milestone

The Open Platform Company

White paper

Ensuring end-to-end protection of video integrity

Prepared by:

John Rasmussen, Senior Technical Product Manager, Corporate Business Unit, Milestone Systems

Date: May 22, 2015

Table of Contents

Introduction

In applications and installations where video plays a critical role as evidence material, it is paramount that the video is transmitted, stored and in general handled in a secure way; from the time it is captured by the camera to the time it is used as evidence, for example in a court of law.

Milestone XProtect® Corporate and XProtect® Smart Client provide a series of security mechanisms that enable users to maintain full end-to-end security and integrity of recorded video data. Video database encryption, digital signing of video databases and a function to prevent re-export of the exported material are core components of Milestone's video management solution for ensuring and protecting the integrity of the video evidence.

Purpose and target audience

The purpose of this white paper is to give a general overview of how video is transmitted from the camera and stored securely in the XProtect® Corporate Recording Server databases, as well as how exported recordings are secured and validated in the XProtect® Smart Client – Player when used as evidence.

The primary audience for this white paper is individuals or organizations with surveillance projects/installations where video and evidence handling is critical. The target group might include (but is not limited to) the following audiences:

- surveillance system architects/designers and
- surveillance project consultants
- security officers
- companies
- organizations and
- law enforcement bodies

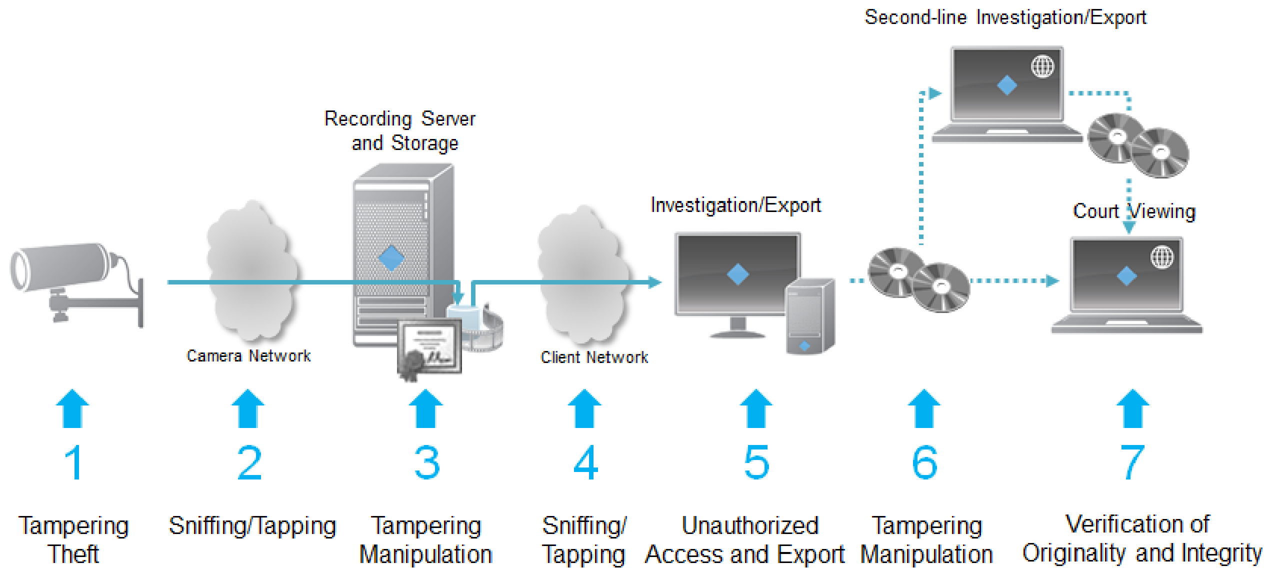
This white paper should enable the reader to understand how recordings are secured from transmission from the camera to viewing exported recordings as evidence, as well as how to implement and use the extended security in the most optimal way.

The reader is assumed to have a general understanding of Milestone XProtect® Corporate and IP video management solutions in general.

