



# VIEVU VERIPATROL Network White Paper

Version 2.2.21

The VERIPATROL system supports the installation of the VERIPATROL software in a network server/client environment. The following document describes the VERIPATROL system, the communication methods used and the installation requirements and instructions.

## Table of Contents

Planning	
System Requirements.....	2
Software Architecture.....	2
Network Architecture.....	3
Data and Communication Processes.....	4
Determining File Storage Requirements.....	5
Data Transfer Rates/Time.....	5
Date/Time Automatic Updating.....	6
Installation/Usage	
Installation Instructions.....	7
Configuring a Video Storage Location.....	9
Set the Video Retention Period.....	10
Export Master Log with Video Copies.....	10
Optional Logging.....	10
Set a File Deletion Schedule.....	11
Silent Installation Switches.....	11
Set a Default Storage Location.....	11
Moving an Existing File Storage Location.....	12
Export/Import Database and Videos.....	12
Security	
User Security Matrix.....	13
VidLock™ Security Suite.....	14
Lockdown Video.....	14
Securing the System.....	15

## Contact Us

If you have any questions regarding a network installation or need assistance installing the VERIPATROL software system, please contact us at 888-285-4548 or [support@viewu.com](mailto:support@viewu.com).



---

## PLANNING

### System Requirements

#### Domain

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

#### Server

1. Operating System: Microsoft Server 2003 or 2008
2. Database Program: Microsoft SQL Server 2005 or 2008
3. Hardware requirements sufficient to install SQL Server. Please check with Microsoft for the current requirements for the version being installed.
4. Microsoft Visual C++ 2005
5. Firewall exception for TCP Port 43690 and UDP Port 123
6. SQL Server configured to allow remote connections with Named Pipes and TCP/IP enabled.

#### Workstations

1. Windows compatible computer with the following specifications:
  - a. Operating System: Windows XP, Vista or 7
  - b. Processor: Pentium III or compatible - 1 GHz
  - c. Memory (RAM): 512 MB
2. Windows Media Player 10 or higher
3. Display with 1024 x 768 resolution or higher
4. Microsoft Visual C++ 2005
5. 2 available USB ports

### Software Architecture

The VIEVU VERIPATROL software system consists of 4 components:

1. 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: Service runs on the server to communicate with the database and manage video files.
2. VERIPATROL Admin: Program used to administer the VERIPATROL system (add/remove users, copy videos, etc).
3. VERIPATROL Client: Program used to transfer video files from a camera.
4. Xvid Codec: MPEG-4 decompression codec required to view video recorded with all VIEVU cameras.

