VERIPATROL Network Whitepaper

INTRODUCTION

This document describes in detail the VERIPATROL system, installation and deployment planning, system requirements, communication methods, and system security.

CONTACT US

If you need assistance or have any questions, contact us by phone at 888-285-4548 or email **support@vievu.com**.

TABLE OF CONTENTS

PLANNING

This section describes system and network requirements to validate before performing a VERIPATROL installation.

Network installation requirements

Domain

- The Server and Client workstations belong to the same Domain. The network installation cannot be performed without a Windows domain.

Server

- Windows compatible server running Windows Server 2008, 2008R2, 2012, 2012R2, or 2016.
- Database Program: Microsoft SQL Server 2008, 2008R2, 2012, 2014, 2016, or 2017.
  SQL Server minimum hardware requirements may be higher than the minimum specifications listed above. Please check with Microsoft for the current requirements for the version being installed and the number of concurrent connections.
- Firewall exception for TCP Port 43690 and UDP Port 123. Add an exception for TCP 80 and TCP 443 if using VERIPATROL Cloud.
- Local or Network storage space sufficient to store the amount of video desired. *Does not apply to deployments that utilize the Cloud*

Note: The hardware requirements vary based on the number of concurrent connections, the video retention period, and the number of cameras. Contact VIEVU if you need assistance selecting a server.

Workstations

- Windows compatible computer running Windows 7, 8.1, or 10.
- 2 available USB ports.

Note: Use the Video Storage Calculator at www.vievu.com to estimate the amount of storage space required for your deployment.

Additional System Requirements for VERIPATROL Mobile:

SERVER

- 1 Public Static IP address
- Firewall exception for TCP 14444

ARCHITECTURE AND COMMUNICATION

System Architecture

The VERIPATROL system consists of 6 components. 4 required and 1 optional:

1. (required) **VERIPATROL Server**:
    - *SQL Database:* Used to store information about the video files and user data. Database named “SvdsDB2”.
    - *Server Configuration:* Program used to connect the VERIPATROL server service to the database instance, set the TCP port used for communication, set the NTP server pool and Proxy settings.
    - *VIEVU VERIPATROL Server service:* Windows service that runs on the server to communicate with the database, file storage location, and client workstations.

Note: The VIEVU VERIPATROL Server service is the ‘brains’ of the system. The system will not function if the service is not running.

---

2. (required) **VERIPATROL Admin**: Program used to administer the VERIPATROL system (add/remove users, delete video, etc.).
3. (required) **VERIPATROL Client**: Program used to transfer video files from a camera and for general users with limited security.
4. (required) **ffdshow Codec**: MPEG-4 decompression codec required to view video recorded with VIEVU cameras.
5. (optional**) VERIPATROL Mobile**: Program used for playback of videos in computers mounted in cars without a constant network connection.

Network Architecture

Each of the system components will be installed in the following locations:

Note: The video storage location can be placed on the same computer as the VERIPATROL server component, or placed on a different storage media (SAN, NAS, File Server, Separate HDD/Partition) including the Cloud.

---

1. **VERIPATROL Server**: Installed on the computer running the SQL database.
2. **VERIPATROL Admin**: Installed on the VERIPATROL Server and any client machines where administrative functions will be performed.
3. **VERIPATROL Client**: Installed on any client machines where direct video downloads or video playback will occur.
4. ***ffdshow* Codec**: Codec must be installed on the server and all computers where video playback will occur.
5. **VERIPATROL Mobile**: May be installed on any computers mounted in cars.

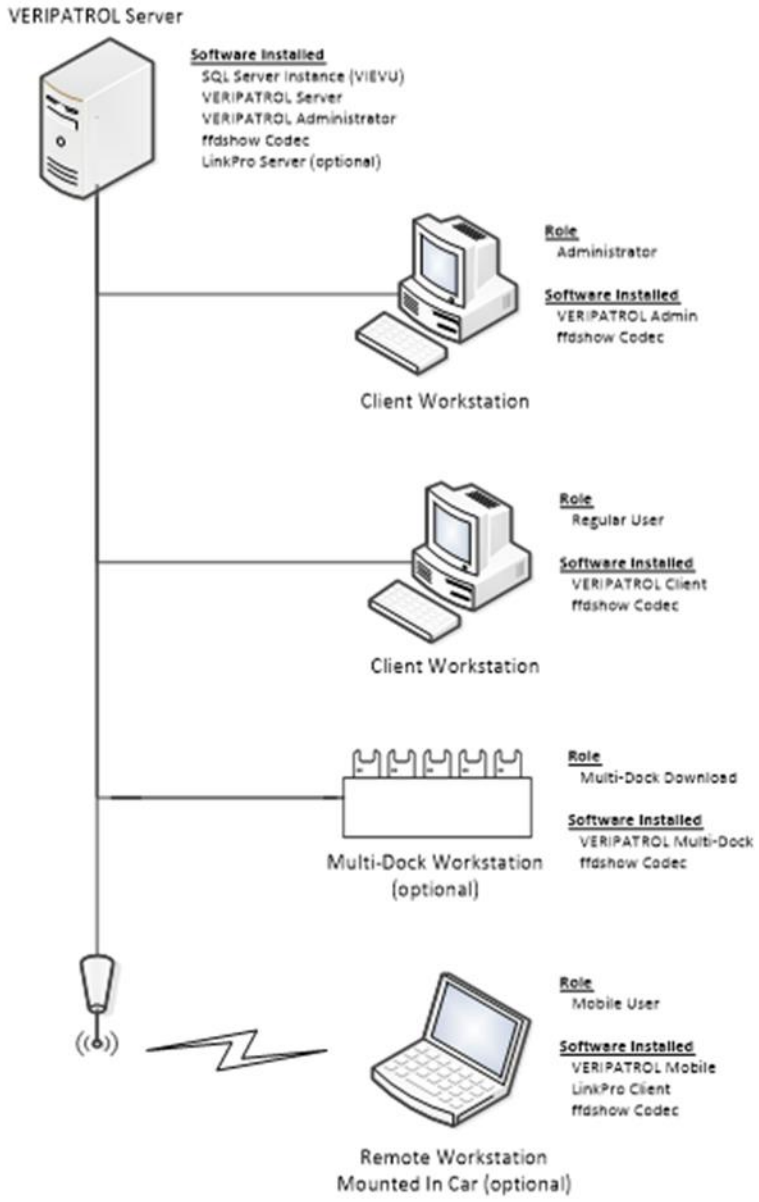

Figure 1

Data and Communications Processes

The VERIPATROL system communicates using the following processes:

Note: Each download cable is given a unique COM port number by the computer. The COM port number must be less than 19.

