MAKE THE
WORLD SEE

November 11, 2021

White Paper

Ensuring end-to-end protection of media integrity

Prepared by:
John Rasmussen, Platform Architect

milestone

Table of Content

Introduction

In applications and installations where video, audio, and metadata[1] play a critical role as evidence material, it is paramount that the media 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 Expert (hereafter jointly referred to as 'XProtect VMS'), and the XProtect Smart Client provide a series of security functionalities that enable users to maintain full end-to-end security and integrity of streamed and recorded media data – for example:

- Encrypted media streams from cameras via VMS servers to VMS clients
- Encrypted media database on recording servers and for XProtect format exports
- Digital signing and verification of media databases
- Secure user authentication and detailed access permissions
- Centralized control of allowed export formats and features, for example functionality to prevent re-exporting media databases that have already been exported

Purpose and target audience

The purpose of this white paper is to give a general overview of the inherent risks and threats that exist when designing and implementing IP-based video surveillance solutions, and how they can be mitigated when using the XProtect VMS.

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

- Surveillance system architects/designers
- Surveillance project consultants
- Security officers and IT managers

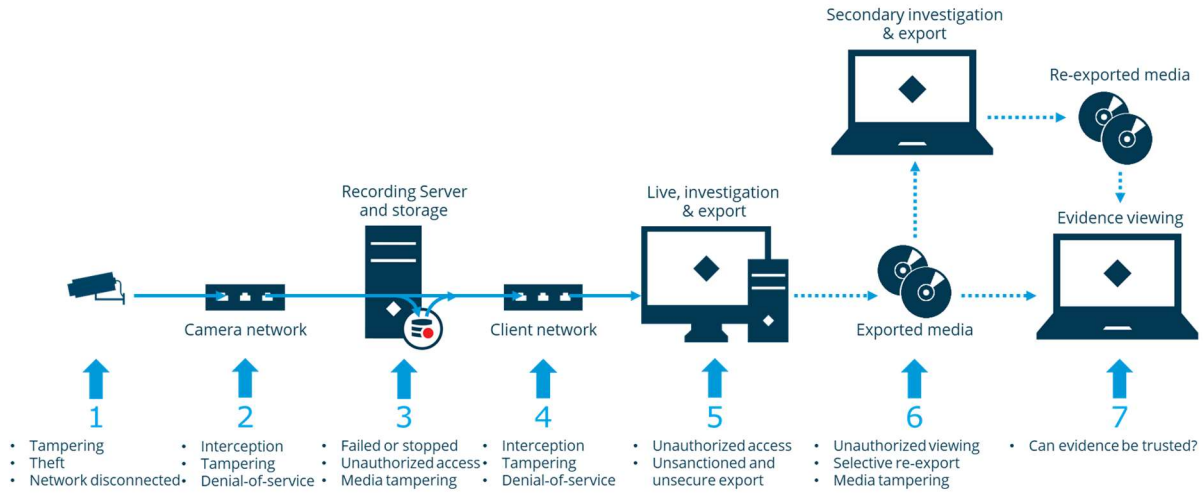
This white paper should enable the reader to understand how media can be secured from initial transmission from the camera to viewing exported media as evidence in the XProtect Smart Client - Player, as well as how authenticity of the exported media can be verified.
The white paper assumes the reader has a general understanding of Milestone's XProtect VMS and standard IT technologies.

[1] In this document all of which are referred to as 'media'.

Media flow and inherent security risks

In any IP-based video surveillance system, there is an inherent security risk in the different parts, components or communication media used. At each step in the media flow or process there is a risk of unauthorized access, interruption of service, unauthorized interception of media or even media tampering.

In the XProtect VMS, the media flow is typically as illustrated below.



