R1
2019
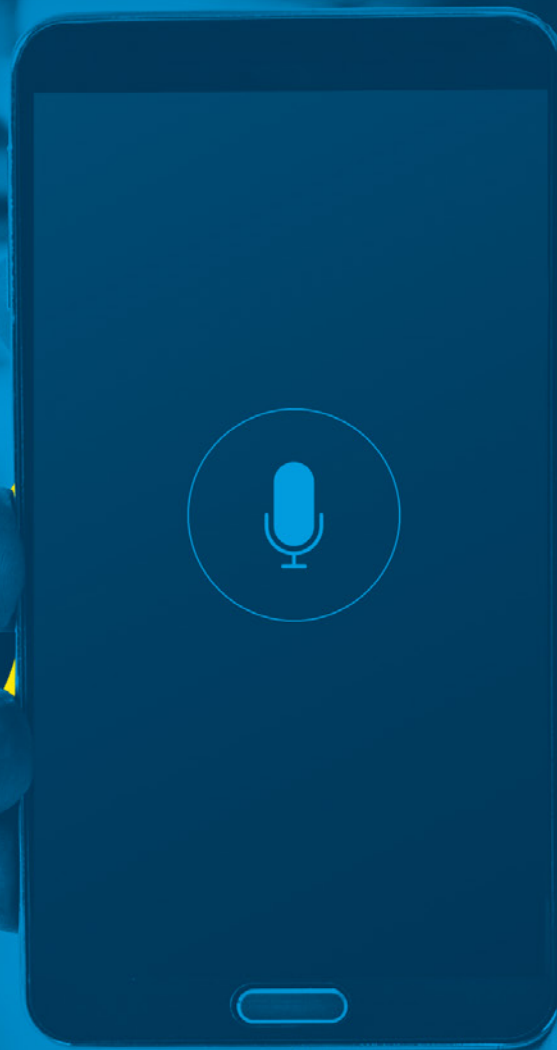
THE WORLD IS LISTENING

Listen to audio and speak through the camera – directly from your phone. Push-To-Talk is here!

GENERAL AVAILABILITY
FEBRUARY 5, 2019

Never miss a beat

Imagine being able to listen to everything that happens around the camera, and communicate with people for quick decision-making incidents prevention before they happen.

The first XProtect® release of 2019 extends the usability of the Smart Client and takes it outside the control room, with support for one and two-way audio in Mobile and Web clients. Listen to audio captured by the camera and speak through the camera speakers directly from your phone with the push of a button (Push-To-Talk) or from the Web Client. Whether on-premise or away from the Smart Client, you can now use your VMS system as an interactive tool.
By listening to audio and speaking through the speaker connected to the camera, you can get the full picture and act quickly from anywhere.
This includes communicating with people via Access Control, warning and directing crowds, or deterring intruders.

Web Client browser support

The new audio features are supported in most browsers, including Firefox, Opera and Microsoft Edge. The feature will not be supported for Internet Explorer due to low usage share worldwide.

▶ See and hear what audio can do for you

Good VMS helps you react quickly to incidents. Great VMS helps you prevent incidents before they even happen. Here are a few examples of how listening to audio and using Push-To-Talk directly from your phone can help you stay on top of things, even when you are on the go.
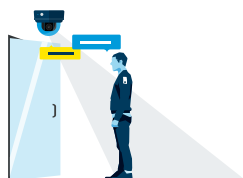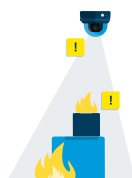
Access Control

Respond to Access Control requests quickly from anywhere by communicating with people on camera.
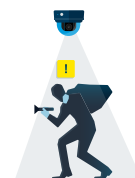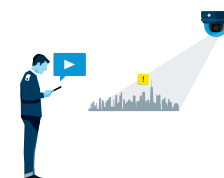
Deter unwanted intruders

Witness suspicious activity while on patrol? Speak through the speakers connected to the cameras and deter unwanted visitors, directly from your phone.

Warn and direct crowds

Detect an obstacle on premise? Warn crowds and direct them to a safe place before an incident occurs.

Be in two places at once

Watch video and listen to audio from one area while patrolling another.

