Appendix A

Scope: This document covers the “Statement of Work” for deploying the VISTA/Evidence Library system at an agency location. The table of contents includes the reference number for the task assigned to the appropriate party.

Table of Contents

SVR-01-Installation of Server in Equipment Rack

If purchasing a 3U Rack-mount server or additional JBOD unit from WatchGuardVideo, the hardware will need to be installed in a four post server rack. The rack can be floor mounted, or on wheels.

SVR-02-Rack Requirements

You will need a standard four post server rack with the following specifications

- Adjustable mounting depth of 6" – 30" (152 – 762 mm)
- Overall rack depth of 39" (990 mm)
- Universal square holes.
- Rolling rack or bolt in rack will both work

Once the rack is installed, it is up to the customer to ensure proper grounding. Preferably to a copper grounding block that has been professionally installed by an electrician.

Non-proper grounding of the server rack could result in failure of the server and will VOID the warranty.

This picture will give you a good idea of the cross section of the server rack with side panels and doors removed. It is important that you abide by these requirements or your rack will NOT fit the server.

SVR-03-Mounting or "Racking the Server"

The server must be mounted prior to the arrival of the WatchGuard Video Personnel. The server weighs 60 lbs. and is very large, therefore we recommend 2 people to rack the server.

- The first step to installing the server is to open the box and find the mounting rails and the installation instructions.
- The mounting rails will be marked left and right, follow the diagrams on the instructions on how to connect the rails to the server rack, as well as, how to connect the rails to the server itself.
- Once the rails are attached to the rack, and the rails are connected to the server, the server can be pushed all the way back in to the server.
- See server documentation (located in server box) for additional details.

SVR-04-Connecting the Server

Once the server is racked, connect power along with the keyboard, mouse, monitor, and network connections.

- WatchGuard highly recommends that the server be plugged into a UPS device that is rated to maintain power to the server and all peripherals in case of a power outage. The time frame should be long enough to allow the server to be powered off normally before the server power completely fails.
  By doing this, it will ensure that the server runs normally in case of brown outs and power surges. **WatchGuard does NOT provide this equipment** and it is the responsibility of the customer to purchase separately.
- The server has two standard 120v power connectors and both will need to be plugged in. The cables to connect the power supplies are included in the box
- Plug the WatchGuard Video server into your local network. Plug a cat 5e or cat 6 Ethernet cable into a switch on your network and plug the other into one of the open Ethernet ports on the back of the WatchGuard Video server.
- Plug in the access point to the open Ethernet port covered in the Access Point Installation section of this document.
- Provide a Keyboard, Mouse and Monitor, or some type of KVM device for the on-site technician to use during software installation and configuration. WatchGuard does not provide these peripherals unless ordered with the server.

SVR-05-Server Specifications – Physical and Virtual

In conjunction with the in-car components, a back end server is required to run WatchGuard Video's Evidence Library software. The server can be a physical standalone server, or installed in a virtual environment. The following specifications must be met to guarantee a successful installation of Evidence Library.

Hardware Requirements (1-5 Concurrent Vehicles)

Physical server, 1-5 concurrent vehicles

Components	Minimum	Recommended
Motherboard	Intel® Socket 1156	Intel 5520 chip set, 96 GB RAM support, PCI-E 2.0
Processor	Intel i5-650 or similar	Intel Xeon Quad Core or similar
RAM	6 GB 1333 MHz DDR3	8 GB 1333 MHz DDR3
Hard drive controller	RAID 5, RAID 6, or RAID 10	
Operating system storage	40 GB	80 GB
Staging	200 GB	500 GB
Final storage	Depends on retention	
Optional expanded video storage	NAS, SAN, JBOD, or cloud (Microsoft® Azure)	
Network cards	1 network card	2 network cards
Disk media drive	Optional	Dual layer DVD reader/burner
Peripherals	Monitor, USB keyboard, USB mouse	Monitor, USB keyboard, USB mouse, speakers

- See Storage requirements below

Virtual Machine:

- The VM should be dedicated to the WatchGuard Application

Components	Minimum	Recommended
Processor	1 virtual processor	2 virtual processors
Network cards	1 virtual network card	2 virtual network cards
RAM	4 GB	6 GB
Operating system volume	40 GB	80 GB
Staging volume	200 GB	500 GB
Final storage volume	Depends on retention	Depends on retention

Hardware Requirements (1-25 Concurrent Vehicles)

- Intel Socket 1156 Motherboard *Minimum*
    - (Intel 5520 Chip set, 96GB RAM support, PCI-E 2.0 ***Recommended***)
- 3.20GHz Intel Core i5-650 processor *Minimum*
    - (Intel Xeon E5620, 2.40GHz Quad Core ***Recommended***)
- 6GB 1333MHz DDR3 Memory *Minimum*
    - (8 GB 1333MHz DDR3 ***Recommended***)
- LSI 9240-4I RAID Controller *Minimum* (Or Similar)
    - (LSI SAS9260-4I, 6Gbps, SAS/SATA w/ Battery Backup ***Recommended*** Or Similar)
- Intel *or* Equivalent Dual NIC card *Minimum*
- 8x DVD+RW Multi Drive DVD reader/burner *Minimum*
    - (Dual Layer DVD Reader/Burner ***Recommended***)
- Monitor, USB Keyboard, USB Mouse ***Required***
- 3 Year Full Service Warranty, Next Day On-Site ***Recommended***
- NAS, SAN or JBOD for expanded video storage ***Optional***
- See Storage requirements below

