VERIPATROL Network Whitepaper

INTRODUCTION

This document details the VERIPATROL system, system requirements, communication methods, and system security. It details them for VERIPATROL Client and Admin, Mobile, RSSS, and Cloud. For additional support material please visit www.vievu.com/support.

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

INTRODUCTION 1

TABLE OF CONTENTS 2

SYSTEM ARCHETICTURE 3

STANDARD VERIPATROL 3
RSSS 4
VERIPATROL MOBILE (REVIEW MODE) 4
CLOUD 5
Bandwidth Requirements 6

DATA AND COMMUNICATIONS PROCESSES 7

STANDARD VERIPATROL 7
RSSS 8
Communication Between RSSS and Primary Server 8
CLOUD 8

DATE/TIME SYNCHRONIZATION 9

RSSS 9

FILE STORAGE 10

STANDARD VERIPATROL FILE STORAGE REQUIREMENTS 10
RSSS FILE STORAGE REQUIREMENTS 10
Temporary Storage Requirements 11
Data Transfer Rates/Time 12

EXPORTING+IMPORTING DATABASES 13

SECURITY 14

SECURING THE SYSTEM 14
VERIPATROL CLOUD SECURITY 15
VERIPATROL MOBILE SECURITY 16

SYSTEM ARCHETICTURE

This section details the architecture and data and communications processes of the VERIPATROL systems.

Standard VERIPATROL

The Standard VERIPATROL system consists of 3 components (Figure 1):

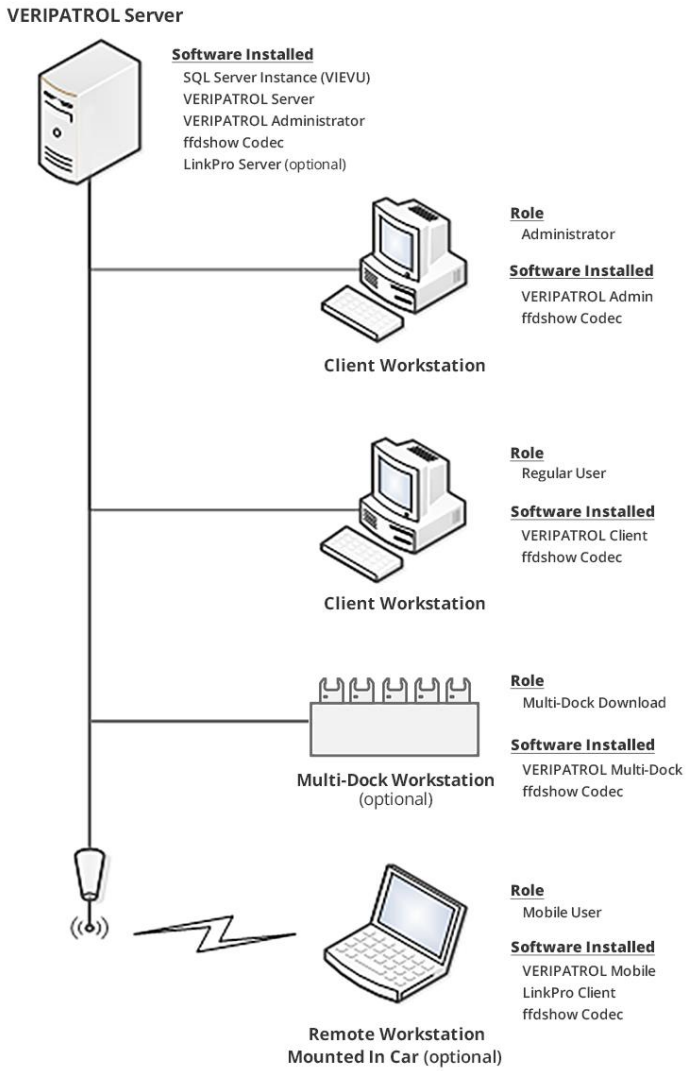

Figure 1

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.

Note: The Mobile Remote Workstation is an optional component.