CAMERA TO CLIENT WORKSTATION

RS-232: Bi-Directional data transfer over Serial RS-232.

USB: Uni-Directional data transfer over Universal Serial Bus.

Note: For large deployments, it is recommended to permanently assign a download cable to each computer to prevent COM port assignment issues.

CLIENT/MULTI-DOCK WORKSTATION TO SERVER

TCP Port: Bi-Directional data transfer over TCP 43690*.

SERVER TO FILE STORAGE

TCP/IP: Bi-Directional data transfer over TCP/IP SMB.

SERVER TO NTP SERVER POOL

UDP Port: Bi-Directional data transfer over UDP 123.

Note: Communication ports listed with an asterisk can be changed in the 'Server Configuration' program located on the VERIPATROL server.

SERVER TO CLOUD (OPTIONAL)

HTTP/HTTPS: Bi-Directional data transfer over TCP 80 and 443.

MOBILE WORKSTATION TO SERVER (OPTIONAL)

TCP Port: Bi-Directional data transfer over TCP 43690*.

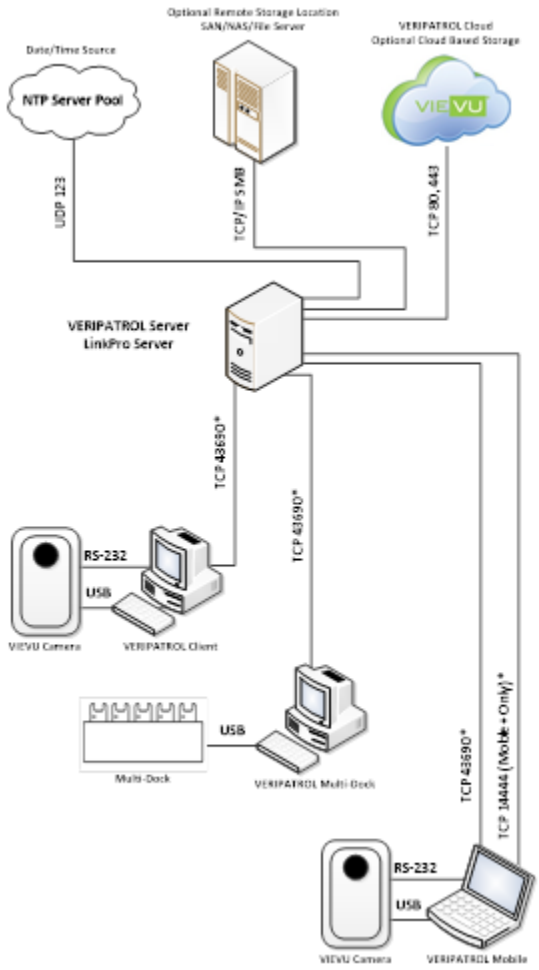

Figure 2

Determining File Storage Requirements

VIEVU cameras record at a rate of approximately 1 gigabyte per hour at standard definition. The LE4 camera records at a rate of 2.3 gigabytes per hour at high definition (720p). Due to compression variations, the exact file size will vary based on the subject of the recording. The file storage requirements are based upon four factors:

1. The number of cameras.
2. The average number of hours of video recorded each day.
3. The retention period in days.
4. Video resolution.

These four factors can be combined in the following equation to determine the recommended storage capacity in gigabytes. Recoding format values are standard definition = 1, high definition = 2.3

(# of Cameras) X (Avg. Hrs Per Day) X (Retention Period) X (Recording Format) = (Size in GB)

1 camera X 1 hr per day X 90 days X 2.3 = 207 GB

Note: A calculator is located on http://www.vievu.com/video-storage-calculator/

to perform this calculation.

Since they are not deleted after the expiration of a retention period, video files marked to **Never Be Deleted** will increase storage requirements.

Data Transfer Rates/Time

Due to the level of processing, digital signature verification, and security employed in the VERIPATROL application, the data transfer rates are reduced from a typical unsecured file transfer across the network.

The LE4 camera download operates at an average speed of ~10 MB/Sec. Adding a remote file storage location may reduce this transfer rate as a second connection is established between the server and the file storage location. Further degradation of the transfer rate can occur from sources such as reduced network bandwidth, high server load, server processing speed, and client processing speed.

Note: A typical user records approximately 1hr of video per day.

Date/Time Automatic Updating

The VERIPATROL server uses UDP port 123 to query the current time from an internet-based Network Time Protocol (NTP) server pool. During the camera assigning or video download process, the Date and Time on the camera is updated.

Greenwich Mean Time (GMT) may also be referred to as Coordinated Universal Time (UTC), or in the Military, as “Zulu” time. The LE4 camera adds the ability to set the Date and Time settings to sync with GMT or with the local time zone of the server. See the section “*Enable Local Time on LE4 Cameras*” in this document for more information.

The default NTP server pool is set to the United States pool (us.pool.ntp.org). If the VERIPATROL server is located in another region of the world, you can change the NTP server pool to use a pool that is geographically closer. This will ensure that the Date and Time being applied to the camera is as accurate as possible.

Note: The NTP server pool and proxy server settings are changed in the ‘Server Configuration’ program found on the VERIPATROL server.

UPDATE TO LATEST FIRMWARE

To be certain that your system is operating at its optimal efficiency and ensure that you're getting the maximum benefits from your VIEVU camera's features and from the rest of your VIEVU equipment, it is critical that you regularly update Camera and Multi-Dock Firmware.

Regular Updates for Equipment Firmware

VIEVU camera firmware can be updated either automatically, generally through a Multi-Dock setup, or manually using the following procedure.