Video flow and inherent security risks

In any video surveillance system, analog or digital, there is an inherent security risk in the different parts, components or data/video transportation media used. These elements of the system may be tampered with or the security of them can be compromised.

In digital video surveillance systems, the video flow is typically as illustrated below.



Each function and component has its own inherent risks, examples of which are listed here:

1. Video is captured by a camera
    - *Camera may be disconnected, stolen or simply vandalized*
    - *Camera may be tampered with by turning it or by covering the lens*
2. Video is streamed over the network to a Recording Server
    - *The network may be disconnected or flooded with unwanted data due to a distributed denial-of-service (DDOS) attack*
    - *The network may be compromised giving unauthorized persons access to tapping into the transmitted video*
3. The Recording Server stores the video in its video database
    - *The Recording Server may be turned off or fail*
    - *Microsoft® Windows® security could be compromised giving local or remote access to the video database files*
4. Live or recorded video is sent over a network to a client

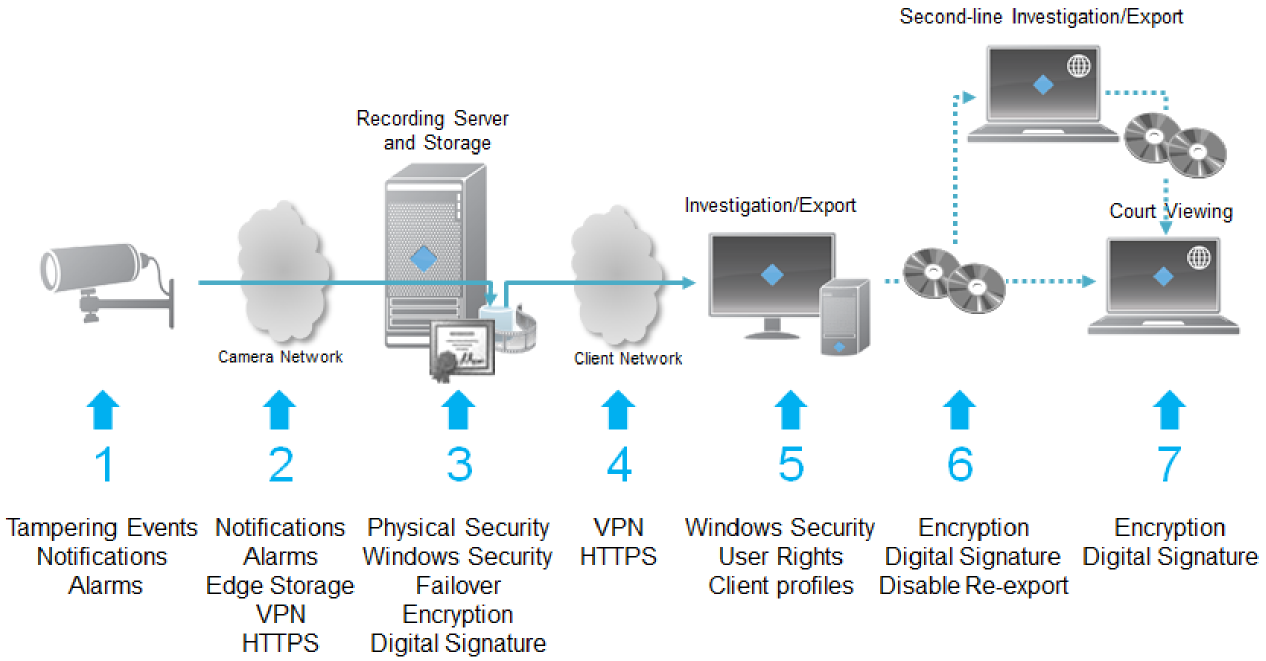
   - *The network may be disconnected or flooded with unwanted data due to a DDOS attack*
   - *The network may be compromised giving unauthorized persons access to tapping into the transmitted video*