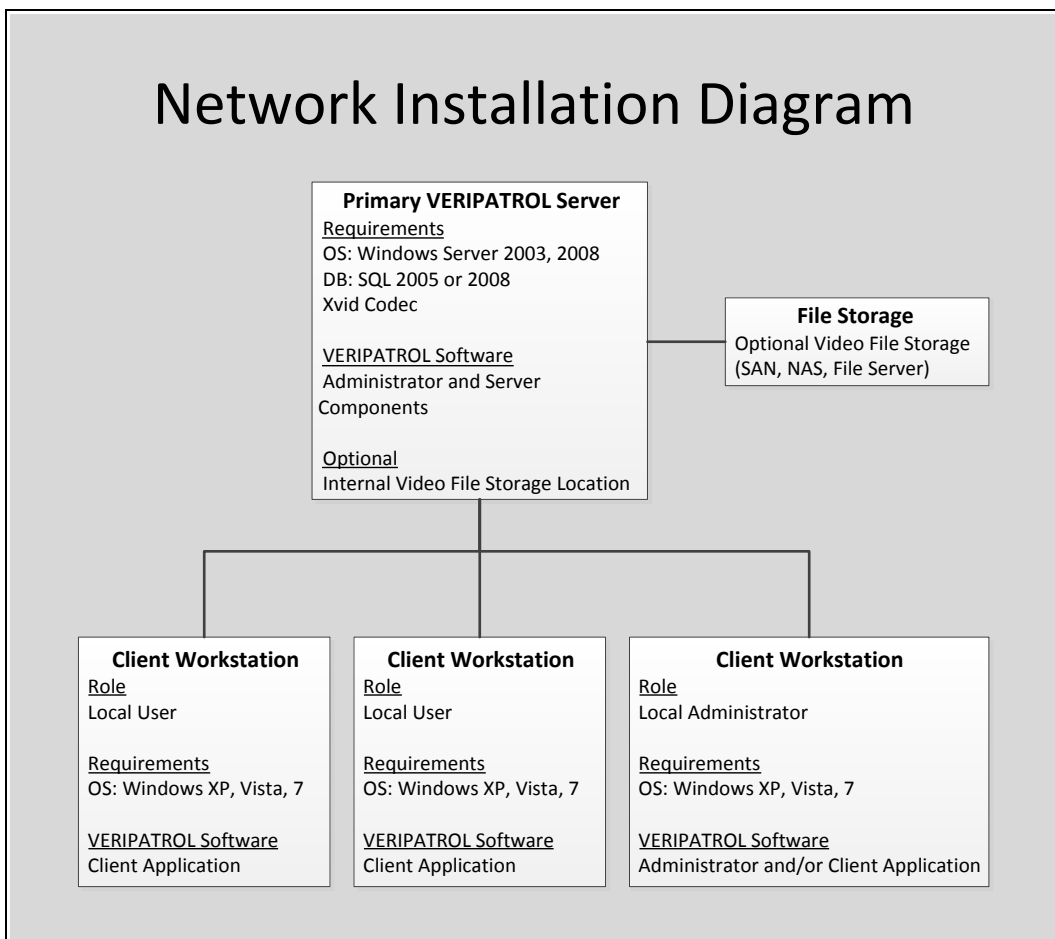


## Network Architecture

Each of the 4 components will be installed in the following locations:

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 video downloads will occur.
4. Xvid Codec: Codec must be installed on the server and all computers where video playback will occur.

Additionally, 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).



## Data and Communication Processes

The VERIPATROL system communicates using the following processes:

Camera to Client Workstation:

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

USB: Uni-Directional data transfer over Universal Serial Bus

Client Workstation to Server:

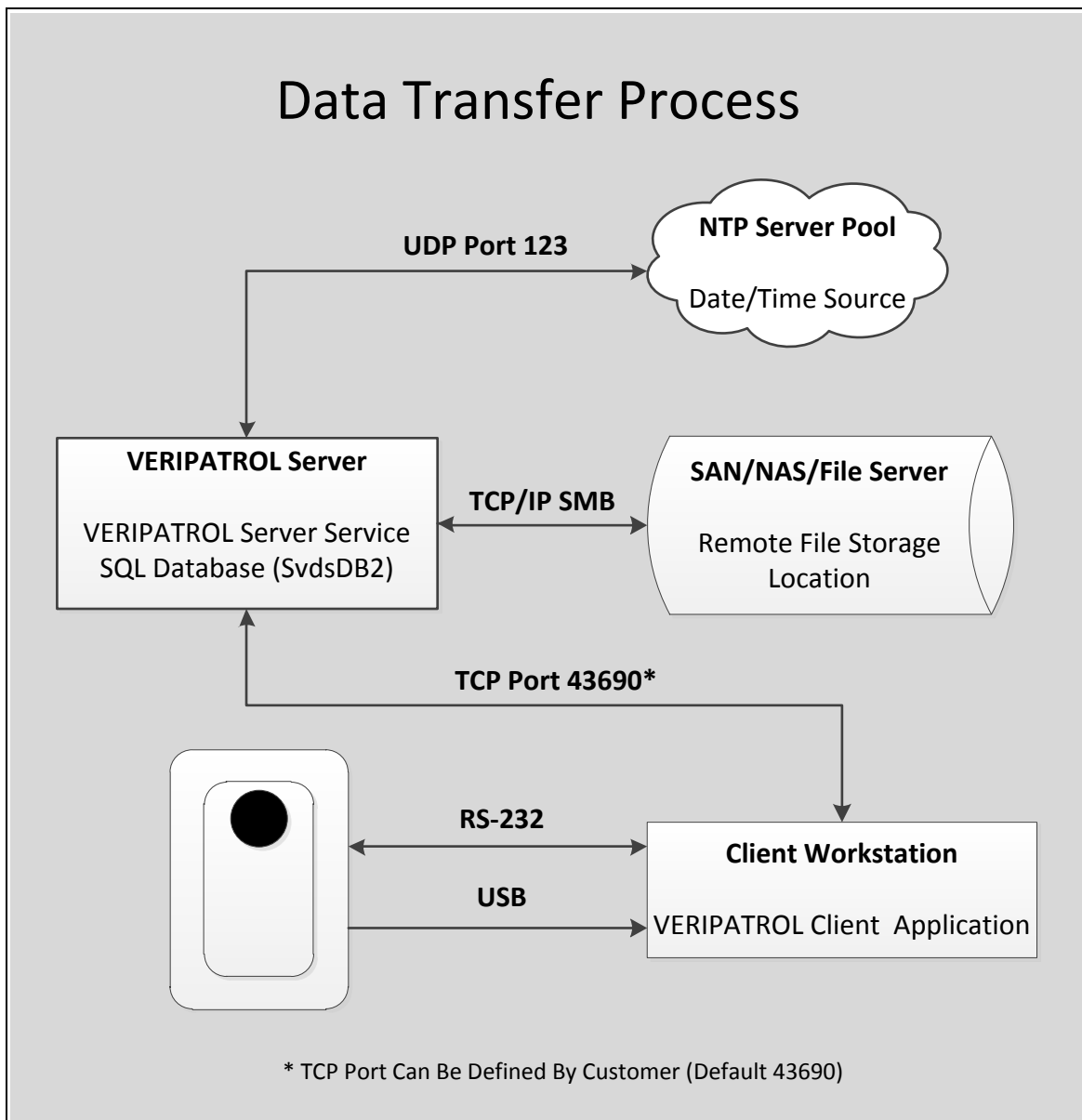
TCP Port: Bi-Directional data transfer over TCP port 43690\*