➔ To manually update VIEVU Camera Firmware:

1. Visit the VIEVU Support page at http://www.vievu.com/support
2. Select your camera model from the camera dropdown list under the Support menu (Figure 1).

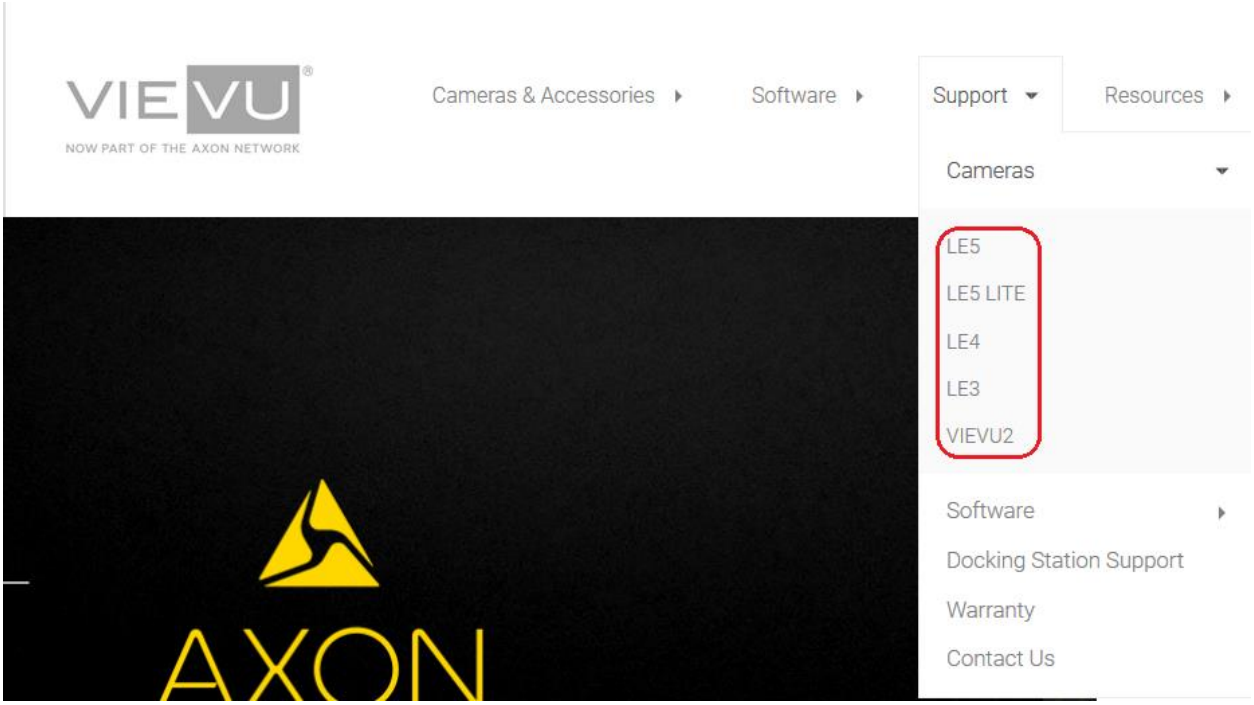

Figure 3

3. The camera page will be opened. Download and run the **Firmware Updater** tool (Figure 4).

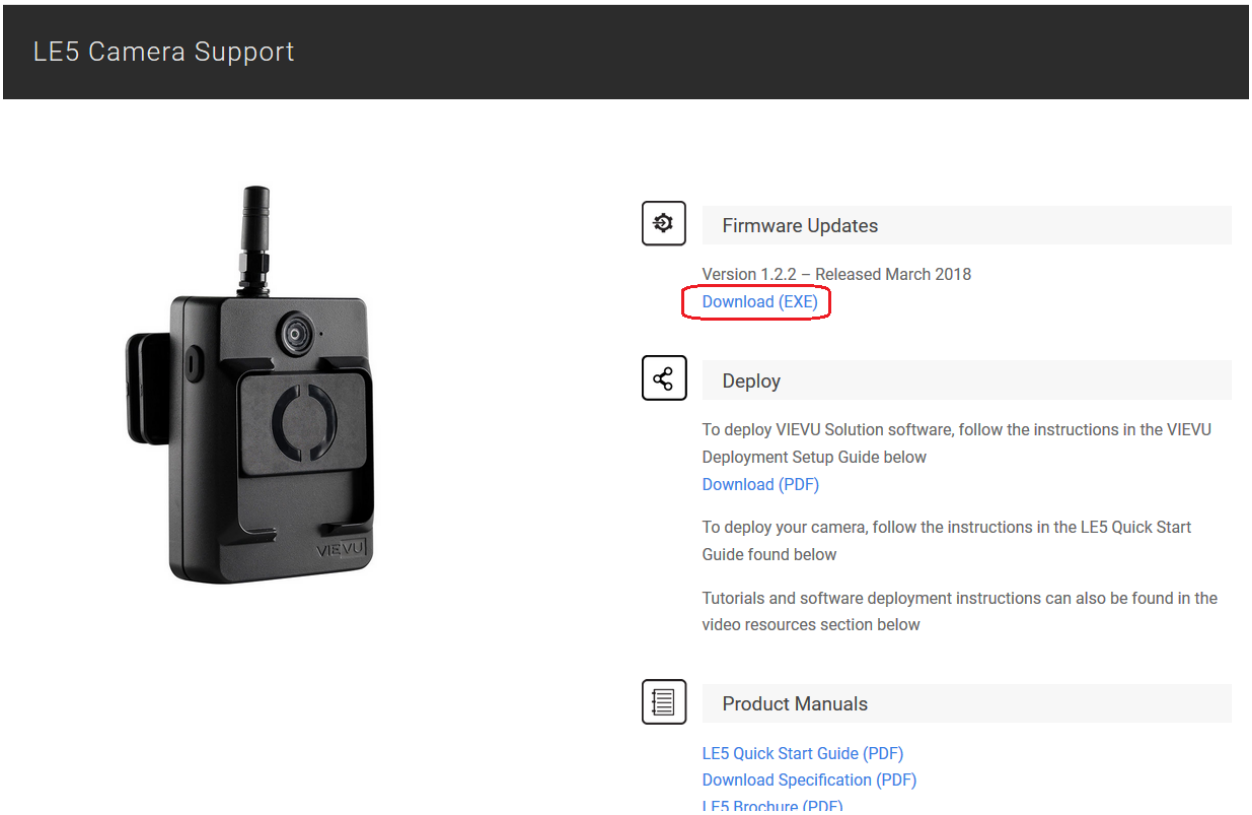

Figure 4

4. Open the executable file from a windows File Browser (Figure 5).

Figure 5

5. Follow the instructions on the screen to update the camera.

NETWORK INSTALLATION

Installation Instructions

You can download *Network Installation instructions* from www.vievu.com/support.

