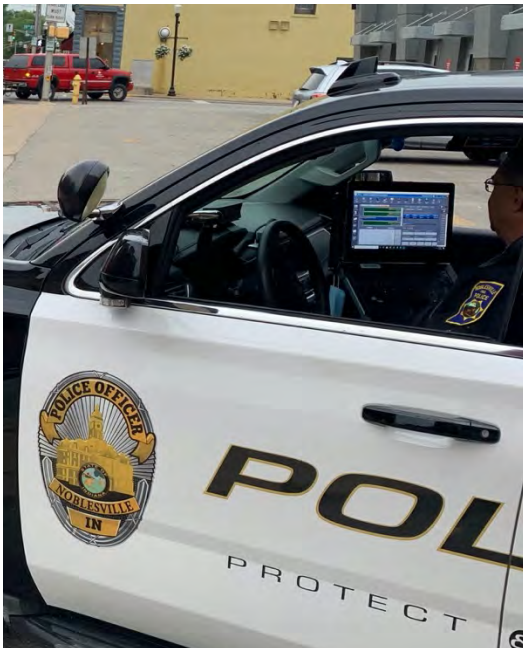
Utility’s ALPR™ technology is installed in in-vehicle applications and fixed stationary applications for customers across the US, with in-vehicle mobile, as well as stationary fixed-mount options.





View of Typical Mobile Vehicle Mounting Option





View of Typical Mobile In-Vehicle AVaiLWeb™ Access





The RocketIoT ALPR™ operates with shore power (120V). Utility's future technology roadmap for the device includes solar power capability.

View of Typical Stationary Fixed- Mounting Option

UTILITY

RocketIoT ALPR™ data is managed by Utility's AVaiLWeb™ platform. AVaiLWeb™ pulls



together all devices and data in the system - ALPR license plate data, meta data (and any Rocketlot in-vehicle DVR video, audio and metadata, if available) — into one platform keeping the process streamlined. All captured images and metadata can be viewed instantly and managed within the platform. The system allows for additional features, such as Live Video streaming for more urgent situational awareness incidents. Additionally, device data is tied together in the system to provide a clearer picture, with timeline and tags of everything that took place. All of these connected data sources (and Utility's ALPR and video camera devices) can be remotely configured through AVaiLWeb™, by sending over-the-air updates.

Accessing Data Bases

RocketIoT ALPR™ data managed by Utility's AVaiLWeb™ provides access to:

NCIC
- Criminal Data
- Wanted Felons
- Stolen vehicles

State
- Expired Plates
- Vehicle Holds
- Suspended Driver Files
- Habitual Traffic Violators

Local
- Be on the Lookout (BOLOs)
- Crime Information Bulletin (BIC)

UTILITY

RocketIoT ALPR™ is a Smarter System

Typical LPR systems use video streams to **capture** pictures, **analyze** the picture to find license plates, then do a **lookup** to find a match within the database, and then it is **displayed** to an officer, either at computer viewing device at a remote location, or in the officer's car.

RocketIoT ALPR™ provides a better way to integrate the system for a real-time approach to ALPR. Utility's development process with Sony had the objective to not only capture and analyze the data at-the-edge, but then share that data with the cloud so that decisions could be made to disseminate that information to officers and other staff within the agency (or outside the agency) who need it as quickly as possible.

Like typical LPR systems, the RocketIoT ALPR™ system captures using camera feeds. RocketIoT ALPR™ uses picture analysis, but uses *artificial intelligence for the analysis* part. The agency using RocketIoT ALPR™ benefits from the advantage of ability of the ALPR BOX to process dozens of pictures per second. It can analyze a substantial amount of data while the vehicle is moving at high speeds or stationary, and even at night.

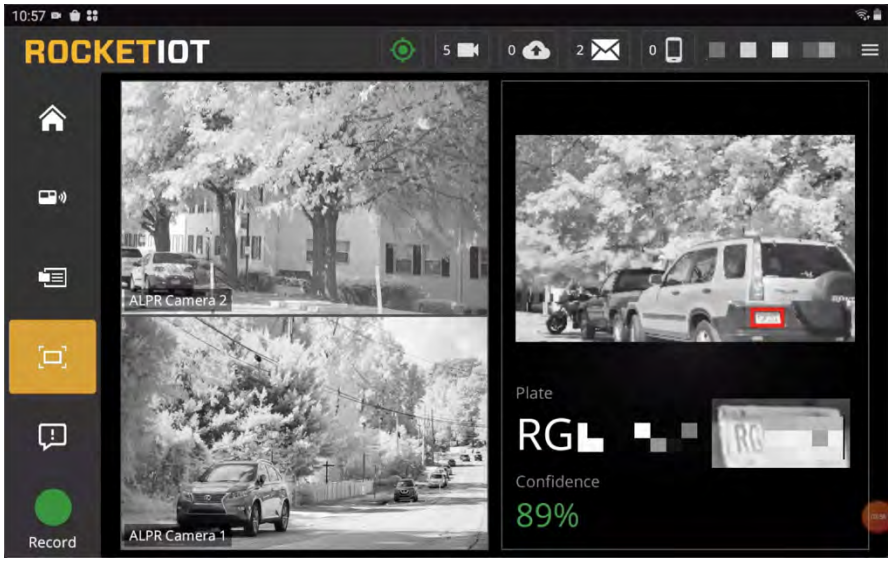
Like typical LPR systems, the RocketIoT ALPR™ lookup is similar. RocketIoT ALPR™ allows lookups from state and NCIC Federal databases. RocketIoT ALPR™ has an additional level of lookup by allowing BOLOs to be sent directly from AVaiLWeb™ into an agency-specific lookup database, immediately.

For Example, if there is a need for an Amber Alert, and you have the vehicle plate information, you can create a BOLO within AVaiLWeb™ and send it out to be accessed within AVaiLWeb™ from within all vehicles, either from a MDC or Utility's in-car mounted ALPR system. This integration enables every patrol vehicle to be on the lookout for that vehicle tag.

UTILITY

Plate Detection of Hits

The AVaiLWeb ™ platform view below shows actual images from two 'live' views of RocketIoT ALPR ™ cameras. Both mobile and stationary mounted cameras can be easily adjusted. Whether the camera is stationary mounted, or a mobile in-car camera out on patrol, the data is constantly being collected and entering the system. Captured data paired to NCIC data, and state and local databases that are downloaded directly to the RocketIoT ALPR ™ box on a daily basis.





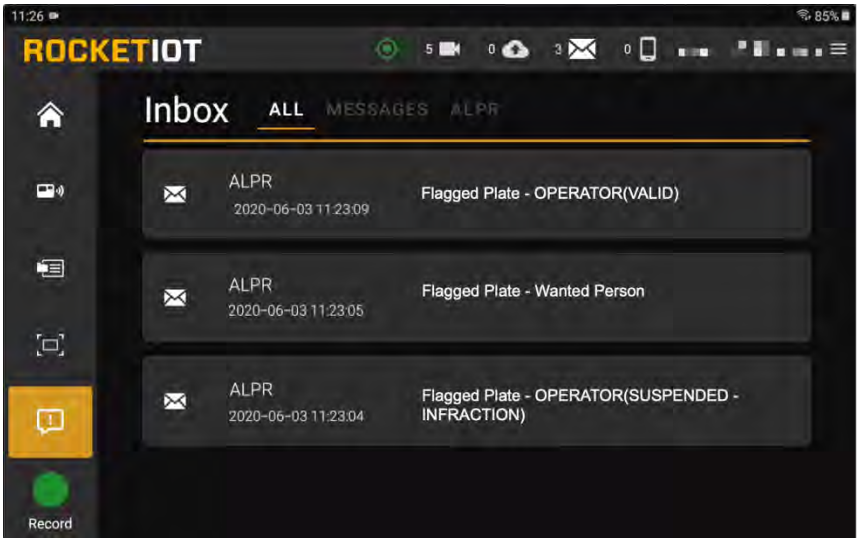
(The plate in the image is redacted since this plate was a real hit).

The RocketIoT ALPR ™ box goes through and compares data, so when a hit is obtained, the system shows it. As user can see when it captures a plate. It will capture an image, and highlight the plate with a red box. Below that is the plate number and how confident it is that it is the correct plate. A hit rated 80% or above is very accurate.

UTILITY

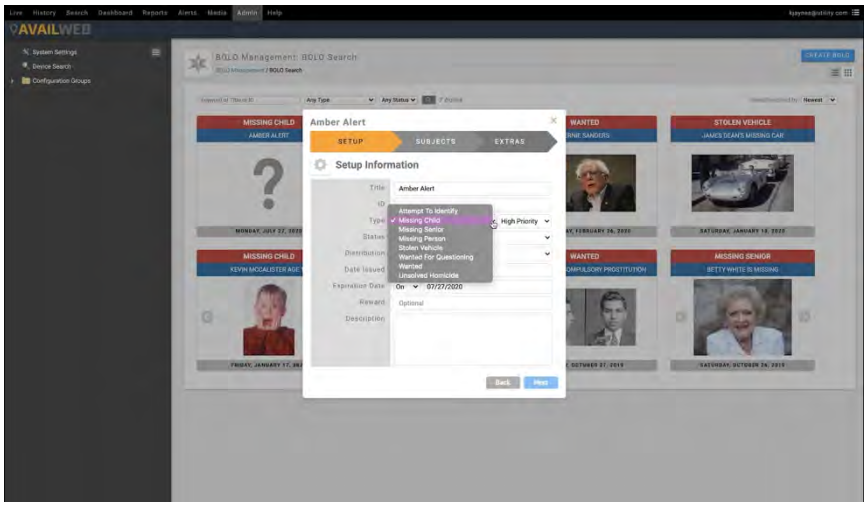
Rapid Processing and Analysis

The RocketIoT ALPR™ analyzes and processes rapidly. The AVaiLWeb ™ platform view above shows the system finding 3 matches within a matter of seconds. In this instance, the RocketIoT ALPR ™ even caught an NCIC plate. In this list view, you can see that these three hits were processed and recognized with 5 seconds. From the list view above, it can be seen that the hits were happening within 5 seconds.



Alerts

Using AVaiLWeb™, the system can inject BOLOs. For any BOLOs or local watch sheets that involve a vehicle plate, the system can automatically ingest that information and push it out to the officers using AVaiLWeb ™ immediately. For officers accessing AVaiLWeb™ in the field, this can provide more ‘eyes on the street’ looking for that vehicle.



UTILITY

Database and Optional Software

Departments will need access to a current desktop Web Browser and Broadband internet connectivity to use the AVaiLWeb™ digital evidence management service. There is no additional or optional Software or Hardware needed to use the AvaiLWeb™ service.

Pathway to Future Integrations for Better Connectivity

The RocketIoT ALPR™ allows a pathway for full integration and connectivity, depending upon the optional devices and other optional agency integrations that are desired. Ultimately, the RocketIoT ALPR™ has the ability to define policies that would allow agencies to integrate and associate the license plate number and the vehicle picture data with the capture of video evidence in addition to getting.

Other optional integrations can enable more connectivity. For example, when a plate is detected in the system, then actionable decisions can be made. Instead of just displaying it to the officer in the vehicle, the system can push that data up to the cloud. Then, from the cloud, the data would be pulled into AVaiLWeb ™ where it would be displayed on the Dispatcher's screen in real-time, with Utility's devices supporting CAD integration.

Taking it one step further, the Department can send the plate alert data to an officer in proximity of where the vehicle was spotted, allowing the agency to have quicker reaction time to critical information, with Utility's camera devices supporting live video and data communications. In this instance, and officer on patrol in a 'district' could have near real-time integration with plate images being captured live by stationary-mount ALPR within the same geographic vicinity, which can enable immediate follow up and more timely pursuit of violations and perceived threats.

The vision of a fully integrated system for law enforcement offers the promise to provide more information for better law enforcement investigation, improved officer safety, and safer communities.

County of San Diego, California
RESPONSE TO SPECIFICATIONS by UTILITY ASSOCIATES, INC.
Request for Bids (RFB # 10493) for Sheriff's Department License Plate Readers
Section C: Exhibit A Statement of Work

Item	Question	Vendor Response
2.1	**SECURITY**	
2.1.1	Must be compliant with California Senate Bill 34 (SB34).	Meets Requirement. Utility has reviewed and understands this requirement and will comply. Provisions of SB34 require an ALPR operator to maintain a specified record of access and require that ALPR information only be used for authorized purposes. Utility's RocketIoT ALPR™ with AVaiLWeb™ digital evidence management system provides a robust audit log of all data and recordings that details access, viewing or playback, edits, deletions, commenting, shares, downloads, transfers, etc. These logs take the form of a detailed Chain of Custody that is an audit trail, which every incident/recording has. AVaiLWeb™'s Chain of Custody report shows information about an incident/recording such as who or what activated the recording, who or what deactivated the recording, any classifications or notes that are added or modified for the recording, any retention action that is taken, any exports to an external source, and any other action that is taken on an incident. Each interaction in this report includes a date/time stamp, the user's username, and IP Address. AVaiLWeb™ includes a User Access Custody report which shows all actions taken by a user for a given time frame, such as videos viewed, shared, or exported. These reports are printable and exportable into PDF format. To clarify, Utility does not collect or review any personal information.

2.1.2	Single Sign-On (SSO) implementation options	See responses below:
2.1.2.1	Security Assertion Markup Language (SAML) 2.0 compliance	Meets Requirement. Utility's RocketIoT ALPR™ with the AVaiLWeb™ digital evidence management system supports Single Sign On (SSO), based on SAML 2.0.
2.1.2.2	Other SSO methods, such as Active Directory and Office 365.	Meets Requirement. Utility's RocketIoT ALPR™ License Plate Reader Camera System with the AVaiLWeb™digital evidence management system supports Single Sign On (SSO), working with your existing Active Directory Federation Services (AD FS) system. When you activate SSO for your users, they don't need to remember another password. They will be authenticated by your Windows Active Directory system. AD FS will forward the authenticated user's information to AVaiLWeb™, and the user will be logged in to AVaiLWeb™ just as if they had supplied the correct username and password.
2.1.3	User and Entity Based Behavioral Analytics (UEBA)	Meets Requirement. Both Utility and our data partner Amazon Web Services maintain robust Standards and Compliance Services, and each performs these activities, including to identify risks, threats and vulnerabilities, as well as the integrity of the data itself. In order to ensure 24/7/365 uptime, Utility employs real-time activity simulation that reproduces and verifies that the system is performing from end-to-end. This simulation allows Utility to uniquely identify performance issues before a client notices or reports them to Utility. AWS maintains security on the underlying virtual infrastructure. AWS Security performs regular vulnerability scans on the infrastructure, web application, and databases in the AWS environment using a variety of tools. Utility's Technology Development Roadmap includes User and Entity Based Behavioral Analytics (UEBA).