5. The client decodes the video and displays it on the monitor and offers a function to export video recordings for evidence
   - *Unauthorized persons may try to hack or otherwise obtain login credentials to gain unauthorized access to viewing and exporting video*
   - *Authenticated surveillance users may try to tamper with exported material*
6. Exported evidence media is transported from the surveillance site to police or a court
   - *The exported video may be viewed and copied by unauthorized persons*
   - *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*
7. The exported evidence is viewed by police or a judge in court
   - *The exported video may have been tampered with removing critical sequences of the recorded video or be modified to give another impression of the recorded evidence*

Addressing security concerns and risks

As highlighted in the previous section, there are several places where security can be breached. To address these security concerns and inherent risks, Milestone has implemented several security functions in addition to the standard security measures that can be used to increase the security of the overall video system and its recordings.

The below illustration shows the possible security measures to counter tampering and fraud in each of the video flow steps.



1. Video captured by camera

Risk: *Camera may be disconnected, stolen or simply vandalized*

Milestone XProtect® Corporate will automatically detect if the camera is not responding or stops streaming video to the system. Once the system detects this it issues a "communication error" event, which triggers alarms or rules that notifies the right people of the issue.

Risk: *Camera may be tampered with by turning it or by covering the lens*

Many cameras can detect tampering events of different kinds, such as tampering, video loss, and temperature. These events can be received by the XProtect® Corporate system that triggers alarms or rules, which notifies the right people of the issue.

2. Video streamed to the Recording Server

Risk: *The network may be disconnected or flooded with unwanted data due to a DDOS attack*

Milestone XProtect® Corporate will automatically detect if the camera is not responding or stops streaming video to the system. Once the system detects this it issues a "communication error" event, which triggers alarms or rules that notifies the right people of the issue.

In addition to creating alarms or notifications via emails, XProtect® Corporate 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.

For more information on Edge Storage support in XProtect® Corporate: http://www.milestonesys.com/SharePoint/White%20papers/Milestone_Edge_Storage_with_flexible_retrieval.pdf

Risk: *The network may be compromised giving unauthorized persons access to tapping into the transmitted video*

Two methods can be used to protect the transmitted video: VPN tunneling and HTTPS.

A virtual private network (VPN) tunnel can be set up between the camera and Recording Server using standard equipment or software. The VPN will encrypt all data transmitted through the tunnel and thus protect against unauthorized access to the video. Using a VPN is a generic solution that can be used with any camera.

In addition to a VPN, XProtect® Corporate also supports HTTP Secure (HTTPS) for a subset of cameras. HTTPS uses Secure Socket Layer (SSL) and offers encrypted communication directly with the camera without a VPN tunnel.

For more information about VPN, HTTPS and SSL:

http://en.wikipedia.org/wiki/Virtual_private_network

http://en.wikipedia.org/wiki/HTTP_Secure

http://en.wikipedia.org/wiki/Transport_Layer_Security

3. Video stored in the Recording Server database

Risk: *The Recording Server may be turned off or fail*

XProtect® Corporate supports Recording Server failover, which is a function where one or more dedicated Failover Recording Servers monitor the state of the primary Recording Servers. If the primary Recording Servers stop responding, due to failure or being turned off, for example for maintenance, the Failover Recording Servers take over the task of recording the video.

In addition to the failover support, Edge Storage can also help because, as described in the previous section, it can record video in the camera, allowing the Recording Server to retrieve the video once it is up and running again.

Risk: *Windows (the operating system) security could be compromised giving local or remote access to the video database files*

To prevent unauthorized access to the video database files several layers of security can be implemented:

- Physical security
    - Access to the room with the physical Recording Server should be limited to a few authorized people only
- Windows Server security
    - Local console and remote desktop access to the server running the Recording Server should be limited to a few authorized people
    - Windows should be set to automatically logout after a short time of inactivity
    - Windows should be kept updated with the newest service releases
- Recording Server database
    - The database can be configured to encrypt the recordings in two modes: “Light” and “Strong”
    - The database can be set to sign the recordings digitally to prevent tampering

Both of the database encryption modes “Light” and “Strong” are secure and use the same DES-56 encryption technology. The difference is how much of the recordings are encrypted.

