milestone

Newport Mesa Unified School District

Newport-Mesa
Unified School District

REQUEST FOR PROPOSALS

FOR

INTEGRATED SECURITY SYSTEMS STANDARDS

Response from:
Milestone Systems Inc.
5300 Meadows Rd, Suite 400
Lake Oswego, OR 97035
Toll-free telephone: +1 877 350 1101
Fax: + 1 503 662 7321

Laurie Dickson
Channel Business Manager, Los Angeles/Orange County
West Sales Field US
Email: Laud@milestone.us
Mobile: +1 504 338 4468

November 17th, 2022

Table of Contents

Table of Contents 1
2. Certification from an individual authorized to represent the Vendor 2
3. Executive Summary 3
Major Solution Attributes that Differentiate XProtect 3
Direct Training, Certification, and Support to NMUSD 4
Products and Services to the District - Integrator/Partner responsibilities 5
4. Solution Narrative – System elements, integrations, deployment, and support 6
5. System Diagram (Architecture) 20
6. System Requirements 21
7. Cyber Security Program 23
8. Price Proposal 25
9 Product data for each of the systems elements 28
10 Certified Integrators 35
11 Complete and detailed copy of the RFP 39
12 Completed Solution Deployment (Reference) 39
13 Other documentation 41
14 Supplemental Data 42

2. Certification from an individual authorized to represent the Vendor

RE: Newport Mesa Unified School District RFP

Please find Milestone Systems Response to the Newport Mesa Unified School District RFP. All statements made in this document are true and correct.

I will be responsible for supporting you and your chosen Systems Integrator in this exciting initiative and project. I will work to ensure the best Milestone team and partners are working with you towards a successful compliant solution, system design and delivery of this important project. Please don't hesitate to contact me for any clarifications or questions about our response and next steps.

Best Regards,

Laurie Dickson
Channel Business Manager, Los Angeles/Orange County
West Sales Field US
Email: Laud@milestone.us
Mobile: +1 504 338 4468

Authorizing Signature: (Submitted electronically, no signature required)

3. Executive Summary

Major Solution Attributes that Differentiate XProtect

An innovative and customizable solution offering with an open platform VMS technology

Newport Mesa Unified School District's goal is to identify and deploy a districtwide integrated security system. Milestone XProtect can empower the Newport Mesa Unified School District with the ability to improve and positively impact its community, operational processes, and risk mitigation strategies.

An easy to use, enhanced situational awareness security and control infrastructure that scales to the Newport Mesa Unified School District needs

The XProtect video surveillance management system is an open platform technology which uniquely enables the customization of a centralized video surveillance system capable of integrating with over 12,000 IP-cameras, multiple access control systems, with customizable deployment and support methodologies.

This means that the Newport Mesa Unified School District can benefit from leveraging several centralized or distributed video sharing applications, improved technology systems, and data analysis capabilities to enable real time, data-driven, problem-solving-based situational awareness methodologies.

Milestone's network video surveillance management system can be designed to suit the needs of the Newport Mesa Unified School District well-defined enhancement strategy which can reduce the number of crimes and misconducts within its facilities.

Highlights of our proposition that differentiates Milestone's solution include:

- Access Control/Third Party Integrations – Milestone's XProtect VMS software integrates with a wide range of third-party software applications including access control (Open Options, RS2, LenelS2) and video analytics (either camera or server based). With over 3500 Milestone Technology Partners, the Newport Mesa Unified School District can leverage cost-effective and best in class solutions to increase its security operational productivity and situational awareness as well as futureproof its system because NMUSD has the freedom to add innovative technologies as they are developed.

- Multiple surveillance methods - Unlimited XProtect Smart Clients, XProtect Web Clients, Milestone Mobiles and Smart Walls allow the ability to access video from various

locations, as well as multiple computer types, smart phones, tablets, and mobile devices.

- Lowest Total Cost of Ownership – Gain key comparative total cost of ownership experience for current/future facilities and IT operations performance with free MIP SDK connections, free device packs for cameras, and free VMS pilot programs. As well as reduced maintenance cost with Milestone Care, hardware costs, number of incidents, and improved loss prevention processes.

Build for the future, unite existing systems

Our solution is powered by the award-winning Milestone XProtect video management software, MIPSDK (Milestone Integration Platform Software Development Kit) and ONVIF bridge which has the flexibility designed to work with other systems, software, and technologies. Thus, the Newport Mesa Unified School District can take advantage of the entire industry's innovation in the future and add new technologies as they are developed.

Direct Training, Certification, and Support to NMUSD

Customer direct on-site pre/post-sales support and training options - Milestone has designed a set of services to help Newport Mesa Unified School District succeed. They include a service and support program that takes care of your product throughout its entire lifetime (including direct support options), a portfolio of system deployment and optimization services, as well as various training options which are listed below. Additional information on these offerings is explained in Section 4.

- Milestone Care (Plus & Premium)
- Milestone Professional Services
- Milestone Learning and Performance Training Program
- Milestone Developer Community
- Milestone Presales Support
- Milestone Technology Partner Program
- Milestone Pilot Program

Milestone's Professional Services Team offers a diverse portfolio of services to enhance the deployment and lifecycle of your XProtect system.

The strength of the Professional Services team lies in our ability to collaborate with our system users and design a strategy that fully leverages the capabilities of the XProtect platform.

Our PreSales and ProServices Services team can maximize the system user's investment and ensure that the projected benefits of the XProtect system are realized to their fullest potential.

By optimizing the capabilities, reducing the downtime and complexity of the system, Professional Services facilitates an increased return on investment and improved system productivity for their deployments or project management needs.

These services typically:

- Reduce long term cost in areas such as overall support, planning and overhead
- Are short-term project-based engagements ranging in duration which is determined by the system size and complexity
- Offer factory support for advanced implementations to decrease support related issues
- Decreasing project costs by minimizing system down-time, and reduction in resources/ time allocation required
- Service engagements include planning sessions, upgrades, deployments, etc.

The ProServices team at Milestone can be engaged and utilized to help aid in the initial deployment, for future upgrades or to help Newport Mesa with preventive maintenance and diagnostic services to ensure the XProtect system is running at peak performance.

At Milestone, we can be as involved with end users as they want/need us to be. We understand that maintaining your security systems is business-critical and needs to be treated with the highest regard, which often means engaging with the manufacturer directly. It is common for customers to want to supplement the Milestone dealers with installation and service of their security systems, since ultimately, they are responsible for the security of their people, property, and assets.

Products and Services to the District - Integrator/Partner responsibilities

Milestone products are sold through a two-tiered channel model. Our sales partners include distributors, and Access Control manufacturers (ACRE/LenelS2) who can resell Milestone products to certified Milestone system integrators in the Orange County area.

Both ACRE and LenelS2 can resell Milestone products and services to their dealer channel who is also trained and certified on XProtect. The distribution partnership with ACRE and LenelS2 provides customers with a lower total cost of ownership as integration fees are waived if Milestone is sourced through the access control partner, a single purchase order can be issued, and a single integrator can be selected with familiarity and responsibility of installing and servicing both integrated solutions.

Information and contact information for the local Milestone dealers is listed below in Section 10 of our RFP response. We are also happy to help identify shared dealers with our Access Control solution partners during the NMUSD manufacturer selection process.

4. Solution Narrative – System elements, integrations, deployment, and support

Newport Mesa Unified School District has identified their ideal deployment would be a tightly integrated solution with Access Control and Video Management that can support 40 simultaneous users, 50 workstation locations, 30 video recorders (1 per facility) and 406 cameras. The proposed solution to NMUSD would be a centrally managed ***XProtect Professional+*** system which can scale to support unlimited cameras, supports unlimited clients (thick, thin, mobile app), and fully supports dozens of integrations to Mercury based access control products. Based on the short-listed products from NMUSD's initial RFI, we have worked to provide a comprehensive response to this RFP that outlines integration capabilities with access control products that were short-listed (Open Options, RS2, LenelS2).

We understand exploring ***analytic options*** is also a key consideration and Milestone customers can take advantage of any of the growing analytic capabilities that are now available with the latest and greatest cameras that are coming to market from Axis, Bosch and Hanwha that support edge-based analytics. The metadata from these market leading camera manufacturers can be sent to XProtect to enable expedited search functionality and alarm notifications based on configuring analytic alarm events within the XProtect system.

Should customers want to take advantage of sophisticated ***analytic capabilities without having to replace their current cameras***, Milestone now offers customers the ability to add XProtect Rapid Review to their XProtect system. XProtect Rapid Review provides customers the ability to leverage Video Synopsis, a patented technology that displays hours/days of footage in a single view and then forensically filter by object type, attire, color, appearance similarity, license plate, direction and more. This product offering is particularly compelling if customers have a large deployment of cameras they do not want to replace soon.

Milestone XProtect VMS is designed for all deployment sizes and ***deployment methodologies*** (on-premises, virtualized environments, hybrid, and cloud solutions). If NMUSD goes with a traditional on-premises video storage solution to start, they can easily take advantage of offloading video storage to the cloud in the future if desired. XProtects flexible deployment methodologies allows customers to easily scale and modify their approach down the road, which becomes particularly handy if/when expansion happens in the future and customers still need to meet required storage requirements while not wanting to invest or install additional hardware.

The management interface enables the efficient administration of the system, including all cameras and security devices, regardless of the system's size or if it is distributed across multiple sites. The Smart Client interface is the main client for the VMS, offering a single pane

interface for most integrations as well as a full set of advanced features and designed for day-to-day use by dedicated operators.

Newport Mesa Unified School District can manage complexity with certainty

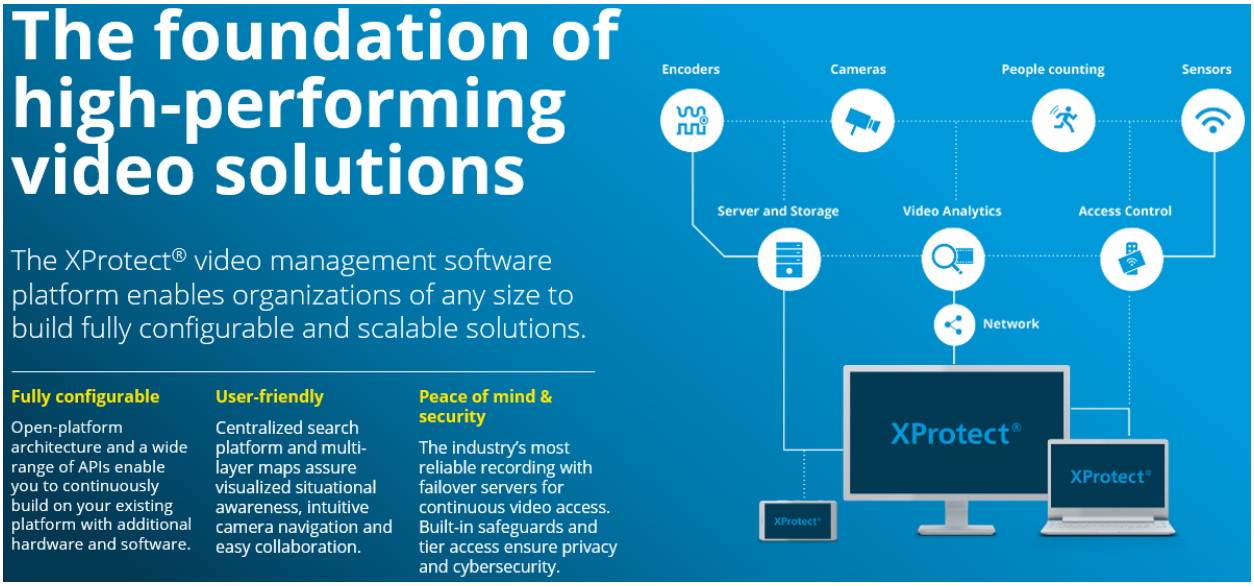
Our open platform video management solution allows for powerful integrations, extensive functionality and enables you to adjust the scope of your system, while also giving you the option to manage your system cost-effectively.

