Video Data Security in Ocularis

White Paper

Document Identification	
Product Name:	Ocularis
Issue Date:	October 2021

PROPRIETARY AND CONFIDENTIAL INFORMATION

All information contained herein is confidential, proprietary and the exclusive property of Qognify Ltd and its affiliates ("Qognify"). This document and any parts thereof must not be reproduced, copied, disclosed or distributed without Qognify's written approval and any content or information hereof shall not be used for any unauthorized purpose. The software described herein and any other feature or tools are provided "AS IS" and without any warranty or guarantee of any kind.

Contents

1 Introduction

In applications where video plays a critical role as evidence, it is paramount to securely transmit, store, and export the video data. Qognify's Ocularis video management system provides a series of security mechanisms that enable users to maintain complete end-to-end security and integrity of video data.

This document provides a general overview of how video is transmitted from the camera and stored securely in the Ocularis Recording Server databases and how exported recordings are secured in the Ocularis Client and Viewer when used as evidence.

1.1 Audience

The primary audience for this white paper is surveillance system architects/designers and surveillance project consultants, security officers, companies, organizations, and law enforcement bodies with surveillance projects/installations where video and evidence handling is critical.

This white paper should enable the reader to understand how recordings are secured from transmission from the camera to viewing exported recordings as evidence and how to implement and use the comprehensive security in the most optimal way.

The reader is assumed to have a general understanding of Ocularis and IP video management solutions in general.

1.2 About Qognify

Qognify helps safeguard your world. Providing solutions that mitigate risks, increase security, and optimize operations, Qognify serves thousands of customers worldwide, who place a premium on their physical security. Qognify's comprehensive portfolio contains video management software and enterprise incident management solutions that optimize outcomes in vertical sectors, including manufacturing, transportation, retail, education, finance, logistics, corrections, critical infrastructures, and city, state & federal government.

In 2018, Qognify acquired OnSSI Group with its brands OnSSI and SeeTec, forming a leading global player in the physical security market.

Qognify is headquartered in Pearl River, New York, and operates major development hubs in Germany, Israel, and the United States, and sales and support offices around the globe.

Qognify Inc., Pearl River, NY (845) 201-5600

Info@qognify.com

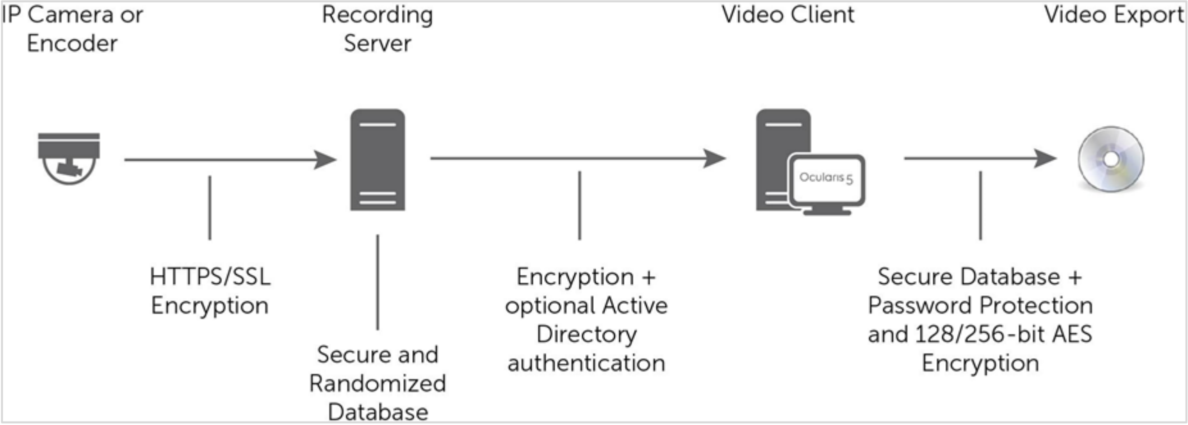
www.qognify.com

2 Video Data Flow

In a digital video surveillance system, the typical flow of data contains these steps:

1. The camera captures video
2. Video data is streamed over the network to the Recording Server
3. The Recording Server stores video data
4. Live and recorded video is streamed to the video client
5. The client exports recorded video

Figure 1: Video data flow


IP Camera or Encoder
Recording Server
Video Client
Video Export
Ocularis 5
HTTPS/SSL Encryption
Secure and Randomized Database
Encryption + optional Active Directory authentication
Secure Database + Password Protection and 128/256-bit AES Encryption

Ocularis employs several methods to ensure the integrity of video data in each of these steps.