- “Strong” encrypts all parts of the video data stored in the database but requires more processing power to do so because everything needs to be encrypted
- “Light” only encrypts the first part of the JPEG or MPEG-4/H.264 video data called the header, and because of this, it uses less processing power to encrypt the video. The video will still be secure if someone tries to hack the database

because the video cannot be decoded without the information contained in the encrypted header

The digital signature is created by calculating a Message-Digest 5 (MD5) algorithm hash of the recordings. The hash is then signed with a Digital Signature Algorithm (DSA) and stored with the recordings. If the content later on is changed or parts of the recordings are removed, the MD5 hash and signature will no longer match, making it possible to detect that the recordings have been tampered with.

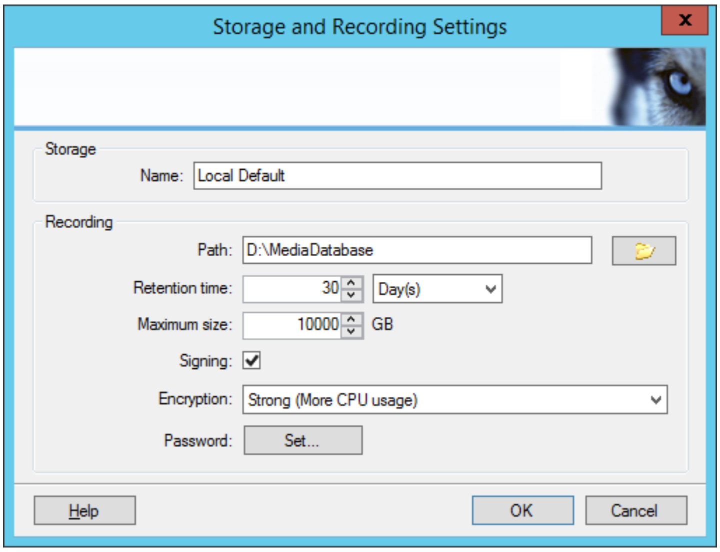
Enabling encryption and digital signature of the recordings does not alter the actual recorded audio or video content in any way. If the recorded audio or video contains some form of embedded watermark information, it will still be possible to verify the authenticity of the audio or video, either by the camera vendor or by a method/tool provided by the camera vendor.

For more information on MD5 and DSA:

http://da.wikipedia.org/wiki/MD5

http://en.wikipedia.org/wiki/Digital_Signature_Algorithm

Configuration of the database is done in the XProtect® Corporate Management Client, and it is a simple matter of selecting the **Signing** check box and selecting either **Light** or **Strong** in the **Encryption** field.



Name: Local Default

Path: D:\MediaDatabase

Retention time: 30 Day(s)

Maximum size: 10000 GB

Signing: ☑

Encryption: Strong (More CPU usage)

Password: Set...

4. Live or recorded video is send to a client over a network

Risk: *The network may be disconnected or flooded with unwanted data due to a DDOS attack*

In case the network is flooded with unwanted data, the connection to the client may be disconnected or rendered inoperable. In this case the operator will immediately see this and can alert the administrator about the issue.

While the clients may not be able to view live or recorded video, the Recording Server can continue to record video unaffected if the network has been designed as two separate networks; one for clients and one for cameras.

Risk: *The network may be compromised giving unauthorized persons access to tapping into the transmitted video*

As with the network connection from the cameras to the Recording Server, the transmitted video from the Recording Server to the client can be protected by using VPN tunneling.

In addition to VPN tunneling, XProtect® Web Client and XProtect® Mobile also support HTTPS.