- Select the cameras, hardware and software that meet your needs and budget
- Choose the most cost-effective storage solutions (on-premises or cloud)
- Reduce the cost of migrating to IP-based by leveraging existing cameras

Newport Mesa Unified School District can explore opportunities with confidence

We empower you to explore unfamiliar territory and rethink your existing processes with solutions that enable you to fully benefit from the positive power of intelligent use of data derived from video recordings.

- Invent new business models driven by Artificial Intelligence (AI) and data derived from surveillance
- Drive innovation and define the future in your industry with help from the global collaboration within the Milestone Community



Key benefits for the Newport-Mesa Unified School District are:

- Situational awareness: Maintain an overview of an entire surveillance system with access to all cameras and locations.
- Scalability: Scale the system to any size, from small systems to systems consisting of thousands of cameras.
- Flexibility: The open architecture of Milestone XProtect, together with the Milestone Integration Platform Software Development Kit (MIP SDK), allows for powerful integrations, extensive functionality and enables users to extend the scope of their systems.
- Certainty: Redundancy capabilities ensure uninterrupted video recording in the event of component failures or network outage.
- Cost efficient storage: Flexible storage options make it possible to set up cost-efficient archiving features that meet the organization's needs.
- Ease of system management: Security system managers receive alerts and notifications when potential issues arise, enabling them to proactively manage the system.
- System optimization: Users can optimize system performance while the system is operational without disrupting video surveillance and recording

XProtect VMS Features (Pros for NMUSD stakeholders)

- Edge Storage with flexible retrieval: A redundancy option that ensures continuous recording of video. Recordings can be retrieved from camera storage based on time schedules and events.
- Video storage monitoring: Easily detect deviations from defined storage policies in situations where video data is overwritten prematurely due to insufficient physical storage.
- Unlimited system scalability: Supports an unlimited number of cameras, users and sites.
- Centralized single management interface: Provides efficient system administration of all connected cameras and devices, regardless of system size or distribution.
- Customizable user interface: Optimize system management interface for different roles and level of administrative users.
- Advanced rights management: Supports inherited user rights and the ability to assign partial management rights.
- Milestone Interconnect™: The top-level VMS product can interconnect with all XProtect VMS, Milestone Arcus and Milestone Husky products providing central operation and cost-effective management of geographically dispersed surveillance sites.
- DLNA Server: The DLNA server runs as a dedicated service, allowing it to be installed either on the same server as other system components.
- Multi-layered maps: A comprehensive overview of cameras and layouts of the entire surveillance installation allows for quick detection of trouble areas.

- Hardware accelerated video decoding on the Smart Client using multiple NVIDIA cards: Video decoding is done to significantly reduce the CPU load and improve performance of the recording servers. Video decoding done in the GPU part of the Intel CPU (requires CPU with support for Intel Quick Sync Video) and in the GPU of additional external NVIDIA cards.
- Alarm Manager: Provides a consolidated overview of security and system alarms for immediate visual verification.
- Bookmarking: Flag video sequences of particular interest and add descriptive notes, enabling users to easily share information and increase efficiency in investigating incidents.
- Centralized Search in Smart Client: Dedicated tab for searching recording sequences, bookmarks, motion, vehicle, people and location. These Search categories can be combined, also with third party search agent plugins.
- High-performance Recording Servers: Multi-stage video storage including video grooming possibilities provide efficient long-term storage, while all video remains online.
- Strict user rights: Protect the integrity of live and recorded video by restricting permission to specific cameras, functions and time periods or controlling individual user access.
- Metadata framework: Features generic framework for handling and storing video-related metadata.

Integration options:

- Milestone Integration Platform Software Development Kit (MIP SDK) enables seamless integration of video analytics algorithms and other third-party applications in XProtect Smart Client and Management Client
- XProtect® Rapid Review: XProtect Rapid REVIEW is an advanced forensic analytics solution that enables rapid video review, search, and analysis. No more countless hours behind a screen watching endless footage. Seamlessly integrated into XProtect, it lets you review hours of video in minutes, and pinpoint people and objects of interest to immediately turn that information into evidence and action.
- XProtect® Transact and XProtect® Retail: Integrate video surveillance with ATMs, point-of-sale (POS) and enterprise resource planning (ERP) systems for managing loss prevention and fraud.
- XProtect® Access: Video enabled physical security, which integrates with access control and intrusion systems.
- XProtect® LPR: Automatic reading and tracking of vehicle license plates.
- Generic event integration: Enables easy and fast integration of third-party applications and systems via a simple message-based socket communication interface
- Milestone ONVIF Bridge: Enables full video interoperability in multivendor installations using a standardized ONVIF compliant video-out interface

- System configuration API: Enables external applications to make changes to the system's configuration. REST API and API gateway enable external applications to make changes to the system's configuration.

Milestone – Access Control Integration

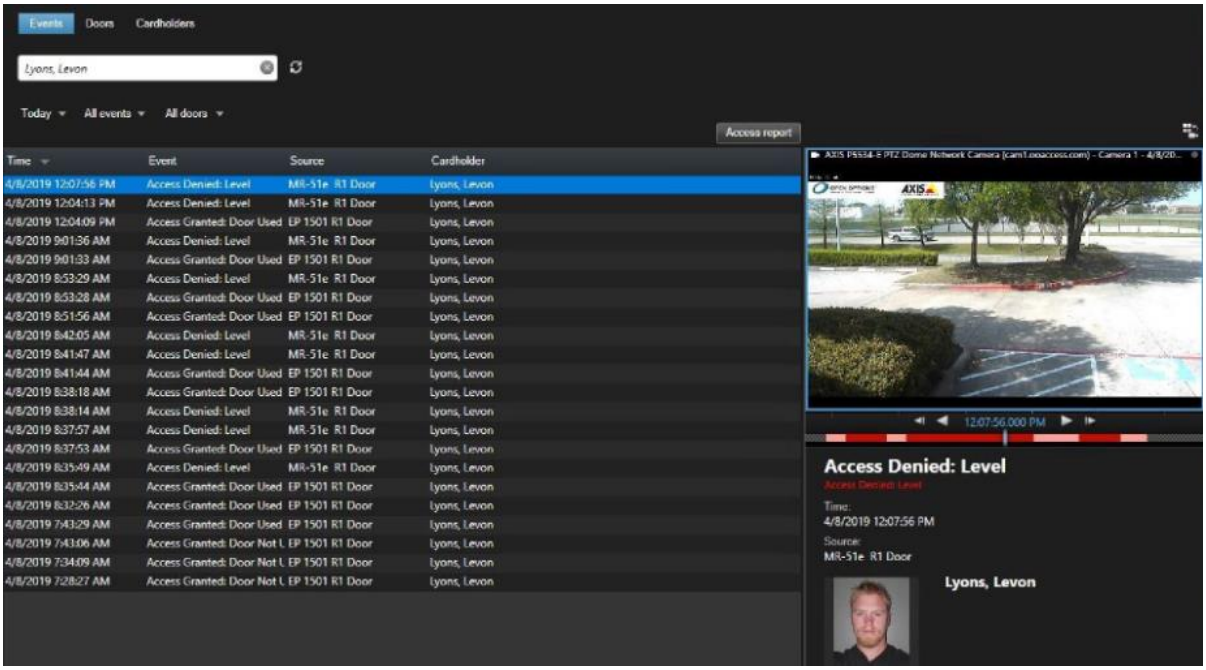
The Access Control integration between Milestone XProtect and many leading access control solutions is easy to use in the XProtect Smart Client User Interface. XProtect integrates with ACRE products (Open Options, RS2, Feenics), LenelS2 (OnGuard, NetBox, Magic Monitor), Motorola (OpenPath), Tyco Software House and many other access control solutions (20+).

Unlike other Video Management solutions that steer customers to their own proprietary access control solution, Milestone provides customers the freedom of choice, and with so many ACAM integrations, customers are not married to a single manufacturer should they want to migrate to a different ACAM in the future.

The bi-directional integration with Milestone's Access Control Technology partners allows NMUSD operators to display access control and alarms in a separate tab with associated video in the XProtect Smart Client. Also, operators can utilize standard XProtect video search, export, and review functionality. XProtect operators can use XProtect Map functions to display doors status on a graphical map, as well as lock and unlock doors. By using Milestone VMS as the viewing client, operators may also manage other third-party applications in the same user interface such as intercoms, people counting, heat mapping, loitering and other types of video analytics. These applications are installed separately.

XProtect VMS & Access Control Bi-Directional Integration allows:

- XProtect Rules engine support on Access Control alarms
- XProtect Smart Client Map support for door controllers
- Viewing access control alarm events in real time in the XProtect Smart Client



Additionally, this integration supports the following standard features that NMUSD operators can find value in:

• Retrieve and refresh configuration from the access control system, e.g., doors and event types.

• Receive access control event streams and hardware status changes from the access control system.

• Display and search cardholder information - both data and images.

• Create alarms in XProtect alarm manager based on ACAM events.

• Synchronization of alarm status between XProtect and ACAM.

• Association of access control events to cameras for simultaneous display of events and video.

• Association of access control hardware to cameras for simultaneous display of doors and video.

• Select and categorize events from the ACAM system to view and work with events in groups.

• Trigger system actions based on ACAM hardware events. For example: start recording, go to PTZ preset, display access request, triggered video for door forced, access granted, access denied, etc.

• Personalized login to support segmented database systems.

• ACAM hardware status display and command interaction on VMS client map user interface.

• Create customized access reports with video snapshots, based on search queries in XProtect Smart Client.

• Smart Client pop-up access request notifications.

• ACAM hardware interaction via XProtect web and mobile clients.

• Connect to the ACAM web administration interface from the XProtect Smart Client

• Reduced or waived integration license Fees if Milestone product is sourced from ACRE or a LenelS2, Milestone dealer.

For additional information, please see the following websites:

- LenelS2: https://www.milestonesys.com/marketplace/milestone-systems/lenels2-onguard-access-integration---xpa/
- ACRE Open Options: https://www.milestonesys.com/marketplace/open-options/dna-fusion-and-xprotect-access/
- ACRE RS2: https://www.milestonesys.com/marketplace/rs2-technologies/access-it-universal-net/

Video Analytics Options

Milestone Rapid Review - Add on – Analytic Option

With XProtect Rapid Review you get an intelligent video analytics solution that enables you to quickly review and analyze forensic video content to find what you are looking for, fast, with this easy-to-use Milestone Add-On software.



• Case management: Organize all video assets of an investigation in a single container, bookmark objects of interest and summarize case findings (including all relevant exhibits) in an exportable report, while dynamically collaborating on cases with other users.
• Video Synopsis: VIDEO SYNOPSIS solution simultaneously presents objects that have appeared at different times within the video. The result is a dramatically shorter video segment that fully preserves the viewer's ability to analyze the scene, enabling the review of hours of video in minutes and sometimes seconds.
• Multi-camera search: Powerful and advanced multi-camera search capabilities for all Rapid REVIEW search filters and Visual Layers.
• Proximity identification: Search for and identify the distance between individuals over time and location for compliance with physical distancing and contact tracing, as well as criminal investigations.
• Face mask detection: Forensically search and filter video to identify face mask usage.
•Face recognition: Accurate face recognition for rapidly pinpointing persons included or excluded in watchlists, based on images extracted from existing video or data uploads.
• License plate recognition: Differentiated license plate recognition, designed especially for "in the wild" surveillance scenarios and ease of operation in finding license plates through watchlists, existing video, or data uploads.
• Line crossing: Detect, filter, and count objects that cross a demarcation in a pre-defined direction to drive perimeter protection and directional object count.