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 port 123





---

## Determining File Storage Requirements

The VIEVU LE series cameras record at a rate of approximately 1 gigabyte per hour. The exact file size will vary based on the subject of the recording due to compression variations. The file storage requirements will be determined based upon three factors:

- 1) The number of cameras
- 2) The average number of hours of video recorded each day
- 3) The retention period in days

These three factors can be combined in the following equation to determine the minimum storage capacity in gigabytes.

$$(\text{Number of Cameras}) \times (\text{Avg. Hrs Per Day}) \times (\text{Retention Period}) = (\text{Storage Size in GB})$$

$$10 \text{ cameras} \times 1 \text{ hr per day} \times 90 \text{ days} = 900 \text{ GB}$$

Alternatively, a storage calculator is located on our website to perform the calculation.  
<http://www.viewu.com/storagecalculator>

**NOTE: Video files that are marked to 'Never Be Deleted' will increase the storage requirements as they will not be deleted after expiration of the retention period.**

## Data Transfer Rates/Time

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

The typical transfer of 4GB of video files from a camera to a local storage hosted on the server will take approximately 22 minutes at 3 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.



---

## **Date/Time Automatic Updating**

All VIEVU LE series cameras have Date and Time settings in sync with Greenwich Mean Time (GMT). GMT may also be referred to as Coordinated Universal Time (UTC) or in the Military as “Zulu” time. The VERIPATROL server will use 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.

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 may 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.

The NTP server pool and proxy settings can be changed in the VERIPATROL Server Configuration application that is installed on the VERIPATROL server.



## INSTALLATION

**\*WARNING\*** - Before installing the server component on Windows Server 2008, you must enable the “desktop experience” feature on the server. Failure to do so will cause system instability and failure to generate thumbnails. <http://support.microsoft.com/kb/947036>

### Server Setup

1. Install a SQL instance named “VIEVU”
2. Configure the VIEVU SQL Instance to allow remote network connections using named pipes and TCP/IP
3. If a firewall product is used, add an exception for TCP port 43690 and UDP port 123
4. Download the Network Server Installation software from the “Support” tab of the VIEVU website
5. Install the VERIPATROL software
  - a) Extract the contents of the installation file
  - b) Open the VERIPATROL Software folder
  - c) Double click on “VERIPATROL Network Setup”
  - d) Click “Next” on the welcome screen
  - e) Accept the software license agreement after review
  - f) Select the installation folder and click “Next”
  - g) Place a check next to the following components: Server and Administrative Application. Click “Next”
  - h) Click “Next” to begin the installation
  - i) The installation complete window will appear. Place a check mark in “run Xvid Codec installation after finishing this wizard”. Click “Close”
  - j) The Xvid setup wizard will appear
    - i. Click “Next”
    - ii. Accept the license agreement after review and click “Next”
    - iii. Click “Next”
    - iv. Click “Next”
    - v. Click “Next”
    - vi. Add a check mark to “Decode all supported FourCCs” and click “Next”
    - vii. Click “Install”
    - viii. Click “Finish”
6. Configure the VERIPATROL server using the Server Configuration application
  - a) Launch the Server configuration application located in START>All Programs>VIEVU Veripatrol
  - b) Change the “MS SQL Instance” drop down box to “VIEVU”
  - c) Input the port “43690” to listen to. This is the port workstations will use to connect to the server.
  - d) Click the Date/Time button to input proxy server information for internet access.
  - e) Click “Apply”