Solve issues faster

Need help taking care of an issue? Announce your need for assistance through the speakers connected to the cameras and ask for backup directly from your phone.

Coordinate responses with ease

Communication is the key to a successful operation. Communicate with other security personnel in real time via the camera speakers and maximize your operational efficiency.

Best performance.
Encrypted end-to-end.

Ensuring the security and integrity of all Milestone installations is our top priority. We want to minimize our customers' exposure to risk by ensuring our software and hardware is secure by design, secure by default and secure by deployment.

Milestone is committed to providing XProtect users with a great-performing VMS that is durable and highly resistant against cyber threats. The first release of 2019 follows up on that commitment with yet another cyber security tool implemented in XProtect: an SSL/TLS certificate-based encryption of all communication between the Recording Server and the servers and clients connected to it.

This means that any use of data originating in the recording server goes out to components like management, mobile, or event servers. It can also goes out to the management, mobile or smart clients. The data is fully encrypted to guarantee the highest level of security of the servers' network. Third-party developers are also required to align their solutions with XProtect's 2019 R1 version of MIP SDK, making all communication between the Recording Server and any integrated solutions just as cybersecure. The encryption is enabled by default in the 2019 R1 installation process, where a notification pane explains the encryption and its implications on all components and solutions communicating with the Recording Server. It is also possible, to complete the installation of the 2019 R1 version without enabling the encryption to complete the certification process at a later time.

For a step by step guide to certificates encryption, please click here.

End-to-end encryption and fully authenticated evidence

Management Server

Smart Client

Smart Client Player

Law Enforce- ment
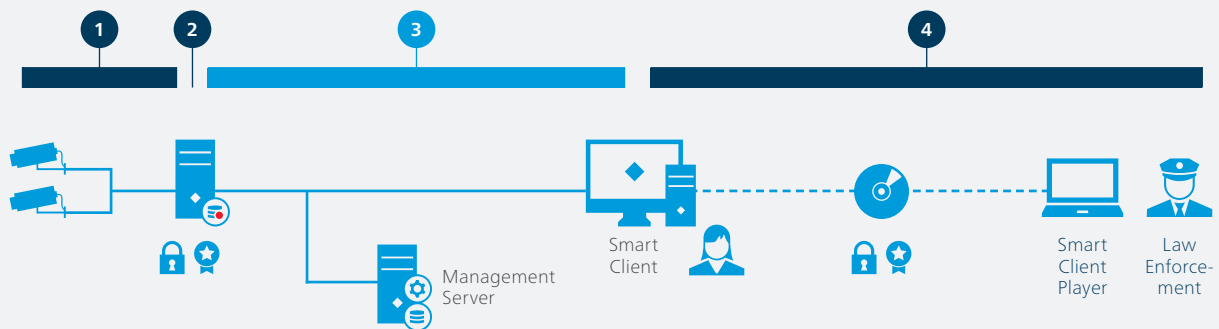
1. HTTPS for bidirectional encryption of the communication in the cameras' network.

2. Encryption, password-protection and digital signature of the data stored in the Recording Server.

3. SSL/TLS certificate-based encryption of all communication between the Recording Server and its connected servers and clients (coming in 2019 R1) in addition to other security tools like role definition, support for Windows AD and two-step verification.

4. Encryption and digital signature to assure the credibility of exported evidence in transit.

End-to-end encryption without compromised performance

One of today's biggest challenges in software development is implementing new and advance security tools without hindering the system's performance. Security and performance stand in the core of our commitment to our customers. Introducing the new encryption tool in this release was no exception.