Each step in the media flow has its own inherent risks and threats – of which examples are listed here:

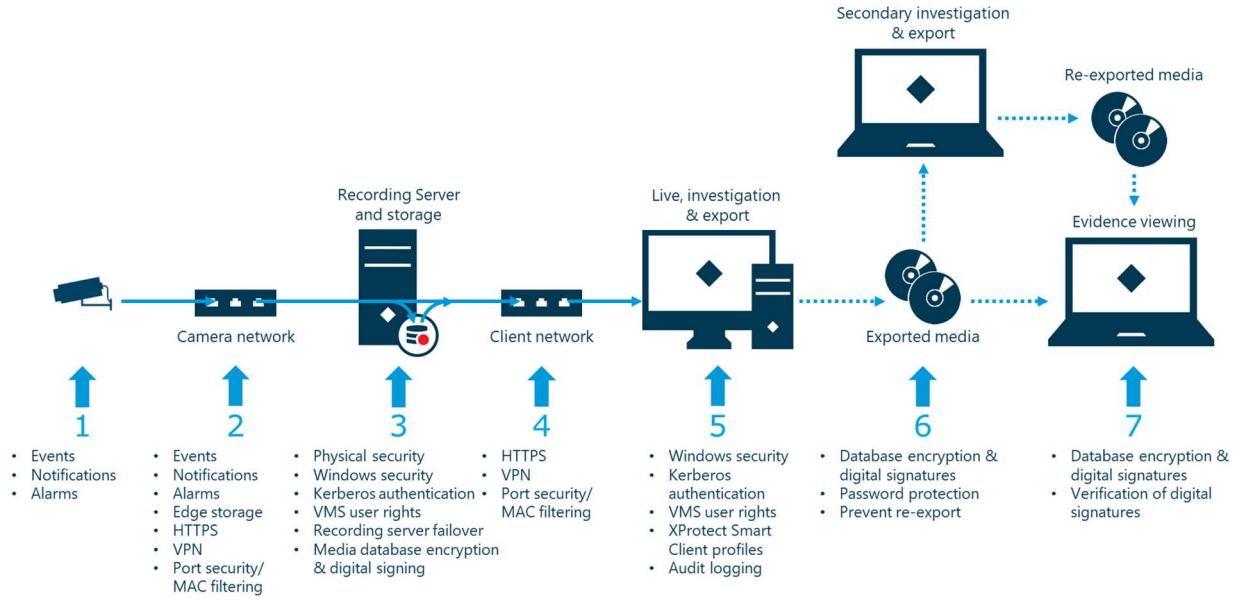
1. Media is captured by a camera
   - *Camera may be tampered with by moving it or by covering the lens*
   - *Camera may be stolen, disconnected, or simply vandalized*
2. Media is streamed to the recording server
   - *Unauthorized equipment may be connected to the network, potentially enabling the capture and modification of transmitted media streams*
   - *The network may be disrupted with a denial-of-service attack performed by someone connecting malicious equipment to the network*
3. Recording server stores media and provides access for clients
   - *Recording server may fail or be turned off*
   - *Unauthorized access to the recording server could be attempted via the network using either Milestone XProtect Clients or the underlying APIs*
   - *The recording server and media database files could be compromised by someone obtaining remote or physical access to the recording server and storage system, and thus obtain direct access to the media database files*
4. Live or recorded media is sent over the network to the clients
   - *Unauthorized equipment may be connected to the network, potentially enabling the capture and modification of transmitted media streams*

- *The network may be disrupted with a denial-of-service attack performed by someone connecting malicious equipment to the network*

5. Live or recorded media viewed and exported to removable media
   - *Unauthorized persons may try to hack or otherwise obtain login credentials to gain access to view and export media*
   - *Legitimate users of the VMS may export recorded media without proper reason, for instance with the intent to publish "funny" videos on social media such as Facebook or YouTube*
6. Exported media is in transit
   - *The exported media may be viewed by unauthorized people*
   - *"Carefully" selected parts of the exported media may be re-exported to make the evidence appear different from the originally exported media, or it may be re-exported to an unsecure format making it possible to post the exported media on social media such as Facebook or YouTubes*
   - *The exported media may be tampered with by removing, adding, or modifying critical sequences of the recorded media to give another impression of the recorded evidence*
7. The exported evidence is viewed
   - *The exported media may have been tampered with either in the VMS's recording server media database or after the media was exported to give another impression of the recorded evidence*

Addressing security concerns and risks

As highlighted, there are several places where security and integrity can be breached. In addition to applying standard physical and IT security practices, Milestone has implemented several security functions in the XProtect VMS to further increase security and reduce risks, threats, and concerns. The illustration below shows a selection of security measures that can be used to counter tampering, manipulation, and unauthorized access in each step of the media flow.



1. Media is captured by the camera

Risk:

Camera may be tampered with by moving it or covering the lens.