5. Live or recorded video viewed and exported to a media

Risk: *Unauthorized persons may try to hack or otherwise obtain log-in credentials to gain unauthorized access to viewing and exporting video*

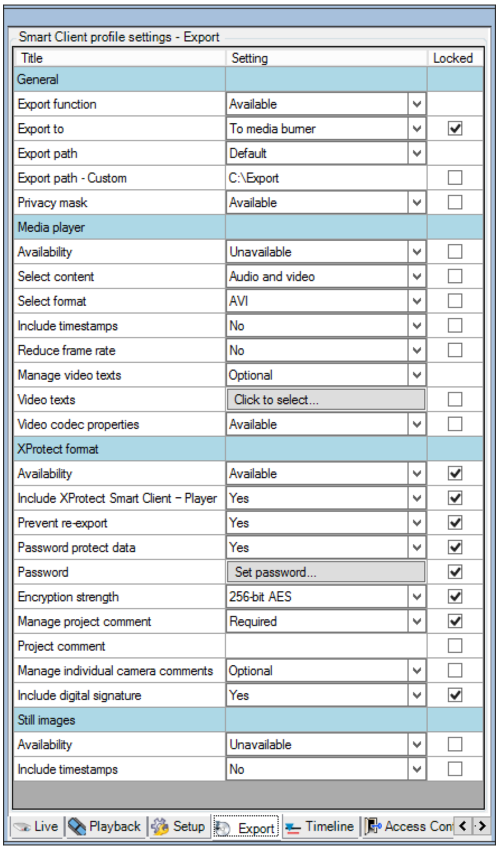
To prevent someone from hacking into the system, XProtect® Corporate relies on secure Windows Active Directory® (AD) authentication that offers strong protection against hacking.

In extension to the built-in technical security in Windows AD, it is important that all users of the system have their own separate Windows AD account because a single account, or just a few shared accounts, will make it hard to control who knows the user name and password and thus who can access the system. Using separate accounts for each user will also make it easier to investigate in the XProtect® Corporate audit log who logged in, viewed live or recorded video or who exported video from the system.

In addition to securing access to the client, XProtect® Corporate offers centrally controlled security settings with time profiles that set when and which cameras can be viewed live, played back and exported by the user. Furthermore, XProtect® Corporate can control all export settings available in the XProtect® Smart Client via a so-called XProtect® Smart Client profile.

Below is highlighted a few of the XProtect® Smart Client profile's export settings with the recommended value for the most secure export.

- **Export to** set to **To media burner**
- **XProtect® format** set to **Available**
- **Media player** and **Still image** formats set to **Unavailable**
- **Include XProtect® Smart Client – Player** set to **Yes**
- **Prevent re-export** set to **Yes**
- **Password protect data** set to **Yes**
- **Password** set to a predefined password
- **Encryption strength** set to **256-bit AES**
- **Manage project comments** set to **Required**
- **Include digital signature** set to **Yes**



Smart Client profile settings - Export

Title	Setting	Locked
General		
Export function	Available	
Export to	To media burner	☑
Export path	Default	
Export path - Custom	C:\Export	☐
Privacy mask	Available	☐
Media player		
Availability	Unavailable	☐
Select content	Audio and video	☐
Select format	AVI	☐
Include timestamps	No	☐
Reduce frame rate	No	☐
Manage video texts	Optional	
Video texts	Click to select...	☐
Video codec properties	Available	☐
XProtect format		
Availability	Available	☑
Include XProtect Smart Client – Player	Yes	☑
Prevent re-export	Yes	☑
Password protect data	Yes	☑
Password	Set password...	☑
Encryption strength	256-bit AES	☑
Manage project comment	Required	☑
Project comment		☐
Manage individual camera comments	Optional	☐
Include digital signature	Yes	☑
Still images		
Availability	Unavailable	☐
Include timestamps	No	☐

The **Locked** check box must be selected for all of the above settings to ensure that an XProtect® Smart Client user cannot override them.

The full list of the XProtect® Smart Client profile's export settings can be seen in the screenshot to the right on the previous page.

6. Exported evidence media is transported from the surveillance site to police or a court

To prevent unauthorized persons from viewing or copying exported video, Milestone's XProtect® Smart Client support three levels of security on the exported video database:

1. Database encryption with password protection
2. Disable re-export
3. Digital signature

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

The database encryption supports up to 256-bit advanced encryption standard (AES) and access is protected by a password.