VERIPATROL Mobile installation instructions are in a separate document which you can also download from vievu.com.

Unattended Installation/Upgrade

The VERIPATROL installation executables file contains the ability to automate the installation or upgrade of the VERIPATROL software on a client computer using a preconfigured answer file– it cannot be used to install the VERIPATROL server. This answer file supplies the executable files with the configuration options desired for the computer on which it is deployed. When the answer file exists, the GUI interface is suppressed. An unattended installation is the most reliable option for use with remote installation software to push the VERIPATROL software to computers on the network.

The answer file uses XML format which can be downloaded from www.vievu.com/veripatrol-support/.

The answer file is compatible with the VERIPATROL_Installer executable:

Configuration

To configure the answer file, update the following sections with values for your specific installation and configuration.

<LicenseAgreement>: Indicate your acceptance of the VERIPATROL EULA.

<IPAddress>: Input the IP Address of the VERIPATROL server.

<Port>: Input the port used by the VERIPATROL server. The default is 43690.

<UpgradeExistingComponentsOnly>:

This option is only valid for upgrading the VERIPATROL software. When this option is set to YES, the Network Upgrade file will upgrade the components currently installed on the computer. Using this option allows deployment of the same answer file across computers that have different VERIPATROL components installed. If this option is set to YES, the Admin/Client/Mobile sections are ignored.

<Admin>: Indicate if the Admin component should be installed.

<Client>: Indicate if the Client component should be installed.

<Mobile>: Indicate if the Mobile component should be installed.

Once the answer file is configured, place the XML file in the same directory as the VERIPATROL executable. Upon launch, the executable reads the XML file and performs the operation without a GUI. When deploying the software using an automated system, simply deploy the answer file and the executable to the same directory, and then launch the executable file.

Note: The VERIPATROL executable must be launched as a user with Administrative permissions on the computer.

SYSTEM CONFIGURATION & OPTIONS

Configuring a Video Storage Location

The VERIPATROL system can be configured to store video files on the same server as the VERIPATROL server component or placed on a separate storage device. The video storage locations are managed from the **Server Setup** tab in the Admin application. The default video storage location is as follows:

Note: Creating a file storage location will not change any user storage mappings. Use the 'Set Default Storage' process to change the file storage location for users configured to use the default storage location or change the storage by editing the user in the Admin application.

Server 2008/2012

C:\Program Data\VIEVU\VIEVU VERIPATROL Server\FileStorage

If the storage location is not local to the server (I.E. internal/external HDD or separate partition) the "VIEVU VERIPATROL Server" service's log on credentials will need to be changed to allow for authentication with the video storage location. This service is used by the VERIPATROL system to access the SQL database and the video storage location.

➔ To grant log on as a service permission:

1. Click **Start** and select **Run**.
2. Type in **services.msc** and click **OK**. The services window is displayed.
3. Double click on **VIEVU VERIPATROL Server**.
4. Click on the **Log on** tab at the top of the window.
5. Change **Log on as:** to **This Account**.
6. Complete the **User ID** and **Password** fields with a valid domain account that has read/write access to the remote storage location.
7. Click **OK**.
8. Stop and restart the service.
9. After the service has been changed and restarted, you can create the storage location.

➔ To create a new storage:

1. On the **Server Setup** tab click the **New Storage** button.
2. Enter the storage path into the box or click the **Browse** button to select the location.
3. When complete, click **OK**.

    - If an error is received, the network path is incorrect, or permissions are not set up properly.

Note: In network installations, the Server Setup tab in the Admin application is only accessible from the server. The Server Setup tab is not available from the Admin application on a client workstation.

Setting a Default Storage Location

To allow for the easy management of the video storage locations, you can set a default storage location. Any users who are configured to use the default storage location are automatically updated when the default storage is changed. Changing the default storage location changes the location where new video files are stored; existing files remain in their current location.

➔ To set a default storage location

1. Log in to the Admin application on the server:
2. On the **Server Setup** tab, highlight the storage to be set as the default.
3. Click the **Set Default Storage** button.
4. (Default Storage) will now be listed to the left of the storage path.

Moving an Existing File Storage Location

The VERIPATROL system can move video files from one existing storage location to another. Use this process when migrating to a new storage location, or to quickly move files if videos were accidently uploaded to an incorrect location.

Note: We have attempted to make the file transfer process as safe and error free as possible; however, there will always be a risk of information being lost or corrupted during the transfer. A backup prior to the transfer is highly recommended.

➔ To move an existing file storage location:

1. Log in to the Admin application on the server:
2. On the **Server Setup** tab, highlight the storage location to be moved.
3. Click the **Move Files** button at the bottom of the window.
4. Select the location to which the files will be moved and click **OK**.

    - A progress bar is displayed while the files are being transferred.

Note: In network installations, the Server Setup tab in the Admin application is only accessible from the server. The Server Setup tab is not available from the Admin application on a client workstation.
Before you can move files, the new storage location needs to be added to the system before files can be moved.

VERIPATROL Cloud Functionality & Activation

VERIPATROL Cloud is an optional Cloud-based video storage solution. Configuring Cloud storage directs the VERIPATROL system to store the video files in the Microsoft Azure Cloud.

Note: To estimate the costs associated with utilizing VERIPATROL Cloud, please contact a VIEVU sales representative.