Virtual Server Requirements

- The VM should be dedicated to the WatchGuard Application
- 2 Processors *Minimum*
    - 4 processors are ***Recommended***
- 2 Virtual Network Cards
- 6-12 GB of RAM

SVR-06-Installation and Configuration of Windows Operating System/ Disc Storage System

- Install Server Operating system
- Change Password of local administrator to WGV standard (unless agency has a different policy)
- Provide and Activate Windows Server License Key
- Set the local Security Policy to 0 days (unless different from department policy)
- Power Options – " Put the computer to sleep: NEVER" (applies to Windows client operating system)
- Set the Administrator password to "Never Expires" (preferred)
- Configure IE/ESC security settings to OFF for Administrators
- Change windows update to the desired state for agency

SVR-07-Provide Operating System License key

Specified party will purchase/provide license key for compatible Windows operating system.

Software Requirements

An account with local Administrative level permissions is required to install the WatchGuard Video Evidence Library Software on the server. **If integrating with Active Directory, domain user with Local Admin rights is required**. Additionally the system requires the following software components.

- Operating System – (Please note it must be one of the two options below)
    - Microsoft Windows 7 Professional 64-bit or Windows 10 Professional 64-bit ***Minimum***
    - Microsoft Windows Server
        - 2008R2 64-bit
        - 2012 64-bit
        - 2012R2 64-bit ***Recommended***
- SQL Server – (Please note that we require one of the EXACT versions of SQL Listed Below)
    - Microsoft SQL Server 2008 R2 Standard with 5 or more CALs
    - Microsoft SQL Server 2012 Standard with 5 or more CALs
    - Microsoft SQL Server 2014 Standard with 5 or more CALs

SVR-08-Configure Operating System

(Optional) Install the following features or roles on the Operating System. These roles are installed at installation of the Evidence Library Software

- .NET Framework 4.5 features
- (AD/LDS) Active Directory Lightweight Directory Services
- Web Server
    - Management Tools
        - IIS Management Console
        - IIS Management Scripts and Tools
        - Management Service
    - FTP Server
        - FTP Service
        - FTP Extensibility
- Application Server
    - .NET Framework 4.5
    - TCP Port Sharing
    - Windows Process Activation Support
        - HTTP Activation
- Files Services

SVR-09-Setup and Preform Backups:

WatchGuard Video does not perform backup of the “operating system” or “video storage” on the server, this is the responsibility of the agency.

SVR-10-Setup Recommended Disk Configuration (virtual and physical)

Drive partition	Volume contents	Recommended storage size	Preferred RAID type	Preferred disk type
1	Windows operating system, SQL Server application, Evidence Library application/installation directory	50 - 200 GB	RAID 5	HDD or SSD
2	SQL Server database, Evidence Library working directory (video staging: **Import** and **Export** storage locations), processing tier (**Online Video** first tier)	200 GB - 1 TB	RAID 5 or RAID 10	SSD
3	Video and case storage	2 - 50 TB	RAID 5, RAID 6, or RAID 10	HDD or cloud (Microsoft® Azure)
Other	Optional backup or additional storage	TBD	TBD	TBD

*Video and Case Storage volume will vary based on the number of cameras, video quality, and video retention. Contact a WatchGuardVideo Project Manager to receive a proper storage estimate.

SVR-11-Install TeamViewer

Teamviewer can be installed and made available to WatchGuard Video to provide remote support. Other remote applications can be used. Teamviewer is the preferred choice for remote access by WatchGuardVideo.