3 Video Captured by the Camera

Risk: Cameras may be disconnected, stolen, or simply fail.

Ocularis will automatically detect if the camera is not responding or stops streaming video to the system. Once the system detects this, it triggers a "communication error" event that can trigger alarms or rules notifying system administrators and operators via email, SNMP monitoring, and on-screen alerts.

Users should also be aware that video recorded on the camera's SD card for Edge Recording support (as described in section 3) may be vulnerable if the camera is stolen.

If a camera fails or becomes disconnected, any historical video data already stored on the Recording Server may be played back. It is not necessary to replace the camera first to playback video.

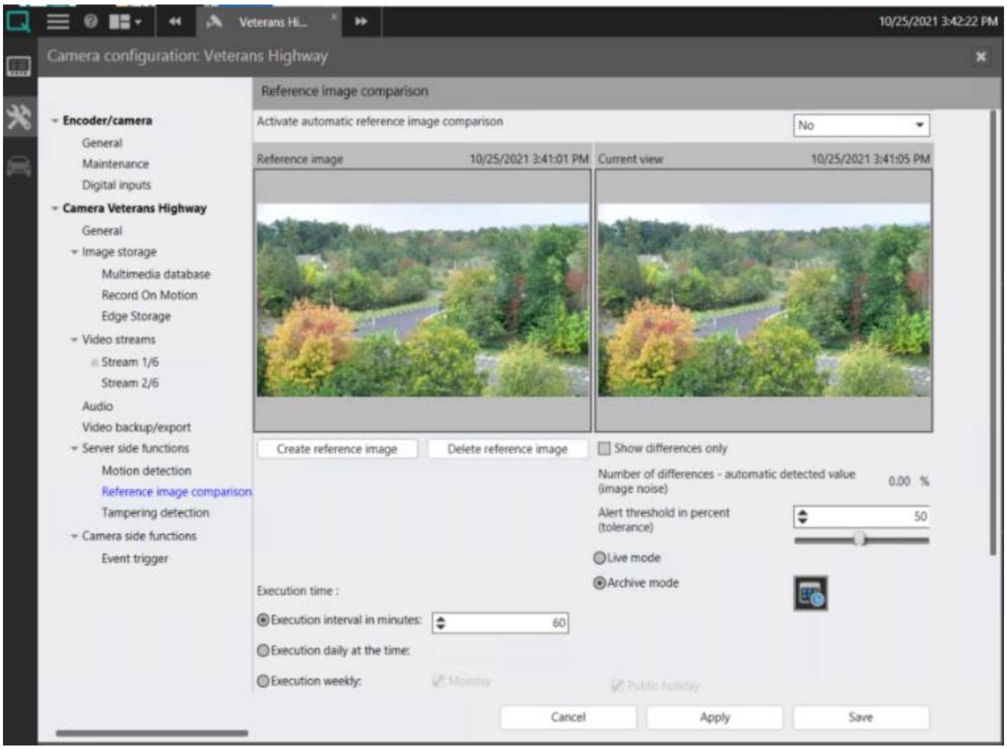
Risk: Cameras may be tampered with by turning it or by covering the lens.

Ocularis includes server-based tampering detection. Many cameras also include tampering events of different kinds, such as tampering, video loss, and temperature. The Ocularis system can receive these events and use them to trigger alarms or rules notifying operators and system administrators of the issue.

Risk: Cameras can become unfocused, move over time, or become obscured by dirt or other obstructions.