How it Works

1. Video is downloaded from a camera to the VERIPATROL server. The video file is temporarily stored locally for immediate playback.
2. After ~1hr, the VERIPATROL system transfers the video file to the Cloud for permanent storage.
3. All video files stored in the Cloud will be streamed for playback.

Note: Once the Cloud is activated, any videos currently stored in the 'Default Storage Location' will be transferred to the Cloud. If you do not want existing videos to be transferred, change the default storage location to a location that is empty before configuring the Cloud.

Cloud Architecture

The Cloud uses a hybrid architecture to provide a low cost/maximum performance system. The hybrid architecture requires an on-site VERIPATROL server with an SQL database.

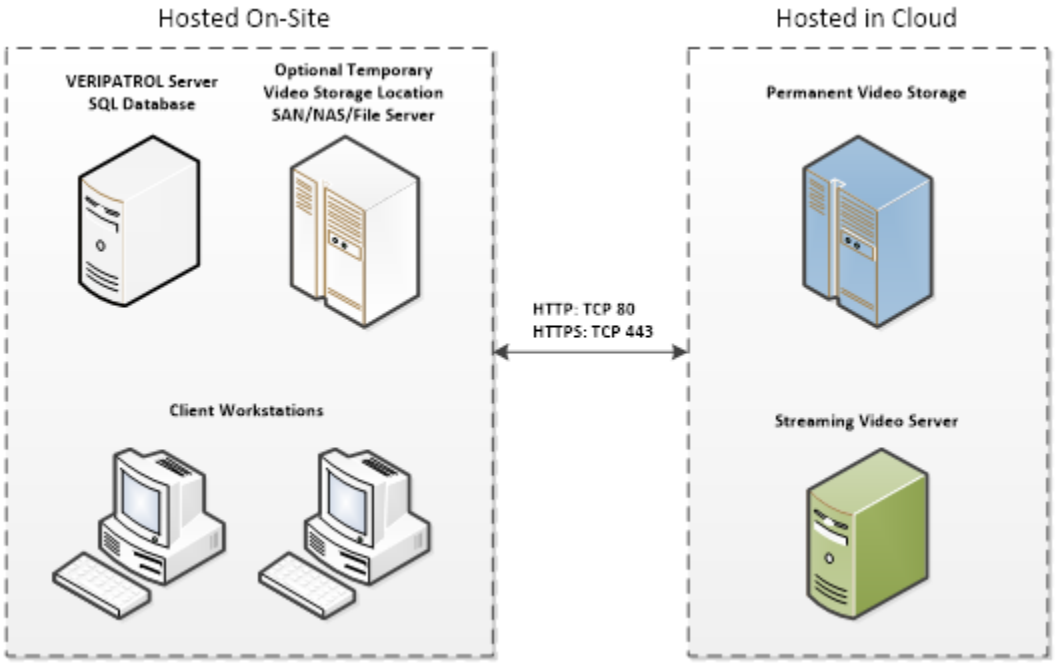

Figure 6

Cloud Bandwidth Requirements

For VERIPATROL Cloud to work efficiently, the internet upload bandwidth must be sized appropriately. If the upload bandwidth is too low, the upload queue may continuously grow as video files are being created faster than they can be transferred to the Cloud. Low bandwidth may also cause impacts to other internet enabled systems.

The table below lists minimum internet upload bandwidths required for VERIPATROL Cloud (Table 1):

Number of Cameras	Internet Upload Bandwidth (Mbps)
15	10
16-30	15
31-45	25
46-75	40
76-105	55
106+	55+

Table 1

Activating the Cloud

First, you must sign up for Cloud service by contacting a VIEVU Sales Representative. Access to the cloud is licensed. A VIEVU Solution license will give you access to the Cloud.

Please be aware that you must maintain an accurate number of licenses for the number of cameras that are assigned in VERIPATROL. Assigning more cameras than licenses may prevent VERIPATROL from transferring video to the Cloud. However, access to existing videos would be retained.

Additional signup instructions are available in the "*VERIPATROL Admin User Guide*."

Note: In network installations, the 'Server Setup' tab in the Admin application is only accessible from the server. The Server Setup tab is not available from the Admin application on a client workstation.

➔ To configure Cloud Storage:

1. Log in to the Admin application on the server:
2. On the **Server Setup** tab, click the **Configure Cloud Storage** button.
3. Input the **Account Name** and the **Access Key** provided to you by VIEVU.
4. Click the **Start Integration** button.
5. After the integration is finished, click the **Finish Integration** button.

Video files are automatically transferred to the Cloud approximately 1 hour after download. Video files that have been transferred to the Cloud are listed in *italics* in the video list.

Creating Secure Video Links

Secure links can be created for any video file stored in the Cloud. These secure, expiring links allow for effortless sharing of video files without burning copies onto a disc. Secure links are only available for video files stored in the VERIPATROL Cloud.

Note: Secure links allow playback of the video from any computer with internet access and the ffdshow codec installed. If you cannot watch the video, you may need to install the ffdshow codec. The ffdshow codec is available for download at www.vievu.com.

➔ To create a video link:

1. Begin playback of the video file from the Admin or Client application.
2. Click the **Pause** button, located in the lower-left corner of the screen.
3. Input the desired link expiration Date/Time into the **Video Link** box at the top of the playback window.
4. Click the **Generate Link** button. A message will be given indicating the link has been copied to the clipboard. You can now paste the link into the desired location, such as an email.

Disabling the Cloud

You can activate VERIPATROL Cloud at any time. You are free to move to and from the Cloud without any impact on the setup of the VERIPATROL system or how the users interact with the system.

Note: In network installations, the Server Setup tab in the Admin application is only accessible from the server. The Server Setup tab is not available from the Admin application on a client workstation.

➔ To disable the cloud:

1. Log in to the Admin application on the server

2. On the **Server Setup** tab, click the **Configure Cloud Storage** button.
3. Click the **Disable Cloud** button on the top-right corner of the window.
4. Select the location where the video files should be moved to.
5. VERIPATROL will now transfer all video files stored in the Cloud to the local storage location.

    - If the network connection drops or the file transfer is interrupted, VERIPATROL will display an error message.
    - When the network connection has recovered, repeat the disable Cloud process again.
    - The transfer process will begin from where it left off.