- f) Click “Yes” to restart the VERIPATROL server services. The physical server will not be restarted
- g) If the configuration was successful a “Server is Restarted” message will appear. Click "Ok”
- h) Click “Quit”

## **Workstation Setup**

1. Install the VERIPATROL Software
  - a) Extract the contents of the installation file
  - b) Open the VERIPATROL Software folder
  - c) Double click on “VERIPATROL Network Setup”
  - d) Click “Next” on the welcome screen
  - e) Accept the software license agreement after review
  - f) Select the installation folder and click “Next”
  - g) Place a check next to the following components: Administrative Application and/or Client Application. Click “Next”
  - h) Click “Next” to begin the installation
  - i) The installation complete window will appear. Place a check mark in “run Xvid Codec installation after finishing this wizard”. Click “Close”
  - j) The Xvid setup wizard will appear.
    - i. Click “Next”
    - ii. Accept the license agreement after review and click “Next”
    - iii. Click “Next”
    - iv. Click “Next”
    - v. Click “Next”
    - vi. Add a check mark to “Decode all supported FourCCs” and click “Next”
    - vii. Click “Install”
    - viii. Click “Finish”
2. Configure the Admin application to connect to the server
  - a) Launch the Admin application
  - b) On the server connection window input the server address and port (43690). IP address or machine name are acceptable. Do not include any slashes in the address. Place a checkmark in “Update Computer Default Address/Port” to replicate the address/port change to all users of the computer.
  - c) Click “Connect”
3. Configure the Client application to connect to the server
  - a) Launch the Client application
  - b) On the server connection window input the server address and port (43690). IP address or machine name are acceptable. Do not include any slashes in the address. Place a checkmark in “Update Computer Default Address/Port” to replicate the address/port change to all users of the computer.
  - c) Click “Connect”



---

## Configuring a Video Storage Location

**NOTE: Video locations can only be set when accessing the Admin application from the server. The Server Setup tab is not available from the Admin application on a client workstation.**

The VERIPATROL software 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:

Server 2000 and 2003 - C:\Documents and Settings\All Users\Application Data\VieVU\VieVU VERIPATROL Server\FileStorage

Server 2008 - 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 storage location. This service is used by the VERIPATROL software to access the storage location.

From the Server:

1. Click "Start" and select "Run"
2. Type in "services.msc" and click "OK". The services window will appear
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.
6. Click "OK"
7. Stop and restart the service

Once the service has been changed and restarted, the storage location can be created.

From the Server login to the Admin application:

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. When complete click "OK". NOTE: If an error is received the network path is incorrect or permissions are not setup properly.

**NOTE: Creating a file storage location does not change any user storage mappings. Use the "Set Default Storage" process to change the file storage location for all users configured to use the default storage location or manually change the storage mapping by editing the user in the Admin software.**



---

## Set the Video Retention Period

The VERIPATROL system is pre-configured with the retention period turned off. If the retention period is activated, all video files that exceed the retention period will be removed unless the video is marked to 'never be deleted'. 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 or as long as 99999 days (273.9 years). The retention period is set in the VERIPATROL Admin application.

### From the Server login to the Admin application

1. On the Server Setup tab click the "Retention Period" button.
2. Change the "By Default Store Files For:" to the new value (1-99999)
3. Click "Ok"
4. Click "Yes" to restart the Server processes (the physical server will not restart)
5. Once the server is restarted click "Ok"

**NOTE: Caution should be used whenever the retention policy is modified as any videos that are removed cannot be recovered with the software.**

## Export Master Log with Video Copies

**NOTE: Export Master Log with Video Copies can only be set when accessing the Admin application from the server. The Settings button on the Master Log tab is not available from the Admin application on a client workstation.**

When enabled, this feature will create 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 record will provide a chain of custody record of the time the video was download, when the copy was made and any additional logging events that may have occurred while the video was stored in the system. This feature is enabled by default.