• Appearance similarity: Instantly locate people, vehicles, and other items of interest by searching for objects with similar attributes.
• Visual layers: Create visual analytics for activity, dwell time, common paths, and background changes.
• Filter tolerance: Adjust tolerance levels to refine search results.
• Density & speed control: Increase or decrease the number and speed of events shown at once.
• Sort control: View events by relevance or by order of occurrence and easily zoom in on items of interest.

Additionally, a few of our third-party analytic partners include

- Briefcam https://www.milestonesys.com/marketplace/briefcam-usa/
- SenTRACK https://www.milestonesys.com/marketplace/sensen/sentrack/
- IPSOTEK https://www.milestonesys.com/marketplace/ipsotek/
- Agent VI https://www.milestonesys.com/marketplace/agent-video-intelligence-agent-vi4/
- All Go Vision https://www.milestonesys.com/marketplace/allgovision-technologies-pvt-ltd/
- Oosto https://www.milestonesys.com/marketplace/oosto-formerly-anyvision/

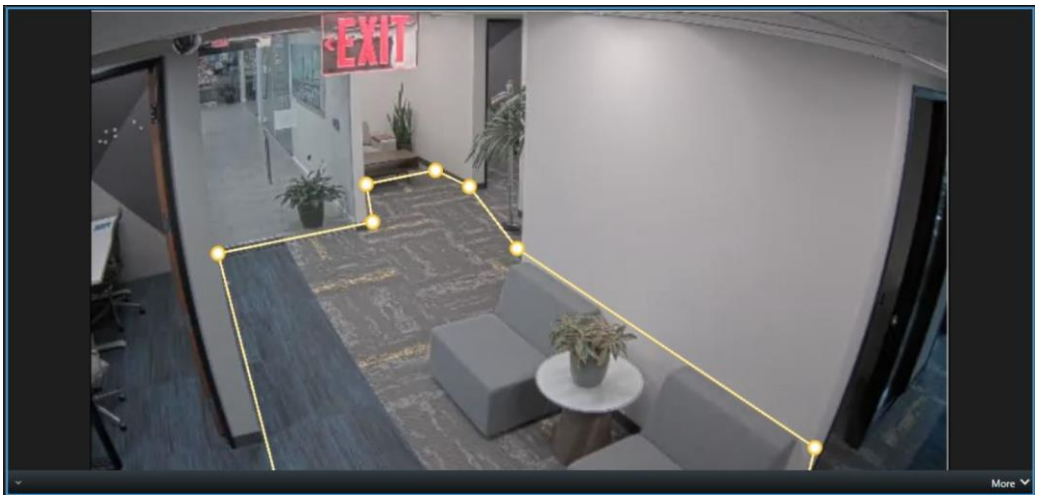
Intrusion Detection Integration Options

The Milestone XProtect VMS supports the ability to define and monitor perimeter control via partner and advanced cameras.

An example of a few third-party intrusion detection partners includes: (Perimeter intrusion detection system) PIDS as well as

- Spotter RF https://www.milestonesys.com/marketplace/spotterrf/ground-perimeter-detection--3d-drone-detection/
- Optex https://www.milestonesys.com/marketplace/optex-europe-ltd/lidar/
- Digital Barriers https://www.milestonesys.com/marketplace/digital-barriers-plc/
- FLIR https://www.milestonesys.com/marketplace/flir-networked-systems/
- MAGOS https://www.milestonesys.com/marketplace/magos-systems/

Most major IP camera manufactures provide internal or external in-frame perimeter detection.



Milestone Support

Milestone Care is a complete service and support program that takes care of a Milestone product throughout its entire lifetime. It helps ensure partners and end-customers, like Wayne County Airport Authority, can take full advantage of the product and get the most out of the investment.

The Milestone Care Basic service package is included in all Milestone products.

Designed for all Milestone customers as an effective way to learn, operate, and maintain the solution and take full advantage of its capabilities, it provides:

- Access to extensive self-help resources in an easy-to-navigate eCare support portal
- Free online eLearning courses
- Live chat assistance
- New Device Pack every second month
- Unique 30% trade-in credit on software products when upgrading

Additional Milestone Care packages

Designed to provide peace of mind, the Care program includes two additional packages. So, whether the need is frequent software updates, 24/7 access to Milestone Support, or critical incident resolution, there is a package that fits.

Milestone Care Plus



Milestone Care Premium



Milestone Care Plus

Milestone Care Plus is a sub-package belonging to the overall Milestone Care service and support program. Milestone Care Plus is designed to ensure that the installation is ready for the future. Whether the future brings new technological innovations or responses to security challenges, this package helps keep the system up-to-date and ready to react quickly to changes and opportunities.

Three annual product updates - With instant access to new software updates three times annually, users are given access to all the releases' new capabilities, all intended to make the product better, safer, and more powerful. With three releases a year, users get the ultimate peace of mind because potential threats or challenges in the IT landscape are instantly addressed via frequent product updates.

System health monitoring - Ensure a continuously functioning system by giving resellers access to the Milestone Customer Dashboard. It provides a complete overview of the health and performance of a system. Customer Dashboard is an online system health monitoring service for your system integrator or system administrator that monitors a system and notifies the reseller of potential technical incidents that need attention.

Full return on the investment - The present security installation might meet current needs, but in time, users may wish to expand the installation or upgrade it to a more advanced Milestone solution. With Care Plus, users receive the full trade-in value (100% credit of original purchase) when upgrading to a more advanced product – providing a cost-effective way to adapt the system to changing needs and providing full return on the investment.

Milestone Care Premium – Direct End User Support

Milestone Care Premium is a sub-package in the overall Milestone Care service and support program. When support cannot wait for Monday, Milestone Care Premium acts as an extension to Milestone Care Plus and is primarily designed for business-critical installations that want to ensure that any potential system issues are addressed promptly. Care Premium supplements the service and support already provided via our broad and highly qualified network of resellers and integrators.

24/7 access to Milestone Technical Support - With access to our worldwide support teams, all specialists in our products, users can rest assured that any potential issue with the Milestone product will be dealt with quickly and with a minimal disruption to the business.

Prioritized support - Based on a service-level agreement with committed response times, Care Premium ensures prioritized support, in English, and that critical issues are addressed promptly.

Support in selected languages - Localized support allows users to engage with Milestone's experts in their preferred location and, where possible, in their preferred language.

Please reference the provided Milestone Care Policy and Milestone Care Premium Agreement (SLA).

Milestone Technical Support

At Milestone, we understand the importance of providing excellent support for all our users. We deliver this by providing support through a global network of Authorized and Certified Milestone Partners who have trained in our products and solutions. As a Milestone user, your first contact for support should be your local Milestone Partner. If needed, your local Partner can engage the Milestone Technical Support engineers, giving you an additional level of support. If you cannot contact your local Partner, Milestone Technical Support is also available to help you directly and can be contacted during the support times listed below.

- North America is supported from Lake Oswego, Oregon, USA.
- North America's Support e-mail support@milestone.us or phone 503-350-1100 select '2' for support.
- Support hours are 6:00am - 5:00pm PST Monday-Friday.

Additional Support Tools Provided by Milestone Includes:

User Forum - Find and share solutions with Milestone users around the world.

Download software - Get the latest software updates for your product (in English or 27 other languages).

Manuals and guides - Learn how to set up, use and troubleshoot Milestone products.

Knowledge Base articles - Milestone solutions for common support questions and issues.

Video tutorials - Watch videos on how to install and use XProtect

Online Assistance - is available through online support over a wide range of hours.

FAQ Listings - Milestone Systems offers e-mail support Monday through Friday during the hours of 6:00 am to 5:00 pm PST and 8:00 am to 5:00 pm CET. Web Support including FAQ's and Knowledge base solutions are available 24 x 7 at http://www.milestonesys.com/support

Milestone Learning and Performance

The Learning & Performance team aims to encourage and support people in the Milestone community as they progress on their journey from novice to expert - wherever they are, whenever they need it, and whatever their role entails:

- End-user operators, investigators, and managers
- Solution designers
- Deployment and service engineers
- Integration developers

We offer both instructor-led training classes and free online eLearning courses to help learners build the knowledge and skills needed to perform on the job.

eLearning and Video Tutorials - Our collection of eLearning courses provides convenient and immediate access to free, online training. We offer an ever-increasing number of eLearning courses for integrators and reseller partners as well as end-users. These courses are free and available 24/7 on a computer or tablet.

Popular eLearning courses include:

- Milestone Fundamentals of IP Surveillance Systems
- Getting Started with Milestone XProtect VMS
- Getting Started with Milestone XProtect Smart Client
- Designing Small to Medium Milestone XProtect VMS Systems
- Using the Deployment Best Practice Checklist

Many of our courses are also available in video tutorial format on the Milestone Systems YouTube channel Closed captioning options are available in multiple languages.

Instructor-led Training - Milestone's expert trainers teach classes around the world in several different languages. Our instructor-led training workshops use a combination of real-world scenarios and hands-on exercises to build the knowledge and skills necessary to successfully design, install, and configure Milestone XProtect VMS products. Those looking to dive deeper into Milestone products can attend our instructor-led training workshops.

Milestone Certifications: Applicable NMUSD Training Certifications

Milestone Certified Integration Technician (MCIT) - Milestone Integration Technicians install and configure moderately complex XProtect VMS installations with camera counts of 100-500 cameras.

Milestone Certified Integration Engineer (MCIE) - Milestone Integration Engineers install and configure complex XProtect VMS installations with camera counts of approximately 100-10,000 cameras, multiple Management Servers, multiple Mobile Servers, edge storage, multicast, clustering, and other advanced configuration options.

Milestone Professional Services

Milestone Professional Services is a portfolio of system deployment and optimization services designed to unlock the full potential of Milestone installations while optimizing the system performance for a problem-free and stable operation.

Quick Start-Up Service: The Quick Start-Up service is a remote installation and configuration service for new Milestone installations. Drawing on Milestone's broad system experience, the service ensures that the implementation is in accordance with best practices and that the system is tuned to ensure optimal performance for the specific customer application.

System Start-Up Services: The System Start-Up service is an onsite installation and configuration service for new Milestone installations. Drawing on Milestones broad system experience the service ensures that the implementation is executed according to best practices and that the system is tuning for optimal performance for the specific customer application. During the on-site service execution, the Milestone Engineer work together with the Milestone Partner and the end-customer, which not only ensures that everything is installed and configured properly, but also that competence about the installation is transferred.

Full installation and configuration of Milestone VMS: You need to install and configure a complex XProtect VMS on your own, or the task may take too long? Choose our team of experts to get a functional and properly configured XProtect system meant to last.

Upgrade Assistance Services: The Upgrade Assistance service is designed to assist end-customers who want to upgrade their existing Milestone XProtect software to the newest version, and gain access to the latest functions and capabilities. The service is relevant to customers that subscribe to the Milestone Care Plus service.