6. When the file transfer is complete, VERIPATROL confirms the Cloud is now disabled.

Setting Video Retention Periods

The VERIPATROL system is pre-configured with a blank file category that has a retention period that keeps videos indefinitely. If a new retention period is defined, all video files that exceed the retention period will be removed unless the video is marked "**never be deleted**". Each file category has its own retention period. The retention period is calculated from the date of upload, not the date of record. The retention period can be set to as short as 1 day. The retention period is set in the VERIPATROL Admin application.

Note: Caution should be used whenever the retention policy is modified. Any videos that are removed cannot be recovered with the application.

➔ To set a video retention period:

1. Log in to the Admin application on the server:
2. On the **Server Setup** tab, click the **Categories & Retention** tab.
3. Highlight the category to change and click the **Retention Period** button.
4. Change the **By Default Store Files For:** field to the new value (1-99999).
5. Click **Ok**.
6. Click **Yes** to restart the Server processes (the physical server will not restart).
7. Once the server is restarted, click **Ok**.

Note: In network installations, the Server Setup tab in the Admin application is only accessible from the server. The Server Setup tab is not available from the Admin application on a client workstation.

Optional Logging

VERIPATROL allows for the customization of several logging features. In addition to required logging, 5 additional actions can be logged.

Optional Logging Criteria:

1. **Log User Login:** Log each time a User accesses the Admin or Client application.
2. **Log Camera Download:** Log each time a camera is downloaded.
3. **Log Viewing Video Files:** Log each time a User views a video.
4. **Log User Comments:** Log each time a video comment is added or modified.
5. **Log Category Change:** Log each time a video category is selected or changed.

➔ To enable optional logging, log in to the Admin application on the server:

1. Click the **Master Log** tab.

2. Click the **Settings** button on the bottom-left.
3. Remove the checkmark next to **Export Master Log with Video Copies**.
4. Click **Ok**.

Note: In network installations, the Settings button on the Master Log tab in the Admin application is only accessible from the server. The Settings button is not available from the Admin application on a client workstation.

Exporting Master Log with Video Copies

When enabled, this feature creates a text file containing all Master Log records related to a video file when a copy is made. The text file name will be the same as the video file name. This will provide a chain of custody record of the time the video was downloaded, when the copy was made and any additional logging events that may have occurred while the video was stored in the system.

Note: This feature is enabled by default.

➔ To disable this feature:

1. Log in to the Admin application on the server.
2. Click the **Master Log** tab.
3. Click the **Settings** button on the bottom-left.
4. Clear the **Export Master Log with Video Copies** check box.
5. Click **Ok**.

Note: In network installations, the Settings button on the Master Log tab in the Admin application is only accessible from the server. The Settings button is not available from the Admin application on a client workstation.

Setting a File Deletion Schedule

The VERIPATROL system deletes video files based upon the retention policy. The deletion process can be set to run at any time during the day.

➔ To set a file deletion schedule:

1. Log in to the Admin application on the server:
2. On the **Server Setup** tab, click the **Categories & Retention** tab.
3. Click the **Cleanup Schedule** button.
4. Input the time the deletion process should begin.
5. Set the deletion interval.
    - The interval is the number of days between deletion cycles.
6. Click **Apply**.

Note: In network installations, the Settings button on the Master Log tab in the Admin application is only accessible from the server. The Settings button is not available from the Admin application on a client workstation.

Alternatively, the deletion check can be triggered from an external program such as **Scheduled Tasks**. The deletion process begins by running the *SvdsServer* executable, located in *C:\Program Files\VIEVU VERIPATROL\bin*, with the */forcecleanup* switch.

Note: Use the Force Cleanup button on the Cleanup Schedule window to manually start the deletion check.

Camera Settings

The default settings are originally set to **Not Set**, however, the firmware on the LE4 camera will determine its own default settings when you assign it. When the camera settings are changed in VERIPATROL, VERIPATROL will update the settings on each camera as they are assigned. The **Not Set** option tells VERIPATROL to make no changes to a camera when it is assigned. This is useful when requiring cameras operating with multiple configuration profiles.

Note: Settings are only applied when the cameras are assigned. If setting changes are made in VERIPATROL, the cameras will not be updated unless it is reassigned.

LE3 Camera Settings

1. Video Resolution: **SD**, **720**, or **Not Set**
2. Microphone: **On**, **Off**, or **Not Set**

LE4 mini Camera Settings

1. Video Resolution: **SD**, **720**, **1080**, or **Not Set**
2. Microphone: **On**, **Off**, or **Not Set**
3. Wi-Fi: **On**, **Off**, or **Not Set**.
4. SSID Broadcast: **On**, **Off**, or **Not Set**
5. Wi- Fi Password

LE4 Camera Settings

The LE4 camera supports multiple device settings:

1. Video Resolution: **SD**, **720**, **1080**, or **Not Set**
2. Pre-Record: **On**, **Off**, or **Not Set**
3. Post**-** Record **On, Off** or **Not Set**
4. Microphone: **On**, **Off**, or **Not Set**
5. Wi-Fi: **On**, **Off**, or **Not Set**.
6. SSID Broadcast: **On**, **Off**, or **Not Set**
7. Wi- Fi Password
    - When Wi-Fi is set to **On**, Wi-Fi password must be included in the **Wi-Fi Password** field.

Note: The camera settings should be selected before assigning LE4 cameras. The camera settings are only applied to the LE4 camera during the assigning process.

LE5 LITE Camera Settings

1. Video Resolution: **SD**, **720**, **1080**, or **Not Set**
2. Microphone: **On**, **Off**, or **Not Set**
3. Wi-Fi: **On**, **Off**, or **Not Set**.
4. SSID Broadcast: **On**, **Off**, or **Not Set**
5. Wi- Fi Password

LE5 Camera Settings

The LE5 camera supports multiple device settings:

1. Video Resolution: **SD**, **720**, **1080**, or **Not Set**
2. Pre-Record: **On**, **Off**, or **Not Set**
3. Pre-Record Audio: **On**, **Off**, or **Not Set**
4. Pre-Record Length: **5-180** seconds.
    - **30** by default
5. Post-Record: **On**, **Off**, or **Not Set**
6. Post-Record Length: 1**-60** seconds
    - **10** by default
7. Field of view: **70**, **90**, **120**, or **Not Set**
8. Covert Mode: **On**, **Off**, or **Not Set**
9. Vibration: **On**, **Off**, or **Not Set**
10. Microphone: **On**, **Off**, or **Not Set**
11. Wi-Fi: **On**, **Off**, or **Not Set**.
12. SSID Broadcast: **On**, **Off**, or **Not Set**
13. Wi-Fi Password
    - When Wi-Fi is set to **On**, Wi-Fi password must be included in the **Wi-Fi Password** field.