Ocularis includes a scene change detection which compares a reference image to the current view. This feature can detect changes in the scene such as obstructions, a camera's slow movement (such as occurs if the mount is not tightened correctly), or accumulation of dirt and debris that may not be noticeable to operators over time. This scene change detection ensures proper recording of video evidence by cameras that may not be frequently monitored.

Figure 2:Scene change detection in the Ocularis Recorder.



Reference image comparison

Activate automatic reference image comparison: No

Reference image 10/25/2021 3:41:01 PM

Current view 10/25/2021 3:41:05 PM

□ Show differences only

Number of differences - automatic detected value (image noise): 0.00 %

Alert threshold in percent (tolerance): 50

○ Live mode

● Archive mode

Execution time :

● Execution interval in minutes: 60

○ Execution daily at the time:

○ Execution weekly: ☑ Monday ☑ Public holiday

4 Video is streamed over the network to the Recording Server

Risk: The network may be compromised, giving unauthorized persons access to tapping into the transmitted video or accessing the cameras directly.

To protect against potential hacking of passwords and commands communicated between the cameras and the Recording Server, Ocularis supports modern TLS 1.2 encryption protocols with cameras and encoders that support this feature. (For devices that do not support TLS 1.2, SSL 3.0 may be used but is not recommended as SSL 3.0 is no longer secure.)

In addition to encrypting the video stream from the camera, the Ocularis architecture allows users to place cameras on a completely separate subnet from client workstations. This prevents direct access to the cameras from the public network, further enhancing the system security.

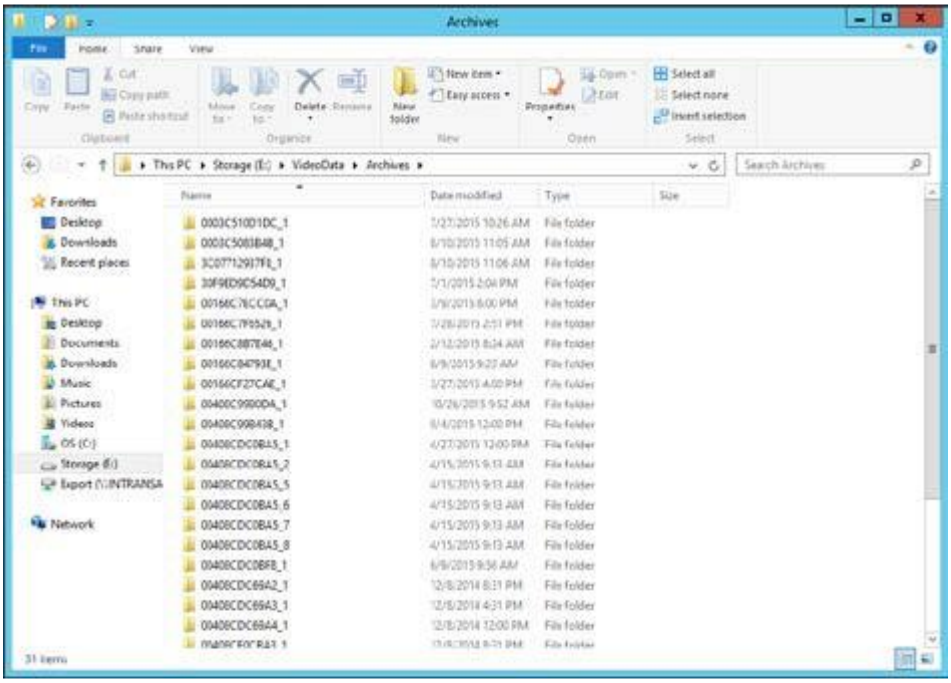
5 Video stored in the Recording Server database

Risk: Video recordings stored on the server may be tampered with

Ocularis does not provide any tools or options for the system's client operators to access or manipulate the content or the authenticity of the recorded video. However, to prevent video tampering and provide for detection of such actions by persons that may have access rights to the actual recording server, Ocularis employs the following prevention and detection methods:

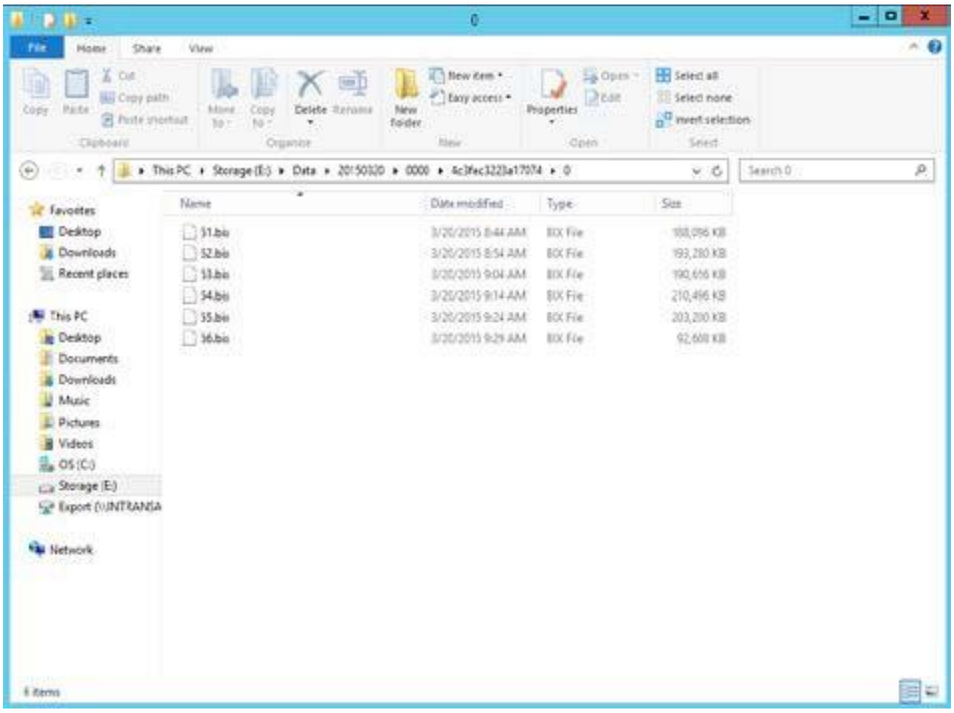
- Ocularis utilizes a proprietary video database specifically designed to increase video recording speed and performance over standard databases and, more importantly, handle video security and authentication.
- Video data stored in the database can be read-only by the Ocularis Recording Server software.
- Video data from all cameras and encoders is randomized in the database so that a person with access to the server will not be able to identify and possibly delete specific sequences for specific cameras.

Figure 3:Data stored in a typical VMS – organized by the MAC address of the camera allowing unauthorized persons to identify specific camera sequences



Name	Date modified	Type	Size
0003C510D1DC_1	7/27/2015 10:26 AM	File folder	
0003C5083B48_1	8/10/2015 11:05 AM	File folder	
3C07712937FE_1	8/10/2015 11:06 AM	File folder	
30F9ED9C54D9_1	7/1/2015 2:04 PM	File folder	
00166C7ECCDA_1	3/9/2015 6:00 PM	File folder	
00166C7F6528_1	7/28/2015 2:51 PM	File folder	
00166C887E46_1	2/12/2015 8:24 AM	File folder	
00166C84793E_1	6/9/2015 9:27 AM	File folder	
00166CF27CAE_1	3/27/2015 4:00 PM	File folder	
00400C9900DA_1	10/26/2015 9:52 AM	File folder	
00408C998438_1	8/4/2015 12:00 PM	File folder	
00408CDC0BA5_1	4/27/2015 12:00 PM	File folder	
00408CDC0BA5_2	4/15/2015 9:13 AM	File folder	
00408CDC0BA5_5	4/15/2015 9:13 AM	File folder	
00408CDC0BA5_6	4/15/2015 9:13 AM	File folder	
00408CDC0BA5_7	4/15/2015 9:13 AM	File folder	
00408CDC0BA5_8	4/15/2015 9:13 AM	File folder	
00408CDC0BFB_1	6/8/2015 9:56 AM	File folder	
00408CDC69A2_1	12/8/2014 8:31 PM	File folder	
00408CDC69A3_1	12/8/2014 4:31 PM	File folder	
00408CDC69A4_1	12/8/2014 12:00 PM	File folder	
00408CF0CBA3_1	12/8/2014 8:21 PM	File folder	