System Health Check Services: The System Health Check service is an audit of installed software and hardware configurations. This service ensures that the configuration of the installation is aligned with Milestone's best practices and ensures optimal performance. Observed deficiencies and system optimization recommendations will be documented in a service report and delivered upon completion of the service.

Customized Services: At the customer's request, Milestone can provide tailored and customer-specific solutions. All concluded service engagements are fully documented.

For additional information, see the following website https://www.milestonesys.com/video-technology/services/professional-services/

5. System Diagram (Architecture)

To enable scaling of thousands of cameras across multiple sites, the XProtect system consists of several components that handle specific tasks. You can install all components on a single server if the server can handle the load, or you can install the components on separate, dedicated servers to scale and distribute the load.

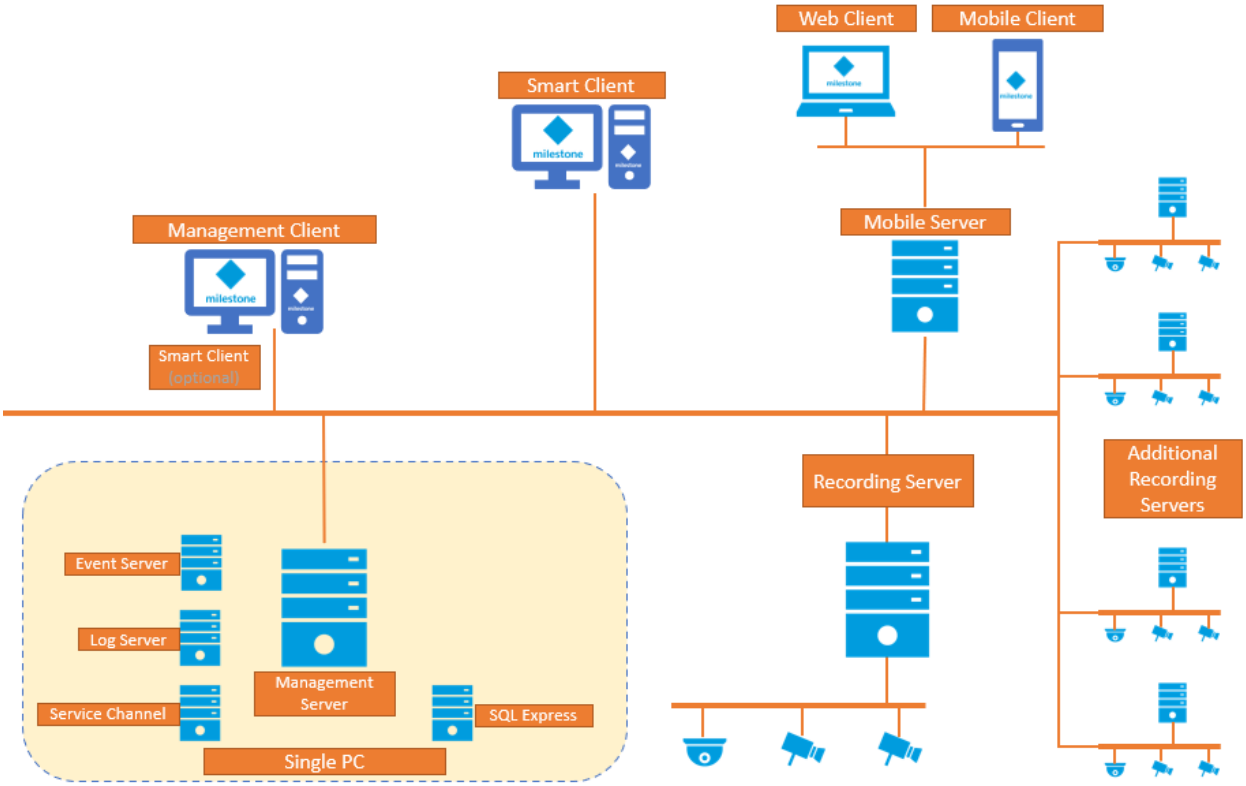
Depending on hardware and configuration, smaller systems with between 50~100 cameras can run on a single server.

For systems with more than 100 cameras, Milestone recommends that you use dedicated servers for all or some of the components.

You do not need all components in all installations. However, you can add them if the functionality they offer is needed at a later time, for example, failover recording servers or mobile servers for hosting and providing access to both XProtect Web Client and XProtect Mobile.

The diagram below shows an overview of the system components.

XProtect System Architecture



Our end-customers have flexibility in designing the IT infrastructure for Milestone XProtect VMS. Having the freedom to choose hardware allows the mixing of brands and technologies into optimized solutions with a reduced total cost of acquisition and ownership.

6. System Requirements

Milestone Xprotect VMS software runs on standard IT equipment

- Standard servers of your choice
- Standard storage of your choice; SATA, SAS, SSD, DAS, SAN, NAS, iSCSI, etc.
- Standard storage configuration of your choice; RAID 0, 1, 5, 6, 10, etc.
- Standard network equipment with configuration and layout of your choice including support for VLAN's, VPN, and firewalls etc.
- Standard certificate-based HTTPS encryption of network communication
- Integrates with the standard Microsoft Active Directory
- Use standard Microsoft SQL Server for storing the VMS configuration and logs

Xprotect Professional Plus 2022 R3 Software System Requirements

Name	Description
Operating System	Microsoft® Windows® 10 Pro (64 bit)
	Microsoft® Windows® 10 Enterprise (64 bit)
	Microsoft® Windows® 10 IoT Enterprise LTSB (Long-Term Servicing Branch)2016 (version 1607 or later)
	Microsoft® Windows® 10 IoT Enterprise, version 1803 or later (64 bit), IoT Core
	Microsoft® Windows® 11 Pro (64 bit)
	Microsoft® Windows® 11 Enterprise (64 bit)
	Microsoft® Windows® Server 2016 (64 bit): Essentials, Standard and Datacenter
	Microsoft® Windows® Server 2019 (64 bit): Essentials, Standard and Datacenter
	Microsoft® Windows® Server 2022 (64 bit): Essentials, Standard and Datacenter
	To run clustering/failover management servers, you need a Microsoft® Windows® Server 2016 Standard or Datacenter edition, Microsoft® Windows® Server 2019 Standard or Datacenter edition or a Microsoft® Windows® Server 2022 Standard or Datacenter edition
File system	For the Recording Storage Location, NTFS file system is recommended
SQL Versions	Microsoft SQL Server® 2014
	Microsoft SQL Server® 2016
	Microsoft SQL Server® 2017
	Microsoft SQL Server® 2019
Software	Microsoft® .NET 4.7.2 Framework
	Microsoft® .NET 6 Runtime
	DirectX 11 or newer

Hardware acceleration	Hardware acceleration with Intel® Quick Sync requires an Intel® CPU from 6th generation, supporting Intel Quick Sync and Intel® GPU enabled in BIOS.
	Using Intel® Quick Sync on Intel® CPU 12th generation, requires at least driver version 31.0.101.3413 from Intel.
	Decoding with NVIDIA graphics card is supported with GPU capability version 6.x (Pascal) or newer.

For additional information, see the following website
https://www.milestonesys.com/support/tools-and-references/system-requirements/

7. Cyber Security Program

At Milestone, we strive to ensure that our software and hardware is **secure by design, secure by default, and secure by deployment.**

Milestone XProtect VMS products are designed to provide end-to-end security against external and internal cybersecurity threats. Milestone XProtect VMS the perfect choice for organizations that focus on cybersecurity.

The Milestone XProtect security framework includes the following procedures:

- Network separation - Separating the camera network and the core server/client network with the recording server as a gateway between the camera and the system networks prevents direct routing between the two network segments, making it difficult to penetrate beyond that point.
- HTTPS secure camera connection - HTTPS communication between the recording servers and the connected cameras and other security devices provides bidirectional encryption of communication and prevents eavesdropping and tampering with the content of the communication.
- Strict server-side authorization - Authentication and authorization across all clients and integration interfaces are enforced on the server side for all services accessing the XProtect VMS system via the Milestone Integration Platform (MIP) SDK or Milestone ONVIF Bridge.
- Recording Server-server/client communication encryption – Certificate-based encryption on all clients and servers communicating with the Recording Server to guarantee their identification.

- Build on Windows security infrastructure – Milestone XProtect supports Windows Active Directory (AD), where both native Windows NTLM and Kerberos authentication may be used.
- Secure remote user access – A dedicated mobile server acts as a gateway to the system and protects its integrity when used by remote users. Also, the communication between the mobile server and the two clients supports HTTPS, which provides secure authentication and bidirectional encryption of all information exchanges, including user credentials, configuration, and media data.
- Secure system integration via MIP SDK – The same certificate-based encryption procedure and strict authentication and authorization policies are forced on all integrated third-party applications.
- External video access using Milestone ONVIF Bridge – External systems must run under a registered account to apply the same strict authentication and authorization policies on integrated applications and users.
- Protection of evidence material – When exporting forensic material, the video material can be password-protected, encrypted, and digitally signed.
- Federal Information Processing Standards (FIPS 140-2) Compliance - XProtect uses the latest encryption technology provided by Microsoft, making sure user information such as usernames, passwords, and devices are encrypted end-to-end, so you can rest assure that your personal information is always secure and projected. These developments include using only FIPS approved cryptography modules such as Microsoft's Cryptography New Generation (CNG).
- System hardening - Our continuously updated System Hardening Guide outlines best practices for system design, operating system configurations, servers, and workstations. It also provides input for cybersecurity policies, risk evaluation and mitigation.

For additional information, see the attached Milestone Hardening Guide and XProtect System Security Feature Brief.

8. Price Proposal

Software Licensing	Quantity of this Type	Licensing Cost	
		Unit	Total
XProtect Professional+ Base License	1	$393.00	$393.00
Device Licensing	406	$132.75	$53,896.50
Camera Device Packs (every two months)	1	$0.00	$0.00
Clients (Smart Client, Web Client)	Unrestricted	$0.00	$0.00
Mobile App (iOS & Android)	Unrestricted	$0.00	$0.00
Active Directory Integration	1	$0.00	$0.00
ACM: Access Control Integration Per Door	130	$0.00	$0.00
Camera Analytic Forensic Search (Axis, Hanwha, Bosch)	406	$0.00	$0.00
API/SDK (future development needs)	Free download	$0.00	$0.00
One Time Purchase Total:			$54,289.50
5 Year Annual Support - Optional	Quantity of this Type	Support Cost	
		Unit	Total
5 YEAR CARE PLUS (Annual Support)	406	$80.25	$32,581.50
Optional: 5 YEAR CARE PREMIUM (End User Direct Access Annual Support)	406	$36.75	$14,920.50
5 Year Total:			$32,581.5/ $47,502
Training - Optional	Quantity of this Type	Training Costs	
		Unit	Total

MCIT (Milestone Technical Training - I & II)	3 Day (remote)	3 Day (remote)	$1,595.00
Smart Client - End User Operator Training	2 Day (remote)	2 Day (remote)	$795.00
Remote Custom NMUSD Milestone Training	1 Day	1 Day	$1,900.00
Custom NMUSD Milestone Training	1 Day	1 Day	$5,000.00
E-Learning Training Courses (75+ courses)	Unrestricted	Unrestricted	$0.00
YouTube XProtect Training Courses	Unrestricted	Unrestricted	$0.00
Milestone ProServices - Optional	Quantity of this Type	Milestone Direct Service/ Support	
		Unit	Total
Install Assist (406 cameras)	1	406 cameras	$12,525.00
Upgrade Assist	1	1	$2,505.00
Mini System Health Check	Onsite/Remote Daily Rate	Onsite/Remote Daily Rate	$2,505.00
System Health Check	Onsite/Remote Daily Rate	Onsite/Remote Daily Rate	$5,010.00

Xprotect 2022 R3 License Structure

Milestone XProtect VMS solution has a transparent and simple license structure.