Note: The default settings are originally set to Not Set, however, the firmware on the LE5 camera will determine its own default settings when you assign it. When the LE5 camera settings are changed in VERIPATROL, VERIPATROL will update the settings on each LE5 camera as the cameras are assigned. The Not Set option tells VERIPATROL to make no changes to the LE5 camera when it is assigned. This is useful when you want to have cameras operating with multiple configuration profiles.

Configuring Camera Settings

➔ To configure camera settings

1. Log in to the Admin application:
2. On the **Cameras** tab
3. Click the **Camera settings** button.
4. Select the desired settings.
5. Click **Ok**.

Note: The camera settings should be selected before assigning VIEVU cameras. The camera settings are only applied to the LE5 camera during the assigning process. Settings are only applied when the cameras are assigned. If setting changes are made in VERIPATROL, the cameras will not be updated unless it is reassigned.

Enabling Local Time on LE4 and LE5 Cameras

The **Date and Time** stamp on the LE4 camera can be set to sync with GMT or the local time zone of the server. The **Date and Time** setting on LE4 cameras are updated when a camera is assigned or downloaded. VERIPATROL only changes the date and time on a camera if it can successfully receive the current time from the NTP internet time pool. If the server is unable to obtain the current time, the cameras are not updated.

Note: The default setting is GMT.

➔ To change the date and time setting:

1. Launch the Server Configuration program from the server.
2. Click the **Date and Time Settings** button.
3. Under the **LE4 Time Settings** heading, select the correct option.
4. Click **Ok.**
5. Click **Apply**, then **Yes** to restart the VERIPATROL service.

Exporting/Importing Databases and Videos

The VERIPATROL system supports an import/export feature to make moving the system between computers, migrating between different versions of SQL, and combining existing installations into a simple process. The export process makes copies of all videos in the export location. You must have enough free space in the export location to contain all the video files currently in the system.

Note: The Export/Import process should be done with the same version of VERIPATROL. To prevent errors, ensure both the source and target systems are using the same version of VERIPATROL.

➔ To export the database and videos:

1. Launch the 'Server Configuration' program from the server.
2. Select **File** and choose **Import/Export**.
3. Select **Export**.
4. Select a time period or **All** and choose **Next**.
5. Select an export location and choose **Next**.
6. The export process begins. When you're finished, click **Finish**.

Note: The 'Server Configuration' program is located in the program folders group at START>All Programs >VIEVU VERIPATROL.

➔ To import a database and videos:

1. Launch the 'Server Configuration' program from the server.
2. Select **File** and choose **Import/Export**.
3. Select **Import** and choose **Next**.
4. Select the *SvdsDB2.xml* file to import and click **Next**.
5. The import begins. Users are matched based on the login ID. If a user does not currently exist in the database, you are prompted for an action. If the user has a different login, select the correct user to map the user to and click **Match User**. If the user is new, select **Create New User**. The **Apply for all** feature remembers the selection and applies the same selection to any future users.
6. When the import is finished, click **Finish**.

Note: During Import, all video files are transferred to the current default storage location.

VERIPATROL Mobile

VERIPATROL Mobile is a free add-on that facilitates the review of video files currently stored on a camera for report writing and analysis in the field, where a connection to the server is not available. Video files are encrypted while stored on the computer to prevent unauthorized access or manipulation.

VERIPATROL Mobile does not remove the videos from the camera. You must go back to the station and download the camera later. The video is available on the computer for playback for 1 hour. After 1 hour, the video is deleted.

Logging

The same level of logging available in VERIPATROL continues with VERIPATROL Mobile. Actions performed and logged in VERIPATROL Mobile on remote computers are transferred to the VERIPATROL server to provide one central location for all user action reporting and monitoring.

Video Transfer Priority

There are 3 video transfer priorities. The priority levels are used to define the order to transfer the videos and the connection methods to use. The priority levels are: **Normal**, **High**, and **Emergency**. All videos are uploaded at the lowest **Normal** priority level. You can choose to enable **High** priority or **Emergency** if necessary. When a video is in **Normal** or **High** priority, the video is held on the computer for 1 hour for playback and adding comments/category information. When a video is placed in **Emergency** priority, the transfer begins immediately and the video is no longer available for playback or adding comments/category information.

Net Transcripts Audio Transcription Services

VIEVU has partnered with Net Transcripts to offer VIEVU customers with transcription services. VERIPATROL includes the ability to export an audio-only copy of a video file. This audio file can be securely uploaded to Net Transcripts through an internet portal for transcription services. Net Transcripts transcribes the audio onto the selected file and provides you with an evidence quality transcription.

To sign up for Transcription services or to upload an audio file for transcription, visit: http://nettranscripts.com/vievu/vievu-client-registration.htm

For more information about pricing, features, service levels, and supported languages contact Net Transcripts or visit http://nettranscripts.com

SECURITY

User Security Matrix

VERIPATROL allows for the customization of user access security/permissions. Four security check boxes create five separate security levels plus lockdown video access. Use the security selection matrix below to determine the correct security level for each user (Table 2).