Mitigation:

Most cameras can send events to the VMS when detecting different kinds of tampering, for example: moving the camera, covering the lens or in other ways obstructing the video. Once this is detected a camera event is triggered, which can be used to trigger alarms or send notifications via SNMP Traps, emails, or via 3rd party integrations.

Alternatively, if the camera does not support detecting tampering natively, 3rd party solutions that offer this can be found on the Milestone Marketplace:
https://www.milestonesys.com/community/marketplace/what-is-marketplace/

Risk:

Camera may be stolen, disconnected, or simply vandalized.

Mitigation:

The Milestone XProtect VMS will automatically detect if a camera is not responding or stops streaming media to the system. If this is detected, an event is triggered which can be used to trigger alarms or send notifications via SNMP Traps, emails, or 3rd party integrations.

2. Media is streamed to the recording server

Risk:

Unauthorized equipment may be connected to the network, potentially enabling the capture and modification of transmitted media streams.

Mitigation:

Two methods can be used to protect the media transmitted from the cameras to the recording server: HTTPS and VPN tunneling.

In extension to various unencrypted communication protocols, the XProtect VMS supports HTTPS (Hypertext Transfer Protocol Secure) for encrypted communication with cameras. HTTPS uses Transport Layer Security (TLS) and certificates to secure and encrypt the communication between the camera and the recording server, which prevents unauthorized capture or access to the streamed media.

HTTPS is not supported by all cameras. It is therefore recommended to check the driver database to find devices that support HTTPS or check if HTTPS is supported for a specific camera.

https://www.milestonesys.com/community/business-partner-tools/supported-devices/

Furthermore, a virtual private network (VPN) tunnel can be set up between the camera and the recording server using standard IT and network equipment. A VPN will encrypt all data transmitted through the VPN tunnel and thus protect against unauthorized access to the streamed media. Using a VPN is a generic solution that can be used with any camera.

For more information about HTTPS, TLS, and VPN:
http://en.wikipedia.org/wiki/HTTP_Secure
http://en.wikipedia.org/wiki/Transport_Layer_Security
http://en.wikipedia.org/wiki/Virtual_private_network

Risk:
The network may be disrupted with a denial-of-service attack performed by someone connecting malicious equipment to the network.

Mitigation:
As with the case of completely disconnecting the camera, should the network communication be disrupted, the XProtect VMS will automatically detect it and trigger an event that can be used to trigger alarms or send notifications via SNMP Traps, emails, or 3rd party integrations.

Furthermore, on devices supporting 'Edge Storage', the XProtect VMS can retrieve any media recorded and stored on the camera's internal edge storage once communication is reestablished. This ensures that any missing recordings can be retrieved and recorded even for periods where connection to the cameras temporarily have been interrupted.

For more information on Edge Storage in Milestone XProtect VMS products, see the 'Edge Storage with flexible retrieval whitepaper':

https://content.milestonesys.com/l/3ab3e02a2d866132/

Securing network
In extension to the risk mitigations covered above, a wired network can also provide additional protection against denial-of-service attacks and unauthorized access by enabling port-security/MAC-filtering on the switches in the network.

The port-security/MAC-filtering functions basically protect the network against communication with unknown devices connected to the switch ports, thus blocking them from reading or sending data on the network.

For more information on MAC filtering:
https://en.wikipedia.org/wiki/MAC_filtering

3. Recording server stores media and provides access for clients

Risk:

Recording server may fail or be turned off.

Mitigation:

The XProtect VMS supports failover recording servers, which can be used to monitor the operation of the recording server, and in case of a failure or manual shutdown, completely take over the original recording server's tasks.

Risk:

Unauthorized access to the recording server could be attempted via the network using either Milestone XProtect Clients or the underlying APIs.

Mitigation:

The XProtect VMS are designed to provide a strong protection against unauthorized access by using multiple layers of security, such as: user authentication using Active Directory (AD) with Kerberos support, detailed VMS permissions per role/user, time limited access tokens, server-side access authorization by each individual VMS server as well as AES-256 encrypted communication based on trusted certificates.

These VMS security measures, combined with the general IT and network security measures, provide a very strong protection against unauthorized access or tampering.

Risk:

The recording server and media database files could be compromised by someone obtaining remote or physical access to the recording server and storage system, and thus obtain direct access to the media database files.