XProtect® Smart Client offers the option to prevent the exported video from being re-exported when viewed again in the XProtect® Smart Client – Player. This ensures that the video cannot be exported in another format or be exported to the XProtect® format again but without encryption and digital signing.

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*

When video that should be exported is protected with a digital signature on the Recording Server, the signature of the recorded video will be checked during the export to ensure that the video has not been tampered with on the Recording Server.

If the recorded video passes the signature check, including the original digital signature, the video is exported to a new database created by XProtect® Smart Client on the client PC. During the export, XProtect® Smart Client adds its own signature so the video is protected by two signatures – the original one made during recording and the one created by XProtect® Smart Client during the export.

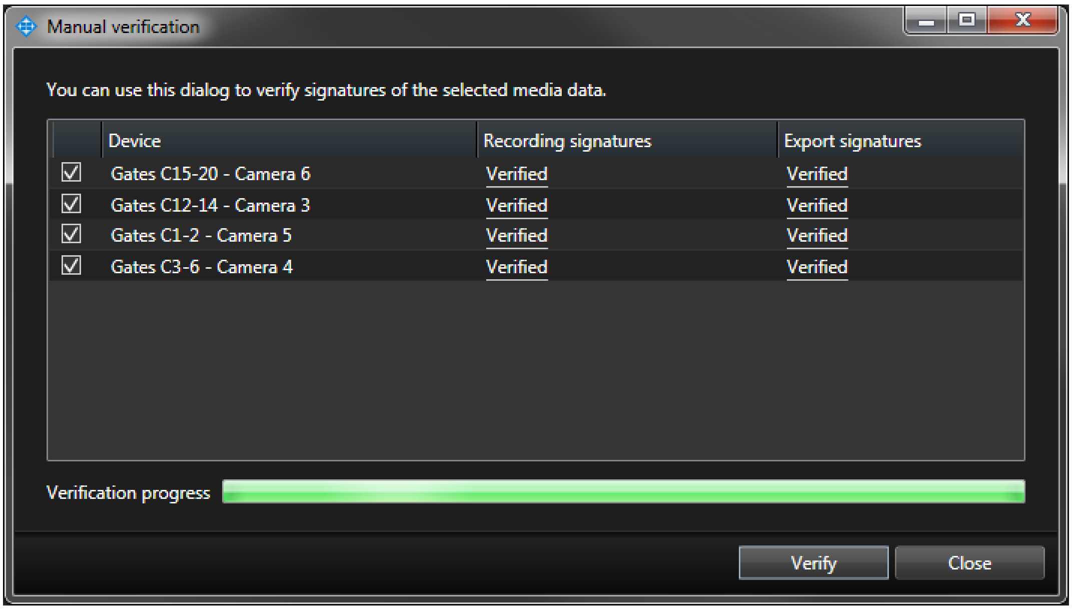
7. The exported evidence is viewed by police or a judge in a court

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

When the exported recordings protected by encryption and digital signing are viewed again by police or a judge in court, the XProtect® Smart Client – Player will request the user to enter the password to decrypt the recordings. Once the correct password has been entered, the client informs the user that the video is signed and can be verified by clicking the **Verify Signatures…** button.

This indicates for the person viewing the video that the recordings have been protected by an encryption and in addition to this have a digital signature that can be verified for authenticity. Activating the digital signing verification will open a new window and may take some time to complete depending on the size of the recordings and amount of cameras in the export. When completed, it will display if the recordings have been tampered with or if the integrity is intact.