The Base License unlocks all software functionality and can be used on multiple sites when owned by the same legal entity.

A Hardware Device License is required per connected hardware device such as a camera or encoder (one hardware license per IP/MAC).

Milestone Care Plus (software assurance) is only required for the XProtect VMS installation for the first year and gives access to new product versions for free.

Milestone does not have hidden fees and does not charge for a wide variety of activities typically found amongst manufacturers.

- ✓ No additional license cost on storage devices or number of storage/devices used.
- ✓ No additional license cost for unlimited clients or client connections including Smart Clients, Web Clients, Android or iOS Clients, SDK-derived clients.

- ✓ No additional license cost for SDK utilization, or connections made by 3rd party applications.
- ✓ No additional license cost for Active Directory integration.
- ✓ No additional license cost for multiple servers, or server changes.

Server base license

XProtect server base license is mandatory for installing the product.

The base server license permits the following deployments within the legal entity purchasing the base server license:

• Unrestricted number of Management Servers

• Unrestricted number of Recording Servers

• Unrestricted number of XProtect Smart Clients, XProtect Web Clients and XProtect Mobile applications

IP device license

• To connect cameras, video encoders, NVR/DVR, video services or other types of video devices to XProtect, one device license is required per enabled video channel. For Non-Video devices, one license is required per IP device. License per enabled video channel rule do not apply for the multichannel cameras and encoders (up to 16 Channels) that are on the Supported Devices List and will require only one license per IP device. Mile-stone Supported Device List governs and provides information on the number of required device licenses for IP devices connected to and enabled in XProtect. Always refer the Milestone Supported Device List to see how many device licenses you shall purchase for your use of XProtect with IP devices.

• In total, for all copies of the product installed under this license, the product may only be used with IP devices as you have purchased IP device licenses for. An unlimited number of IP device licenses can be purchased. To extend an installation with additional IP device licenses, the base server license number (SLC) is required when ordering.

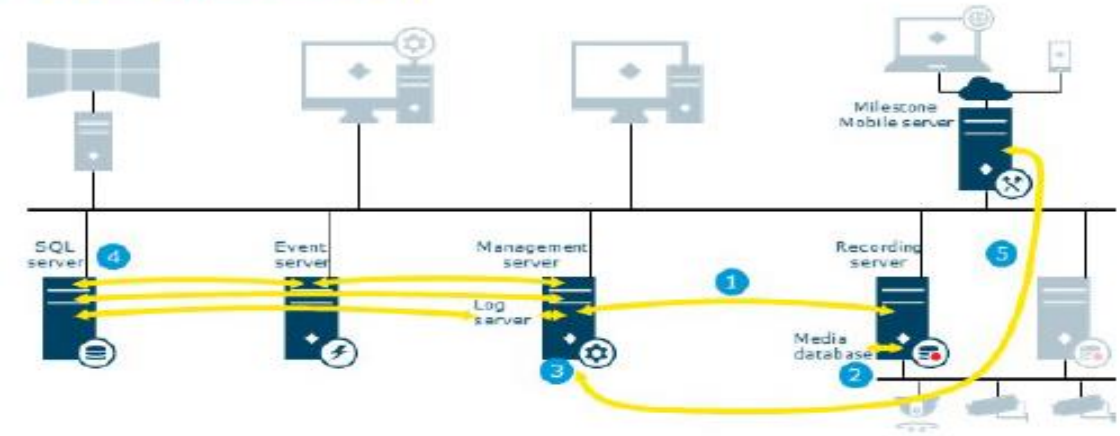
Licensing of Video Processing Service Driver (included in the MIP SDK)

• The Video Processing Service Driver when receiving modified video from any connected video processing system or any directly or indirectly connected device, requires one device license per enabled video channel.

9 Product data for each of the systems elements

System communication and data flow

Server communication



	Component	Port	Protocol	Bandwidth
1	Management server - Recording server	9993	TCP	1 kbit/call
2	Recording server - Media database	-	-	-
3	Management server - Internal	8080	UDP	1 kbit/call
4	SQL database communication	1433	TCP	1 kbit/call
5	Management server - Mobile server	80	HTTP	1 kbit/call

Server Components

Management Server

The management server is the central VMS component. It handles the system configuration, distributes the configuration to other system components, such as the recording servers, and facilitates user authentication.

The configuration is stored on a standard Microsoft SQL server installed on either the management server itself or on a separate dedicated server.

Recording Server

The recording server is responsible for all communication, recording, and event handling related to devices such as cameras, video and audio encoders, I/O modules, and metadata sources. Examples of actions the recording server handles:

• Retrieve video, audio, metadata, and I/O event streams from the devices.

- Record video, audio, and metadata from devices.
- Provide operators with access to live and recorded video, audio, and metadata.
- Provide operators with access to device status.
- Trigger system and video events on device failures or events.
- Perform motion detection and generate smart search metadata.

The recording server is also responsible for communicating with other Milestone products when using the Milestone Interconnect technology.

Event Server

The event server handles the tasks related to events, alarms, maps, and third-party integrations via the Milestone Integration Platform.

Events:

All system events are consolidated in the event server so there is a single place and interface for partners to make integrations that use system events.

The event server offers third-party access for sending events to the system via the Generic events or Analytics events interface.

Alarms:

The event server hosts the alarm feature, alarm logic, alarm state and handling of the alarm database. The alarm database is stored in the same SQL server as the management server uses.

Maps:

The event server also hosts maps. You configure and use maps in the XProtect Smart Client.

Milestone Integration Platform:

You can install third-party developed plug-ins on the event server and utilize access to system events.

You can get failover support on the event server by installing the event server in a Microsoft Windows Cluster. The cluster ensures that another server takes over the event server function in case the first server fails.

Log Server

The log server is responsible for storing all log messages for the entire system. The log server uses the same SQL server as the management server and is typically installed on the same server as the management server. If you want to, you can install it on a separate server if you need to increase the management or log server performance.

The system can create three types of logs:

a. System log: the system administrator can choose to log errors, warnings and information or a combination of these. The default is to log errors only.
b. Audit log: the system administrator can choose to log user activity in clients in addition to login and administration logs.
c. Rule log: the system administrator can use the rule log to create logs on specific events.

Mobile Server

The Mobile server is responsible for giving Milestone Mobile client and XProtect Web Client users access to the system. In addition to acting as a system gateway for the two clients, the Mobile server also can also transcode video as the original camera video stream in many cases is too large to fit the bandwidth available for the client users. Milestone recommends that you install the Mobile server on a dedicated server.

SQL Server

The management server, event server and log server use an SQL server to store, for example, configuration, alarms, events, and log messages. The XProtect Corporate installer includes Microsoft SQL Server 2012 Express which you can use freely for systems up to 300 cameras. For larger systems over 300 cameras, Milestone recommends that you use the latest SQL Server 2014 Standard or Enterprise on a dedicated server as these editions can handle larger databases and offer backup functionality.

XProtect Smart Client

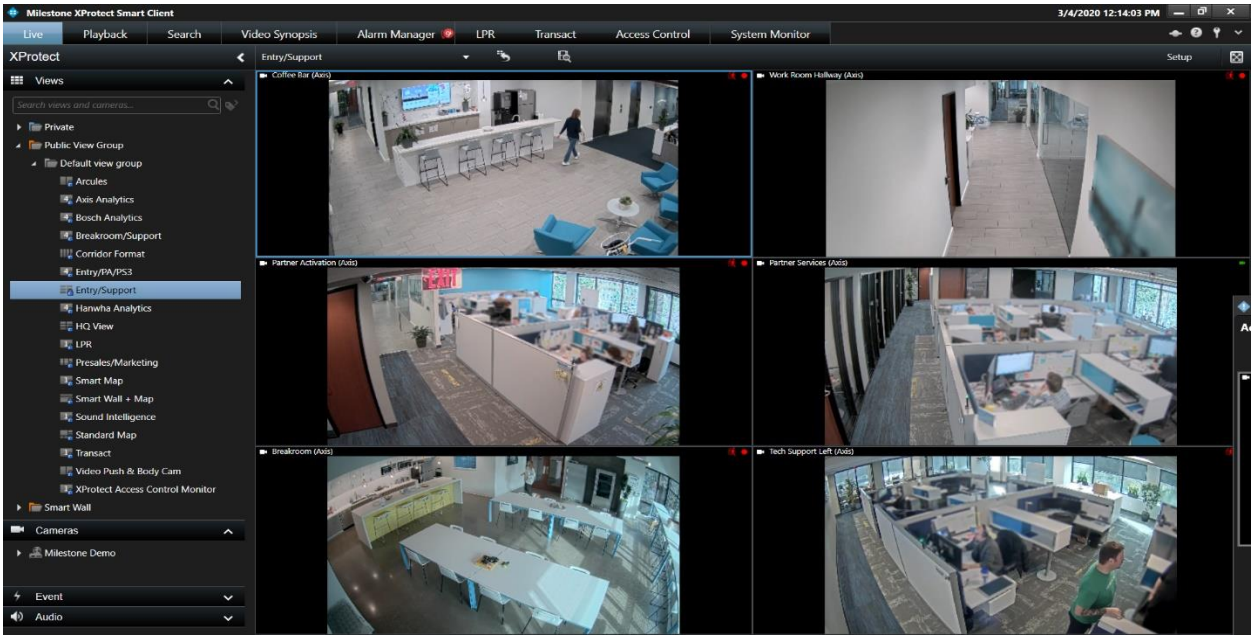
XProtect Smart Client is the main client for the VMS, offering a full set of advanced features and designed for day-to-day use by dedicated operators.

XProtect Smart Client is designed to run remotely from the operators' computer and supports multiscreen usage in full screen mode as shown below or in floating windows mode where the user can resize the windows and move them around freely.

NMUSD system users can easily gain intuitive control and unparalleled situational awareness via:

- Overlay buttons: Streamline workflows and improve operator efficiency by allowing operators to control cameras, camera-integrated devices, and other connected systems directly from the camera view.
- Virtual joystick control: Easily control pan-tilt-zoom (PTZ) cameras from an integrated on-screen window.

- Advanced multi-screen handling: Offers a general overview and enables users to efficiently work with many cameras across multiple screens.
- Seamless integration of XProtect add-on products: Operators can access and manage all XProtect add-on products directly from the Smart Client, optimizing their workflow when responding to incidents and alarms.
- Hardware accelerated video decoding on the Smart Client using multiple NVIDIA cards: Video decoding is done to significantly reduce the CPU load and improve performance of the recording servers. Video decoding is done in the GPU part of the Intel CPU (requires CPU with support for Intel Quick Sync Video) and in the GPU of additional external NVIDIA cards.



Effective incident response capabilities for the system users include:

- Alarm Manager: Single-point alarm function provides a clear and consolidated overview of security and system-related alarms and gives instant access to cameras for immediate detection of terrorist or other type security incidents.
- Bookmarking: Flag video sequences of particular interest and add descriptive notes to easily share information and increase efficiency in investigating incidents.
- Independent playback function: Replay events on one camera while simultaneously viewing live video from other cameras in the same view.