RSSS

RSSS adds 2 components; The remaining architecture of the VERIPATROL system remains the same (Figure 2):

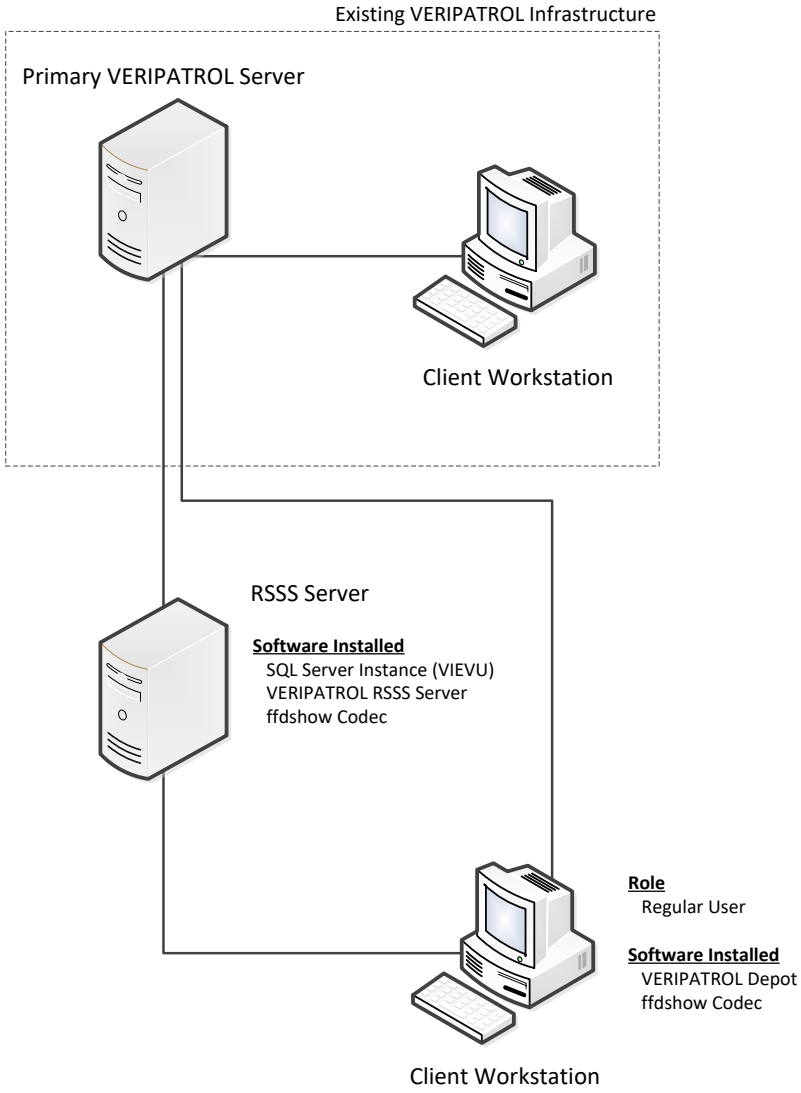

Figure 2

1. **VERIPATROL RSSS Server**: The server that is physically located at a remote site. Videos will be temporarily stored here until they are transferred to the primary VERIPATROL Server.
2. **VERIPATROL Depot**: Installed on any client machines where video downloads or video review will occur.

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

VERIPATROL Mobile (Review Mode)

VERIPATROL Mobile Review Mode adds 1 additional component; The remaining architecture of the VERIPATROL system remains the same (Figure 3):