AP-01-Access Point Wiring and Installation

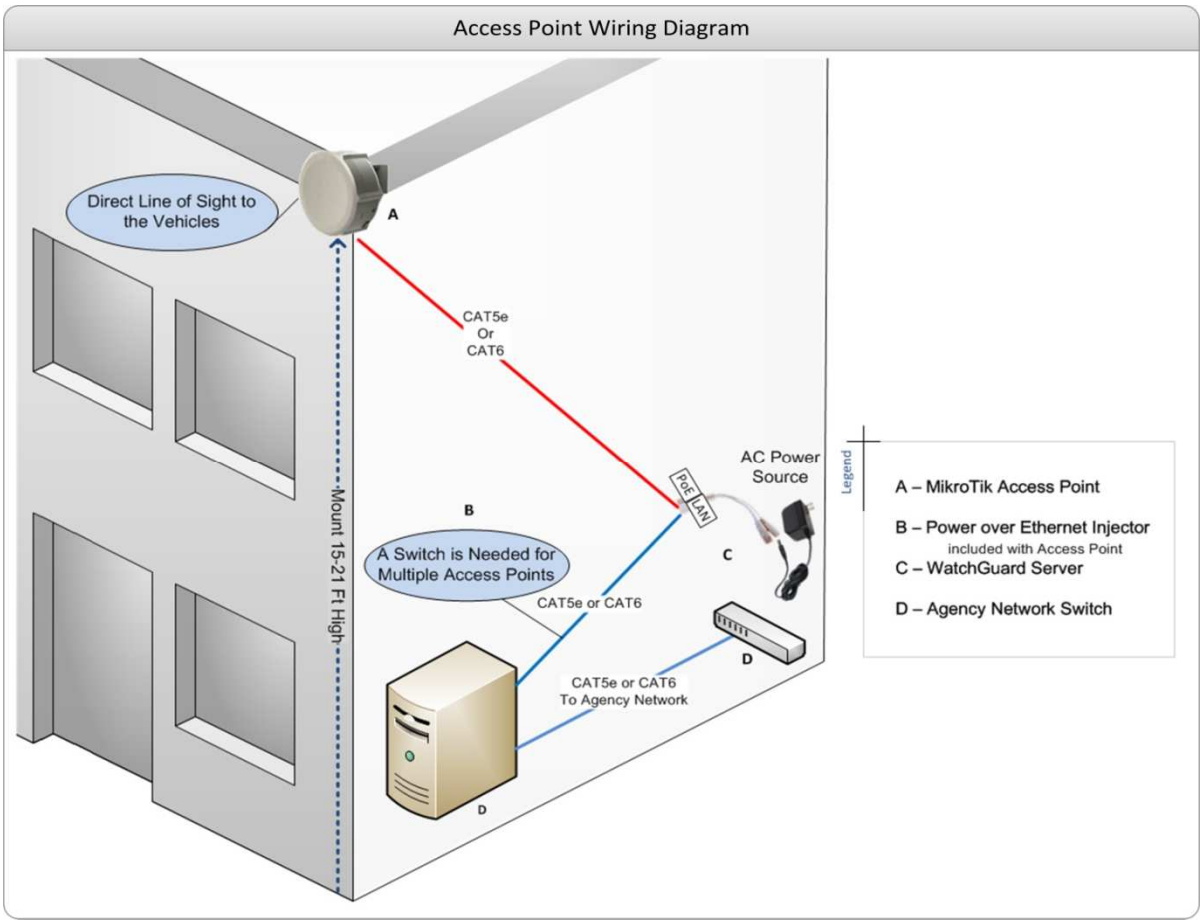
This section will cover the Access Point (AP) installation and wiring. Some items in this section are specific to the “Ubiquiti” or “MikroTik” product. If using a different Access Point or In Car wireless Radio, some sections may not apply. Contact the WatchGuard Video Project Manager for details if using a different wireless solution. The party responsible for the Access Point wiring and installation needs to have the following completed:

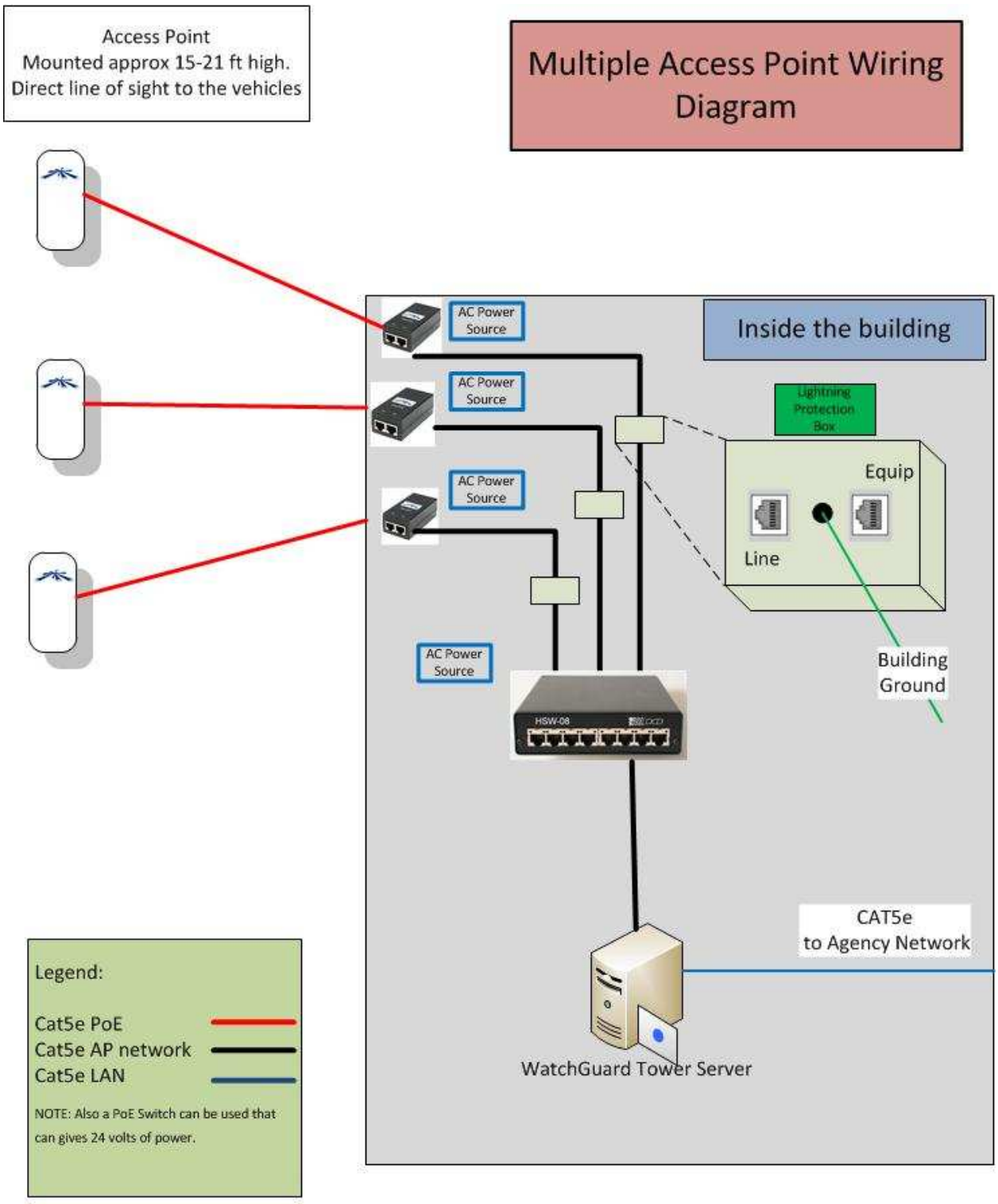
AP-02-Cabling

- Party will provide CAT5E or CAT6 Cable for the Access Point. **NOTE**: If mounting the Access Point on the exterior of a building, ensure the cable is protected. Protecting the cable can happen in 2 forms:
    - Supply an External grade CAT5E/CAT6 cable
    - Supply a conduit for the internal grade CAT5E or CAT6 cable
- Terminate the CAT5E or CAT6 cable at ALL ends to ensure there is a good connection.
- Test Connection with a cable tester or verify through AP web interface
- If using a VLAN to connect the AP to the server, ensure there is connectivity from AP to server through the managed switch.

AP-03-Mounting the Access Points

- Guidelines to mount the Access Point:
    - The AP height should be 15-21 ft. high from the ground. (any higher and the signal can overshoot the vehicles)
    - The AP needs to have direct line of sight to the vehicles with the DVR systems.
    - The AP needs to be mounted vertically.
- Ensure there is a 3 to 6 inch “Drip Loop” for the CAT5E or CAT6 cable. The drip loop prevents water from going into the RJ45 port and damaging the AP.


Access Point Wiring Diagram
Direct Line of Sight to the Vehicles
A
CAT5e Or CAT6
Mount 15-21 Ft High
AC Power Source
PoE
LAN
B
A Switch is Needed for Multiple Access Points
C
CAT5e or CAT6
D
CAT5e or CAT6 To Agency Network
D
Legend
A – MikroTik Access Point
B – Power over Ethernet Injector
included with Access Point
C – WatchGuard Server
D – Agency Network Switch


Access Point
Mounted approx 15-21 ft high.
Direct line of sight to the vehicles
Multiple Access Point Wiring Diagram
AC Power Source
AC Power Source
AC Power Source
AC Power Source
Inside the building
Lightning Protection Box
Equip
Line
Building Ground
HSW-08
CAT5e to Agency Network
WatchGuard Tower Server
Legend:
Cat5e PoE
Cat5e AP network
Cat5e LAN
NOTE: Also a PoE Switch can be used that can gives 24 volts of power.

AP-05-Access Point and Radio Configuration

This section will cover the Statement of Work for the software configuration of the Access Points and Wireless radios.

AP-06- Provide Access Points

Provide Access Points that can communicate with the specifications below:

AP-07- Configure Access Points:

- Access Point should be configured to the following:
  - SSID (hidden)
  - Security: WPA2 – AES
  - Pre-shared Key (PSK)
  - Agency specified Network (e.g. 192.168.2.X/24)
- Access Points (Ubiquiti or other manufacturer) need to use the following channels if using the Ubiquiti Bullet for the in car wireless solution:

  NOTE: The FCC is requiring wireless radio manufactures in the US to limit the 5Ghz frequencies to the following channels:
  - 5805 (freq. 161)
  - 5785 (freq. 157)
  - 5765 (freq. 153)
  - 5745 (freq. 149)
- Ubiquiti AP's should be used on the approved firmware versions (contact Customer service for up to date versions)
- WatchGuardVideo recommends the Wireless Radio(s) AP and in Car radio should be on the 5Ghz Range (more available channels, higher throughput). WatchGuard Video systems ship defaulted to the 5Ghz range unless otherwise specified
- If the Access Points are from a Manufacturer other than Ubiquiti, please ensure the following ports are not blocked anywhere from the AP connection to the WatchGuard server:
  - 5001
  - ICMP (ping)
  - 21
  - 20

AP-08- Configure In-Car Wireless Radio configuration:

- The in-car radios need to match the Access Point configuration
  - Refer to IP address network excel document (document created by WGV with supplied information from Agency)
  - Same subnet (statically assigned IP addresses)
  - Same SSID
  - Same PSK
  - Same Security WPA2- AES
  - Enable NAT

- For a complete configuration guide, please contact WatchGuard Video Customer Service, or contact an IT person with knowledge on configuring the Ubiquiti or MikroTik wireless radios with the WatchGuard Video DVR.