Easy evidence handling for NMUSD system users with:

- Integrated video timeline: Easy-to-use timeline with navigation, playback, and export controls to simplify the evidence collection process.
- Enhanced Centralized Search: Uses motion metadata to identify sequences quickly and accurately with motion in specific operator-defined areas of a camera view.
- Storyboard function: A vital tool that turns video into evidence by documenting a sequence of events from multiple cameras in a cohesive flow that allows for easy, objective, and straightforward revision. The technology helps to solve criminal or terrorist activity.
- XProtect® Smart Client – Player: A video viewer for evidence that has strong password protection and digital signing to prevent unauthorized access to exported video.

XProtect Web Client

XProtect Web Client is an intuitive, web-based interface to view, play back and share video. It provides instant access to the most common functions and is quick to learn and operate for users of all levels. Available in 30 languages, XProtect Web Client provides remote access to the surveillance system from all common browsers and computer operating systems.



XProtect Web Client runs on any Internet-enabled computer or device without installation, including optional browser plug-ins. It offers system scalability and an optimized user experience in systems with many users.

Simple to use features that NMUSD system users can find value in includes:

- Essential surveillance functions: Instantly view live video from one or multiple cameras, play back video recordings and control pan-tilt-zoom cameras. Counter terrorism mitigating work by operators can be performed from any location globally.
- Wide compatibility: Works with all of the most common operating systems and web browsers including Microsoft® Windows®, Linux, OS X®, Microsoft Internet Explorer®, Safari®, Google Chrome™ and Mozilla® Firefox®.
- Easy evidence sharing: Send video (AVI) or still images (JPEG) with other online users, eliminating the need to burn evidence to a DVD or put it on a USB flash drive.
- HTTPS support: Provides secure communication between XProtect Web Client and Milestone Mobile server.
- Output control: Even when off-site, users can trigger outputs, such as opening/closing doors and switching lights on/off.

XProtect Mobile Client

The XProtect Mobile client is a client designed for the user on the go. It offers easy access to live monitoring, playback and export of video, and access to activating system events and outputs.



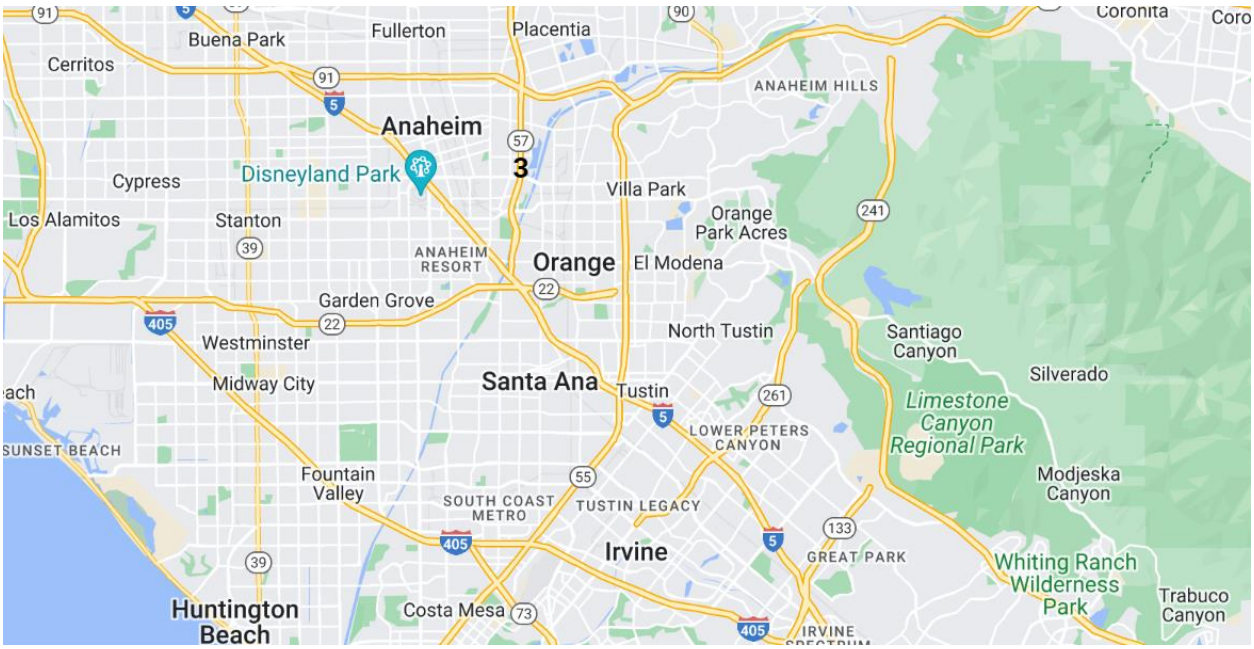
You can use the XProtect Mobile client as a remote recording device by using the device's built-in camera and the Milestone Video Push feature. With Video Push activated, video from the device's camera is streamed back to the VMS and recorded as if it is a standard camera.

With XProtect Mobile, system users can access the system from anywhere:

- Instant access anywhere: View and play back incidents and manage access requests on smartphones and tablets for uninterrupted security operations.
- Stay informed: Milestone Mobile includes push notifications, which notify you when alarms are triggered and when access is requested to your premises.
- Secure connectivity: All communication between the Milestone Mobile app and server is encrypted, ensuring superior security
- Easily share video: Take immediate action by creating and watching exports on-the-go.
- View video across distributed surveillance sites: Users can access cameras from all sub-sites in large, multi-site installations.
- Respond to incidents when they happen: Users can push live video from the device's camera directly into the XProtect system allowing you to document terrorist or other security incidents as they happen.
- Know exactly where to send first responders: Users can document the location of pushed video by associating a GPS position with the live video they capture.
- Address security situations promptly: When an alarm is triggered, push notifications are sent to designated users, so they can respond immediately when a situation arises.
  Control outputs remotely: Whether or not they are physically on-site, users can control outputs, granting or denying access, and switching lights on/off.

10 Certified Integrators

The new Partner Program has three Partner tiers: Authorized, Advanced and Premier. Partner eligibility for each tier is based on their engagement level and productivity. As Partners complete trainings, earn certifications and produce higher levels of revenue, they rise in the program tiers which unlocks more benefits and support options.



PREMIER

Stone Security, LLC (Corona, CA) *
Marvin Barnes (marvin@stonesecurity.net)
4 Latitude Way Ste 103-104
Corona, CA 92881
1-310-729-2481
Stonesecurity.net

ADT Commercial (5 locations in LA/OC Area)

Cory Schultz (crschultz@adt.com)
210 W Baywood Ave
Orange, CA 92865
1-714-685-8100
Adt.com

CML Security
Ron Green (rgreen@cmlsecurity.com)
2081 H Third St
Riverside, CA 92507
209-747-3607
Cmlsecurity.us

Convergint Technologies, LLC (2 locations LA/OC)*
Erik Freking (eric.freking@convergint.com)
2211 E Howell Ave
Anaheim, CA 92806
1-714-937-1440
Convergint.com

TRL Systems*
Gary Chavarria (gchavarria@trlsystems.com)
9531 Milliken Ave
Rancho Cucamonga, CA 91730
1-909-3908392
TRLsystems.com

Allied Universal Technology Services *
1815 E Wilshire Ave #910
Santa Ana, CA 92705
1-714-288-2227
Aus.com

Vector USA
Skyler Peterson (Speterson@vectorusa.com)
20917 Higgins Court
Torrance, CA 90501
1-310-436-1000
Vectorusa.com

Paladin Technologies*
Joe Morris (jmorris@paladintechnologies.com)
12742 Knott Street

Garden Grove, CA 92841
1-714-940-1783
Osf.digital

CDW Global
Daniel Cisneros (Danicis@cdw.com)
200 N Milwaukee Ave
Vernon Hills, IL 60061
1-619-813-8047
CDW.com

Continental Computers
Ronen Isaac (ronen@conticomp.com)
620 N Nash St Bldg. B
El Segundo, CA 90245
1-310-416-1200
Conticomp.com

ADVANCED

HCI Systems, Inc.
Jason Beardley (jbeardsley@hcisystems.net)
1354 S Parkside Pl
Ontario, CA 9171
1-909-628-7773
hcisystems.net

ASSI*
Bill Vuono (bvuono@assisecruity.com)
1370 Reynolds Ave Ste 201
Irvine, CA 92614
1-949-955-0244
Assisecurity.com

Secure Site Solutions
Michael Cowell (Mcowell@securesitesolutions.com)
14252 Culver Dr St A500

Irvine, CA 92604
1-714-458-8548
Securesitesolutions.com

Ollivier Corporation *
Charles Denney (Charlesdenney@olliviercorp.com)
8726 S Sepulveda Blvd Ste D311
Los Angeles, CA 90045
1-888-320-2220
Olliviercorp.com

AUTHORIZED

Enterprise Security, Inc.*
Beth Remmelsberger (beth@entersecurity.com)
22860 Savi Ranch Pkwy
Yorba Linda, CA 92887
1-714-630-9100
Entersecurity.com

IES Communications*
Ryan Letchford (Ryan.letchford@iescomm.com)
1350 Reynolds Ave Ste 107
Irvine, CA 92614
1-949-226-3752
iescomm.com

11 Complete and detailed copy of the RFP

Acknowledged

Milestone acknowledges the reception of RFP and addendum documents.

12 Completed Solution Deployment (Reference)

A summary of at least one similar and completed solution deployment with similar direct end user support as required by the district, preferably from a comparable K12 school district. Include project references and contact information.

Anaheim Union High School District

As one of the largest school districts in California, the Anaheim Union High School District office oversees 21 schools spanning 46 square miles across 20 campuses, including eight junior high schools, 10 high schools, two alternative education schools, and one virtual school. Responsible for the safety of 29,000 students and 3,000 employees, the district is among the top 10 largest employers in the city of Anaheim. Connected to five Orange County Police Departments, the system is designed to prevent petty crime and protect lives during an active shooter scenario.

Challenge: Proactively keeping students safe The Anaheim Union High School District (AUHSD) lacked a centralized video security system that would allow administrators to prevent, monitor, and investigate incidents on campuses. Ongoing occurrences of theft and vandalism were financially impacting the district. In addition, parents and staff members were increasingly concerned about active shooter incidents happening at other schools across the country.

Solution: Consolidated district-wide monitoring AUHSD expanded and upgraded its existing security infrastructure with a campus-wide solution using 1450+ Hanwha Techwin IP security cameras and DDN storage servers, plus fencing at all schools with strategically placed perimeter sensors — all integrated with the Milestone XProtect Expert open-platform VMS for easy monitoring, prevention, and incident investigation. Local law enforcement and Orange Country Public Safety have direct access to all the cameras and the VMS during emergencies.

Result: Decrease in property loss and added crime prevention
The Milestone VMS was selected based on a range of included features, ease of use, devices supported, technical support, performance, and cost evaluation. When an incident occurs, administrators can quickly access the VMS and review the security footage to investigate the

event. The VMS's consolidated view of all the cameras across the district helps improve response time to threats and incidents because administrators can precisely locate trouble spots and security breaches on campuses. Interactive, multilayered maps provide a comprehensive overview of cameras and layouts of the entire surveillance installation, allowing quick detection of trouble areas. The camera navigator increases visual verification — whenever a school administrator views a camera feed, nearby cameras are automatically displayed on screen, making it easy to switch between cameras to follow a moving object in different directions, helping to authenticate evidence of vandalism, theft, or other potential incidents of violence on campus. School administrators can quickly review footage of incidents by using the VMS's instant playback to view recorded video for one or more cameras. With smart search, an image can be searched for motion by time, creating thumbnail images for fast delivery of evidence to authorities. "The VMS also gives us the ability to better manage the cameras in terms of giving the appropriate people the appropriate permissions to only the cameras they need to see," said Greenwood. The VMS uses Active Directory, making it simple to manage user rights for many aspects of the system, including control of privileges and camera actions, which helps protect students' privacy. In addition, Greenwood found that Milestone licensing was favorable compared to other companies with its automatic online activation of system and camera licenses. The VMS gathers all camera information and automatically requests the corresponding licenses online, enabling faster deployment as newly added cameras are fully functional during a 30-day grace period.