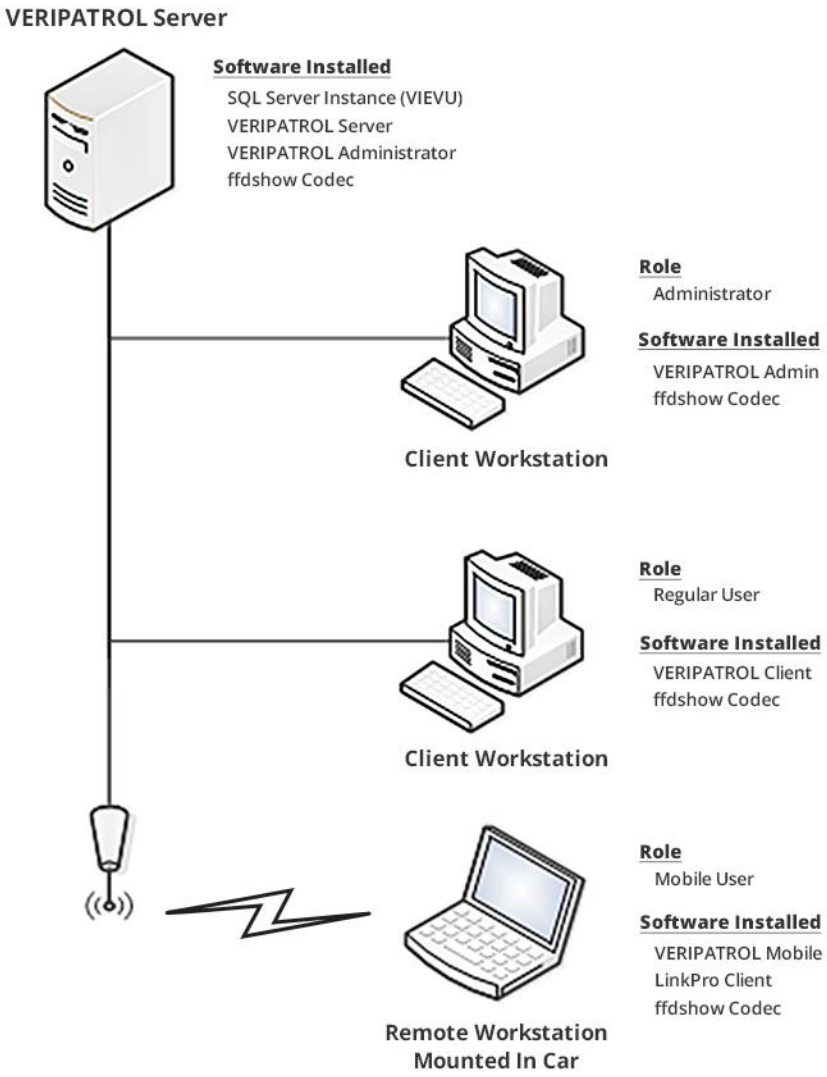

Figure 3

1. **VERIPATROL Mobile software**: This is installed on each remote computer in a car and is used to review videos stored on VIEVU cameras, add metadata, and make video copies.

Cloud

The Cloud uses a hybrid architecture to provide a low cost/maximum performance system. The hybrid architecture requires an on-site VERIPATROL server with a SQL database (Figure 4).