AP-09-MDC Configuration

- If using the MDC/MDT application, the in-car wireless radio and the MDC will need to be configured to give out a specified DHCP address: from: 10.1.100.22 to 10.1.100.22 Subnet: 255.0.0.0
- Contact Customer Service for a configuration guide to configure the Bullet to give a DHCP address to the DVR.
- The Police Agency needs to have purchased the MDC application to have it installed on the MDC/MDT (In car laptop/computer)

SQL-01-Installing Microsoft SQL Server (Full Version)

Provides services and utilities to support and manipulate the Evidence Library database.

Prerequisites on SQL Server:

- Microsoft Windows 7 Professional 64-bit SP2, Windows Server 2008 R2 64-bit SP2, Windows Server 2012 64-bit, Windows Server 2012 R2 64-bit or Windows Server 2014 64-bit.
  NOTE: Some versions of SQL are not fully compatible with all Microsoft Operating systems. Check with Microsoft to find the compatible versions
- 64-bit processor, 1.4 GHz CPU, 2GB RAM minimum.
- *The Server hosting the WatchGuard Database must **NOT** be operating as a Domain Controller.*
- Before starting the installation of SQL, decide the storage paths for the Evidence Library database and other SQL Program files. If the server has a single volume, the default paths are probably fine.
- Logged on user must have local administrator rights on the server, and Full Control of all volumes on the server that will contain WatchGuard information.

SQL-02-Provide License Key

- Provide SQL Server license key for one of the following versions:
  - SQL Server 2008 R2
  - SQL Server 2012
  - SQL Server 2014

SQL-03- Install and Configure SQL Server:

- Execute **Setup.exe** from the SQL installation folder. Click "Next" through the initial pre-setup screens.
- Choose **Feature Installation** and select **ONLY** the following Instance Features:
  - Database Engine Services
  - Client Tools Connectivity
  - Client Tools SDK
  - SQL Server Books Online
  - Management Tools – Basic
    - Management Tools – Complete
  - SQL Client Connectivity SDK
- Select the predetermined path for the Shared Feature Directories, or use the defaults, and click "Next".
- The **Instance Configuration** screen allows the installer to specify the name of the SQL instance and the instance file path (where the actual database will be stored). The default (non-named) instance is MSSQLSERVER. If a new "Named instance" is used, it must be referred to explicitly (ServerName\NamedInstance) during all Evidence Library component installations. Choose and click Next.

- On the **Server Configuration** screen, the SQL Service Account settings are defined. Configure the following settings for each, then click Next.
    - SQL Server Agent…NT AUTHORITY\SYSTEM…Automatic Startup
    - SQL Server Database Engine……NT AUTHORITY\NETWORK SERVICE…Automatic Startup
    - SQL Server Brower…NT AUTHORITY\LOCALSERVICE…Automatic Startup
- The **Database Engine Configuration** screen allows the installer to configure the allowed SQL authentication methods, and access permissions to the instance.
    - Select Mixed Mode (mixed mode not required, however windows authentication is required)
    - Create the SQL Server Administrator password
    - Click **Add Current User**, and then **Add**, and add the **Administrators** group from the local server to the SQL Server Administrators box, and click "Next."
    - Review settings on the Installation Summary page, and click **Install** to perform the installation.
- Once **the SQL Server Installation complete** message is displayed, click OK, then open **SQL 2008 R2 Management Studio** and login into the new SQL instance one time to verify that authentication is working.

SQL-04- Setup SQL Backup and Maintenance Plan:

- Setup a SQL Maintenance Plan to back up the following Databases (after Evidence Library is installed) every day at 11:00pm or 1:00am (avoid backup at 12:00am or during the same time as the Evidence Library cleanup schedule):
    - master
    - WGEvidenceLibrary

SQL-05-Special Considerations:

- If using a preexisting SQL server, WatchGuard recommends that the WGEvidenceLibrary database be put on a separate SQL instance
    - The **Instance Configuration** screen allows the installer to specify the name of the SQL instance and the instance file path (where the actual database will be stored). The default (non-named) instance is MSSQLSERVER. If a new "Named instance" is used, it must be referred to explicitly (ServerName\NamedInstance) during all Evidence Library component installations. Choose and click "Next."

EL-01-Installing and Configuring Evidence Library Server components

This section outlines the requirements for installing the Evidence Library core server services and components and the configuration of all tertiary settings needed for effective system reliability and function. Please get up to date instructions to installing the software from the Project Manager.