Protecting lives during emergencies in terms of active shooter response, the hybrid on-premise VMS uses a cloud mobile server so that Orange County Public Safety and the police departments that serve the five cities located in the district boundaries can access the system during an emergency situation. With video sharing, law enforcement can view live feeds. Getting critical data to first responders is important when it comes to preventing or protecting lives during campus incidents.

Read the entire Milestone AUHSD Customer Story attached.

Anaheim Unified High School District
Erik Greenwood (greenwood@auhsd.us)
Chief Technology Officer
714-999-3765

Fullerton Joint Unified High School District
Brian Poetner (bpoertner@fjuhsd.org)
Electronic Technician, Cameras
714-870-2963

13 Other documentation

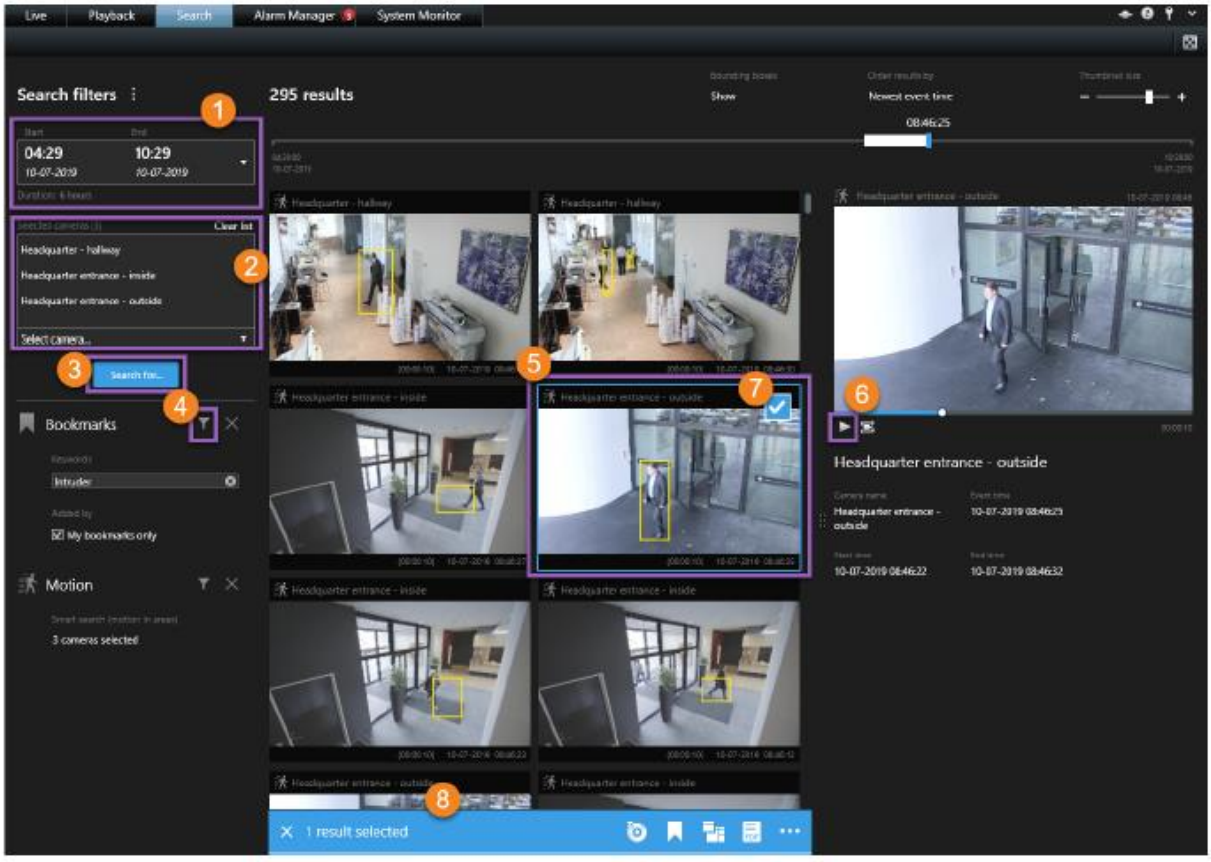
- XProtect Professional Plus CSI A&E Specification Sheet 2022 R3
- Milestone XProtect VMS Products System Architecture Document 2022 R3
- Milestone Cyber Security Development Policy
- Learning and Performance Catalog
- Milestone Care Document
- Milestone Hardening Guide
- Milestone-XPA-OnGuard-User-Guide
- Open-Option-Milestone-ACM-Plugin-Manual
- XProtect Rapid Review Product Sheet
- XProtect System Security Feature Brief
- ProServices Offerings Full List
- Milestone AUHSD Customer Story

14 Supplemental Data

Centralized Search

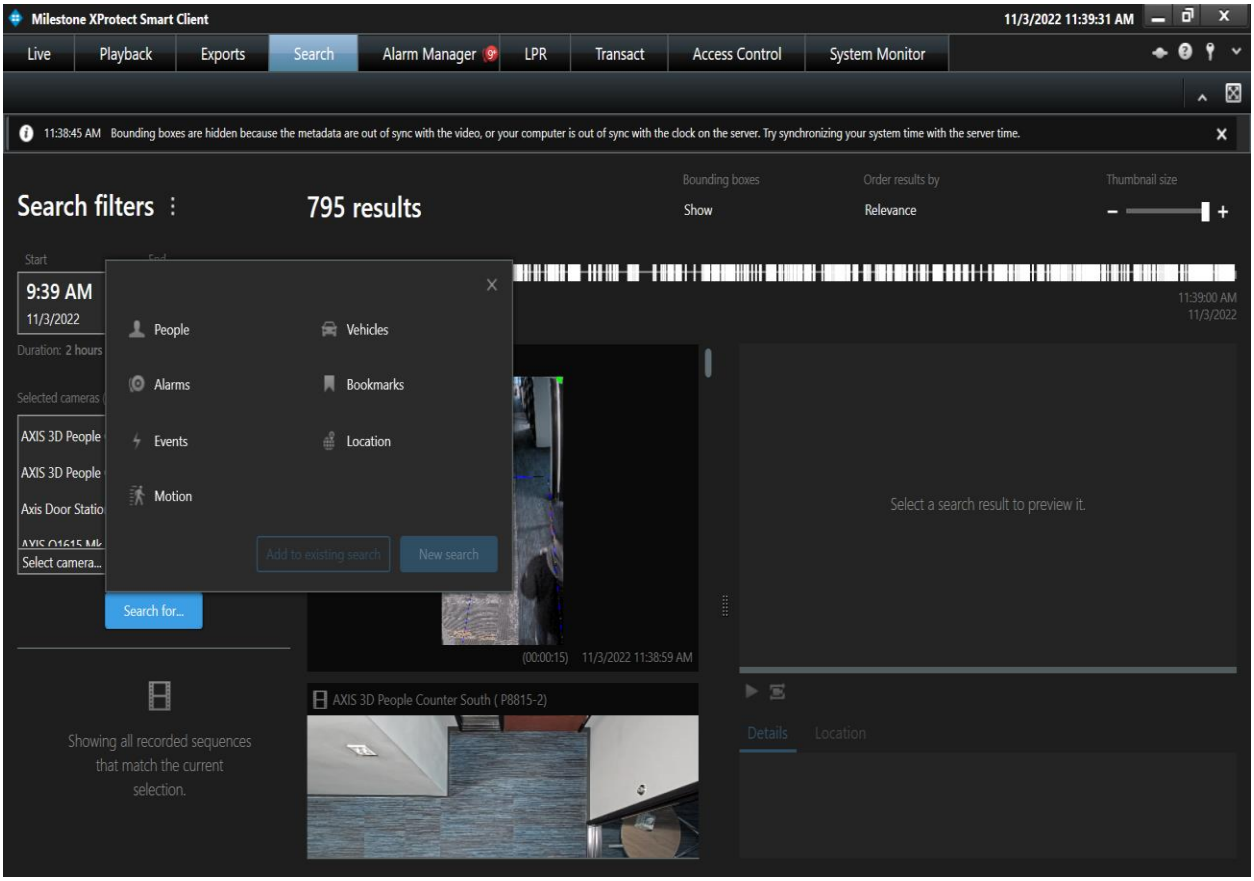
The new centralized search platform in XProtect Smart Client makes it possible for users to search for everything in one place. With the new Search tool users can search for motion, alarms, events, bookmarks, and other types of data, in one single place enabling rapid and efficient video investigations.

Moreover, the new Search platform also smoothly embeds partner integrations and their powerful analytic capabilities via dedicated filtering options. Through specific plug-ins and devices, search criteria such as line-crossing and object-in-field will be enabled directly in the Search Tab, saving time, and increasing efficiency.



1. Select a timespan, or define your own Custom interval (1)
2. Add the cameras by using the search function or selecting the cameras in the tree structure (2).
To add all the cameras within a view, click the name of the view.

3. Select the search categories (3).
4. Apply filters to narrow down the search results (4).
5. To preview video from a search result, select the search result (5) and click Play Forward in the preview area (6). To view the search result in full-screen mode, double-click the search result.
6. To make the search result actionable, for example to export or bookmark the video, hover over the search result, and select the blue check box that appears (7). The blue action bar appears (8).

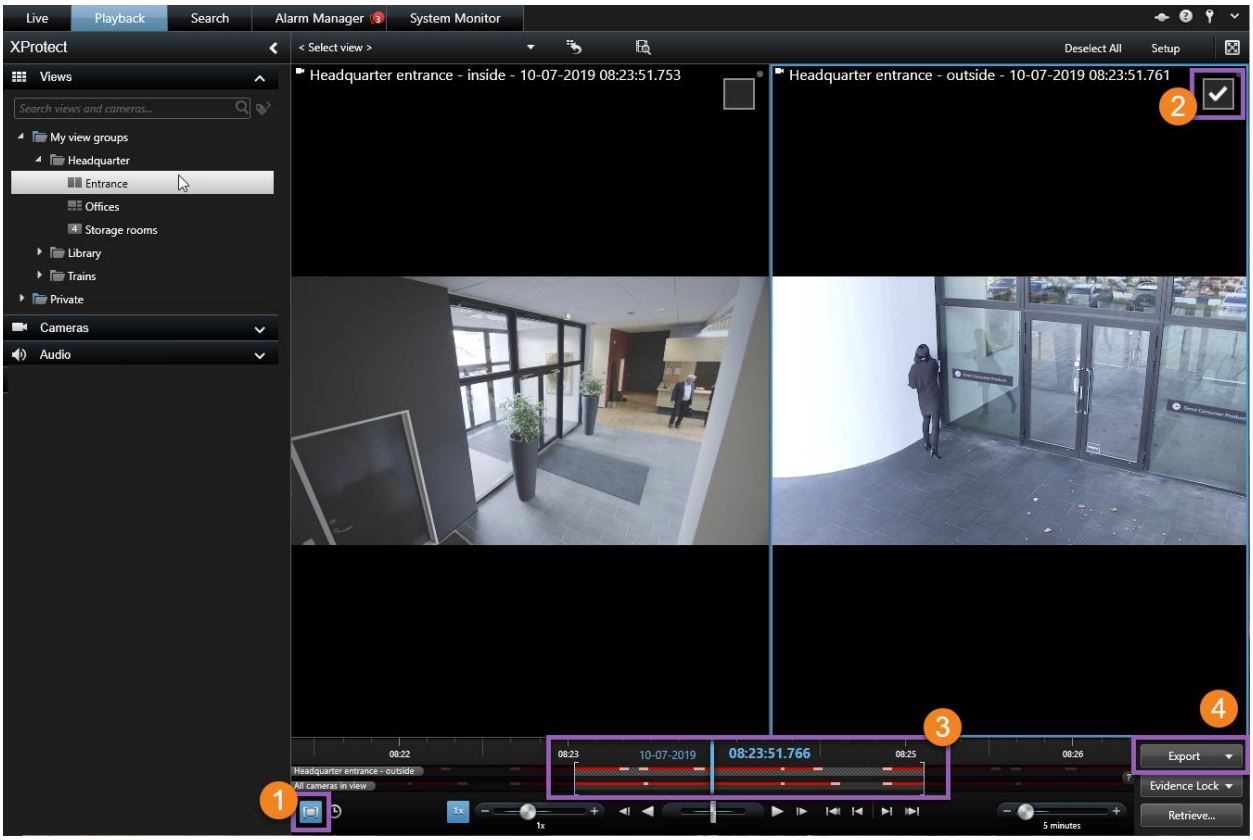


Motion, Bookmarks, Alarms, People, Vehicles, Locations and Events are the standard search categories. Depending on the data available in your VMS system, additional search categories may be available.