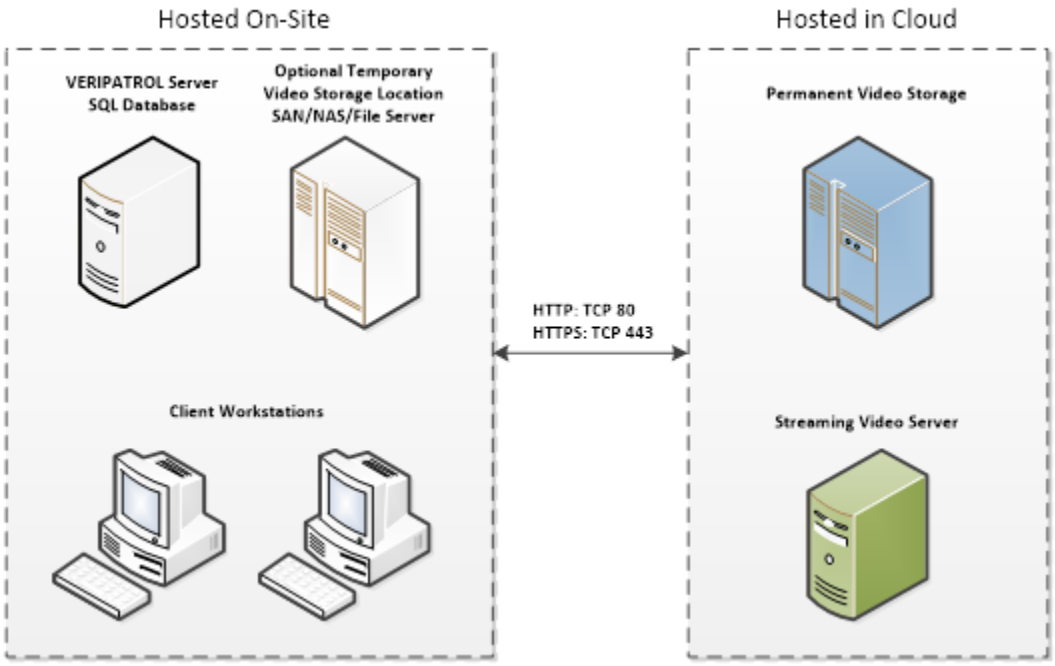

Figure 4

Bandwidth Requirements

For VERIPATROL Cloud to work efficiently, the available internet upload bandwidth must be sufficient. If the upload bandwidth is too low, the upload queue may outpace the file transfer to the Cloud and may impact other internet enabled systems.

The table below lists minimum internet upload bandwidths required (in addition to existing needs) for VERIPATROL Cloud (Table 1):

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+

DATA AND COMMUNICATIONS PROCESSES

This section details the interactions between each of the VERIPATROL components.

Standard VERIPATROL

The VERIPATROL system communicates using the following processes (Figure 5):

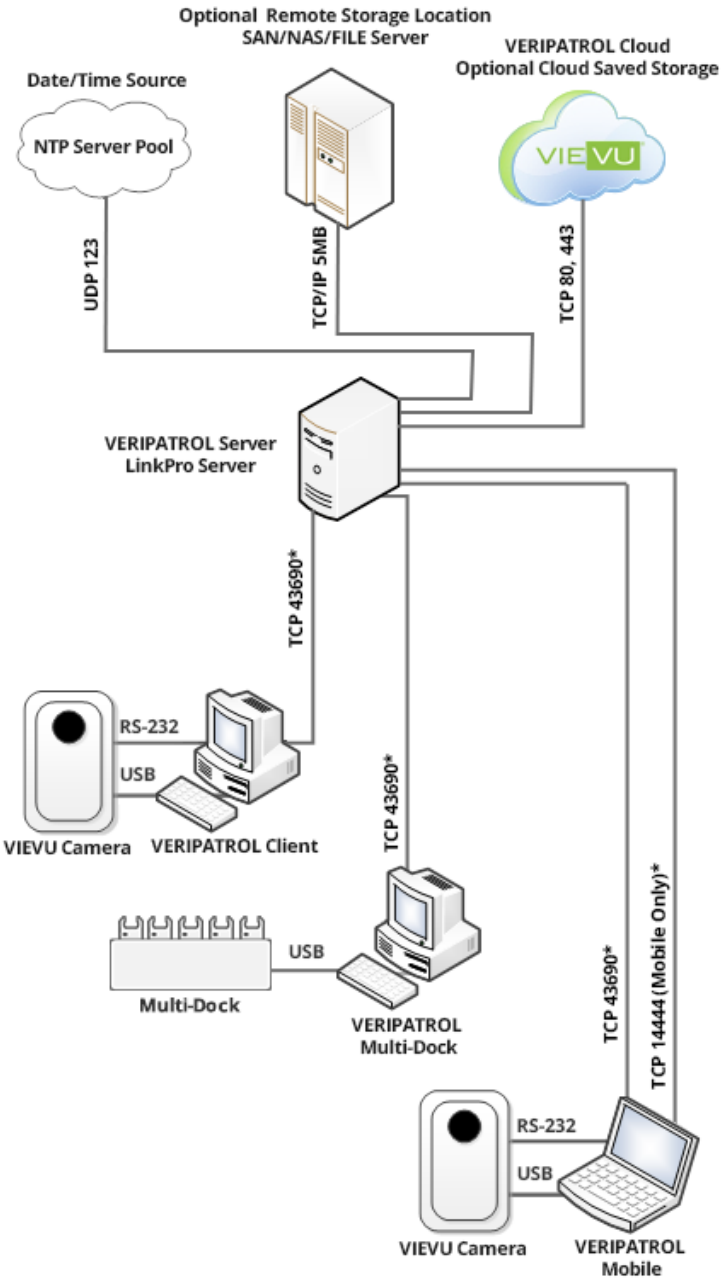

Figure 5

Note: Each download cable is given a unique COM port number by the computer.