System Requirements

The following conditions are expected to be in place when considering this stage of the deployment:

- The primary Evidence Library server (either physical or virtual) has been fully provisioned according to the WatchGuard Video system requirements, and all required Server Roles are present.
- If the server is a domain member, the Active Directory account that will run the WatchGuard services already exists, is a member of the local server's Administrators' group, the required additional management Security Groups have already been created in Active Directory, and the user groups have been populated with at least some of the users that will be using the software.
- The SQL server software to host the primary Evidence Library database has been installed and correctly permissioned for the type of Evidence Library installation chosen.
- Any systems designated as Remote Upload Servers are online and meet the minimum requirements for that role.

EL-02- Evidence Library Server Installation

Install the services and software to collect, process, view, modify, store, and export video evidence collected from the in-car DVR units.

- The installation software and pre-requisite software is copied to the local repository local on the server and shared to Authenticated Users with Full Control, and set Users to have the NTFS Write capability on the shared folder. Run the software from a local drive, not over the network.
- Install the WatchGuard Video Security Token Service, creating the Lightweight Directory Service instance that the software uses for authentication, and ensure the service is started
- Install the WatchGuard Video Hosted, and ensure the service is started
- Install the WatchGuard Web Server
- Install the WatchGuard Video Wireless Import Service, and ensure the service is started, binding the service to the appropriate network adapter on the server
- Install the WatchGuard Video Evidence Library Client, providing an interface to configure the remaining service settings.
- Install the WatchGuard Video JobQueueWork Service, and ensure the service is started.

EL-03-Add Active Directory Groups

The IT Point of contact would create (or use existing) AD security Groups, for the Evidence Library application to set permissions (e.g. Officer's AD group has permission to View video, but cannot make copies of video. Supervisors AD group has permission to view all video and can make copies of video)

EL-04-Configure Evidence Library Settings

- Configure the Evidence Library application for use.
- Add necessary storage locations and shares to system
- Set all automatic retention policies on evidence and cleanup interval.

EL-05-Remote Upload Server (if applicable)

Install the services and software necessary to receive video evidence from vehicle DVRs at a remote, well-connected location, and configure the server to send all uploads to the primary WatchGuard Video server.

- The WatchGuard Video Service is installed, binding the service to the appropriate network adapter on the server, and the service is started.

Remote Evidence Library Server Installation

A WatchGuard Technician will connect remotely to a provisioned server to install the services and software to collect, process, view, modify, store, and export video evidence collected from the 4RE and VISTA WiFi cameras.

- Remote connectivity must be provided to the server that has been designated as the primary WatchGuard Server.
- The WatchGuard Technician will connect remotely to the server over the Internet prior to the agreed upon time to verify the provided server is properly configured, and to copy any required files and folders to the server.
- At the agreed upon time, the WatchGuard technician will connect to the server again and perform the software installation.
- The WatchGuard technician will configure all desired settings and assist with configuring the 4RE and VISTA WiFi cameras.
- The agency will assist with the VISTA configuration and verify functionality.

EL-06-Configure Evidence Library Rimage Setup

Configure Evidence Library software for exports to an existing Rimage DVD robot and test.

EL-07-Installation of Evidence Library Transfer Agent on Agency Workstations

Party will be responsible for installing the Evidence Library Transfer Agent on specified computers.

The Transfer Agent can be installed remotely with SCCM or other like software. *Contact Project Manager or WatchGuard Support representative to verify the instructions below are up to date*:

Transfer_Agent.exe (installed with El website) is a wrapped version TransferAgent, TransferService and VistaDriver with install choices embedded.

It only accepts a /Q switch for unattended install

TransferAgent.exe (also included on ISO) has TransferService and Vista Driver as pre-reqs, which limits our ability to control their behavior.

TransferAgent accepts the following parameters

/s which silently installs vista driver and transfer service (only valid if upgrade or TransferService registry is pre-populated as below)

CL_HOST_SERVER=computer name (default 'localhost' if Host service detected) computer name where Host service is installed

CL_INSTALLDIR=directory (defaults to C:\Program Files (x86)\WatchGuard Video\) Installation directory

CL_OPERATIONS_DIRECTORY=directory (defaults to C:\WatchGuardVideo\)

CL_STS_SERVER=computer name (default 'localhost' if STS service detected) computer name where STS

/qb quiet basic interface (skipping user inputs with progress bar)

/qn quiet no interface

/l*v drive:\directory\file.log manually specify install log location defaults to

Examples:

Minimum silent install command line (only useful for upgrades or if registry pre-populated with answers) :

TransferAgent.exe /s /v/qn

All Parameters:

TransferAgent.exe /s /v/"qn CL_HOST_SERVER=localhost CL_STS_SERVER=localhost" /v"CL_INSTALLDIR=\"C:\Program Files\WGV\\"" /v"CL_OPERATIONS_DIRECTORY=\"C:\WGV\\""

TransferService.exe (as a pre-req of TransferAgent) can only be configured at install through the use of 32-bit registry keys

[HKEY_LOCAL_MACHINE\SOFTWARE\WatchGuard Video\Transfer Service]

"STS_SERVER"="JSAVONAWIN7VM"

"HOST_SERVER"="JSAVONAWIN7VM"

"WEB_API_PORT"="9034"

"UI_URL"=https://jsavonawin7vm.watchguardvideo.local

Please note if you are directly entering into registry on 64-bit systems root key changes to