2.1.4	Distributed Denial of Service (DDoS) protection	Meets Requirement. Both Utility and our data partner Amazon Web Services have built-in protections against DDoS.
2.1.5	Data sanitization and anti-malware prevention. Minimizing attack vectors throughout the LPR solution using a multi-layered approach	Meets Requirements. See responses below:
2.1.5.1	Anti-malware scanning and threat prevention with up to date signatures	Not Applicable. The RocketIoT ALPR™ with AVaiLWeb™ solution is provided as a System as a Service (SaaS) subscription, and is accessed a computer desktop or in the field, via the internet, using a common web browser. There is no requirement to install software on County computers, and as such the County will not be subject to this threat.
2.1.5.2	Alerts and notifications	Not Applicable. See response above.
2.1.5.3	Input sanitization: All data coming into the system from users or application programming interfaces (API's)	Meets Requirement. Utility sanitizes all user input and API input.
2.1.5.4	White list of file types for attaching/uploading for all purposes	Meets Requirement. The RocketIoT ALPR™ with AVaiLWeb™ supports a client configurable white list of file types for uploading files to cases. This is the only feature in the system where uploading files is applicable.
2.1.5.5	File Contents Disarm and Reconstruction (CDR)	Meets Requirement. AVaiLWeb™ has this capability built-in as part of input sanitization.
2.1.6	Disaster Recovery	Meets Requirement. See responses below: Utility's RocketIoT ALPR™ and AVaiLWeb™ is an all-inclusive solution, provided as a 'System as a Service' (SaaS) subscription, which is hosted in

		AWS GovCloud, and all evidence is stored redundantly and within AWS geographically separated CJIS-compliant cloud environments. This methodology provides 99.999999999% resiliency for your data. Utility Associates, Inc. is an approved elite Launch Partner in the AWS Public Safety & Disaster Response Competency program. See details about the program at AWS' upcoming conference event Re:Invent 2020, and at this link: *https://aws.amazon.com/stateandlocal/justice-and-public-safety/partner-solutions/?partner-solutions-cards.sort-by=item.additionalFields.partnerNameLower&partner-solutions-cards.sort-order=asc*
2.1.6.1	Data protection, backup, and recovery strategy	The RocketIoT ALPR™ with the AVaiLWeb™ digital evidence management system is hosted in the CJIS-compliant AWS GovCloud. The hosted solution resiliency programs identify, respond to, and recover from a major incident, with contingency management, business continuity, and disaster recovery plans. It identifies critical system components required to maintain the availability of the system, recovers services in the event of an outage from physically separate locations, maintains authoritative backups, employs continuous infrastructure capacity planning, and monitors to ensure successful replication. Further information on disaster recovery can be found at: http://bit.ly/2NA4rRV.
2.1.6.2	Disaster recovery liability in case of catastrophic event	Meets Requirements. See the responses in 2.1.6, and 2.1.6.1 above. Both Utility and our data partner Amazon Web Services maintain robust disaster recovery in case of catastrophic event, which is ongoing, continuous and geographically distributed. As such there, our disaster recovery liability is minimized effectively to zero.

2.1.7	California Consumer Privacy Act (CCPA) compliance	Meets Requirement. Utility has reviewed and understands this requirement and will comply. To clarify, Utility does not collect or review any personal information.
2.1.8	Contractor shall provide a secure, database encrypted and web-based system that provides real-time access to uploaded data	Meets Requirement. The RocketIoT ALPR™ with AVaiLWeb™ is hosted in AWS GovCloud. All evidence is encrypted at rest and in transmission using AES 256-bit encryption. AVaiLWeb™ is a robust evidence management system. Users interact with on a computer desktop or in the field, for real time access to uploaded data, via the internet, using a common web browser.
2.1.9	Contractor shall allow authorized users access to LPR data in a number of LPR-specific dashboards	Meets Requirement. The RocketIoT™ ALPR dashboard is accessed in AVaiLWeb™ on a computer desktop or in the field, via the internet, using a common web browser. AVaiLWeb™ provides authorized users access to LPR data in a number of LPR-specific dashboards.
2.1.10	Dashboard will show LPR vehicle scans in an easy to read graphical format	Meets Requirement. AVaiLWeb™ is a robust evidence management system, and the AVaiLWeb™ dashboard is accessed on a computer desktop or in the field, via the internet, using a common web browser. AVaiLWeb features an intuitive, easy to use graphical user interface, and has the capability to integrate with GPS, CAD and RMS.
2.1.11	LPR dashboard will show vehicle location, images captured and provide the ability to search using the license plate	Meets Requirement. The AVaiLWeb™ RocketIoT ALPR™ dashboard will show vehicle location, images captured and provide the ability to search using the license plate.

2.1.12	Contractor shall provide an option to purge data at specified intervals or dates	Meets Requirement. Retention within AVaiLWeb™ takes place automatically based on custom retention periods by classification type to be defined by the Department. There is also a retention period for unclassified incidents. These retention periods can easily be configured, or modified, to maintain consistency with Department-defined policy.
2.1.12.1	Provide notification of purge date.	Meets Requirement. AVaiLWeb™ provides a purge notification report that is easy to access.
2.1.12.2	Provide confirmation and notification that specified data was purged.	Meets Requirement. AVaiLWeb™ authorized users can easily access records to confirm whether they are active or already purged.
2.1.13	Data uploaded will only be shared at the discretion of an administrator designated by the San Diego County Sheriff's Department	Meets Requirement. Exports and redactions are owned by, and accessible to, the AVaiLWeb™ user who is working with that specific export or redaction job. Other users will have access to that export or redaction job only if the owner shares it with them. Authorized AVaiLWeb™ users can share cases. The AVaiLWeb™ platform has the ability to create case files to maintain all relevant information for a specific case in one file. File data can be sourced from LPR (both Portable fixed stationary, and Mobile vehicle mount cameras), in-vehicle cameras, body cameras, surveillance video and other sources. When sharing is initiated, the recipient receives an email that includes the case title. The use can also include a free form 'reason' message for the sharing action. When the recipient accesses the shared case within AVaiLWeb™, they have access to all of the case meta data including: case title, notes, case creation date, included media, etc.

2.2	LPR CAMERAS	
2.2.1	Contractor shall have LPR systems capable of being installed on a fixed object (i.e. light pole), marked patrol vehicles, covert vehicles and speed trailers.	Meets Requirement. RocketIoT ALPR™ can be used for Portable fixed object stationary mounted applications, and can be easily relocated and re-mounted. RocketIoT ALPR™ is also deployable as a Mobile mounted application for marked patrol vehicles, covert vehicles, and speed trailers, etc. The in-vehicle installation comprises ALPR, DVR video camera and a high-speed router in a single device, which connects to the agency network. This eliminates the need for separate devices and reduces the cost and space needed in the squad vehicle.
2.2.2	Marked patrol vehicle camera mounting brackets must be compatible with Whelen, Code3, TOMAR, Federal Signal, Arjent S2 light bars	Meets Requirement. RocketIoT ALPR™ mounts (external to the vehicle) with a universal bracket, compatible with standard industry equipment.
2.2.3	Cameras shall be self-illuminating Infrared (IR) for effective license plate image capture in a variety of weather and lighting conditions	Meets Requirement. RocketIoT ALPR™ has the capability for automatic and manual day and night modes. RocketIoT ALPR™ has the capability for color, with an infrared range of 40M (131 ft.).
2.2.4	LPR cameras shall be water-resistance with few moving parts that can be damaged	Meets Requirement. RocketIoT ALPR™ is a solid state, cast aluminum device that has few moving parts that can be damaged. RocketIoT ALPR™ is rated IP67 weatherproof, rated MIL-810 for vibration, rated for a temperature range of -30 degrees Celsius to 50 degrees Celsius, and rated IK10 for vandal proof housing.
2.2.5	LPR cameras shall have the ability to automatically capture all variations of California license plates, to include California dealer issued plates (paper plates)	Meets Requirement. The RocketIoT ALPR™ ability to capture California dealer issued plates (paper plates) requires custom configuration.

2.2.6	Cameras shall have a dual lens configuration in a single camera housing, featuring both an IR lens for license plate capture and a color overview image of the vehicle for verification purposes	Meets Requirement. The RocketIoT ALPR™ has the ability to run in color continuously, delivering superior performance.
2.2.7	Cameras shall be sealed to NEMA 6 (IP67) standards	Meets Requirement. RocketIoT ALPR™ cameras are rated IP67 weatherproof, rated MIL-810G for vibration, shock temperature (range of -30 degrees Celsius to 50 degrees Celsius), and rated IK10 for vandal proof housing.
2.2.8	Dual lens camera shall be capable of capturing up to 60 frames per second	Meets Requirement. RocketIoT ALPR™ captures images at an adjustable rate of 30 fps or 60 fps.
2.2.9	Cameras shall have the ability to adjust shutter, brightness, and gain settings to ensure a high-quality image regardless of weather or lighting conditions	RocketIoT ALPR™ has the capability for automatic and manual day and night modes.
2.2.10	The cameras shall be able to have a fixed focal point or target distance from the camera to the vehicle's license plate from 9 ½ feet to 30 feet	Meets Requirement. RocketIoT ALPR™ has a capture range that meets and exceeds the 9 ½ feet to 30 feet requirement.
2.2.11	The camera shall be capable of various configurations to capture plates in any of the following modes depending on the configuration:	Meets Requirements. See responses below:
2.2.11.1	An adjacent lane on either side of the vehicle while driving through traffic and/or parking lots	Meets Requirement. The RocketIoT ALPR™ has single or multiple camera image capture capability, and includes the ability to capture plates in adjacent lane on either side of the vehicle while driving through traffic and/or parking lots.

2.2.11.2	Traffic in an adjacent lane while parked on the side of the shoulder of a roadway	Meets Requirement. The RocketIoT ALPR™ has single or multiple camera image capture capability, and includes the ability to capture plates in traffic in an adjacent lane while parked on the side of the shoulder of a roadway.
2.2.11.3	Parked vehicles in parking lots	Meets Requirement. The RocketIoT ALPR™ has single or multiple camera image capture capability, and includes the ability to capture plates from parked vehicles in parking lots.
2.3	**LPR PROCESSOR**	
2.3.1	Processor shall have a "self-trigger" mode to detect the presence of correctly mounted vehicle license plates in the camera's field of view for image capture from the camera	Meets Requirement. The RocketIoT ALPR™ is in a self-trigger mode upon activation.
2.3.2	Processor's installed in vehicles shall be equipped with an intelligent Power Supply Unit (PSU) that provides for a safe start and shut-down each time the vehicle's ignition is turned on and turned off	Meets Requirement. The RocketIoT ALPR™ device monitors ignition and will intelligently turn on and turn off in a safe manner with a configurable shut down timer.
2.3.3	Processor controls the power supplied to the cameras and provides video connection points for simplified system wiring	Meets Requirement. Power and control to the cameras is provided by the RocketIoT ALPR™ system, using PoE.
2.3.4	Processor shall have at least four (4) LPR camera connections and multiple USB ports	Meets Requirement. RocketIoT ALPR™ has the ability to connect up to four cameras, as well as a USB port that is capable of generating a hub for multiple USB ports.

2.3.5	Vehicle mounted processors shall meet the environmental conditions associated with being mounted in a trunk	Meets Requirement. RocketIoT ALPR™ vehicle mount is rated IP67 weatherproof, rated MIL-810G for vibration, rated for a temperature range of -20 degrees Celsius to 70 degrees Celsius.
2.4	**LPR SOFTWARE**	
2.4.1	Application software shall be capable of running on a Windows based mobile computer	Meets Requirement. AVaiLWeb™ and RocketWeb™ are browser-based applications which supports the RocketIoT ALPR™. They can be accessed on a computer desktop, or on a tablet or MDC in the field, using a common web browser. It runs on standard web browsers, including Chrome, Internet Explorer, Edge, and Firefox. It is capable of running on a Windows based mobile computer. There is no requirement for installation of the application software on County computers.
2.4.2	There shall be no Java programming or Java derivatives	Meets Requirement. RocketIoT ALPR™ is accessed using a standard web browser. There is no requirement for installation of the application software on County computers.
2.4.3	LPR system shall have real time alerting and the ability to program custom hotlist	Meets Requirement. RocketIoT ALPR™ has real time alerting, and the ability to program custom hotlist.
2.4.4	There shall be a secure login and password function on the LPR software; The user's access shall be controlled by an administrator designated by the San Diego County Sheriff's Department	Meets Requirement. The RocketIoT ALPR™ License Plate Reader Camera System operates with AVaiLWeb™, Utility's centralized web based digital evidence management system.

		AVaiLWeb™ provides a simple way to manage individual user profiles and security settings by providing administrators a way to define security roles with a unique set of permissions. Since each user has a security role tied to them, you always have a quick way to manage what a user has access to. The various permissions assigned to roles define exactly what users are allowed to do and not allowed to do within the system. Permissions include field video review, managing video markers and notes, who can review whose and which videos (by classification or sealed status), export and redaction, user permission and group management, etc.
2.4.4.1	API capable of integrating user defined active directory	Meets Requirement. RocketIoT ALPR™ with the AVaiLWeb™ supports Single Sign On (SSO), working with your existing Active Directory Federation Services system.
2.4.5	The software shall provide live, simultaneous display of all the following data:	Meets Requirements. See responses below:
2.4.5.1	The IR license plate image	Meets Requirement. For each capture within the RocketIoT ALPR™ system, a snapshot of the tag is presented to the officer/operator.
2.4.5.2	The license plate interpretation or system read	Meets Requirement. For each capture within the RocketIoT ALPR™ system, the officer/operator is presented with the system read of the tag.
2.4.5.3	A corresponding color overview of the vehicle displaying the captured IR license plate	Meets Requirement. The RocketIoT ALPR™ has the ability to run in color continuously, and when it is in color mode, it will present the corresponding color overview of the vehicle displaying the captured IR license plate, as well as the captured license plate.