## Optional Logging

**NOTE: Optional Logging can only be set when accessing the Admin application from the server. The Settings button on the Master Log tab is not available from the Admin application on a client workstation.**

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

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



---

## Set a File Deletion Schedule

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

### From the Server login to the Admin application

1. On the Server Setup tab click the "Cleanup Schedule" button
2. Input the desired time the deletion process should begin.
3. Set the deletion interval. The interval is the number of days to wait between deletion cycles.
4. Click Apply

**NOTE: The "Force Cleanup" button on the Cleanup Schedule window will manually start the deletion process.**

Alternatively, the deletion process can be triggered from an external program such as 'Scheduled Tasks'. Running the SvdsServer executable, located in C:\Program Files\VieVU VERIPATROL\bin, with the /forcecleanup switch will begin the deletion process.

## Silent Installation Switches

An installation MSI file (VieVu VERIPATROL.msi) has been included in the MSI folder in network installation media that supports the use of silent installation switches. The switches are as follows: "/q ADDLOCAL=D,S,A,C" where S = Server component, A = Admin component and C = Client Component.

Example:

"VieVU Veripatrol.msi" /q ADDLOCAL=D,S,A	This will install Admin and Server components
"VieVU Veripatrol.msi" /q ADDLOCAL=D,C	This will install Client component
"VieVU Veripatrol.msi" /q ADDLOCAL=D,A,C	This will install Admin and Client components

## Set a Default Storage Location

To allow for the easy management of the video storage locations, a default storage can be set. Any users who are configured to use the default storage location will be automatically updated when the default storage is changed.

From the Server login to the Admin application

1. On the Server Setup tab highlight the storage to be set as the default.
2. Click the "Set Default Storage" button.
3. (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. This is most helpful when migrating to a new storage system, or if videos were accidentally uploaded to the incorrect location.

**\*WARNING\* - 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 corrupt during the transfer. A backup prior to the transfer is always recommended.**

From the Server login to the Admin application

1. On the Server Setup tab highlight the storage to be set as the default.
2. Click the "Set Default Storage" button.
3. (Default Storage) will now be listed to the left of the storage path.

**NOTE: The new storage location needs to be added to the system before files can be moved.**

## Export/Import Database 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 databases an easy process. The export process will make copies of all videos in the export location. You must have enough free space in the export location to contain all of the video files currently in the system. The Export/Import process should be done with the same version. Ensure both the source and target systems are using the same version of VERIPATROL to prevent any errors during import.

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" and choose "Next".
4. Select an export location and choose "Next".
5. The export process will now begin. Once finished, click "Finish".

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 will begin. Users will be matched based on the login ID. If a user does not currently exist in the database, you will be 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 will remember the selection and apply the same selection to any future users.
6. Once finished, click "Finish".



# SECURITY

## User Security Matrix

VERIPATROL allows for the customization of user access security/permission. 4 security check boxes create 5 separate security levels plus lockdown video access. Use the security selection matrix below to determine the correct security level for each user. All user security changes are made on the Officer's tab in the Admin application.

### Security Selection Matrix

Admin Application	Administrator	Nothing Checked	Make Copies in Client	View All Videos in Client	Make Copies in Client and View all Videos in Client
Login 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				
<b>Client Application</b>					
Login 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
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
Make a Copy of a Video Recorded by Me	X		X		X
Make a Copy of a Video Recorded by Others	X				X
* Additional Security Prevents All Administrators from Making These Changes					
'View Lockdown Video' security adds additional security to any user. Once a video has been locked down, only users with Lockdown video security can view, make changes or copies of the video. The security works with the limits of their existing security group.					



---

## **VidLock™ Security Suite**

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

- All LE series cameras are secured to prevent unauthorized access to the content of the camera.
- VERIPATROL pairs a camera with an installation of the software through the assign camera 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.
- Access to the video file storage location is secured using windows NTFS file security.
- 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.
- All video files recorded on the PVR-LE2 cameras are marked with a 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).
- All video files recorded on the LE series cameras are time stamped with date and time in GMT. The date and time stamp cannot be changed to local time.

## **Lockdown Video**

A 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 view 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.



---

## Securing the System

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

To secure the system, first change the "VIEVU VERIPATROL Server" service to a domain account.

### From the Server:

1. Click "Start" and select "Run"
2. Type in "services.msc" and click "OK". The services window will appear
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

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

SQL Database: Permissions to the database "SvdsDB2" can be restricted so that the only domain account that has access to the database and tables is the account that was setup above. If assistance is needed on best practices for securing SQL please see the following Microsoft document: [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 that has access to the location is the account the "VIEVU VERIPATROL Server" Service was setup to log on with above. Please see the following Microsoft document: [Securing Files with NTFS](#)



[www.VIEVU.com](http://www.VIEVU.com)