Figure 4: Randomized data stored in Ocularis with no identifying camera information



This PC ▸ Storage (E:) ▸ Data ▸ 20150320 ▸ 0000 ▸ 4c3fec3223a17074 ▸ 0

Name	Date modified	Type	Size
51.bix	3/20/2015 8:44 AM	BIX File	188,096 KB
52.bix	3/20/2015 8:54 AM	BIX File	193,280 KB
53.bix	3/20/2015 9:04 AM	BIX File	190,656 KB
54.bix	3/20/2015 9:14 AM	BIX File	210,496 KB
55.bix	3/20/2015 9:24 AM	BIX File	203,200 KB
56.bix	3/20/2015 9:29 AM	BIX File	92,608 KB

6 items

Risk: The Recording Server may be turned off or fail

Ocularis Enterprise and Ultimate versions support Recording Server failover, which is a process in which the camera streams are redirected to an alternate Recording Server if the primary Recording Server is unavailable. If the primary Recording Server stops responding due to failure or being turned off, for example, for maintenance, the Failover Recording Server takes over the recording task.

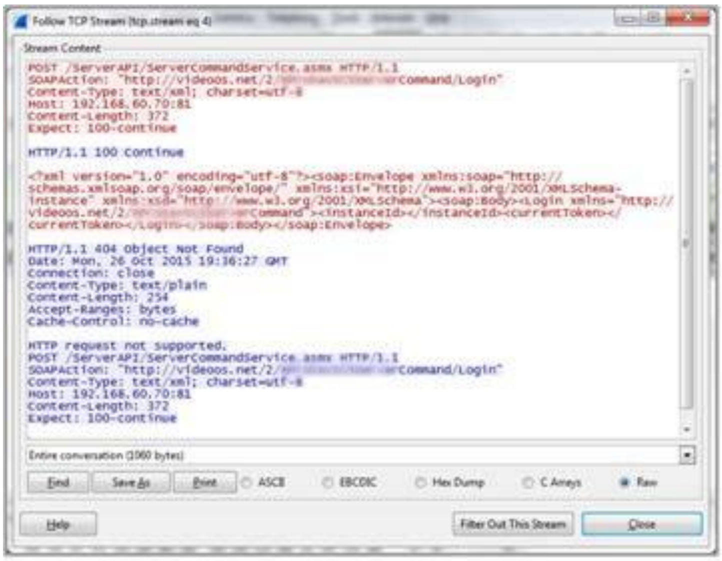
In addition to Recording Server Failover, Ocularis Ultimate also supports Edge Storage on select devices. Edge Storage offers the function to record video in the camera itself and let the Recording Server retrieve these recordings after a network failure, effectively ensuring video recording even for periods with no connection to the camera.

6 Live or recorded video is sent over a network to a client

Risk: The network may be compromised, giving unauthorized persons access to communication between the Recording Server and the Client.

In Ocularis, all communication between clients and the Recording Server is secured using 128-bit AES encryption. Ocularis also utilizes a proprietary video streaming protocol that cannot be accessed using commonly available media players. Only the Ocularis Client can decode the video stream from the server.

Figure 5: Typical unencrypted communication between VMS Recorder and Client (Data captured using the free Wireshark packet analyzer application)