2.4.5.4	The date and time stamp	Meets Requirement.
2.4.5.5	Identification of the camera capturing the image	Meets Requirement.
2.4.6	Software shall capture GPS coordinates for every recorded license reads	Meets Requirement.
2.4.7	Software shall have the ability to GPS stamp all the reads	Meets Requirement.
2.4.8	Software will give a unique audible and visible alert when a wanted license plate is discovered	Meets Requirement. The RocketIoT ALPR™ will present to the officer both audible alert, as well as a 'red flashing area' around the tag.
2.4.9	The Alert Screen remains displayed until acknowledged by the user, and, while displayed, the system continues to process license plate data in the background	Meets Requirement.
3.0	**DEMONSTRATION OR SAMPLE**	
3.1	County reserves the right to request an on-site demonstration of the LPR camera system being bid or a sample be sent to determine if it meets the requirements stated. All specifications listed in the General Requirements shall be confirmed. All travel, demonstration supplies and/or shipping expenses shall be at the contractor's expense.	Utility would be honored to provide the County an on-site demonstration of the unique features and capabilities of the RocketIoT ALPR™ License Plate Reader Camera System, operated with AVaiLWeb™.
4.0	**INSTALLATION**	
4.1	Contractor shall provide the option to purchase systems as a "kit" that includes all hardware, wiring and software for standard installations	Utility's RocketIoT ALPR™ License Plate Reader Camera System and AVaiLWeb™ is an all-inclusive solution, provided as a 'System as a Service' (SaaS), and includes all equipment, installation, services, training, customer

		support, Smart Redaction, and unlimited Cloud storage. The RocketIoT ALPR™ 'kit' is all-inclusive, and the County will be provided with training and installation. The technical system functionality is fully managed by our software engineers to ensure that it will always be up to date for all of our customers on our Cloud-based platform. All system upgrades are all done over-the-air (OTA), without requiring ALPR operator/officer effort.
4.2	Contractor shall provide installation and warranty repair options on vehicles within San Diego County.	Utility's APR is provided as a Service as a System (SaaS) subscription. Utility warranties are in full effect for the term during a current paid annual SaaS subscription. Hardware failure outside of malicious intent is fully covered free of charge by Utility. Utility will provide product installation, and Utility can certify local installers to the Product. Utility provides 24/7/365 technical support. All users have access to the help desk service phone number for technical support during or after normal business hours. Should there be an outage notification, users will receive a call back within one hour. Should the County need to return hardware, authorized stakeholders will need to email Utility's support team with all relevant information on the device, including the serial number and the reason for the return. Once the necessary information is received, our team will send a shipping label for the County to complete the return. Replacement equipment is cross-shipped the day after Utility is notified about an issue. Please refer to the Appendix for a summary and links to Utility's warranty, terms and conditions, and System as a Service (SaaS) agreement

<table>
<tr><td>4.3</td><td>Contractor shall provide a technician or representative to visit customer site for system start-up, configuration and commissioning of LPR system</td><td>Utility’s ALPR implementations are all-inclusive. They include training, technical support and assistance, devices, networking equipment, video uploading, charging, connectivity, system software and upgrades, and video retrieval software and procedures.</td></tr>
<tr><td colspan="3">5.0 CUSTOMER SUPPORT</td></tr>
<tr><td>5.1</td><td>The Contractor shall provide technical advice and sales support within 72 business hours.</td><td>Meets Requirement.

Utility provides 24/7/365 technical support. Our technical support associates are located at our home office in Decatur, Georgia, in Metropolitan Atlanta. Utility has employees in all time zones. All users have access to the help desk service phone number for technical support during or after normal business hours. Should there be an outage notification, users will receive a call back within one hour.

Utility has a tiered response to support that will escalate the level of support depending on the situation. Tier 1 would be onsite support by County staff after they have been trained by Utility, which will alleviate most day-to-day issues that may arise. Problems beyond Tier 1 scope will be escalated to Tier 2 and from there to Tier 3, which is onsite technical support from a Utility field engineer.

<table>
<tr><th>Item Priority</th><th>Fatal</th><th>Severe</th><th>Medium</th><th>Minor</th></tr>
<tr><td>1</td><td>1 Hour</td><td>1 Hour</td><td>2 Hours</td><td>3 Hours</td></tr>
<tr><td>2</td><td>2 Hours</td><td>2 Hours</td><td>4 Hours</td><td>6 Hours</td></tr>
<tr><td>3</td><td>4 Hours</td><td>4 Hours</td><td>8 Hours</td><td>16 Hours</td></tr>
</table>

Please refer to the Appendix for a detailed copy of Utility’s Customer Service Agreement (SLA).</td></tr>
</table>

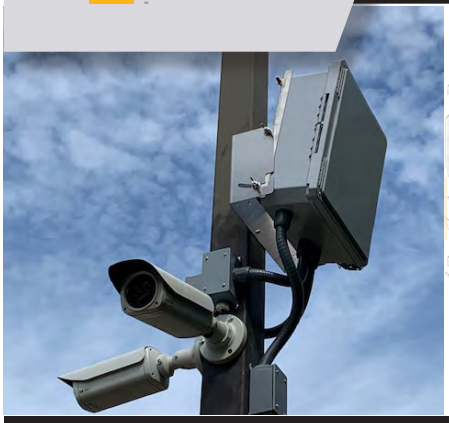
6.0	**TRAINING**	
6.1	The County reserves the right to request up to eight (8) hours of training at a San Diego County Sheriff's Department facility within 30 days of delivery at no additional charge. This is in addition to the requirement set forth in 4.3.	Utility's RocketIoT ALPR™ implementations are all-inclusive. They include training, technical support and assistance. Training is on-site, in-person, and online and interactive.
7.0	**DELIVERY REQUIREMENTS**	
7.1	Delivery address: San Diego County Sheriff's Department Attn: Ivy Scites - Grants Unit 9621 Ridgehaven Court San Diego, CA 92123	Utility will comply with the County's delivery requirements.
8	**INVOICE**	
	Only new products shall be accepted. An LPR system that has been used in any way, refurbished, reconditioned, or gray market is unacceptable and will be rejected and returned. The County shall be given credit for damaged and returned items within five (5) business days. There shall be no restocking fees or other charges for returns of damaged or incorrect items. Deviations to the terms, conditions and/or specifications shall be conspicuously noted in writing by the respondent.	Utility will comply with the County's delivery requirements.
9	**LEAD TIME**	
9.1	Department requested deliver lead time: 60 days.	Utility has reviewed and understands this requirement and will comply.

ROCKETIOT™

by

UTILITY

4 AUTOMATED LICENSE PLATE RECOGNITION MUST HAVES



RocketIoT ALPR is fundamentally better.

No other LPR solution has these 4 Must Have capabilities. Your Officers and Citizens deserve the best.

1 CONNECTIVITY

With Smart ALPR on patrol, your officers have total system connectivity directly to the AWS GovCloud for real-time access to Federal, State and local databases for purposes of automatically searching for hotlisted vehicles.

2 REAL-TIME ALERTS

Central Dispatch can start live video streaming from any in-car camera system. Video is automatically uploaded as it is recorded to secure CJIS compliant storage. Video can be available immediately.

3 INTELLIGENCE BUILT IN

Unlike traditional LPR systems, ALPR is powered by artificial intelligence (AI) which provides a new ability to read license plates at high speeds and through windshields all while comparing data on the edge. ALPR runs passively the background throughout an officer's patrol shift allowing unknown threats to become known in real-time. (Built in collaboration with SONY.)

4 FORCE MULTIPLIER

ALPR provides greater efficiency for the patrol officer which translates to increased productivity for your agency. ALPR allows officers to focus on their job functions while patrolling as it leverages AI and the total system to maximize the officer's effectiveness. The ALPR total system gives an agency the ability to do more with less makes which makes it cost-effective for today's efficiency-focused law enforcement leaders.

bodyworn.com

Automated License Plate Recognition

Product Features & Specifications



Made in the USA

ALPR BOX

Dimensions: 172mm(l) x 122mm(w) x 38mm(h)

Material: Cast Aluminum

Power: Dual (DC: 9 to 24Vdc or PoE 802.3at compliant)

Processor:
- CPU: Dual Core nVidia Denver 2 64-bit & Quad Core ARM Cortex-A57
- GPU: 256 Core nVidia Pascal

Memory: 16GB

Connectors: color coded, water tight, locking
- RED: Power
- BLUE: 10/100 Ethernet (802.3 PoE)
- BLACK: USB 2.0 (optional) | 5V /1.5A output

Environmental:
- Operational Temp Range: -20 to 70 deg C
- Storage Temp Range: -40 to 85 deg C
- IP-67: (submerge 1M for 30min w/ no water ingress)

Certifications:
- FCC
- MIL-810G: Shock, Vibration and Temperature

FEATURES:

- **Extension of the RocketIoT System:** Utilizes the Connectivity and Video Functionaily
- **Real-Time Connectivity to Hot Lists:** Federal, State and Local Data Sources
- **Ability to Inject Local Data** in Real-time
- **Agency Force Mulitipler:** Passively and Continuously Collects Data Throughout an Entire Shift
- **Uses Artificial Intelligence** to Analyze Data at Fast Speeds
- **Real-Time Configurable Alerts:** Transmit to BodyWorn Device, In-Car Video Display, Command & Dispatch, Other Officers in the Area
- **Plate Lookup:** Provides Historical Plate Data with Location and Time
- **Enhances Officer Safety:** Live Situational Awareness Component
- **Cost Effective:** Outfit More Locations and Vehicles within Your Agency

ALPR CAMERAS

- 2MP Full HD
- Up to 60 FPS at 1080p (H.264)
- 12mm Lens
- 0.1 LUX in color Minimum Illumination for Optimal Low Light

Performance

- 0.0 LUX in B/W (IR on 40m Range)
- Auto Day / Night mode
- Action Button (Start/Stop)
- AAC Encoding, Integrated Mic
- Multiple Mounting Options

© Copyright 2020 Utility, Inc. All Rights Reserved.

AVAILWEB™

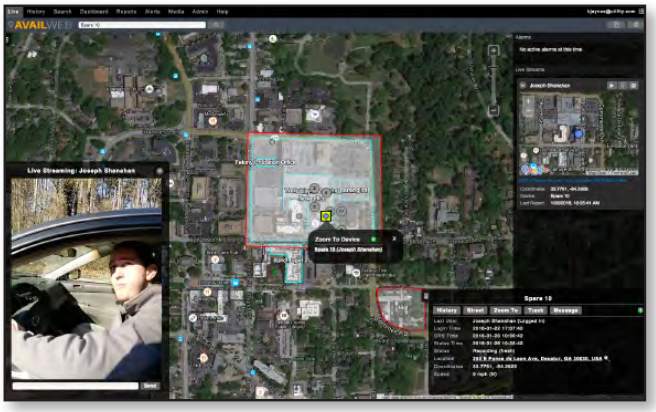
Smarter Digital Evidence Management

AVaiLWEB™ is a powerful web-browser solution that makes it easy yet secure to search, play, manage, redact, and share video and data with a secure chain of custody. The media interface allows multiple related video and audio feeds to be played simultaneously. AVaiLWEB also has live video streaming allowing dispatchers and supervisors to have complete situational awareness. It also provides an automatic real-time, map-based view of location and status of all mobile operations, including vehicles, personnel, and assets. AVaiLWEB provides Geofence alerts, live tracking, traffic and weather overlays, asset overlays and Street Views.

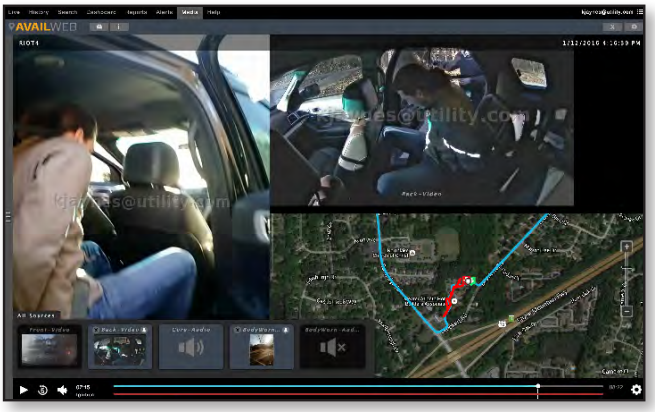
- All-In-One Web-Browser Platform
- Seamless Transfer of Video
- Secure & Unlimited Cloud Storage
- Geofence & Action Zone Activation
- Synchronized Video & Audio
- Video Redaction Tools
- Comprehensive Chain of Custody
- Customizable Configurations
- Multiple Videos from an Incident
- Live Map View
- Live Video Streaming
- Interactive Reporting
- Send Real-Time Alerts
- Ultimate Witness Portal



LIVE VIDEO STREAMING



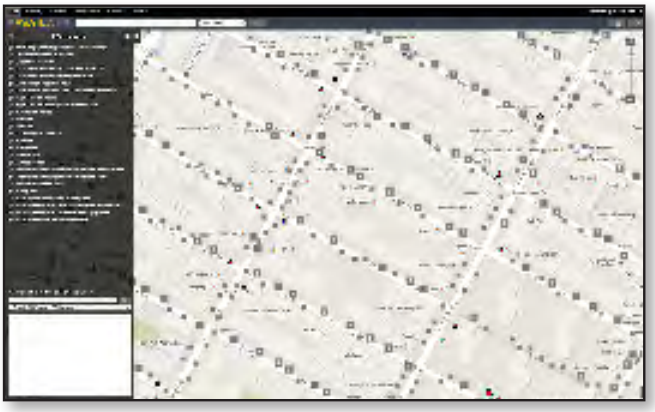
VIDEO TRACKING AND PLAYBACK



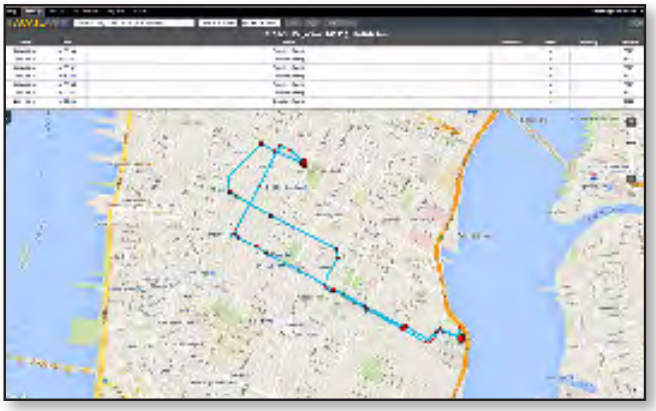
CUSTOM GEOFENCES



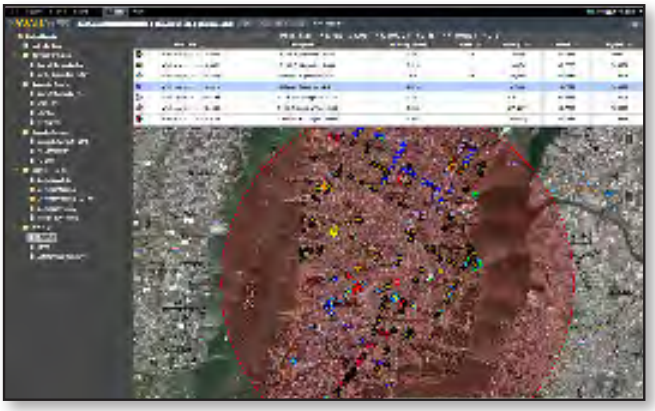
GIS/ESRI DATA OVERLAYS



HISTORICAL GPS TRACKING



CUSTOM DEVICE REPORTS



Smart Redaction

Automated Video Redaction

With SmartRedaction™, law enforcement agencies have the ability to redact video more effectively and efficiently when responding to Public Records Requests for video evidence, such as Freedom of Information Act (FOIA). The process of preparing videos for public dissemination, while maintaining privacy rights of those involved, can be time consuming and expensive. Not with Smart Redaction.



Smart Redaction identifies, tracks and redacts objects and people in a video, alleviating the need for large staff to work long hours to review and manually redact video. Smart Redaction is an industry-leading redaction tool, that protects the privacy of victims, innocent bystanders, minors and undercover officers, while saving time and money for the agency using it.



SMART ALPR

PAIRED WITH ROCKET IOT IN-CAR VIDEO

By incorporating ALPR into our in-car system, we've made LPR more cost-effective for agencies to outfit more vehicles within their agency.

The vehicle cameras catalog license plate data while searching hot-lists. Once detected, the system automatically sends an alert enabling the department to respond quickly.