Mitigation:

To prevent unauthorized access to the media database files and thus the recorded media, several layers of security can be implemented:

- Physical security
    - Access to the room with the physical servers should be limited to a few authorized people only
- Windows security
    - Local console and remote desktop access to the servers running the XProtect VMS should be limited to a few authorized people only
    - Windows should be set to automatically log out after a short time of inactivity
    - Windows should be kept updated with the newest service releases and security patches

  - Windows and the general network and IT installation should be "hardened" (see 'Additional recommendations and guides' section)
- Recording server media database
  - The media stored in the media database should be protected by enabling media database encryption
  - When enabled, encryption can be configured in two modes:
    - '*Light (Less CPU usage)*'
    - '*Strong (More CPU usage)*'
  - The media database can be set to digitally sign the recorded media to enable detection of post recording tampering

Encryption

Both '*Strong (More CPU usage)*' and '*Light (Less CPU usage)*' media database encryption modes are secure and use the same AES-256 encryption technology. The difference is how much of the media data is encrypted.

- '*Strong (More CPU usage)*' encrypts all parts of the media data stored in the media database but requires more processing resources to do so because everything needs to be encrypted. This is especially the case for video since the bitrate is much higher than with audio or metadata
- '*Light (Less CPU usage)*' only encrypts the first ~1000 Bytes of the media data, which includes the header. Because of this, less processing resources are needed to encrypt the media data. Even though only part of the media data is encrypted, the media data is still secured against unauthorized playback since the audio and video data cannot be decoded without the information contained in the encrypted header

For more information on AES:
https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Digital Signature

The digital signature is created by calculating a hash of the recorded media using SHA-256 (Secure Hash Algorithms). The hash is then signed with a Digital Signature Algorithm (DSA) and stored with the recordings. If the content later is changed or parts of the recordings are removed, the SHA-256 hash and signature will no longer match, making it possible to detect that the media databases or their content have been tampered with.

For more information on SHA-256:
https://en.wikipedia.org/wiki/Secure_Hash_Algorithms
For more information on DSA:
http://en.wikipedia.org/wiki/Digital_Signature_Algorithm

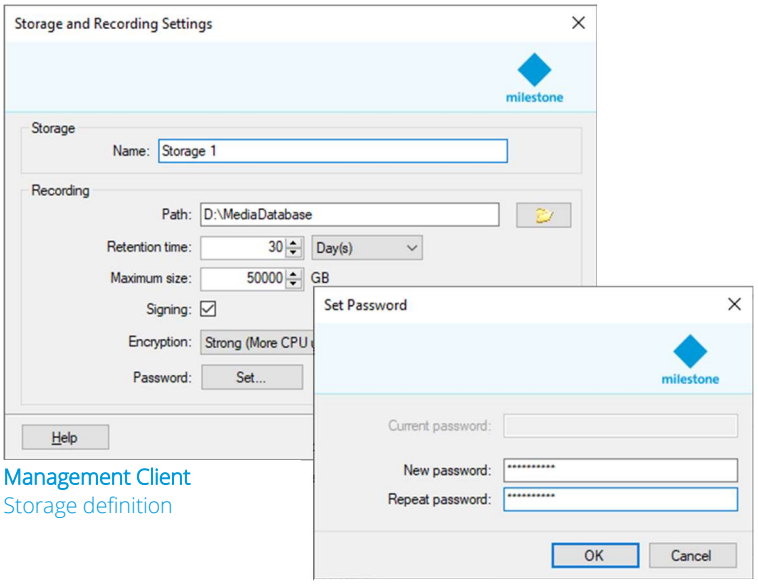
Media data authenticity

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

Configuration

Configuration of the media database is done in the Management Client per recording server. Enabling encryption and digital signing is a simple matter of opening the storage configuration, and:

- Check the '*Signing*' check box
- Select '*Light (Less CPU usage)*' or '*Strong (More CPU usage)*' in the '*Encryption:*' drop down menu
- Enter a media database password



Management Client
Storage definition

Management Client
Password definition

4. Live or recorded media is sent over the network to the clients

Risk:

Unauthorized equipment may be connected to the network, potentially enabling the capture and modification of transmitted media streams.

Mitigation:

As with the camera to recording server communication, there are two methods for protecting the media transmitted from the recording server to the clients: HTTPS and VPN tunneling.