In order to evaluate the impact that encryption might have on performance, our engineering teams performed rigorous tests to measure the system's CPU load in different stream constellations with and without encryption enabled. The tests measured the impact that encryption has on the CPU load on the Smart

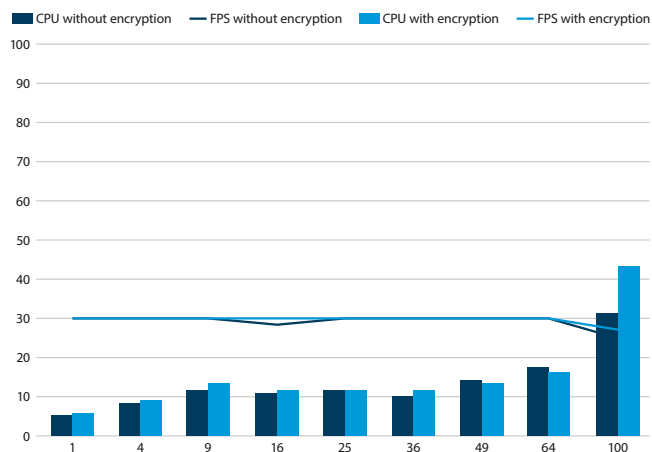Client and Recording Server sides for H.264 and H.265 streams to verify the smallest impact possible.

Impact on the Smart Client

We tested our system with up to 100 streams of H.264 720p and H.265 Full HD and measured the CPU load while maintaining a constant 30 frames
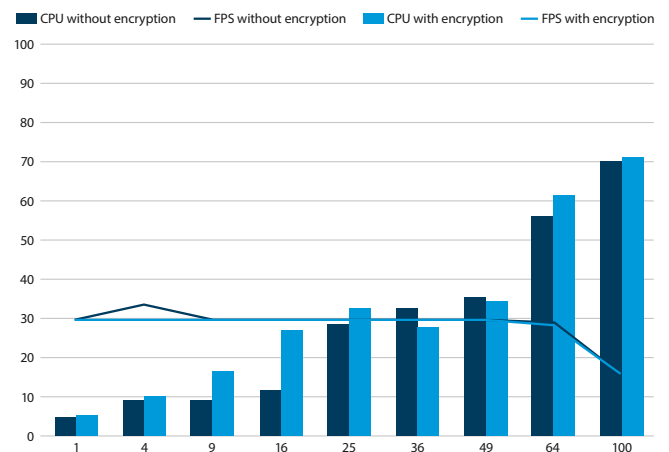
per second rate. Our tests showed minimal (close to none) impact on the system's performance, when hardware acceleration (Nvidia graphics cards)

took an active part only in displaying video in the Smart Client. It was not at all triggered by enabling encryption.

H.264 720p Only Nvidia

■ CPU without encryption   — FPS without encryption   ■ CPU with encryption   — FPS with encryption

H.265 Full HD Auto Nvidia

■ CPU without encryption   — FPS without encryption   ■ CPU with encryption   — FPS with encryption

Smart Client performance measured on: Intel® CoreTM i7-8700K 3.7GHz CPU, 32GB memory, 2 X Nvidia GeForce GTX 1080 Graphics cards, Microsoft Windows 10 Enterprise OS.

Impact on the Recording Server

Impact on the Recording Server can vary depending on the hardware, the chipper used for encryption, the size of the streams, etc. We tested our system with up to 100 connections of

both H.264 and H.265 and measured the CPU load. Our tests showed approximately 7% and 10% increase in CPU load (respectively) when encryption was enabled.

Recording Server performance measured on: Intel® CoreTM i7-3610QE 2.30GHz CPU, 16GB memory, Microsoft Windows 10 OS.

We have more great news for you

1 Milestone's License Plate Recognition now open for third-party integrations

Your LPR operator needs to add or remove license plates to match a certain list. But do you want to give the operator access to the Management Client? Milestone's LPR 2019 R1 now supports third-party integrations, meaning that you can create and fully manage match-lists via a simple webpage of an external application.

2 Smart Client Player now supports 64-bit

Make the most of your system and enjoy the full Smart Client experience even when exporting video with a 64-bit player – now with better H.265 and plugin support.

3 An even better add-hardware wizard

Easily grow your video installation as your business grows by multi-selecting device types when adding more devices.

Download center

Price list ⬇

XProtect Comparison Chart ⬇

Specification sheets ⬇

New features presentation ⬇

eLearning release course ⬇

Certificates guide ⬇

Join the community

f in 𝕏 ▶

milestonesys.com

Previous product releases

⬇

Excel your performance with ease

Let us help you empower on-the-job performance through learning

START EXPLORING

milestone