IN COLLABORATION WITH SONY

REAL-TIME CONNECTIVITY TO HOT LISTS

FROM STATE, LOCAL & FEDERAL DATA SOURCES

MOBILE & STATIONARY ALPR

UTLITIZES A.I. AT THE EDGE

PLATE LOOKUP

PROVIDES HISTORICAL PLATE DATA WITH LOCATION & TIME

WHEN A HOTLIST PLATE IS DETECTED

CONFIGURABLE ALERTS TRANSMIT TO ONE OR ALL OF THE FOLLOWING:

- BODYWORN DEVICE
- IN-CAR DISPLAY
- COMMAND & DISPATCH
- OTHER OFFICERS IN AREA

COST EFFECTIVE

OUTFIT MORE VEHICLES WITHIN YOUR AGENCY

FURTHER ENHANCES THE DEPARTMENT'S ENFORCEMENT CAPABILITIES

EXTENSION OF THE ROCKETIOT SYSTEM

CAMERAS & CONNECTIVITY CAN BE MANAGED BY THE ROCKETIOT



Smart ALPR Specifications

Dimensions: 172mm(l) x 122mm(w) x 38mm(h)

Material: Cast Aluminum

Power: Dual (DC: 9 to 24Vdc or PoE 802.3at compliant)

Processor:
- CPU: Dual Core nVidia Denver 2 64-bit & Quad Core ARM Cortex-A57
- GPU: 256 Core nVidia Pascal

Memory: 32GB

RF Connectors: 2x RP-SMA
(802.11a/b/g/n/ac 2x2 867Mbps | Bluetooth 4.1)

Connectors: color coded, water tight, locking
- RED: Power
- BLUE: 10/100 Ethernet (802.3 PoE)
- BLACK: USB 2.0 (optional) | 5V /1.5A output

Environmental:
- Operational Temp Range: -20 to 70 deg C
- Storage Temp Range: -40 to 85 deg C
- IP-67: (submerge 1M for 30min w/ no water ingress)

Certifications:
- FCC
- MIL-810G: Shock, Vibration and Temperature

Delivering Intelligence on a Scale Never Before Imagined.

© Copyright 2019 Utility, Inc. All Rights Reserved.

Communications & In-Car Video

Product Features & Specifications

Made in the USA



FEATURES:

- 4G LTE CAT-12 Internal Cellular Modem
- Supports All Major US Carriers
  AT&T, FirstNet, Verizon, Southern Linc, Sprint, US Cellular
- Dual WiFi: Hotspot around the vehicle
  Access Point for high-speed offload
- Integrated Crash Sensor
- Integrated Battery Monitoring & Internal Temperature Sensor (for health monitoring)
- Optically Isolated Trigger Inputs & 1 Relay Output (5 total, 4.5V to 24V)
- Integrated Siren Trigger Interface
- Integrated On-Board Diagnostics: J1979 (ISO 15675-4), J1939 (The ISO 15675-4 was mandated in 2008 for all US cars: Is CAN interface)
- Under Voltage Warning / Shutdown
- Software Adjustable Shutdown Timer
- Integrated GPS with Antenna Detection Technology (for health monitoring)
- Remotely manage network configurations: Firewall, IPSec, Port Forwarding, Split networking, black and white list, bandwidth management

ROCKET IOT

Dimensions: 197mm (l) x 150mm (w) x 43mm (h)

Material: Cast Aluminum

Power: 9 - 24Vdc / 14W

Storage: 120GB Solid State Drive

Processor: Intel Dual Core Atom Processor, 1.33GHz

Memory: 2GB RAM, 1066 MT/s

Connectors: Color Coded, Water Tight, Locking

- 1 RED: Power and On-Board Diagnostics
- 2 DARK BLUE: 4 Ethernet (802.3af PoE 10/100Mb)
- 1 BLUE: 1Gb Ethernet
- 1 BLACK: Triggers (1 Ignition, 4 Programmable Inputs, 1 Siren, 1 Relay Output)
- 1 Radar Interface (RS-232)
- 1 USB 2.0 (optional)

RF Connectors

- 2 Cellular
- 2 WiFi 2.4/5 GHz (WiFi 802.11 g/n/ac MIMO) Hotspot
- 2 WiFi 2.4/5 GHz (WiFi 802.11 g/n/ac MIMO) Access Point
- 1 SMA GPS

Environmental

- Temperature Range: -20° to 70° C
- IP-67 (submerge 1M for 30min w/ no water ingress)

Certifications

- FCC
- MIL-810G: Shock, Vibration & Temperature
- PTCRB
- FirstNet

IN-CAR CAMERAS

Front Camera

- 2MP Full HD
- 60 FPS at 1080p (H.264)
- 0.1 LUX Minimum Illumination for Optimal Low Light Performance
- Auto Day / Night mode
- 4mm Lens (Wide Angle)
- Robust Low Profile Mounting
- Action Button (Start/Stop)
- AC Encoding, Integrated Mic

Back Seat

- 2MP Full HD
- 30 FPS at 1080p (H.264)
- 0 LUX Min Illumination
- Auto Day / Night mode
- Integrated Microphone
- 2.9mm Lens (Wide Angle)
- Robust Mounting Design

© Copyright 2020 Utility, Inc. All Rights Reserved.



XLE Installation Guide

Apr 2020

Notices

The contents of this document and the associated software are the property of Utility, Inc. Any reproduction in whole or in part is strictly prohibited. For additional copies of this document or software, please contact Utility, Inc.

Information in this document is subject to change without notice and does not represent a commitment on the part of Utility, Inc. The software as described in this document is furnished under a license agreement or non-disclosure agreement. The software may be used or copied only in accordance with the terms of the agreement. It is against the law to copy said software on any medium except as specifically allowed in the license or non-disclosure agreement. No part of this manual may be reproduced or transmitted in any form or by any means, for any purpose, without the express written permission of Utility, Inc. Companies, names, and data used in examples herein are fictitious unless otherwise noted.

Table of Contents

Introduction and Overview 4

Solution Components 5

1. Rocket IoT XLE 5
2. Quadband Permanent Mount Antenna 9
   Alternative Antennas 10
3. Power Cables 12
4. Cameras (Optional) 13
5. Video Controller Tablet (Optional) 14
6. Door Sensor (Optional) 15
7. LED Recording Light (Optional) 16
8. Vehicle Diagnostics Cable (Optional) 17
9. RS-232 and USB (Optional) 19
10. ALPR Graphics AI Co-Processor 20

Rocket IoT XLE Mounting and Placement 22

Antenna Placement and Installation 24

Providing Power to the Rocket IoT XLE 26

Providing Power to the Graphics AI Co-Processor 28

GPIO Trigger Cable 29

Antenna Connections to the Rocket IoT XLE 30

SIM Card Installation 31

Finishing the Hardware Installation 32

Rocket IoT XLE Blink Codes 33

Recommended Fuse Sizes 34

GPIO Expanded Wiring View 35

Support Help Desk Contact 36

Introduction and Overview

This document is designed to instruct an experienced and qualified installer how to properly install all Utility Associates (UA) hardware for the Rocket IoT XLE (RIoT-XLE) system. This guide includes detailed specifications about the hardware as well as optimal power, and installation locations/techniques.

Rocket IoT XLE Hardware Installation Locations

1. The first step of installing any of the Utility Video and BodyWorn equipment is to first determine where existing equipment is currently located, or is going to be mounted in a vehicle. Here are the main components to consider:

- Rocket IoT XLE processing and communications unit
- ALPR Co-Processor unit - optional
- Antennas
- Power / Cabling
- Cameras (Front and/or Rear) – optional
- Tablet – Video Controller inside the front windshield - optional
- Video Recording and Data Capture Triggers – Door Sensor, Lightbar, Siren, etc. – optional
- LED Recording Light - optional
- Vehicle Diagnostics Interface cable – OBD-II or JBUS – optional
- Ethernet Devices in the vehicle – Laptop, ALPR processor, other - optional
- RS-232 or USB Devices in the vehicle – Radar Gun, Printers, other – optional
- ALPR Graphics AI Co-Processor - optional

2. When deciding on where the equipment is going to be installed, you need to take a few things into consideration especially because they are criteria for a "Certified Installation". These criteria are emphasized here first because they always seem to come up first.

- Never use self-tapping screws to mount the Rocket IoT XLE to the vehicle. The only approved method is bolts, washers and Keps nut or locking nylon nuts can be used.

- Only factory or power distribution center power, ground, and ignition sense breakouts should be used for these main power connections.
  - In most police package or public safety vehicles there will be multi-amperage breakouts.
  - When in doubt go straight to the battery's positive/negative terminals for power and ground and find a factory ignition sense to splice into.
  - Do not use "T" or Splice taps or Scotch locks for any wiring connections.

Solution Components

1. Rocket IoT XLE:



Rocket IoT XLE with Category 12 4G-LTE modem chipset.

- Vehicle power connector - Red
- Two dual 10/100 PoE Ethernet Port connectors – medium Blue
- One Gigabit non-POE Ethernet Port connector – Dark Blue
- Vehicle Diagnostics connector - Black
- RS-232 and USB connectors - Black
- Internal 128GB Solid State Hard Drive
- Cellular Modem Chipset slot and cover with rubber gasket
- External Antenna connectors – Two Cellular, Four WiFi, one GPS – on the back of the unit
- MIL-STD 810G – Dust and Vibration
- IP-67 – Dust and Waterproof up to one meter of water for 30 minutes
-

Rocket IoT XLE Dimensions:

- Long 197mm 7.756 inches
- Wide 150mm 5.905 inches
- High 43mm 1.693 inches

The distance between the centers of the two attach slots on the left and right edges of the housing is 184mm / 7.244 inches

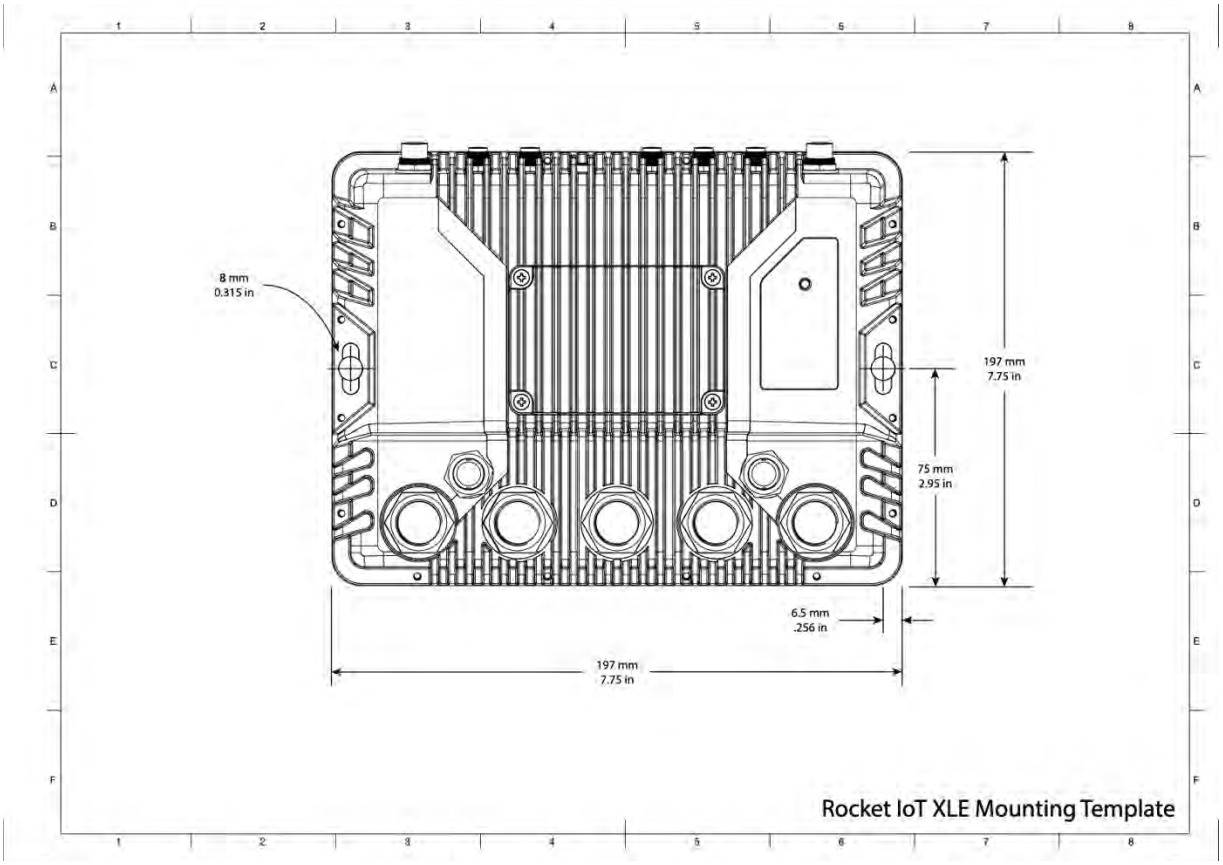


The edges of the cooling fins do not extend beyond the edges of the housing.

Rocket IoT XLE Mounting Template:

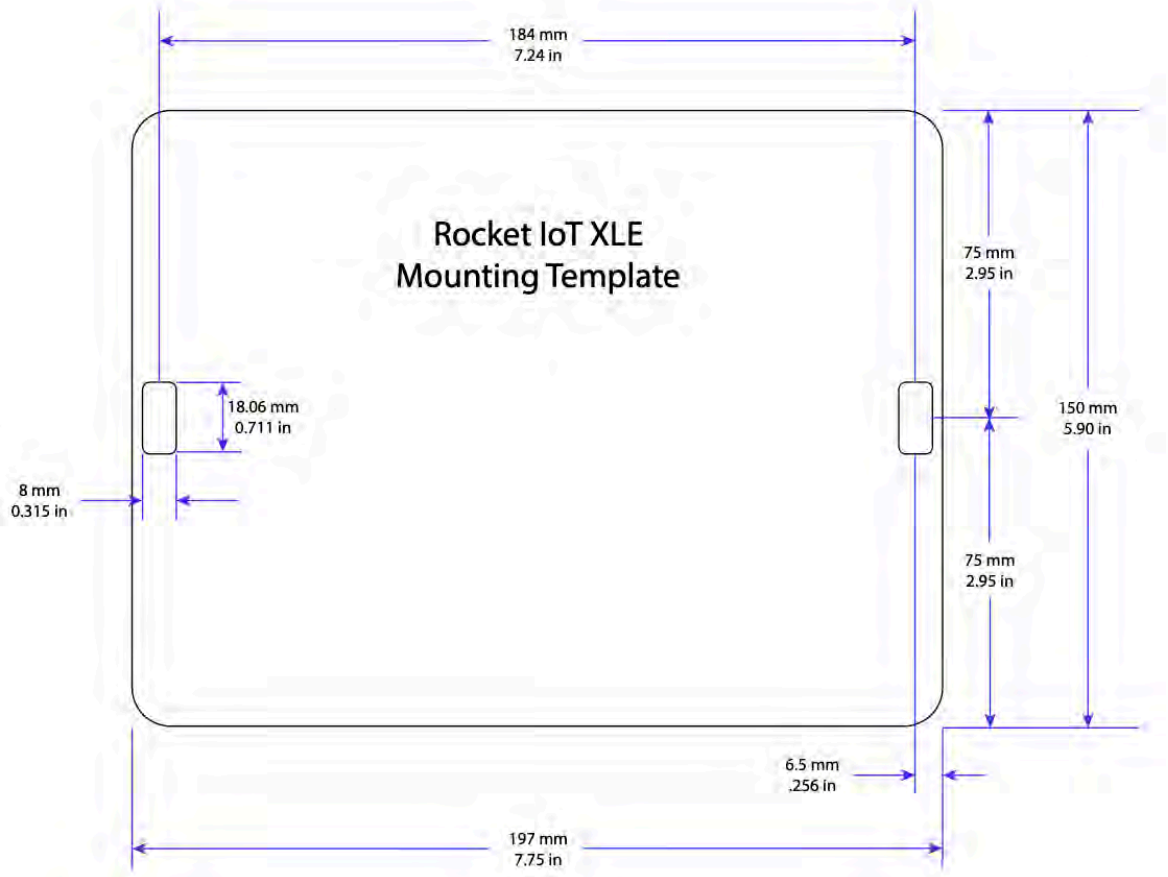
This template displays the footprint dimensions of the Rocket IoT XLE, and the location and dimensions of the mounting slots on the left and right edges of the housing.