The recording server supports encryption of media streamed to the clients using HTTPS. As opposed to the camera to recording server encryption, which relies on cameras supporting HTTPS, the recording server to client encryption is independent of the camera's HTTPS support. This is because the media stream data is now managed by the recording server allowing it to encrypt it using HTTPS, even if it originally is not encrypted from the camera.

Furthermore, a virtual private network (VPN) tunnel can be set up between the recording server and the client using standard IT and network equipment. A VPN will encrypt all data transmitted through the VPN tunnel and thus also protect against unauthorized access to the streamed media.

For more information about HTTPS, TLS, and VPN:
http://en.wikipedia.org/wiki/HTTP_Secure
http://en.wikipedia.org/wiki/Transport_Layer_Security
http://en.wikipedia.org/wiki/Virtual_private_network

Risk:

The network may be disrupted with a denial-of-service attack performed by someone connecting malicious equipment to the network.

Mitigation:

Depending on where in the client-side network it is disconnected or flooded with unwanted data, the VMS itself may not be able to detect it. However, clients connected to the VMS will immediately see that they lost connection to the VMS servers enabling users to alert the VMS administrator.

Furthermore, any issues on the client-side network of the recording server do not impact the recording server performance and recording of media. So, once the issue has been addressed, all recordings are again available for playback and investigations.

Securing network

In extension to the risk mitigations covered above, a wired network can also provide additional protection against denial-of-service attacks and unauthorized access, by enabling port-security/MAC-filtering on the switches in the network.
The port-security/MAC-filtering functions basically protect the network against communication with unknown devices connected to the switch ports, thus blocking them from reading or sending data on the network.

For more information on MAC filtering:
https://en.wikipedia.org/wiki/MAC_filtering

5. Live or recorded media is viewed and exported to removable media

Risk:

Unauthorized persons may try to hack or otherwise obtain login credentials to gain access to view and export media.

Mitigation:

The XProtect VMS are designed to provide a strong protection against unauthorized access by using multiple layers of security, such as: user authentication using Active Directory (AD) with Kerberos,

detailed VMS permissions per role/user, time limited access tokens, server-side access authorization by each individual VMS server as well as AES-256 encrypted communication based on trusted certificates. Furthermore, it is important that when using shared client computers, each VMS user has and uses their own separate AD account to log in to both Windows and the VMS. If more users share the same account to log in to Windows and the VMS, it is impossible to control who has access to the VMS, since the password will be known by current and former employees – and anyone they have told it to.

Furthermore, in the VMS's audit log all user actions, for example exports, will appear as being done by the same shared user, making it impossible to track who did what.

Risk:

Legitimate users of the VMS may export recorded media without proper reason, for instance with the intent to publish "funny" videos on social media such as Facebook or YouTube.

Mitigation:

In extension to authenticating users that want to access the VMS, the VMS also supports detailed security permissions controlling what devices the user may view and what functions are allowed – for example: view live and playback, export, bookmarks, evidence lock, and so forth.

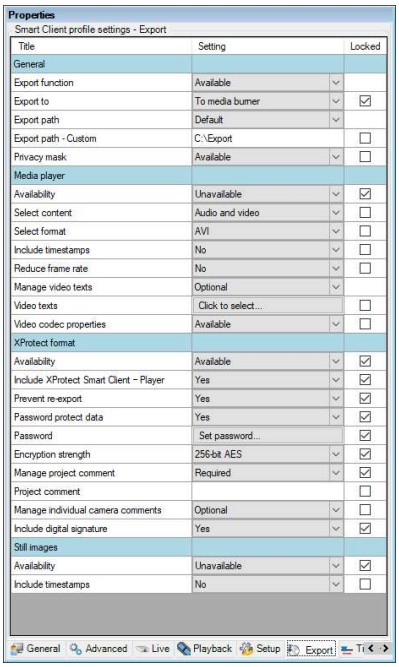
Using the security permissions, it is recommended to only allow users access to devices and functions that are needed to do their job. It is furthermore recommended to limit export permissions to a few trusted 'super' users that are educated in proper handling of their export permissions and the media they may export.

To further control how exported media are handled, the VMS - in extension to security permissions - supports '*Smart Client Profiles*' which control how the XProtect Smart Client behaves and what features or functions are available for the user – including what export formats and functions are available to the VMS user with export permissions.