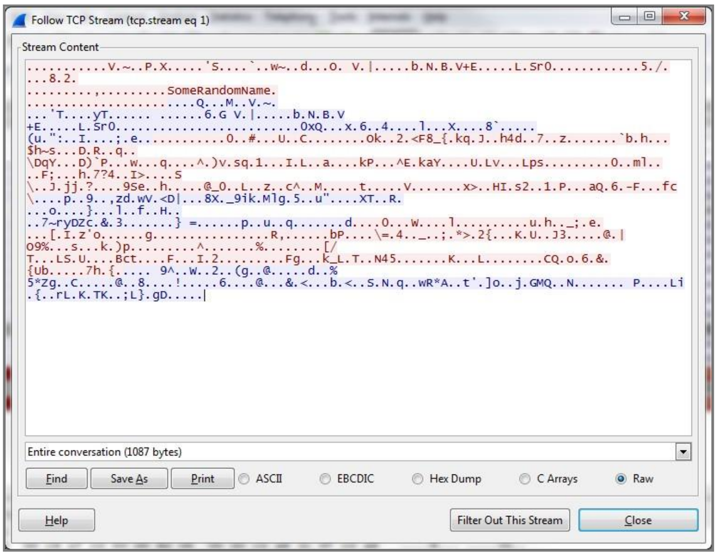


```
POST /ServerAPI/ServerCommandService.asmx HTTP/1.1
SOAPAction: "http://videoos.net/2/[redacted]Command/Login"
Content-Type: text/xml; charset=utf-8
Host: 192.168.60.70:81
Content-Length: 372
Expect: 100-continue

HTTP/1.1 100 Continue

<?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:soap="http://
schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"><soap:Body><Login xmlns="http://
videoos.net/2/[redacted]Command"><InstanceId></InstanceId><currentToken></
currentToken></Login></soap:Body></soap:Envelope>

HTTP/1.1 404 Object Not Found
Date: Mon, 26 Oct 2015 19:36:27 GMT
Connection: close
Content-Type: text/plain
Content-Length: 254
Accept-Ranges: bytes
Cache-Control: no-cache

HTTP request not supported.
POST /ServerAPI/ServerCommandService.asmx HTTP/1.1
SOAPAction: "http://videoos.net/2/[redacted]Command/Login"
Content-Type: text/xml; charset=utf-8
Host: 192.168.60.70:81
Content-Length: 372
Expect: 100-continue
```

Entire conversation (1060 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

Figure 6:Encrypted communication between Ocularis Recorder and Ocularis Client (Data captured using the free Wireshark packet analyzer application)



```
...........V.~..P.X.....'S....`..w~..d...O. V.|.....b.N.B.V+E.....L.SrO............5./.
...8.2.
.........,.........SomeRandomName.
.......................Q...M..V.~.
...'T....yT...... ......6.G V.|.....b.N.B.V
+E.....L.SrO.........................OxQ...x.6..4....l...X....8`.....
(u.":..I....;.e...........O..#...U..C........Ok..2.<F8_{.kq.J..h4d..7..z.......`b.h...
$h~s...D.R..q..
\DqY...D)`P...w...q....^.)v.sq.1...I.L..a....kP...^E.kaY....U.Lv...Lps.........O..ml..
..F;...h.7?4..I>....S
\..J.jj.?....9Se..h.....@_O..L..z..c^..M.....t.....V.......x>..HI.s2..1.P...aQ.6.-F...fc
\....p..9..,zd.wV.<D|...8X._9ik.Mlg.5..u"....XT..R.
...o....}...l..f..H..
..7~ryDZc.&.3.......} =......p..u..q.......d....O...W....l..........u.h.._;.e.
...[.I.z'o......g................R,......bP....\=.4.._..;.*>.2{...K.U..J3.....@.|
O9%...s...k.)p.........^.......%........[/
T...LS.U....Bct....F...I.2.........Fg...k_L.T..N45.......K...L........CQ.o.6.&.
{Ub.....7h.{..... 9^..W..2..(g..@.....d..%
5*Zg..C.....@..8....!.....6....@...&.<...b.<..S.N.q..wR*A..t'.]o..j.GMQ..N....... P....Li
.{..rL.K.TK..;L}.gD.....
```

Entire conversation (1087 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

7 Live or recorded video viewed by unauthorized persons

Risk: The video surveillance system may be hacked by unauthorized persons to obtain login credentials to view and export live or recorded video

Video streamed from the recording server – both live and recorded – is only viewable by the Ocularis Clients (including web and mobile). Ocularis offers centrally controlled security settings that set when and which cameras can be viewed live, played back, and exported by the user. Permissions can be set at a group level and also for each user. Ocularis logs all client operators' actions with color-coded query results for easy identification of system usage.