The recommended install is to use threaded mounting pins or bolts through the mounting slots to firmly attach the Rocket IoT XLE to an underlying metal electronics tray, console, or other hard vehicle surface. Use washers and bolts to secure the Rocket IoT XLE hardware so that it never comes loose and becomes loose inside the vehicle cab, which could become the safety hazard of being a metal projectile flying around inside the vehicle cab in the event of a vehicle crash. Washers, nuts, and potentially gaskets securely tight will also minimize rattles and cable attachments working loose.



A simplified mounting template schematic is shown on the following page.

This diagram shows the outer dimensions and the location of the mounting slots on the left and right side of the Rocket IoT XLE.



2. Quad-Band External Permanent Mount Antennas:

- Two separate quad-band antennas for each Rocket IoT XLE
- Dual antennas are required to provide Cellular and WiFi diversity required by the Category 12 4G-LTE Cellular Modem chipset, and 802.11ac WiFi. Only one antenna is not acceptable, and will not allow the Rocket IoT XLE to reliability connect to 4G-LTE cellular service. **MUST** be two cellular antennas on every Rocket IoT XLE install.
- Each Antenna includes one Cellular Antenna, one GPS Antenna, and two WiFi Antennas
- Antenna Post: ¾" diameter by ½" length post (1" option – fire trucks)
- Antenna Cable length: 15 feet (20' and custom length cables available).
- Each quad band antenna has four antenna elements:
    - 1 x Cellular. Deigned to cover 694-894 Mhz (3 DBi gain) and 1.7 – 2.7 Ghz (5 DBi gain) frequency ranges; FME connector.
    - 1 x GPS. 1575.42 Mhz (+/- 2 Mhz), 5 DBi gain. SMA connector.
    - 2 x WiFi. 2.1-2.5 Ghz (5 DBi gain) and 4.9 – 6 GHz (5 DBi gain); RPSMA connector.
- Antenna Colors: White or Black.



Alternative Antennas

Magnetic mount Quadband external antenna. Same format and configuration as a permanent mount Quadband antenna with one cellular, one GPS, and two WiFi antennas, but magnetically affixed to the outside of the vehicle. Proper ground plane required for magnetic mounted antennas. Antenna cable exits the antenna housing at the side, and the cable enters into the vehicle cabin between the vehicle frame and a door. The door gasket more or less seals the gap around the antenna cable. This antenna option is not water-tight. The typical use is for a temporary install, and is not recommended for permanent installations.

Glass-mount internal window Cellular / GPS covert antenna. Includes one cellular antenna and one GPS antenna. Permanently affixed to glass window somewhere inside the cabin of the vehicle, so the antenna cable can be routed directly to the Rocket IoT XLE. Two antennas are required to provide Category 12 4G-LTE Cellular modem diversity. Glass-mount cellular / GPS antennas must be paired with four glass-mount single WiFi antennas, or four WiFi Rubber Duck antennas directly connected to the WiFi RSPMA antenna connectors on the Rocket IOT XLE.



Antenna dimensions are 140mm x 40mm x 18mm. 5.5 inches x 1.59 inches x .71 inches. The antenna cable is ten feet (10') long.

Glass-mount internal window covert WiFi antenna. Require a total of four antennas for the four Rocket IoT XLE WiFi antenna diversity connectors.



Antenna dimensions are 61mm x 17mm x 9mm. 2.4 inches x .65 inches x .35 inches. The antenna cable is twelve feet (12') long.

"Rubber Duck" direct connect WiFi antenna. Require a total of four antennas for the four Rocket IoT XLE WiFi antenna diversity connectors.



Antenna dimensions are 175mm from the bend, and 12mm in diameter. 6.88 inches x .48 inches.

Other Utility BodyWorn certified antennas with a combination of cellular, WiFi, and/or GPS antennas inside an antenna housing may become available in the future. Check with your Utility BodyWorn sales representative about new antenna options that may have become available since this Install Guide was published.

ANTENNA NOTICE

Antennas are a core part of the real-time Situational Awareness and Connectivity solution. Each Rocket IoT XLE requires two cellular antennas, one GPS antenna, and four WiFi antennas, to support MIMO (Multiple Input – Multiple Output) antenna diversity for cellular and WiFi wireless communications.

A single cellular or WiFi antenna (non-MIMO install) cannot be certified for support, performance, or reliability. The Cellular and WiFi chipsets are specifically designed as MIMO requires two antennas to be connected.

Only antennas certified by Utility BodyWorn can be used for Certified installations. Utility takes no responsibility for the performance or reliability of unknown 3rd party antennas that may claim to be "just as good" as the tested and certified antennas provided by Utility.

Utility does not test or warrant 3rd party antennas for performance or reliability. 3rd party antennas void Warranty and Support obligations. Any Utility BodyWorn Help Desk Support and/or Field Engineer time and travel expenses spent to troubleshoot 3rd party antennas are billed at current billing rates then in effect.

3. Cables:

- For a typical police car dual camera install, the Rocket IoT XLE uses four proprietary M12 connector cables for power, PoE cameras, and General Purpose IO (GPIO).
    - Power Cable – Red – Part No: 602-0000075RA
    - PoE Camera Cables – Dark Blue – Part No: 602-0000087
    - Ethernet Docking Cable – Light Blue – Part No: 602-0000079RA
    - GPIO (Trigger Cable) – Black – Part No: 602-0000072RA



- For a non-camera install, only Power and Ethernet Docking cables are required

4. Cameras (Optional):

- Rocket IoT can be upgraded to provide in-car video (ICV) as well as mobile vehicle communications with the addition of two cameras per system.
- Front Camera: Bullet Camera with Utility supplied visor mount.



- Rear Seat Camera: Dome IR Camera with built-in microphone for in-car audio.



5. Video Controller Tablet (Optional):

- The Rocket IoT XLE In-Car Video (ICV) system can be accessed via web browser on a customer's laptop (standard). However, if this is not an option or a separate monitor is required for this purpose, the tablet upgrade option is available.
- The optional tablet upgrade includes the tablet, cradle, and power cable with visor or console mounting options. All of these components are supplied by Utility along with the tablet software.
- Power cable for charging the tablet should always be connected to +12v switched ignition source, not constant power. The USB cable is 5v DC out to tablet. You will install 5v-12v adapter that Utility will supply with the kit.



6. Door Sensor (Optional):

For Triggering of Door opening and closing. This input is used as one of several events that can be used by the Rocket IoT XLE Rules Engine to automatically start or stop video recording, send alerts, and as a trigger for other real-time and audit trail reporting.



7. LED Recording Light (Optional):

(This light will be on when the ICV unit is in record mode)

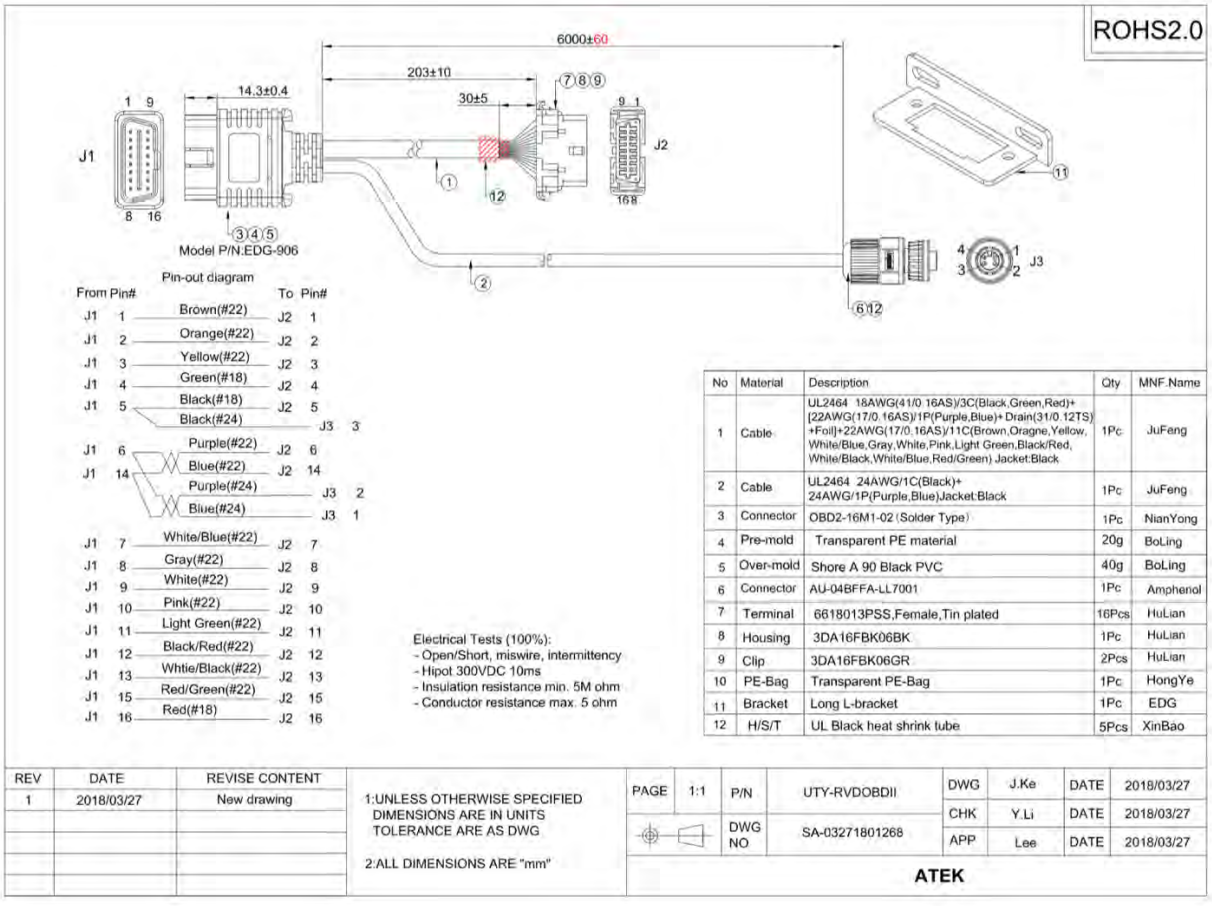


8. Vehicle Diagnostics Cable (Optional):

Cable connecting the Rocket IoT XLE to the vehicle engine diagnostics port. A vehicle will have one of two types of vehicle Diagnostics interface plug. OBD-II or JBUS Type 2.

OBD-II

Cars, Pickup Trucks, SUVs, and Lighter Duty Trucks typically up to about a Ford F250 use the OBD-II standard cable type. The OBD-II plug is typically located within one meter under or nearby the steering wheel. The Y cable is .2 meters long on the short side, and 6 meters with an M-12 connector on the long side to connect to the Rocket IoT XLE. The Y cable allows the vehicle maintenance team to connect to the short cable for vehicle diagnostics reporting, while leaving the Rocket IoT connected to the OBD-II port. Never have to disconnect the Rocket IoT XLE from the vehicle diagnostics port.



No	Material	Description	Qty	MNF.Name
1	Cable	UL2464 18AWG(41/0.16AS)/3C(Black,Green,Red)+{22AWG(17/0.16AS)/1P(Purple,Blue)+ Drain(31/0.12TS)+Foil}+22AWG(17/0.16AS)/11C(Brown,Oragne,Yellow,White/Blue,Gray,White,Pink,Light Green,Black/Red,White/Black,White/Blue,Red/Green) Jacket:Black	1Pc	JuFeng
2	Cable	UL2464 24AWG/1C(Black)+24AWG/1P(Purple,Blue)Jacket:Black	1Pc	JuFeng
3	Connector	OBD2-16M1-02 (Solder Type)	1Pc	NianYong
4	Pre-mold	Transparent PE material	20g	BoLing
5	Over-mold	Shore A 90 Black PVC	40g	BoLing
6	Connector	AU-04BFFA-LL7001	1Pc	Amphenol
7	Terminal	6618013PSS,Female,Tin plated	16Pcs	HuLian
8	Housing	3DA16FBK06BK	1Pc	HuLian
9	Clip	3DA16FBK06GR	2Pcs	HuLian
10	PE-Bag	Transparent PE-Bag	1Pc	HongYe
11	Bracket	Long L-bracket	1Pc	EDG
12	H/S/T	UL Black heat shrink tube	5Pcs	XinBao