To ensure maximum security of the exported media, and to prohibit unauthorized distribution and viewing of the exported media, it is recommended to set the Smart Client Profiles export settings to the following:

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

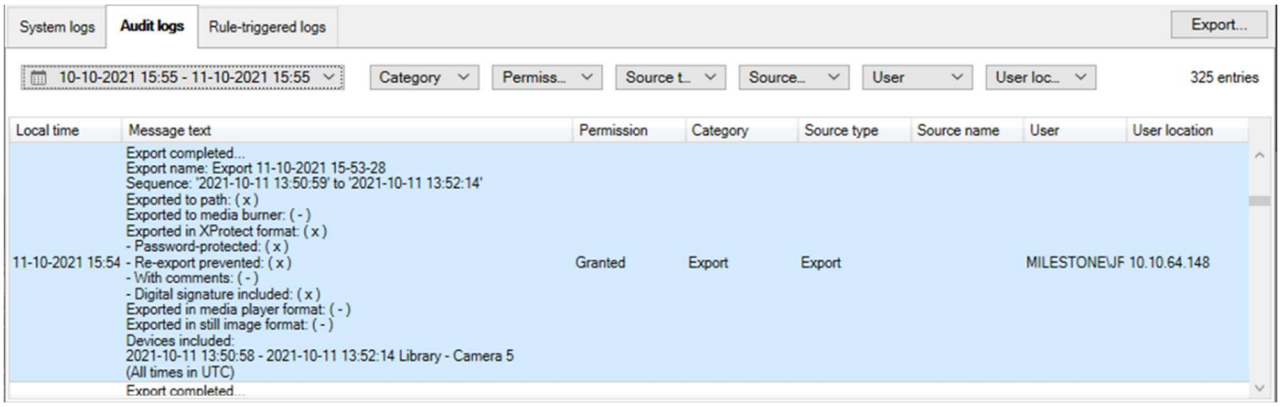
The '*Locked*' checkbox must be selected for all of the above settings to ensure that a XProtect Smart Client user cannot override them.



Management Client
Smart Client Profile, Export options

However, even when security permissions and profile settings are set appropriately, it can be difficult to ensure that the privileged users never export media without good reason.

To track user activity in the VMS, and to discourage users from exporting media without proper reason, the VMS will always create an audit log for every export action. The audit log, as can be seen in screenshot below, includes details about exported devices and time periods as well as formats used, usage of password protection (encryption) and digital signatures, and so forth.



Management Client
Audit log of export action

The audit log can then be used to audit who did what in the VMS and check if there were legitimate reasons for the actions performed.

In extension to the standard creation of audit logs for all administration of the VMS and media exports, the VMS can also be configured to create audit logs for all viewing of live and recorded media, including activation of events, outputs, control of PTZ, and so forth.

6. Exported media is in transit

Risk:
The exported media may be viewed by unauthorized people.

Mitigation:
When recorded media are exported, it can be exported in the XProtect format, which offers the option to encrypt, and password protect the exported media. This ensures that only people who know the password can decrypt and view the exported media.

Risk:
"Carefully" selected parts of the exported media may be re-exported to make the evidence appear different from the originally exported media, or it may be re-exported to an unsecure format making it possible to post the exported media on social media such as Facebook or YouTube.

Mitigation:
The XProtect Smart Client offers an option to prevent the exported media from being re-exported when later viewed in the XProtect Smart Client – Player. Enabling this option during the export ensures the media cannot be re-exported in any way.

Risk:
The exported media may be tampered with by removing, adding, or modifying critical sequences of the recorded media to give another impression of the recorded evidence.

Mitigation:
When media are recorded and stored in the media database, the recording server can add a digital signature to the media database. Later, when the media is exported, the signature of the media database is checked. If the signature check passes, the XProtect Smart Client exports the media to a new media database stored on the computer running the client. In addition, to include the signature from the original media database, the XProtect Smart Client adds its own signature to the media databases. The exported media are thus protected by two signatures – one made when media was recorded, and one created by the XProtect Smart Client during the export. When viewing the exported media, the XProtect Smart Client – Player can be used to check the two signatures to verify that video was not tampered with neither in the VMS's recording server nor after it was exported.