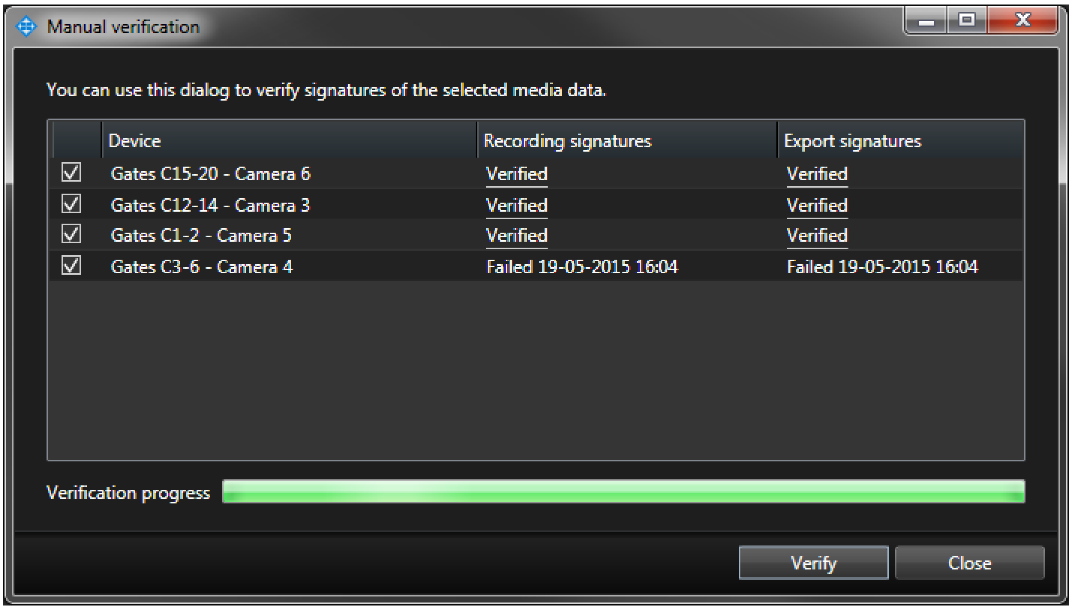
The below screenshot shows an example of correctly validated databases.



You can use this dialog to verify signatures of the selected media data.

	Device	Recording signatures	Export signatures
☑	Gates C15-20 - Camera 6	Verified	Verified
☑	Gates C12-14 - Camera 3	Verified	Verified
☑	Gates C1-2 - Camera 5	Verified	Verified
☑	Gates C3-6 - Camera 4	Verified	Verified

Both signatures can be validated directly in the Player. If the validation fails, the dialog box will display the time of the first failed segment of the database as seen in the screen shot below.



You can use this dialog to verify signatures of the selected media data.

	Device	Recording signatures	Export signatures
☑	Gates C15-20 - Camera 6	Verified	Verified
☑	Gates C12-14 - Camera 3	Verified	Verified
☑	Gates C1-2 - Camera 5	Verified	Verified
☑	Gates C3-6 - Camera 4	Failed 19-05-2015 16:04	Failed 19-05-2015 16:04

Benefits and summary

By combining a set of standard security functions and concepts with a set of solution unique functions, Milestone XProtect® Corporate enables users to deploy video surveillance solutions with full end-to-end security.

With the encryption and signing features in XProtect® Corporate and XProtect® Smart Client, it is possible to keep streamed and recorded video secure and prove the integrity of recordings all the way from the original stream from the camera and to the point where it is viewed, for example in a court of law.

For companies that require strict control of the export format and security settings, the XProtect® Smart Client profile can be used to control export settings and parameters strictly from a central point.

Milestone XProtect® Corporate and XProtect® Smart Client offers secure handling of video all the way from the point where it is captured and streamed from the camera to the video surveillance system and to the time it is viewed as evidence.

The Open Platform Company

About Milestone Systems

Founded in 1998, Milestone Systems is the global industry leader in open platform IP video management software. The XProtect® platform delivers powerful surveillance that is easy to manage, reliable and proven in thousands of customer installations around the world. With support for the widest choice in network hardware and integration with other systems, XProtect® provides best-in-class solutions to video enable organizations – managing risks, protecting people and assets, optimizing processes and reducing costs. Milestone software is sold through authorized and certified partners. For more information, visit **www.milestonesys.com**

Milestone Systems Headquarters, DK
Tel: +45 88 300 300

Milestone Systems US
Tel: +1 503 350 1100