REV	DATE	REVISE CONTENT
1	2018/03/27	New drawing

1:UNLESS OTHERWISE SPECIFIED DIMENSIONS ARE IN UNITS TOLERANCE ARE AS DWG

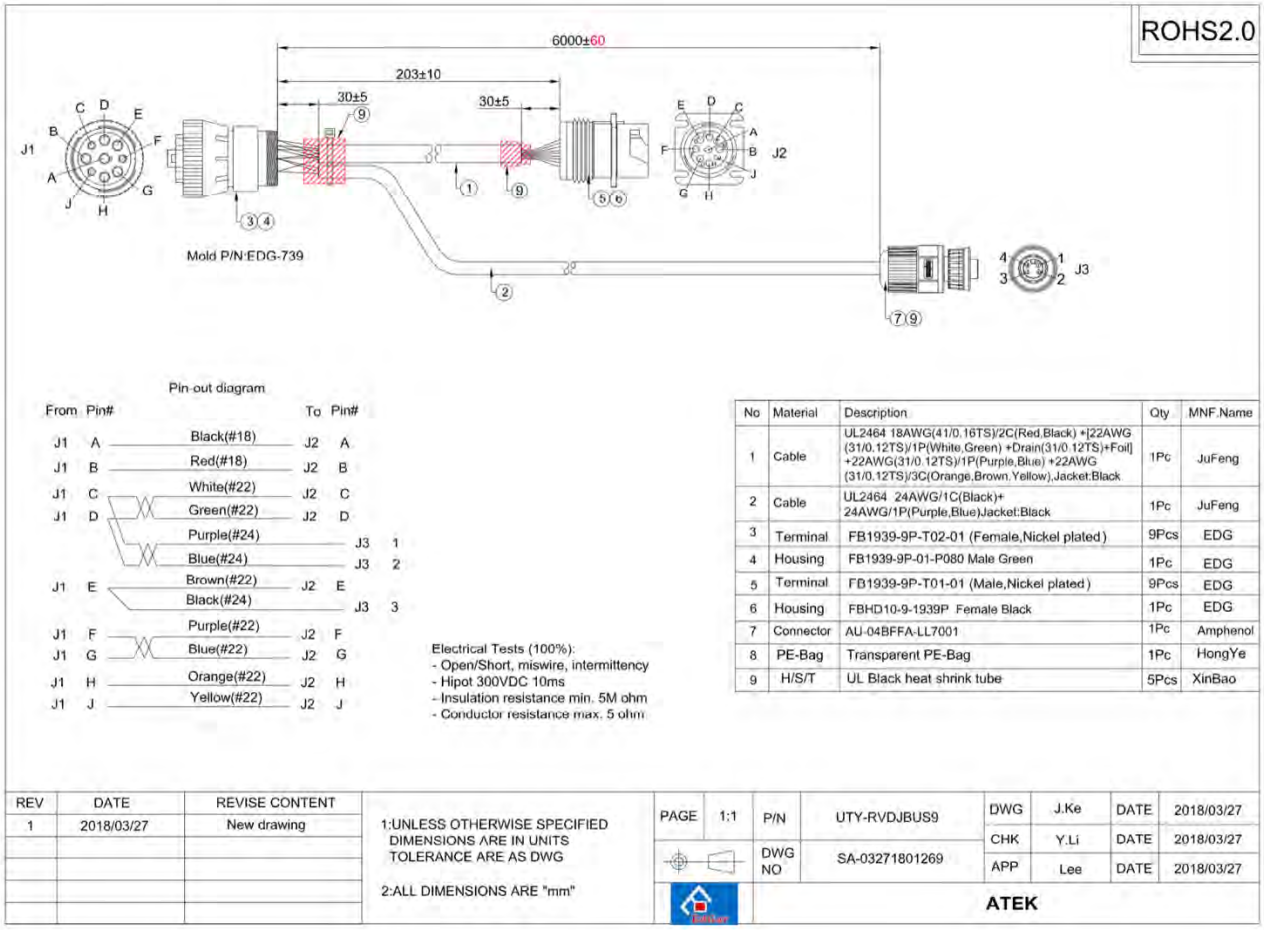
2:ALL DIMENSIONS ARE "mm"

PAGE	1:1	P/N	UTY-RVDOBDII	DWG	J.Ke	DATE	2018/03/27
		DWG NO	SA-03271801268	CHK	Y.Li	DATE	2018/03/27
				APP	Lee	DATE	2018/03/27

ATEK

JBUS Type 2

The JBUS Type 2 standard diagnostics connector is typically used for heavy vehicles – fire engines, ambulances, prisoner transport vehicles, bucket trucks, vactor trucks, crane and heavy inventory transport vehicles, etc. Typically Ford F-350 and up class heavier vehicles.



A Y splitter cable is used so that the Rocket IoT XLE is connected to the JBUS-Type 2 port, leaving one connector available to be connected to Fleet Maintenance Shop diagnostics scanners. The long side of the Y cable splitter with an M-12 connector always remains connected to the Rocket IoT XLE. The second Y cable connector is available to be connected to the Fleet Maintenance Shop vehicle engine diagnostics scanner.

A Y Splitter cable avoids a Shop Mechanic forgetting to plug the Diagnostic cable back into the Rocket IoT XLE. This would cause the Rocket IoT XLE to not report vehicle engine diagnostics Trouble Codes and other data.

The short side of the JBUS Y cable is .2 meters. The long side of the JBUS Y cable is 6 meters.

9. RS-232 Serial Port and USB Devices (Optional):

RS-232 9 pin cables are well known. Vehicle accessories such as a Radar Gun and Ticket Printers sometimes have an RS-232 serial cable interface for using the Radar Gun as a video recording trigger, or for connecting a mobile data terminal to a ticket printer or other similar device.

USB v 2.0 cables are also well known. Ticket printers and other accessory devices may have a USB cable Interface.

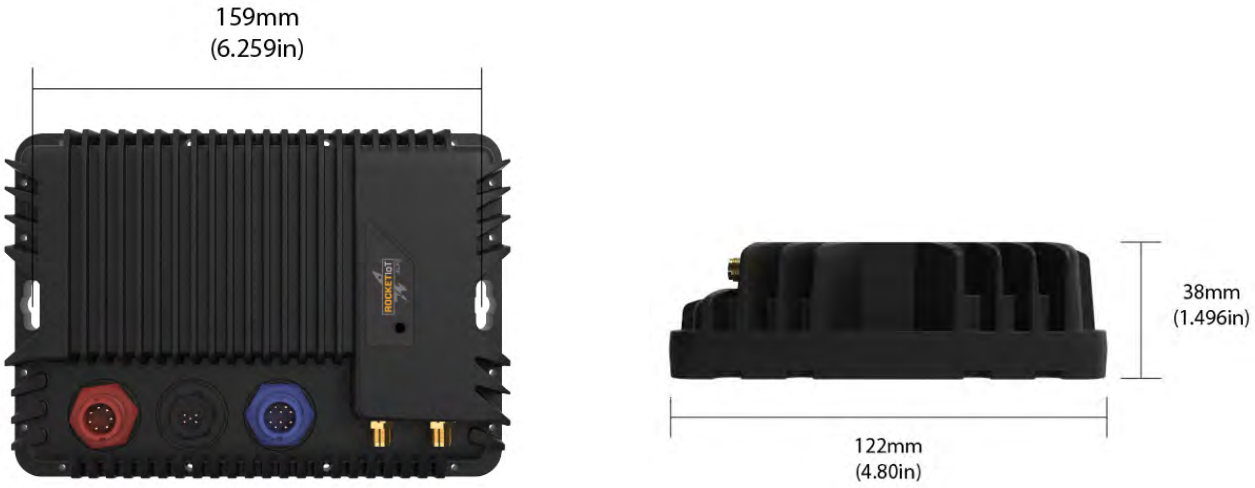
Order an M12 connector RS-232 Serial or USB Cables for the Rocket IoT XLE if you need to attach devices that have an RS-232 9 pin connector or a USB connector.

10. ALPR Graphics AI Co-Processor unit (Optional):

An optional Automatic License Plate Reader Graphics Artificial Intelligence processor connected to a dedicated PoE HD digital camera that reads license plates on vehicles in the front and right lanes in front of the vehicle. The Co-processor contains a very high-performance Graphics AI processor and memory that can perform Video Recognition Artificial Intelligence to identify license plate numbers, and other VR AI recognition as trained.

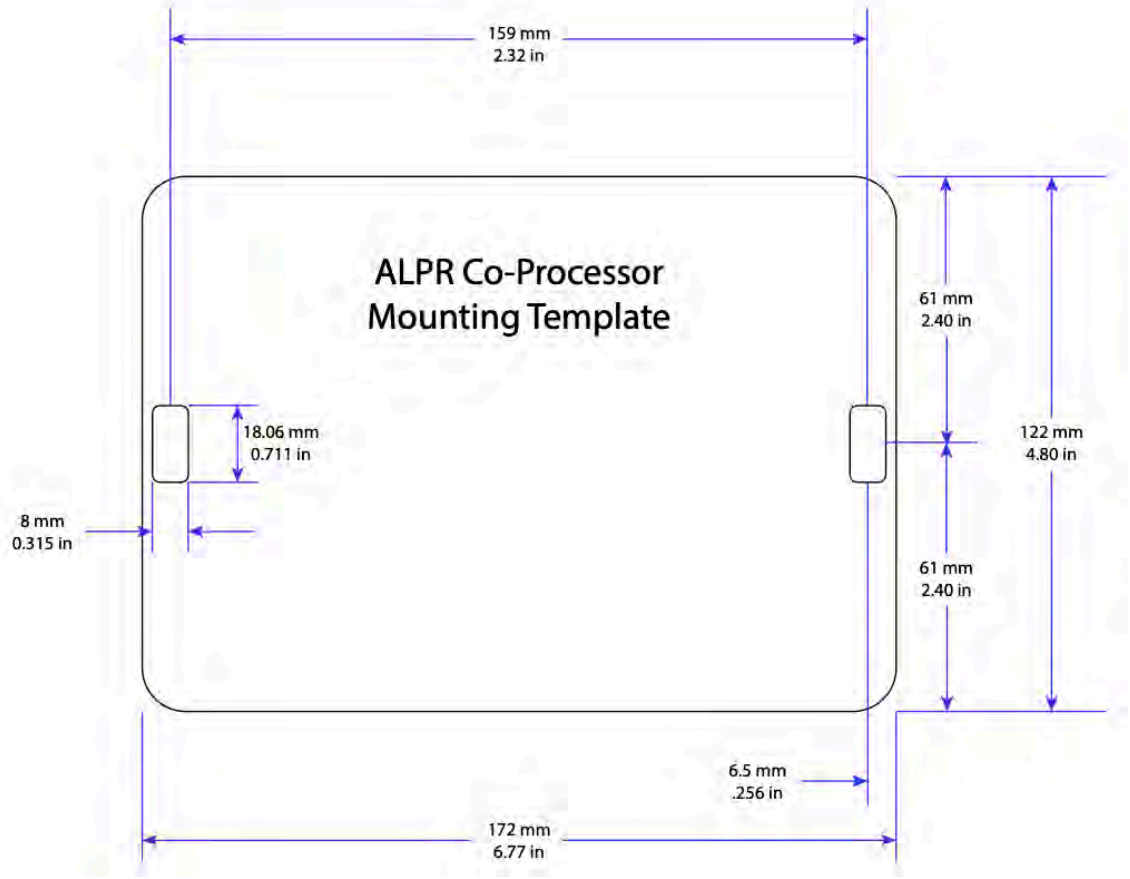


The M12 connector colors are the same as for the Rocket IoT XLE. Light blue is a 1GB Ethernet port to connect to the Rocket IoT XLE. The smaller black connector is USB for peripherals. The Red M12 connector is for vehicle power and ignition, and is the same as power and ignition for the Rocket IoT XLE.



Like the Rocket IoT XLE, the ALPR Graphics AI Co-Processor is MIL-STD 810G for operating temperature and vibration, and IP-67 rated for operating under one meter of water for 30 minutes.

This diagram shows the outer dimensions and the location of the mounting slots on the left and right side of the ALPR Graphics AI Co-Processor.





Rocket IoT XLE Mounting and Placement

1. Mounting Site Selection:

Below are Utility's best practices when considering a proper mounting location for the Rocket IoT XLE.

- Orientation of the Rocket IoT XLE does not matter. The hardware is all solid-state, with no spinning hard drive or other components where the force of gravity might have an impact on hardware operation.
- Must be able to easily access the hardware unit and cable connectors. When choosing an install location, it is important to ensure there is enough clearance to allow for installing and removing the Rocket IoT XLE and associated internal peripherals and cables.
- Mount the Rocket IoT XLE in a secure location in the vehicle i.e., electronics tray, electronics bay, storage area, trunk or rear of the vehicle where possible.
- Vehicles with limited trunk area may require a panel/mounting board or plate to be installed somewhere in the trunk, cab or on the back of the passenger seat to provide a stable mounting surface for the Rocket IoT XLE.
- The bracket should always be mounted to the vehicle using ¼ inch x 1 inch (zinc or stainless steel) bolts, 1 inch fender washers and matching nylon locking nuts.
- Never use self-tapping screws that can work loose from vehicle vibration, and/or rust or corrode over time.

CAUTION: Make sure to check first what is below the mounting hole locations to avoid drilling into brake, transmission, air conditioning, or other lines, or other critical vehicle components.

2. ALPR Graphics AI Co-Processor Mounting Site Selection:

The same best practices apply to the mounting location ALPR Graphics AI Co-Processor hardware unit

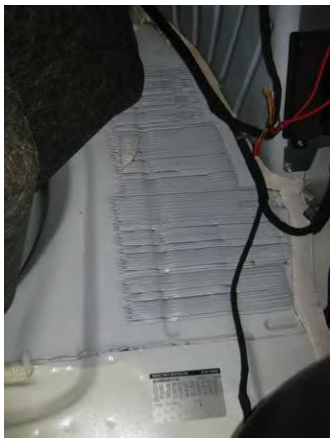
- Orientation of the ALPR hardware does not matter. The hardware is all solid-state, with no spinning hard drive or other components where the force of gravity might have an impact on hardware operation.
- Must be able to easily access the hardware unit and cable connectors. When choosing an install location, it is important to ensure there is enough clearance to allow for installing and removing the ALPR hardware unit and associated internal peripherals and cables.
- Mount the ALPR unit in a secure location in the vehicle i.e., electronics tray, electronics bay, storage area, trunk or rear of the vehicle where possible.
- Vehicles with limited trunk area may require a panel/mounting board or plate to be installed somewhere in the trunk, cab or on the back of the passenger seat to provide a stable mounting surface for the Rocket IoT XLE.
- The bracket should always be mounted to the vehicle using ¼ inch x 1 inch (zinc or stainless steel) bolts, 1 inch fender washers and matching nylon locking nuts.
- Never use self-tapping screws that can work loose from vehicle vibration, and/or rust or corrode over time.

CAUTION: Make sure to check first what is below the mounting hole locations to avoid drilling into brake, transmission, air conditioning, or other lines, or other critical vehicle components.

3. Rocket IoT XLE Install Mounting:

- Locate an appropriate mounting location, in this example the vehicle is a 2013 Chevy Impala and the mounting location is in the trunk on the passenger side.

  - Step 1. Locate and place the Rocket IoT XLE template so that holes can be drilled through the vehicle or electronics tray sheet metal to provide solid base mount points.





  - Step 2. Using a Sharpie marker mark the holes and drill out the holes with a 5/8" drill bit.
  - Step 3. Attach the Rocket IoT XLE using ¼ X 1 inch or ¼ x 1 ¼ inch (zinc or stainless) threaded bolts w/nylon nuts and fender washers (bolts from the bottom up for a cleaner appearance).
  - Step 4. Mount the Rocket IoT XLE and all associated equipment.

- Once the Rocket IoT XLE is mounted in suitable location, attach all cabling and power connections. Wrap (loom) all cables, and check that all components are secure and do not rattle.



Electronics Tray Install



Motorcycle Install

Antenna Placement and Installation

1. **Antenna Site Selection:** The location of the Quad band antennas is extremely important for the proper functioning of the Rocket IoT and all peripherals. Below are Utility's best practices when considering a proper mounting location for the Rocket IoT Locker:

   - The antennas must be installed a minimum of 18 inches away from any other antennas.
   - The antenna should not be installed on a fiberglass roof on inside the vehicle unless a metal ground plane is used under the antenna.
   - Utility's antennas are designed to be installed on the exterior of the vehicle, either on the roof or on the trunk of the vehicle. Use caution when pulling antenna wires through hole not to nick or cut any of the co- axial cables; the antenna will have to be replaced if any of the co-axial cable is nicked.