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 WORKSTATION AND DOCKING STATION 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.

RSSS

RSSS adds 2 communication process; The remaining processes stay the same:

RSSS TO FILE STORAGE

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

RSSS SERVER TO NTP SERVER POOL

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

Communication Between RSSS and Primary Server

The RSSS Server connects to the Primary VERIPATROL server for user authentication, user security and system specific settings (file categories). This connection must always be active. Due to the high 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 network transfer speed between the Remote and Primary Servers should be sufficient enough to allow video to be transferred in a 24-hour period. If the network transfer speed is too slow, the video queue's growth will outpace the transfer rate of files from the Remote Server to the Primary Server.

Cloud

VERIPATROL Cloud adds the following process; All other communications remain the same:

SERVER TO CLOUD

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

DATE/TIME SYNCHRONIZATION

The VERIPATROL server uses UDP port 123 to query the current time from an internet-based Network Time Protocol (NTP) server pool. A camera's Date and time are updated during the camera assigning or video download process.

Greenwich Mean Time (GMT) may also be referred to as Coordinated Universal Time (UTC), or in the Military, as "Zulu" time. The LE4 (and later models) feature the ability to set the Date and Time settings to sync with GMT or with the local time zone of the server.

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, the NTP server can be configured to use one 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. See the VERIPATROL User Guide for further reference material.

RSSS

The RSSS server utilizes its own Date/Time setting configuration. It will not be updated if the primary VERIPATROL server is set to use local time for LE4 and LE5 cameras. Therefore, both the primary VERIPATROL server and the RSSS server must be updated if date and time changes are made.

Note: The NTP server pool and proxy server settings are changed in the 'RSSS Configuration' program found on the RSSS server.

FILE STORAGE

This section details file storage requirements and the average rates in which file transfer occurs.

Standard VERIPATROL 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 depend on the recording. File storage requirements are influenced by 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 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.

RSSS File Storage Requirements

The RSSS server can be configured to temporarily store video files for periods of as little as 1 hour or up to a maximum of 99 days before being transferred to the primary VERIPATROL server. The file storage requirements vary based on the length of time the videos will be stored on the RSSS server (Figure 6).