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\WatchGuard Video\Transfer Service]

Instructions for rebuilding Transfer_Agent.exe on webserver for changes to certificate either 1) or 2) below

1) Re-generate Transfer_Agent.exe package with updated certificate.
a) Copy new certificate to C:\ProgramData\WatchGuard Video\EvidenceLibraryWeb.cer (on Web server)

b) Run "C:\Program Files\WatchGuard Video\Evidence Library Web\WebRoot\Client\buildTA.cmd" 1 (from admin command prompt on Web server)

c) For deployment run new Transfer_Agent.exe /Q

--OR--

2) Use TransferAgent.exe from ISO after pre-populating answers in registry.
a) Create reg file with answers for Transfer Service. (or re-use existing C:\Program Files\WatchGuard Video\Evidence Library Web\WebRoot\Client\TransferAnswer.reg)

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\WatchGuard Video]

[-HKEY_LOCAL_MACHINE\SOFTWARE\WatchGuard Video\Transfer Agent]

[HKEY_LOCAL_MACHINE\SOFTWARE\WatchGuard Video\Transfer Service]
"STS_SERVER"="JSAVONAWIN7VM"
"HOST_SERVER"="JSAVONAWIN7VM"
"WEB_API_PORT"="9034"
"UI_URL"=https://jsavonawin7vm.watchguardvideo.local

b) Deploy reg answer file to target machine (unneeded if upgrading a previous installation of EL4 Transfer Agent)

reg.exe IMPORT TransferAnswer.reg /reg:32

c) Add cert to target machines (certutil -addstore "Root" EvidenceLibraryWeb.cer) or use group policy…

d) Deploy TransferAgent.exe /S /V"/qn /l*v %TEMP%\WatchGuard_Video_Transfer_Agent.log"

EL-08-Minimum Workstation Hardware Requirements

Verify the following minimum hardware requirements

- 1.7 gigahertz (GHz) Dual core comparable or faster processor
- 1 gigabyte (GB) or more of RAM
- 160 megabytes (MB) or more of available hard disk space
- DVD-RW optical drive (if exporting to a DVD disc)
- 1 available USB 2.0 port
- Super VGA video adapter capable of 1024 x 768 resolution or higher
- 100 Mbps Network Card or better

EL-09-Domain / Network Connectivity

- Agencies using a Domain Network
    - Log into the workstation using a domain user login and password
- Agencies using a NON-Domain Network
    - Log into the workstation with a valid user login and password
- Verify the Evidence Library server is visible to the workstation using the ping command

Workstation OS & Browser Requirements

Verify one of the following operating systems is installed on the workstation(s)

- Window 7
- Windows 8.1
- Windows 10

Verify one of the following browsers is installed on the workstation

- Google Chrome v45 or Higher
- Internet Explorer 10
- Internet Explorer 11

- Microsoft Edge

User Permissions

Ensure all Evidence Library users have right to access the workstation and Evidence Library server.

EL-10- Cloud Storage

The agency or WatchGuard Video could provide cloud storage. The type of cloud storage supported depends on the Evidence Library software version. Contact WatchGuard Video Project Manager to get up to date supported cloud storage systems.

- Obtain required Cloud storage account information (i.e. Azure, endpoint suffix, account key)
- Enter in required information in Evidence Library "Evidence Management"

4RE-01-Configuring 4RE DVR units

Prior to first use, each 4RE DVR must be configured. This process involves adding each vehicle to Evidence library, generating a configuration file and deploying this configuration to the DVR using a USB drive. This process is generally shared between the Evidence Library administrator or Fleet Manager Role and the vehicle installer. If On-site services are purchased the technician will assist in creating the Vehicles in Evidence Library from an agency provided list and create the USB Configuration drive for the installer.

4RE-02-Create a Configuration USB

- Adding Vehicle to Evidence library
    - Vehicles are added to Evidence Library by an administrator or user with the Device Management role.
    - Open Device Management and select Edit configuration
    - Click the All Vehicles Node and select New to add a new vehicle.
    - Enter in a "Vehicle ID" (unique name that easily identifies each vehicle)
    - Select the appropriate "Configuration" Group
- Generating a USB configuration drive
    - Open Device Management and select Deploy Configurations Manually
    - Select the Vehicles to be configured or use the Select All function
    - Click the Export Configuration button and select a USB drive

4RE-03-Configure 4RE DVR's

- Press and hold the STOP button for 3 seconds to safely eject the current USB drive.

    - Open the USB vault, remove the USB drive and place the USB Configuration drive in the unit
    - On the display select the correct Vehicle ID and press the LOAD button
    - Replace the original USB drive and close the vault
    - Power cycle (reboot) the DVR
- Test configuration
    - Confirm that the agency name appears in the bottom right corner of the display
    - Press Menu and select Officer and verify that an appropriate list of officers is displayed

Configure the DVR's as they are available.

4RE-04-Change IP Address on DVR (if applicable)

In some instances the DVR IP address parameters may need to be changed from the default settings. When this is required a detail list of assigned addresses will be created and provided to the Agency along with instructions on how to manually change these parameters.