Examples of Correct Placement of Antenna mounting location
(Permanent Roof, Trunk and Magnetic mounted)









2. Antenna Installation:

For this example the antenna is mounted on the trunk of the vehicle (2013 Chevy Impala).

- Step 1. Position the Antenna away from any existing antenna install(s) a minimum of 18 inches from the center of the desired install location point.



- Step 2. Locate the center of your mount point and using an antenna hole saw designed for use on sheet metal and start your hole. In the case of a trunk with a support bracket you will have to drill out a larger diameter hole in the support bracket to allow for the final 3/4" hole to allow for mounting of the antenna.









- Step 3. Once the area is cleared of obstructions drill out the ¾" hole for the multiband antenna ensure that the paint is removed around the ¾" hole for grounding connectivity.

- Step 4. Feed the cables through the hole and cover with loom ensuring that none of wire insulation gets damaged. Always place a bead of silicone around the base of the antenna prior to mounting it to the vehicle. Tighten and secure the multiband antenna to the desired location on the vehicle and secure the extra antenna cables as to not impede with the safety and functionality of the trunk.





Providing Power to the Rocket IoT XLE – Utility Best Practices

The most important part of a Rocket IoT XLE installation is the proper provisioning of power.

1. Power connections for the Rocket IoT.

Several components are generally required.

- Waterproof Inline Fuse Holder (Supplied by UA). ATO or mini-blade fuse. Used on the power and ignition sense (where an "Add-A-Circuit" is not used).



- Power Cable (Supplied by Utility). This includes 20 feet of cable to ensure it can reach the vehicles battery if no factory breakout is available. Constant +12v power (red), chassis ground (black), and ignition (yellow) wires included in this power cable that need to be connected to factory breakouts.

- Add-A-Circuit fuse tap can also be used for Ignition sense (Not supplied by Utility).



- Dual Walled Butt Splice (Supplied by Utility). Used to connect power, ground and ignition sense wiring. This type of connector provides a crimped connection as well as a waterproof seal.



- Dual Walled Ring Terminal (Supplied by Utility). Used to connect power and ground; provides a crimped connection as well as a waterproof seal.



2. Proper Power Connection Fundamentals:

- Ignition power should always be connected to a switched ignition source. The Rocket IoT has a built in timer that is configurable through the Rocket IoT software. This internal timer begins to count down once the system no longer detects ignition voltage on the yellow power wire.

- Do not connect the yellow ignition power wire to another timer in the vehicle, such as a Havis Charge Guard or other similar power timer. Doing this essentially is connecting one power timer to another power timer.

Only connect power from an original equipment manufacturer (OEM) breakout. Vehicles without OEM breakouts should be wired directly to the battery for constant power and chassis ground unless a certified power distribution unit (PDU) is used. Utility will validate any (PDU) used by an installer to ensure compliance with standards.



(Factory Power and Ground Breakout 2013 Chevy Impala)

- Only use 16 or 18 gauge primary wires for any power, ground or ignition sense wiring.
- Check all voltages with a good quality multi-meter before using.
- Power and ignition sense should ALWAYS be fused as close to the main power source or original equipment manufacturer (OEM) factory vehicle power break out or source as possible.

Providing Power to the ALPR Graphics AI Processor

Like the Rocket IoT XLE, the most important part of an ALRP Graphics AI Processor installation is the proper provisioning of power. The power connections for the ALPR Graphics AI Processor are the same as the Rocket IoT XLE.

Several components are generally required.

- Waterproof Inline Fuse Holder (Supplied by UA). ATO or mini-blade fuse. Used on the power and ignition sense (where an "Add-A-Circuit" is not used).



- Power Cable (Supplied by Utility). This includes 20 feet of cable to ensure it can reach the vehicles battery if no factory breakout is available. Constant +12v power (red), chassis ground (black), and ignition (yellow) wires included in this power cable that need to be connected to factory breakouts.

- Add-A-Circuit fuse tap can also be used for Ignition sense (Not supplied by Utility).



- Dual Walled Butt Splice (Supplied by Utility). Used to connect power, ground and ignition sense wiring. This type of connector provides a crimped connection as well as a waterproof seal.



- Dual Walled Ring Terminal (Supplied by Utility). Used to connect power and ground; provides a crimped connection as well as a waterproof seal.



GPIO Trigger Cable

Triggers: The Rocket IoT can provide up to four Digital +12v triggers for the in-car video and/or BodyWorn cameras.

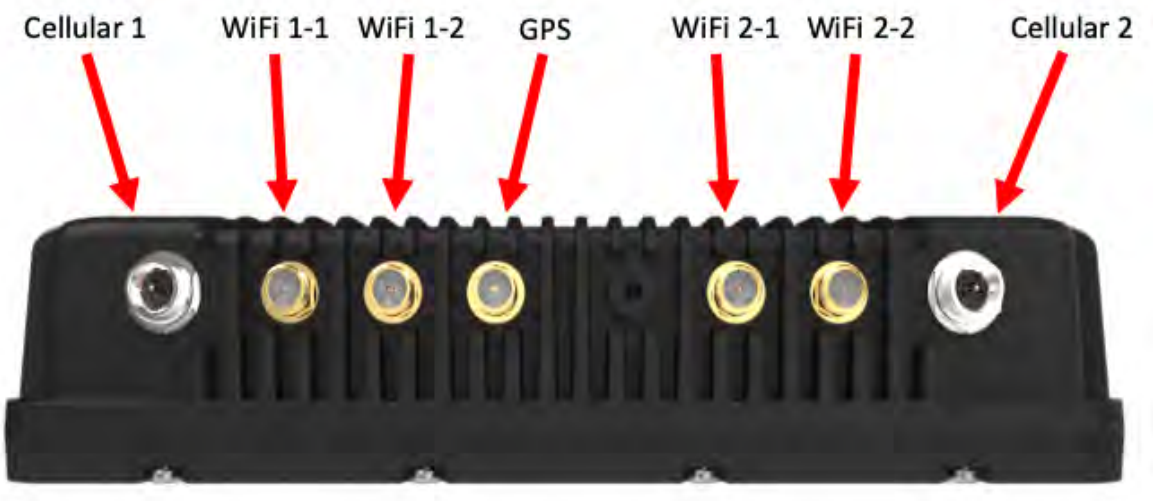
Wire Color	*Description*	*Comments*
Yellow	Ignition	Ign. Input can be connected to the GPIO or the Yellow Wire in the Power Cable. Standard is Connection to the Power Cable.
Orange	Trigger #1	Lightbar (Standard Trigger)
Brown	Trigger #2	Door (Standard Trigger)
Purple	Trigger #3	Brakes (Optional)
White	Trigger #4	Gun Lock (Optional)
Light Green	Siren A	Optional Trigger
Dark Green	Siren B	Optional Trigger
Pink	Relay Output B	Trigger for Red LED Light (Black Wire from LED)
Red	Relay Output A	Required Ground
Black	Primary Ground	Required Ground
Gray	Isolated Ground	Required Ground
Blue	Isolated Ground	Required Ground

NOTE: All four ground wires must be connected to chassis ground or triggers will not function properly.

Antenna connections to Rocket IoT XLE:

NOTE: The main cellular connection, two docking Wi-Fi connections and GPS should come from the same quadband antenna. The AUX cell connection and two AP Wi-Fi connections should come from the other quadband antenna. There will be one GPS cable that is not used.

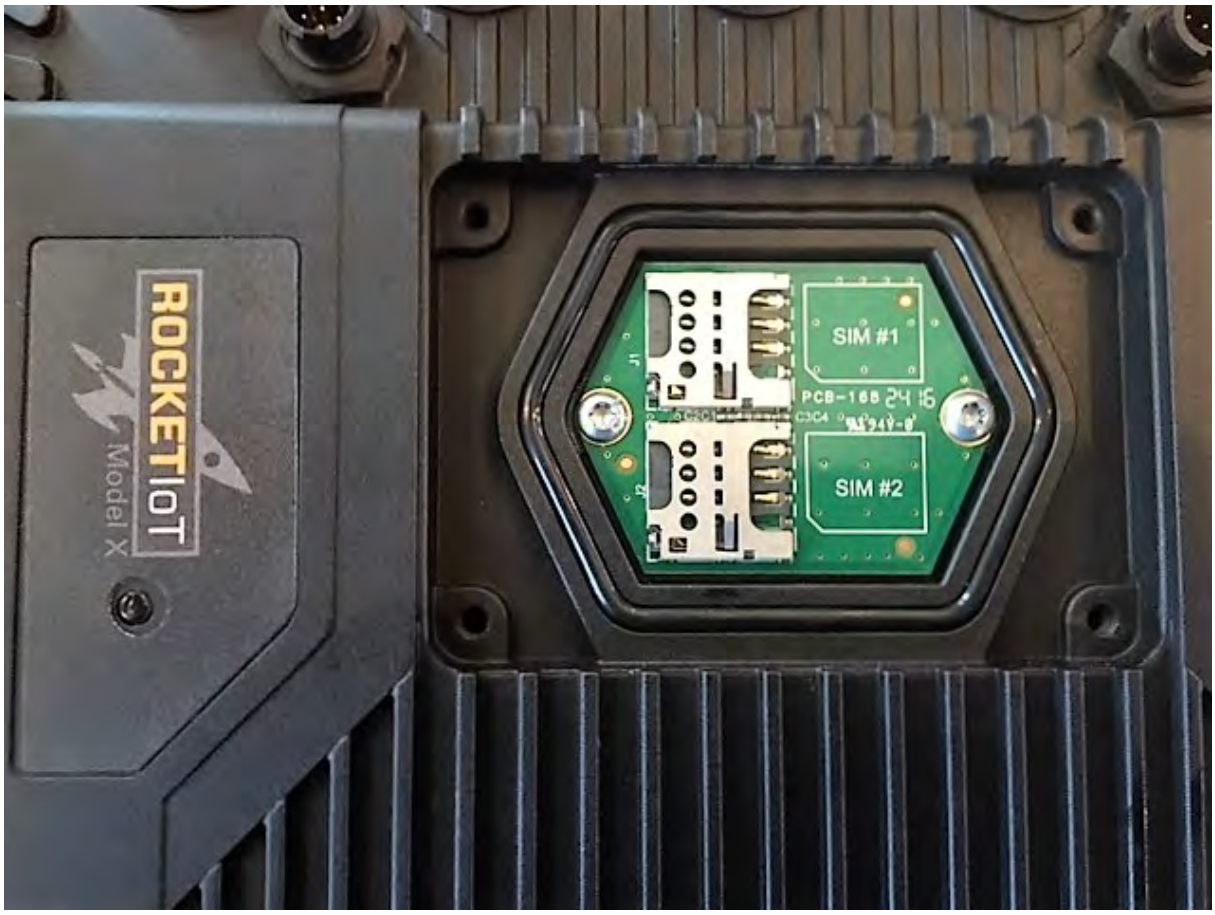




In the case of alternative internal vehicle GlassMount antennas, the cellular antenna cable can be attached to either antenna connector on the Rocket IOT XLE. In a likewise manner, four WiFi Glassmount or Rubber Duck antennas can be connected in any order to the WiFi antenna connectors.

SIM Card Installation

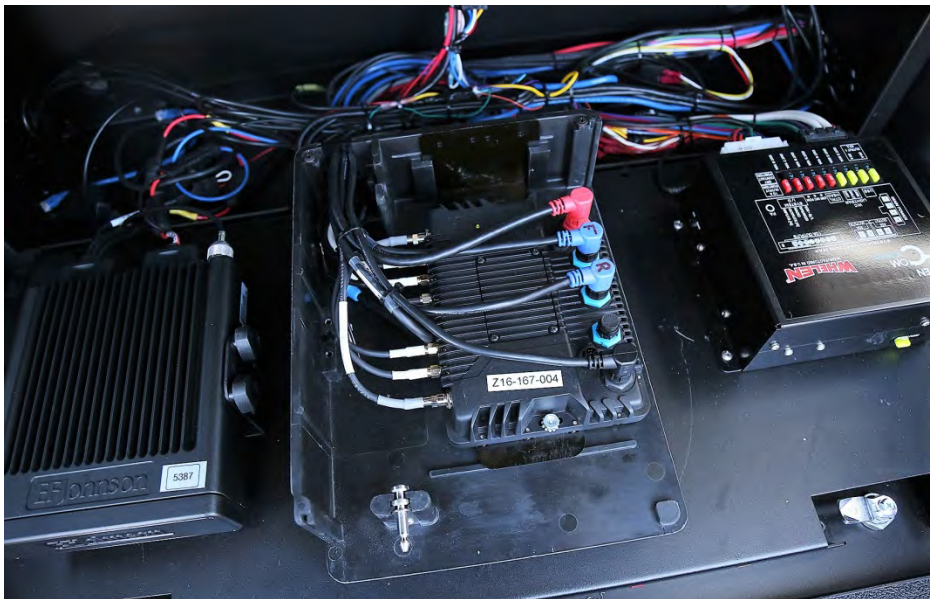
- Utility Associates uses a Micro SIM card (3FF) to provide communications for the Rocket IOT XLE system.
- The SIM card is always inserted into the SIM #1 port located under the SIM card door pictured below.
- If dual carriers are being used, the primary SIM card goes into the SIM #1 slot and the secondary failover SIM card goes into the SIM #2 slot.
- The SIM Card cover and gasket provides an IP-67-rated water tight seal to prevent moisture from getting inside the Rocket IoT XLE case.
- Once the SIM card has been installed, it is important to make sure the SIM Card cover gasket is properly in place before reinstalling the SIM card cover and tightening down the four corner screws. See rubber gasket shown below.



Finishing the Hardware Installation

1. Once the hardware installation is completed there are several items that should be verified:

- Rocket IoT has a built-in power indicator light that shows when the device is powered on (blinking green), when it is in the shutdown process (blinking amber) or when it is off (not lit up).
- Verify that any exposed wiring has been loomed. This includes excess antenna, power, network cabling in the front of the vehicle etc. This also covers any cabling in the engine compartment. Cable must be neatly loomed and electrical taped or zip tied where appropriate.
- Excess cable is hidden wherever possible.
- All dual walled butt splices and ring terminals have been heat shrunk.
- All antennas cables snugged up with an 8mm or 5/16 wrench. Torque seal on the FME connectors (not Loctite).
- All cables checked to make sure they are plugged in correctly.
- All kick plates, body molding, head liners, seat belts, etc. must be re-installed. Try to leave it better than you found it.