Table 2

	Administrator	Delete Videos in Admin	Nothing Checked	Make Copies in Client	View All Videos in Client	Make Copies in Client and View all Videos in Client	Access Lockdown Videos*	Log In to VERIPATROL Mobile**
Log in to Admin Application	X							
Add/Remove/Edit a User	X							
Assign/Unassign a Camera	X							
Make a Copy of any Video	X							
Delete Any Video		X						
Add/Change Details of any Video	X							
View Master Log	X							
Change Logging Settings *	X							
Add/Change/Move/Set Default File Storage Location *	X							
Add/Rename/Remove File Categories *	X							
Change File Retention Period *	X							
Access Lockdown Videos**							X	
Log In to VERIPATROL Mobile**								X

Client Application	Administrator	Delete Videos in Admin	Nothing Checked	Make Copies in Client	View All Videos in Client	Make Copies in Client and View all Videos in Client	Access Lockdown Videos***	Log In to VERIPATROL Mobile**
Log in to Client Application	X		X	X	X	X		
View Videos Recorded by Me	X		X	X	X	X		
View Videos Recorded by Others	X				X	X		
Add/Change Details of a Video Recorded by Me	X		X	X	X	X		
Add/Change Details of a Video Recorded by Others	X				X	X		
Make a Copy of a Video Recorded by Me	X			X		X		
Make a Copy of a Video Recorded by Others	X					X		
Access Lockdown Videos**							X	
Log In to VERIPATROL Mobile**								X
* Additional Security Prevents All Administrators from Making These Changes in Network Installations								
** Security can be Added to any User								

Vidlock Security Suite

The VERIPATROL application includes the VidLock Security Suite. VidLock security provides the strictest evidence management processes available. The security features are as follows:

1. All LE4 and LE5 cameras are secured to prevent unauthorized access to the content of the camera.
2. VERIPATROL pairs a camera with an installation of the server through the camera assigning process. Once paired, the videos recorded on the camera can only be downloaded to your installation of VERIPATROL. If the camera were to be lost or stolen, the video files cannot be accessed by anyone else.
3. Access to the video file storage location is secured using windows NTFS file security.
4. Video files are masked with a GUID to prevent identification of the video files and their contents by a systems administrator with access to the file storage location.
5. All video files recorded on the LE4 and LE5 cameras are marked with an SHA cryptographic hash digital certificate to ensure the video integrity has not been compromised during the transfer from

the camera to VERIPATROL. This cryptographic hash function was designed by the National Security Agency (NSA).

6. VERIPATROL uses an internet time server to determine the exact date/time. This very precise date/time is applied to each camera during download to ensure the date/time does not drift.

Note: All VIEVU cameras MUST be assigned in the VERIPATROL Admin application before recording any video. Failure to assign a camera before recording video will prevent the videos from being downloaded. If you have any questions about the assigning process or VidLock security, please contact us.

Lockdown Videos

The lockdown video feature is available to prevent access, modification, or deletion of a video file by an unauthorized user. Once a video has been marked for **Lockdown**, the video can only be accessed by a user with **View Lockdown Video** security. This can be used to prevent the spread and playback of highly sensitive videos by the user who recorded the video, users with access to view all videos, and administrators. Any user can mark a video for lockdown.

➔ To mark a video for lockdown:

1. Log in to the Admin application:
2. Click the **Videos** button at the top of the window.
3. Highlight the desired video and click the **Add Details** button located in the lower-left corner of the window.
4. Select the **Lockdown Video** check box.
5. Click the **Apply** button in the lower-left corner of the window.

Securing the System

A network installation provides the most robust levels of security available. You can secure the VERIPATROL system so that only a single domain account is used to access the SQL database and the video file storage location. VIEVU recommends you create a domain account that is only used for the VERIPATROL system. Each end user of the VERIPATROL system will never directly access the SQL database or the video file storage location. The VERIPATROL server service accesses the locations on behalf of the user.

➔ To secure the system:

1. Change the “VIEVU VERIPATROL Server” service to a domain account.
1. Click **Start** and select **Run**.
2. Type in *services.msc* and click **OK**. The services window is displayed.
3. Double-click on **VIEVU VERIPATROL Server**.
4. Click on the **Log on** tab at the top.
5. Change **Log on as:** to **This Account**. Complete the **User ID** and **Password** fields with a valid domain account that has read/write access to the remote storage location and the SQL database.
6. Click **OK**.
7. Stop and restart the service.

Note: VERIPATROL Cloud can also enhance security by preventing direct access to the video files by System Administrators outside of the VERIPATROL system.

After the service logon account has been changed, authentication from the VERIPATROL server service to the video storage location and the SQL database will utilize this domain user account.

SQL Database: Permissions to the SQL server and database (*SvdsDB2*) can be restricted so that the only domain account that has access to the database and tables is the account the VIEVU VERIPATROL Server Service was set up to log on with above. If you need assistance securing SQL, please see the following Microsoft document, or the document for your particular version of SQL: SQL Server 2005 Security Best Practices.

Video Storage Location: You can restrict permissions to the storage location using NTFS so that the only domain account with access to the location is the account the VIEVU VERIPATROL Server Service was set up to log on with above. If you need assistance securing folders with NTFS, please see the following Microsoft document: Securing Files with NTFS.

VERIPATROL Cloud Security

VIEVU partnered with Microsoft® to develop the VIEVU Solution™ Cloud platform on Microsoft® Azure Government, the first enterprise Cloud designed specifically for United States government customers that directly supports CJIS. The VIEVU Solution allows government customers to store their data in the Cloud without concern over CJIS compliance. Microsoft® Azure Government has statutory CJIS compliance to state laws, regulations, agency requirements, and is FBI-certified.

Note: Non-United States Government customers are hosted on the public Azure platform.

- Physically isolated datacenter and network, applications, and hardware reside in the continental United States
- Provides true geographic redundancy with datacenters located more than 500 miles apart
- Operated by screened U.S. persons
- Committed to meeting rigorous compliance requirements and government policies

Additional information about Microsoft Azure features, security and compliance can be found at: http://azure.microsoft.com/en-us/features/gov/

VERIPATROL Mobile Security

VERIPATROL Mobile utilizes the same VidLock security suite to prevent unauthorized access to video files stored on the camera. Additionally, VERIPATROL Mobile encrypts all video files on the remote computer to ensure the evidence is protected while stored for playback in the car.

The technologies and processes used in VERIPATROL Mobile are protected by US patents: 8,190,088; 8,351,449; and 8,412,101. Multiple Patents Pending.