The default IP address of the DVR is
10.1.100.20
255.0.0.0
10.1.0.1

The secondary IP standard is:

10.1.100.20
255.255.255.0
10.1.100.1

4RE-09-4RE In-Car System Installation

Follow up to date instructions that are provided in the DVR box.

4RE-10-Interview Room setup

If using an interview room for the 4RE system, the agency must provide the following for each 4RE system (future 4RE software versions may support DHCP).

Soft items:

1. Static IP address
2. Subnet mask
3. Gateway

Physical items:

1. Ethernet connection on a 100 Mbps network or better (4RE must be able to connect to the network where the Evidence Library server is on)
2. Physical location to store 4RE, 4RE display, microphone(s) and camera(s)

WatchGuard Video highly recommends a professional CCTV installer is used to install the equipment. Also each interview room should have a dedicated 4RE system (not required, but highly recommended for improved search ability).

If using "WatchCommander" for live streaming and using more than 1 network card, the interview rooms need to be on the same network where the WatchCommander is bound to.

VISTA-01-Configuring VISTA WiFi cameras

Prior to first use, each VISTA WiFi camera must be configured. This process is called "Checkout" and involves connecting each camera to Evidence library to assign a configuration and officer name. This process can be done each time the officer needs to be assigned a camera, or can be done in scenarios where officers are assigned a Body Camera to use on a more permanent basis

VISTA-02-Create a Configuration

- Through the Evidence Library Administrator you will access VISTA Management to complete the following steps.
    - Set up VISTA default officer preferences.
    - Create initial default configuration(s).
    - Assign enrollments (user groups) to each configuration(s).
    - Set up system event tags if not already done.
    - Set the recording properties for each configuration.
    - Set the device properties for each configuration.
    - Apply VISTA with newest firmware (contact customer service for the latest version)
    - Confirm the configuration settings, save each configuration then close VISTA Management.

VISTA-03-Configure VISTA Cameras

- Ensure the VISTA cameras have the latest firmware version (contact WatchGuardVideo Customer Service)
- Connect the VISTA USB base into the computer where your Evidence Library software is located or set up the VISTA Transfer Station to connect to your Evidence Library software.
- Dock VISTA in the USB base or VISTA Transfer Station connected to your Evidence Library software.
- Using Evidence Library software, create and /or assign a configuration and an officer to the docked VISTA.

VISTA-04-Install/Configure Smart PoE Switch in Vehicle (if applicable)

- Applicable if using the VISTA WiFi in the vehicle with or without 4RE.
    - Install Smart PoE Switch in the vehicle. Use up to date instructions.
    - Install the WiFi Base. Use up to date instructions.
    - If not using the factory default IP address from the 4RE Configure the Smart PoE switch. See the default 4RE IP address below:
      10.1.100.20
      255.0.0.0
      10.1.0.1

TEST-01- Test Function of WatchGuard system

Test functions of the VISTA and Evidence Library system.

TEST-02-Checklist

	Test 4RE USB upload to server via Import Scanner on remote PC client
	Test 4RE Wireless upload to server
	Test Evidence Library Client Audio (Cabin microphone)
	Test Evidence Library Client Audio (Wireless microphone)
	Test wireless configuration changes
	Create a “Test” Case in Case Management
	Test Distributed Multi-Peer recording
	Test VISTA Wireless upload to server
	Test VISTA video upload to server via USB dock and/or VISTA Transfer Station
	Validate VISTA has correct configuration applied
	Test Evidence Library WEB Client Login
	Test Evidence Library WEB Client Video playback
	Test Evidence Library WEB Client Audio
	Test Exporting Evidence Library video to USB
	Test Exporting Evidence Library video to CD/DVD

TRAIN-01-Training

WatchGuard Video provides training on the Evidence Library and VISTA cameras. Online Training is covered as long as the customer is under warranty. Contact the WatchGuard Video Project Manager to setup online training for you agency.

TRAIN-02-4RE and VISTA WiFi End User Training (Officers)

WatchGuard Video will provide training (if needed) to parties who will be using the 4RE and VISTA WiFi cameras. This will cover how to use the system on a daily basis and how to get through a shift using 4RE and VISTA WiFi. Online Training is also available.

This onsite training can be completed in the following scenarios:

- 4RE Basic 5 minutes
- 4RE Full 1 hour
- VISTA/VISTA WiFi Basic 5 minutes
- VISTA/VISTA WiFi Full 45 minutes
- 4RE/VISTA Basic 7 minutes
- 4RE/VISTA Full 1 hour and 30 minutes

TRAIN-03-Evidence Library User Training (Officers/Supervisors)

WatchGuard Video will provide training (if needed) to parties who will be using the Evidence Library system on a computer. This will cover how to use the system on a daily basis, view video and make copies, make necessary changes in the system. This onsite training is typically 1 hour.

TRAIN-04- Evidence Library Administrative Training

WatchGuard Video will provide Administrative training to parties who will be using the Evidence Library on a computer. This will cover how to use administrative functions: Setting up permissions, set video retention policies, applying new configurations, and other management functions of Evidence Library. This onsite training is no longer than 3 hours, but typically can be completed in 1 hour.