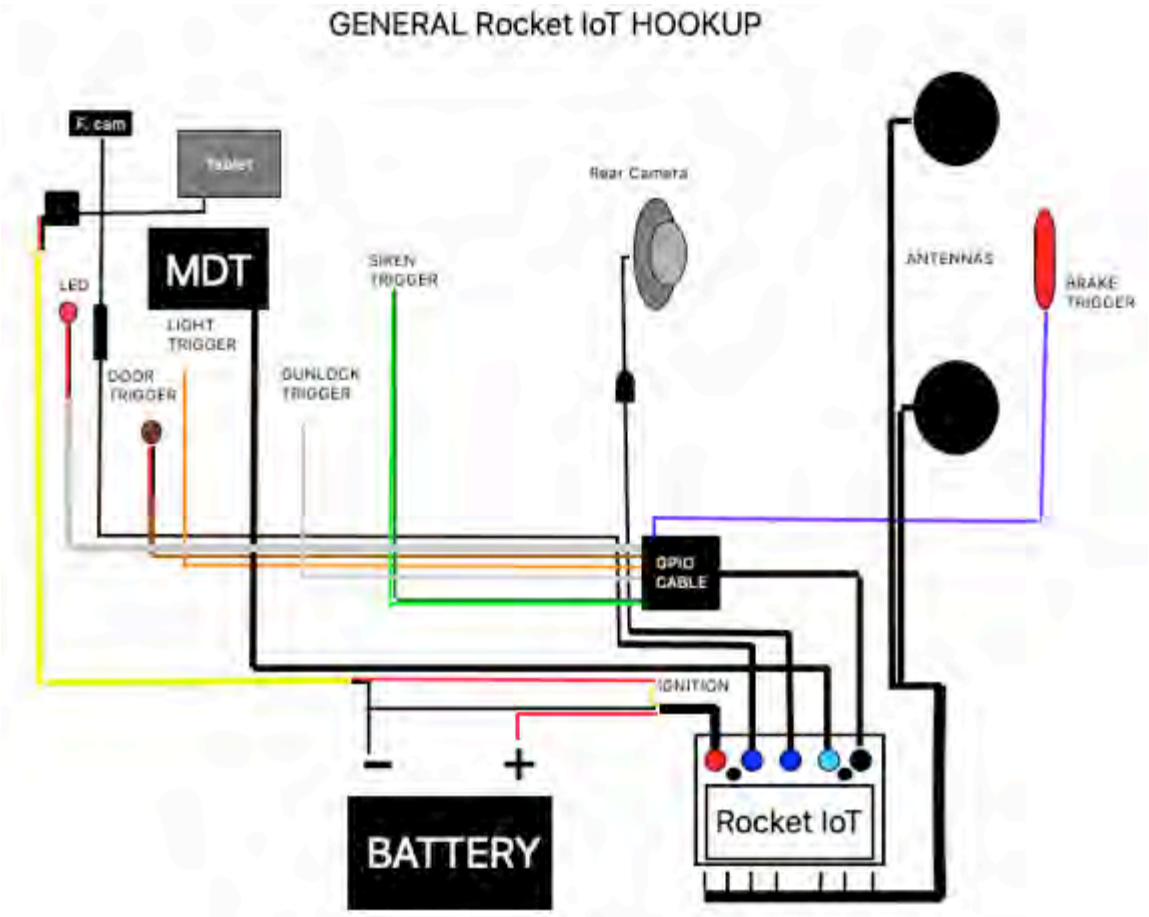


Rocket IoT XLE Blink Codes

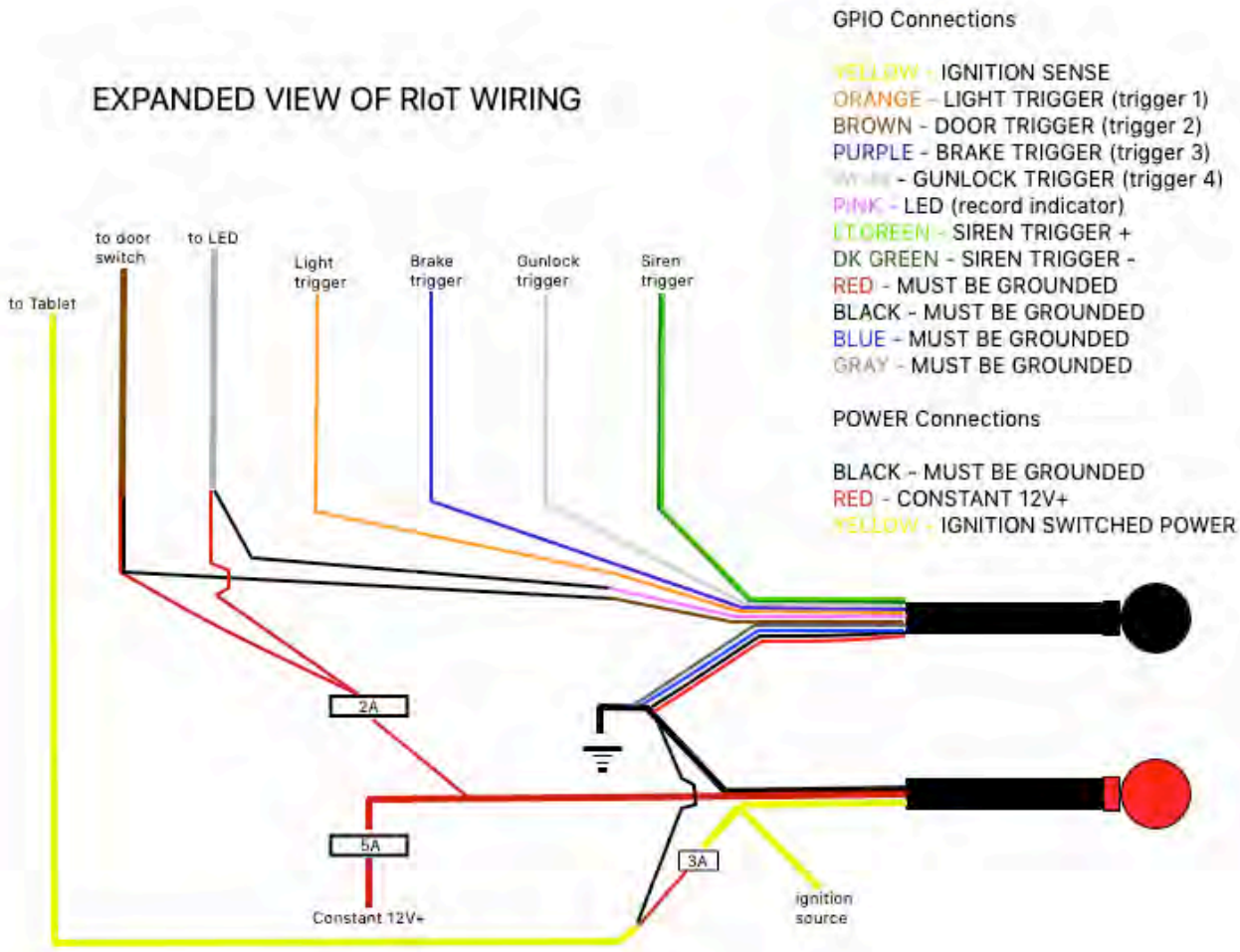
1 Green Blink	System is Running – Input power exceeds 12.75v DC
2 Green Blinks	System shutting down - Input power exceeds 12.75v DC
Orange Blink	System shutting down - Input power below 12.75v DC
Red Blink	Power below 9.5v DC

Recommended Fuse Sizes

Description	*Fuse Size*
Main Power	5 Amp
Ignition	3 Amp
Door & LED	3 Amp Shared
Tablet	3 Amp



GPIO Expanded Wiring View





Support Help Desk

404-816-0300

Suite 700
250 East Ponce de Leon Avenue
Decatur, Georgia 30030
(404) 816-0300

© 2019-2020 Utility, Inc.

Discussion of Warranties, Agreements, Terms and Conditions

Full details regarding Warranties for the Rocket IoT ALPR™ solution can be accessed in the documents described below, and can be accessed through the links provided.

Utility Rocket IoT Hardware Warranty

http://bit.ly/RIOT-Hardware-Warranty

The Utility Rocket IoT Hardware Warranty describes the warranty provided on Utility's Rocket IoT manufactured devices. Under this agreement, Utility guarantees that its devices are free from defects, and agrees to replace any parts or devices that have not been broken under malicious intent or subjected to extreme conditions.

Service Level Agreement

https://www.bodyworn.com/service-agreement

The Service Level Agreement describes the levels of service, software agreement, and terms and conditions that the client will receive from Utility (the supplier).

The client depends on Utility IT equipment, software and services, some of which are of critical importance to the client. As such, the SLA sets out what levels of availability and support the client is guaranteed to receive, forms an important part of the contract, and enables the two parties to work together effectively.

The Utility "System as a Service" Agreement (SaaS Agreement) describes Utility's service commitment of system provided to client. The document details the services that will be provided, the environment under which the software will operate, how the software may be upgraded, the uptime of the service, and the hours where support can be reached. Further, the document details permitted usage of the software, restrictions on software usage, the fees that will be assessed, and the terms under which they are due.

The Utility Terms and Conditions detail the conditions under which Utility conducts sales of its proprietary products. This includes liability limitations, logistics of product transfer, protection of intellectual property, payment information, and the jurisdiction under which legal action may be taken.

Utility Data Security Documentation

bit.ly/UA-Data-Security

This Utility Data Security Documentation is a summary overview of the security, performance, reliability, and scalability for Utility hardware, software as a service, and hosting environment. Utility uses a combined hardware and software defense-in-depth architecture to protect the confidentiality, integrity, and availability of customer information. The security and performance architecture adapts automatically to changes in technology, internal and external threats to networks and applications, and to client operations. Third party security risk evaluations are performed to assure the effectiveness of our procedures, methodology, equipment, facilities, and personnel.

Amazon Web Services (AWS)

Utility purchases services from Amazon Web Services to provide backend processing and storage for its software packages. The following documentation explains Amazon's security standards, obligations, and assurances provided for the safety, security, and accessibility of all client data.

AWS Service Organization Controls 3 Report - bit.ly/AWSControls

The AWS Service Organization Controls 3 Report provides an overview of how Amazon maintains operation of technology, people, data, and infrastructure supporting its AWS services.

AWS Overview of Security Processes - bit.ly/AWS-SecurityReport

The AWS Overview of Security Processes describes the systems put in place to assure that Amazon is able to meet the high service and security standards that its clients demand. This includes an in-depth review of how Amazon maintains both physical and electronic security over its cloud services.

CJIS Compliance on AWS - bit.ly/Utility-is-CJIS-Compliant

The CJIS Compliance on AWS document provides Amazon's perspective on and approach to being fully compliant with Criminal Justice Information Standards (CJIS). These standards are set nationally by the Federal Bureau of Investigation (FBI) for information storage, usage, and sharing within law enforcement.

UTILITY

Procurement Information on CJIS Compliance

Utility's RocketIoT ALPR™ with AvaiLWeb™ is a Cloud-based solutions that meets and exceeds standards for CJIS Compliance, and offer a scalable license plate reader and digital management and storage platform with high availability and dependability. Cloud-based solutions outperform the alternate — on-premise storage — and protect the confidentiality, integrity, and availability of criminal justice information and data. Cloud-based solutions are fundamental to credibility, by projecting transparency, and preserving your Community's trust.

Security - Cloud-based storage is unparalleled security and redundancy.



Rest assured that your video data in the Cloud is much more secure than what lives on a tower or in your server room. Those with the most to protect – from leading defense agencies to global companies - have chosen Cloud-based storage. There is a long and successful track record of law enforcement customers using the Cloud for a wide range of sensitive federal and state government workloads, including CJIS data.

Reliability - Cloud-based storage is unparalleled reliability.



A Cloud-based provider platform virtually eliminates risk of downtime. Amazon S3, for example, is designed to provide 99.999999999% durability and 99.99% availability over a given year, redundantly stored on multiple devices across multiple facilities in geographically separate locations. It is an illusion to think criminal justice information is more reliable in a Department's on-premises local storage facility. One incident with rebuilding 'on-prem' crashed servers - and its unbudgeted cost - is all it takes to prove it. You don't want to be that case study.

Budget - Without the Cloud, agencies spend a lot of the IT budget to manage storage.

That takes funding off the streets, and requires hiring that is difficult to defend and pay for. With cloud storage, that's no longer an issue. Now, you can focus on how the police camera video solution will help you further your law enforcement mission. The video IT piece belongs to somebody else.

Flexibility - Scale up and down to meet your current needs.

In business, this flexibility is key. In government, new expenditures are tough to defend and pay for. With Cloud-based solutions, you no longer have to build for the future, or be constrained by decisions made or contracts signed in the past. You can adjust your video storage expenditures to meet your agency's immediate needs.

Resiliency - No law enforcement agency can ignore resiliency threats.



Yet few have the resources alone to deliver security when your Community itself is in harm's way. Cloud providers' resiliency programs identify, respond to, and recover from a major incident, with contingency management, business continuity, and disaster recovery plans. Cloud-based providers identify critical system components required to maintain the availability of the system, and recover services in the event of an outage from physically separate locations, maintain authoritative backups, employ continuous infrastructure capacity planning, and monitor to ensure successful replication. Cloud-based resiliency means you can keep your promises "To Serve" when most needed in your Community.

Cost - Using Cloud technology reduces your storage and maintenance fees.

No more servers, software, and update fees. Many of the hidden costs typically associated with video storage, (and with software implementation, customization, hardware, maintenance, and training) are rolled into a transparent subscription fee. No more need to explain any unanticipated cost – you are covered.

It's Mobile - Internet standards and web services allow you to interconnect services.

Today's cloud-based solutions for law enforcement are managed under secure controls, and in continuous alignment with federal, state and local law enforcement Criminal Justice Information Security (CJIS) policy. This means that you can centralize your law enforcement video and access it from anywhere in the world, on any computer or mobile device, at any time. Your mission-critical video information is fully mobile.

UTILITY

Utility and AWS CJIS Compliance in the Cloud

Utility is fully committed to continually exceeding industry standards for data security including Criminal Justice Information Standards (CJIS). The following documentation provides details on how Utility ensures customer data is secured.

Utility Data Security Documentation

Utility's Data Security Documentation is a summary overview of the security, performance, reliability, and scalability for Utility hardware, software as a service, and hosting environment.

Utility uses a combined hardware and software defense-in-depth architecture to protect the confidentiality, integrity, and availability of customer information. The security and performance architecture adapts automatically to changes in technology, all threats to networks and applications, and to client operations. Third party security risk evaluations are performed to assure the effectiveness of our procedures, methodology, equipment, facilities, and personnel.

Full Document: bit.ly/UA-Data-Security

Amazon Web Services (AWS)

Utility purchases services from Amazon Web Services to provide backend processing and storage for its software packages. The following documentation explains Amazon's security standards, obligations, and assurances provided for the safety, security, and accessibility of all client data.

CJIS Compliance on AWS

The CJIS Compliance on AWS document provides Amazon's perspective on and approach to being fully compliant with Criminal Justice Information Standards (CJIS). These standards are set nationally by the Federal Bureau of Investigation (FBI) for information storage, usage, and sharing within law enforcement.

Full Document: bit.ly/Utility-is-CJIS-Compliant

AWS Service Organization Controls 3 Report

The AWS Service Organization Controls 3 Report provides an overview of how Amazon maintains operation of technology, people, data, and infrastructure supporting its AWS services.

Full Document: bit.ly/AWSControls

AWS Overview of Security Processes

The AWS Overview of Security Processes describes the systems put in place to assure that Amazon is able to meet the high service and security standards that its clients demand. This includes an in-depth review of how Amazon maintains both physical and electronic security over its cloud services.

Full Document: bit.ly/AWS-SecurityReport