7. The exported evidence is viewed

Risk:

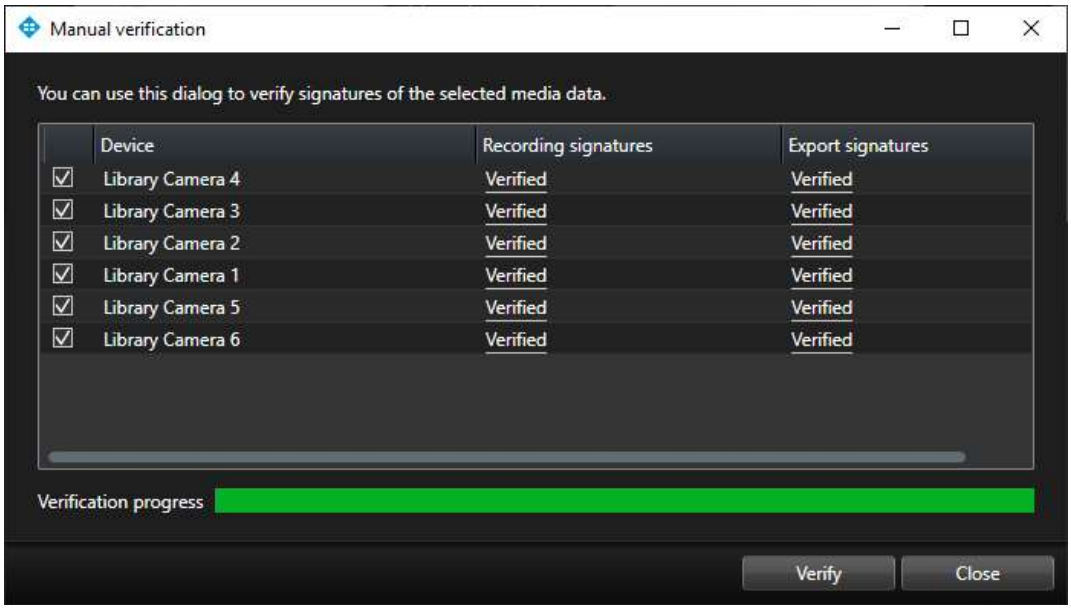
The exported media may have been tampered with either in the VMS's recording server media database or after the media was exported to give another impression of the recorded evidence.

Mitigation:

When media are exported in the XProtect format and digital signatures have been added, the XProtect Smart Client – Player will inform the user that the exported media includes digital signatures and that the authenticity of the exported media can be verified by clicking the '*Verify Signatures...*' button.

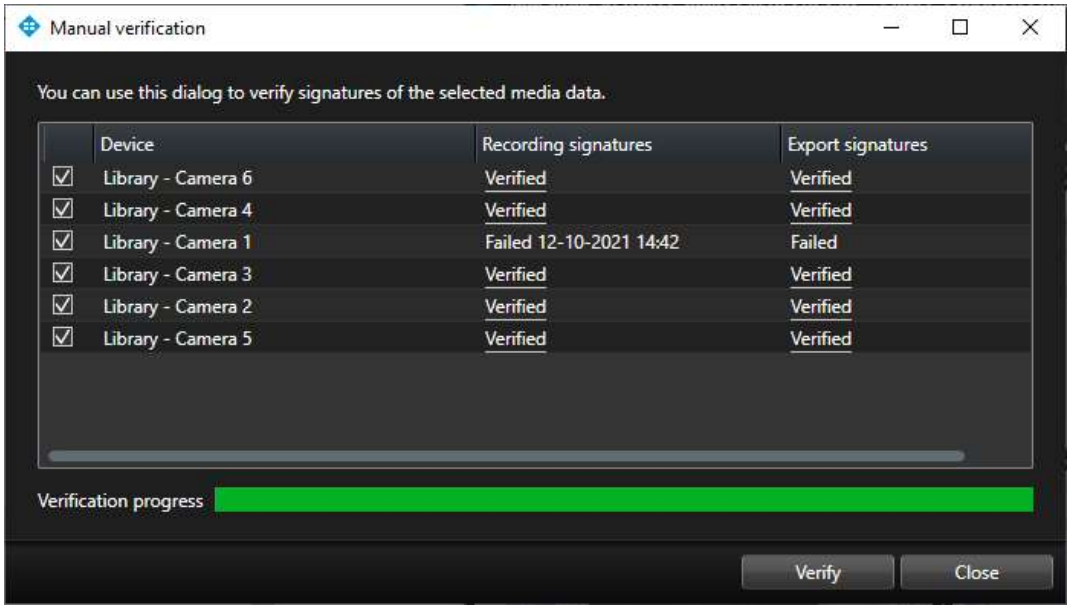
Verifying Digital Signatures:

When clicking the '*Verify Signatures...*' button, a new dialog is opened, and the media database signatures are analyzed one device at a time. Depending on the number of devices included in the export and the length of the exported media, the verification process may take some time to complete – though progress is shown during the verification. Once the verification is completed, XProtect Smart Client will display if the media databases have been tampered with or if the integrity is still intact.
The screenshot below shows an example of correctly validated media databases.



XProtect Smart Client – Player
Digital Signature verification passed

If the validation fails, the dialog box will display the time of the first failed segment of the media database, as shown below.



XProtect Smart Client – Player
Digital Signature verification failed

Additional recommendations and guides

In addition to the topics and recommendations covered in this whitepaper, detailed information about system hardening, certificate use and general VMS configuration can be found in the following documents:

XProtect VMS Hardening Guide
https://doc.milestonesys.com/latest/en-US/portal/htm/chapter-page-hardening-guide.htm
XProtect VMS Certificates guide
https://doc.milestonesys.com/latest/en-US/portal/htm/chapter-page-certificates-guide.htm
XProtect VMS Administrator manual
https://doc.milestonesys.com/latest/en-US/portal/htm/chapter-page-mc-administrator-manual.htm

Summary

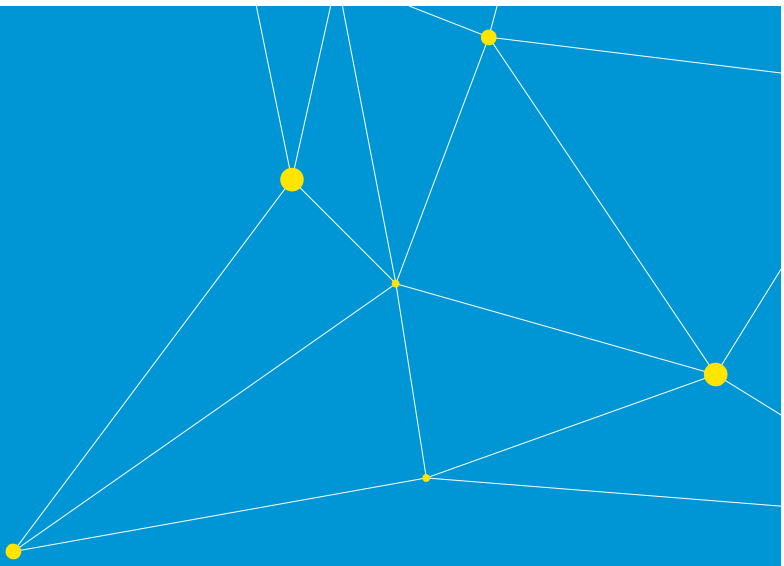
Combining a range of standard IT security methods with a set of unique VMS features in the Milestone XProtect VMS products enables customers to make a secure deployment of video surveillance solutions with full end-to-end security and encryption of the VMS media data.

The XProtect VMS's support of encryption of both streamed and recorded media data ensures that media cannot be captured or accessed by unauthorized people during network transit or at rest in the media database.

The XProtect VMS's additional support of digital signatures in the recording server's media database and in exported media databases ensures that it is possible to verify that the media evidence has not been tampered with, neither in the VMS recording servers nor later during transport or viewing of the exported media.

In extension to the encryption and digital signing functionality, the XProtect VMS furthermore offers the VMS owner strict control over who has access to specific devices and export functionality, including centralized control and enforcement of allowed export formats and destinations, usage of encryption and digital signing, and the option to prohibit re-export of exported media.

Using the entire suite of cybersecurity features in the Milestone XProtect VMS allows customers to operate a secure video surveillance installation, even in environments with heightened cybersecurity needs and risks.



Milestone Systems is a leading provider of open platform video management software; technology that helps the world see how to ensure safety, protect assets and increase business efficiency. Milestone enables an open platform community that drives collaboration and innovation in the development and use of network video technology, with reliable and scalable solutions that are proven in more than 500,000 sites worldwide. Founded in 1998, Milestone is a stand-alone company in the Canon Group.