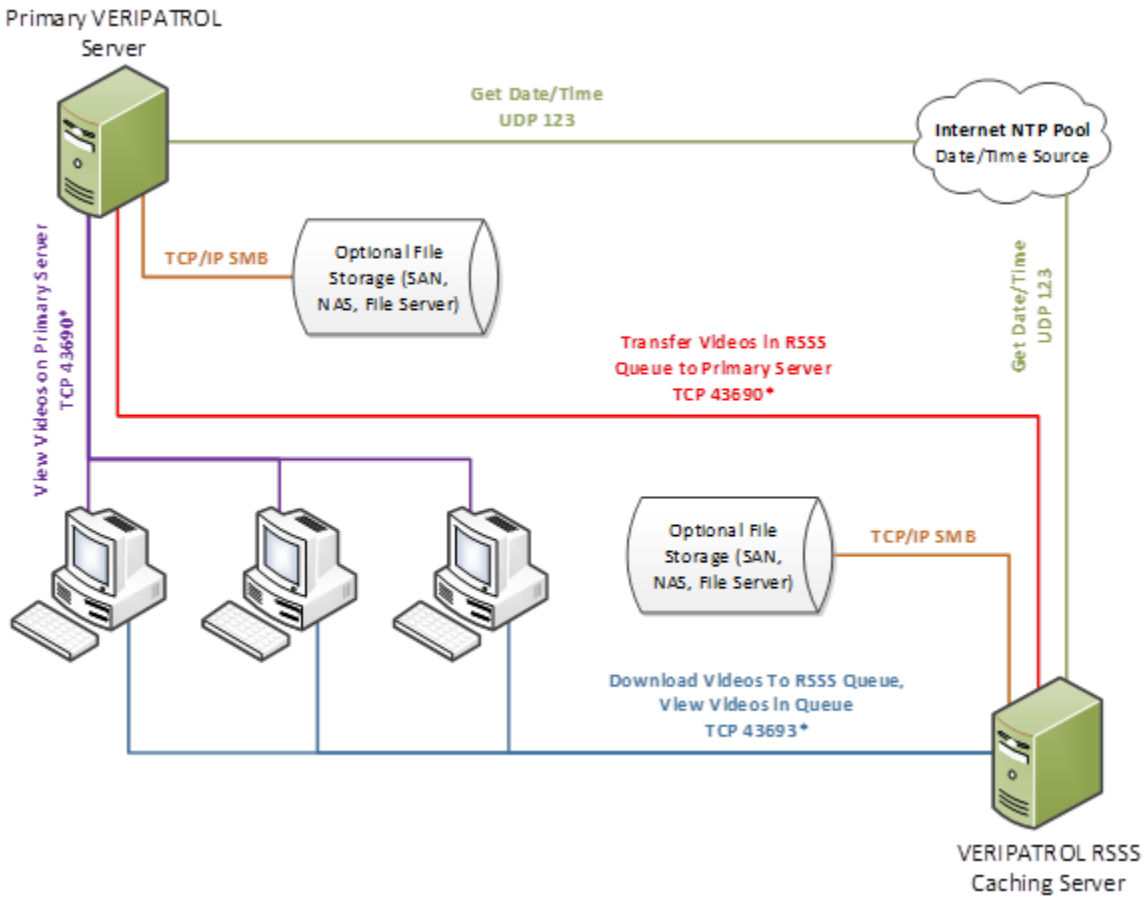

Figure 6

Temporary Storage Requirements

DETERMINED BY HOURS

The equation below assumes that each officer will record approximately 1 hour of video per download session (1 hour is the average an Officer records per day). The file storage requirements are based upon three factors:

1. The average number of cameras that download per hour
2. The temporary video storage period in hours
3. Video resolution

Combine these factors in the following equation to determine the recommended storage capacity in gigabytes.

(# of Downloads Per Hour) X (Storage Period in Hour) X (Recording Format) = (Storage Size in GB)

As an example, 1 camera download per hour X 1 hour storage period X 1 = 1 GB

Note: Recording format values are standard definition = 1, high definition = 2.3

DETERMINED BY DAYS

The calculator below assumes that each officer will record approximately 1 hour of video per day. 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 temporary video storage period in days
4. Video resolution

Combine these four factors in the following equation to determine the recommended storage capacity in gigabytes. Recording format values are standard definition = 1, high definition = 2.3

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

As an example, 1 camera X 1 hour per day X 90 days X 2.3 = 207 GB

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 about 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.

EXPORTING+IMPORTING DATABASES

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 **All** or define a **Custom range** and click on the **Next** button.
5. Select an export location and choose **Next**.
6. Enter destination for the *SvdsDB2.xml* file to populate and click on the **Next** button.
    - Click on the **Browse…** button to select a destination using Windows File Explorer.
7. The export process begins.
8. When the export is complete, click on the **Finish** button.

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

➔ To import a database and videos:

1. Launch the 'Server Configuration' program from the server.
2. Select **File** and click on **Import/Export**.
3. Select **Import** and click on the **Next** button.
4. Enter the *SvdsDB2.xml* file location and click on the **Next** button.
    - Click on the **Browse…** button to select a location using Windows Filer Explorer.
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 different login credentials, 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 complete, click on the **Finish** button.

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

SECURITY

This section details the various security options available to the VERIPATROL system.

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.
2. Click on the Windows **Start** button and select **Run**.
3. Type in *services.msc* and click on the **OK** button.
4. The services window is displayed (Figure 7).