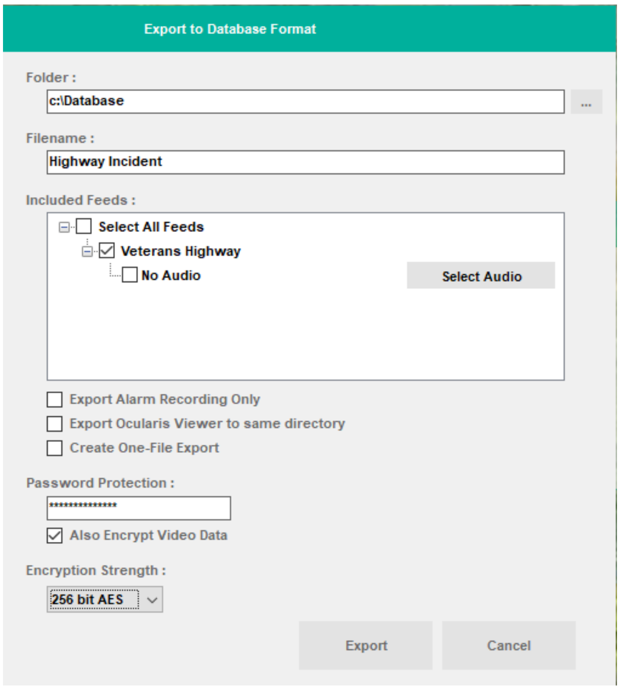
To secure client access to the system, Qognify recommends using secure Windows Active Directory® (AD) for authentication. When using Active Directory for authentication, Qognify recommends that all users have separate accounts. This will make it easier to investigate who logged in, viewed live or recorded video, or exported video from the system in the Ocularis audit log.

Additionally, multiple administrator-level accounts may be configured within Ocularis so that individual administrator-level users can track changes made to the system. As with user-level accounts, administrator-level accounts may also use Active Directory for authentication.

Risk: The exported video may be viewed and copied by unauthorized persons.

Ocularis Client supports password protection and database encryption using 128 or 256 bit AES encryption on the exported video database to prevent unauthorized persons from viewing or copying the exported video.

Figure 7: Password protection and encryption options when exporting video from Ocularis Client



Export to Database Format

Folder : c:\Database

Filename : Highway Incident

Included Feeds :
- ☐ Select All Feeds
  - ☑ Veterans Highway
    - ☐ No Audio

☐ Export Alarm Recording Only
☐ Export Ocularis Viewer to same directory
☐ Create One-File Export

Password Protection : **************

☑ Also Encrypt Video Data

Encryption Strength : 256 bit AES

Risk: The exported video may be tampered with, removing critical sequences of the recorded video or be modified to give another impression of the recorded evidence

Video exported in the proprietary Ocularis database format utilizes many of the same prevention and detection methods to prevent tampering and alteration as are employed on the Ocularis Recording Server:

- A proprietary video database specifically designed to handle video security and authentication
- Video data can only be viewed using the Ocularis Client or stand-alone Ocularis Viewer

8 Recorded video or video exports might be shared with unauthorized users

Risk: A big concern of many customers is that sensitive videos will get leaked to social media or shared with unauthorized parties.

Administrators of Ocularis can enable **Video Protection Mode** per camera and per user to minimize the risks. When **Video Protection Mode** is enabled, anytime Ocularis Client is playing back recorded video, the user sees a randomly floating text overlay on the video showing the name of the user accessing the recorded video. As the text randomly moves over the video pane, it is not easy to record the video using a smartphone or other recording software without showing the user's name that is wrongfully sharing the video. The same approach is used for exports and bookmarks created inside Ocularis Client.

9 Benefits and summary

Combining proper network and IT security policies and procedures, Ocularis enables users to deploy video surveillance solutions with full end-to-end security. With the new encryption and signing features in Ocularis and Ocularis Client, it is possible to keep streamed and recorded video secure and prove its integrity all the way from the original stream from the camera to the point it is exported and then viewed.