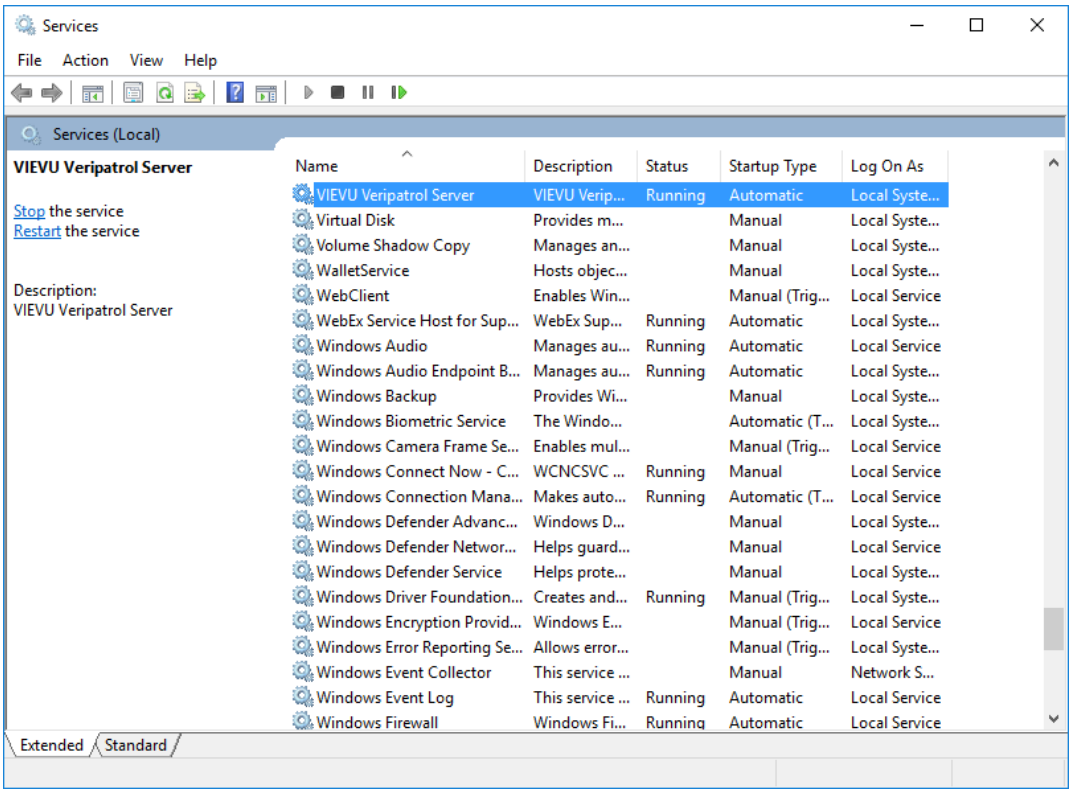

Figure 7

5. Double-click on **VIEVU VERIPATROL Server**.
6. Click on the **Log on** tab at the top.
7. Change **Log on as:** from **Local System account** to **This Account** (Figure 8).

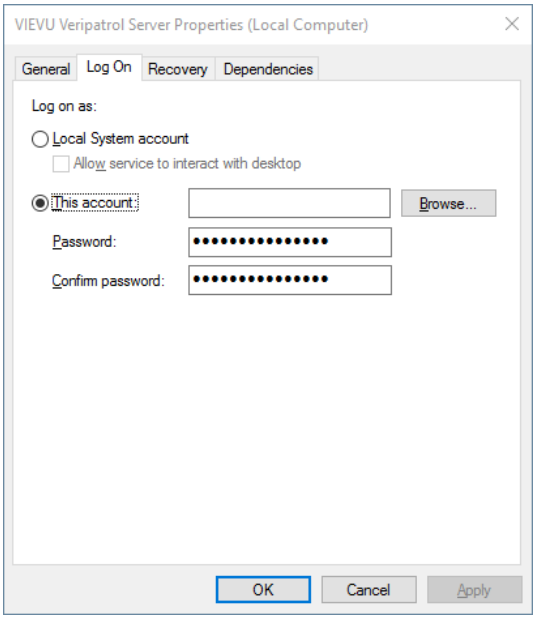

Figure 8

8. 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.
9. Click on the **OK** button.
10. 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: Permissions to the storage location can be restricted 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.

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.

Microsoft Azure
Microsoft

- 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/

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

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.