Export the video

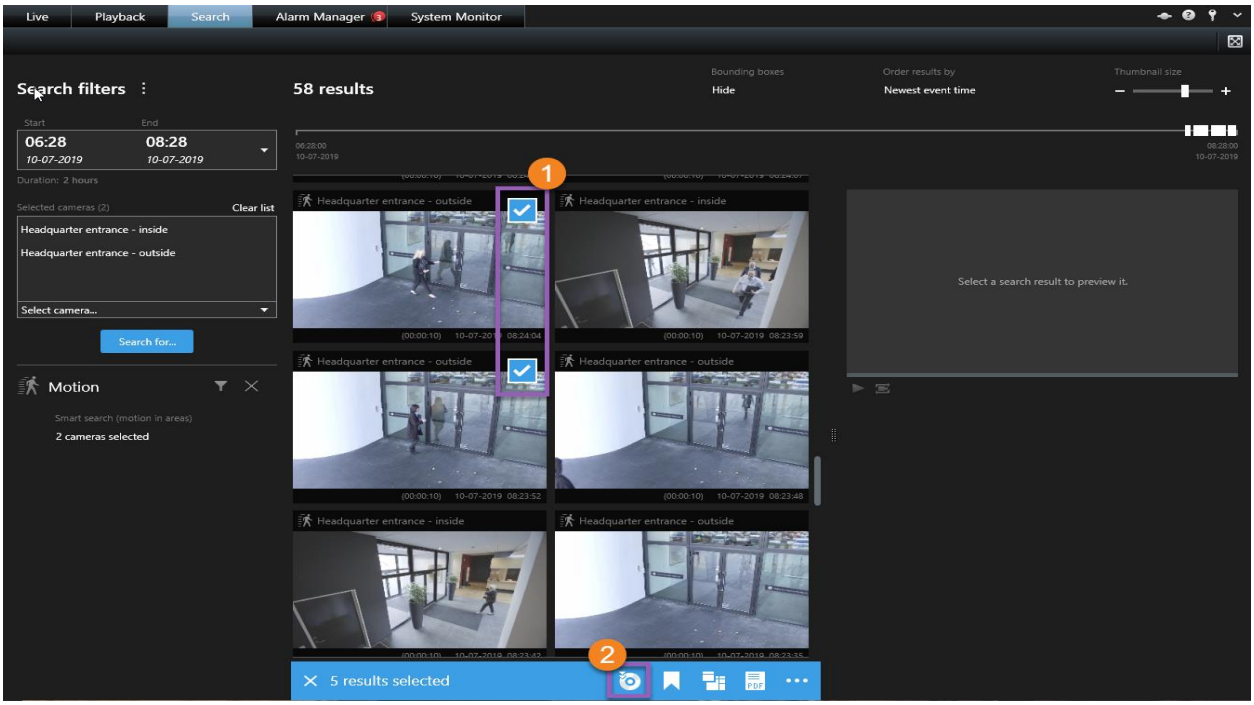
Deliver authentic evidence to public authorities by exporting video to various formats, including video from multiple cameras in encrypted XProtect format with dedicated player application included.

After you locate the video evidence, you can export it. The first illustration shows you how to export video on the **Playback** tab.



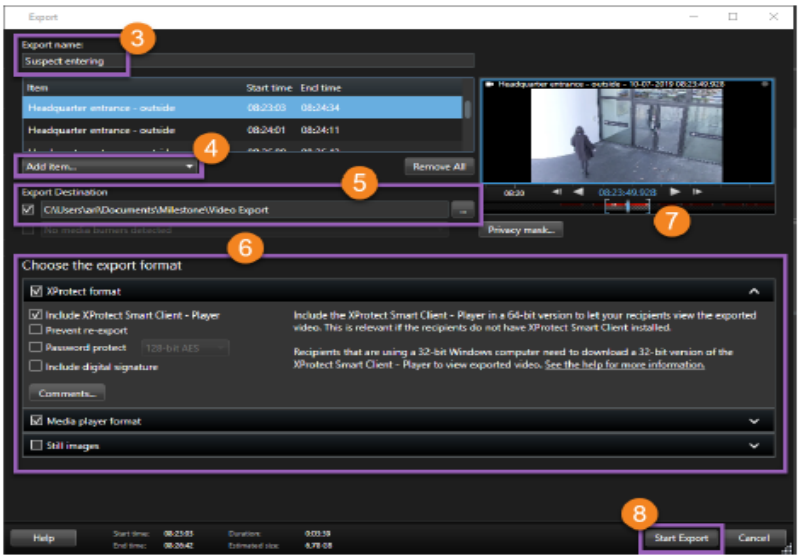
1. Click to turn on time selection mode.
2. Select the cameras you want to include in the export.
3. Drag the square brackets to select a start and end time for the export.
4. Click **Export** > **Export** to open the export window.

Start the export on the Search tab



1. For each search result you want to export, hover over it and select the blue check box that appears ❶.
2. In the action bar, select the export icon ❷.

Specify the export settings



1. Enter a name for the export file (3).
2. If needed, add more cameras (4).

3. Specify the export destination (5).
4. Select a format for the export (6).
5. To adjust the start and end time, use the square brackets (7).
6. Click Start Export to start the export (8).

Export and print functionality include:

• The snapshot function enables operators to produce instant visual documentation of a camera by saving the camera image to a file or sending it directly to a printer.
• The storyboarding function makes it possible to include video sequences from different or overlapping time intervals from different cameras in the same export.
• Export in XProtect format; including the standalone XProtect Smart Client - Player application for instant and easy viewing by authorities.
• Export preview with looped playback
• Create evidence material in media player format (AVI files), MKV format, or still image format (JPEG images).
• Disable re-export option to prevent undesirable distribution of sensitive evidence material.
• Bulk camera export in multiple formats to multiple destinations, including direct export to optical media, results in more efficient video exports and more secure handling of evidence material.
• Export comment function enables users to add general and/or camera-specific comments to a video ex-port when exporting to XProtect format.
• In media player format comments can be added as pre/post slides.

Sharing of Video

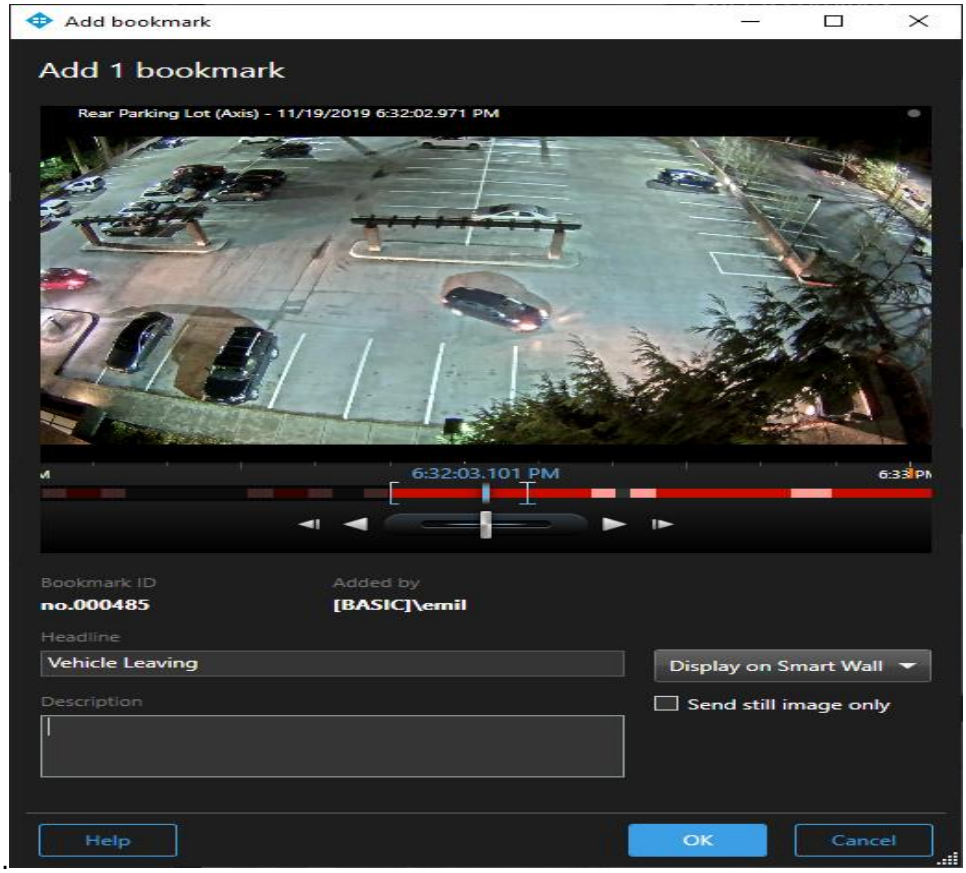
Video sharing is easily handled with the XProtect Corporate VMS to different departments and various Police authorities.

- The XProtect Smart Client supports centralized storage of shared and private camera views, enables coherent access to views across the system.

- The XProtect Web Client supports shared views that can be managed centrally via the server with administrator/user rights and user groups.

- The XProtect Mobile client automatically obtains the user's private and shared views from the system to be used as camera lists.

- The XProtect Bookmarking functionality allows users to mark video sections of interest and add descriptive notes for later analysis or sharing with other users.

I. 

- To facilitate efficient collaboration and information exchange in command-and-control centers, the Smart Map can be shared on Milestone's video wall solution, the XProtect Smart Wall. Operators may likewise send individual, or groups of, cameras on the Smart Map to the XProtect Smart Wall, through a few simple clicks.

Third Party Integrations

The Milestone XProtect Professional Plus VMS provides endless integration possibilities for the Newport Mesa Unified School District.

With access to more than 3500 Milestone Technical Partners you can find applications to meet your needs or even create your own solution with the MIP Software Development Kit.

Newport Mesa Unified School District stakeholders can integrate applications and business systems directly into XProtect VMS software through the Milestone Integration Platform (MIP).

Configurable third-party options include:

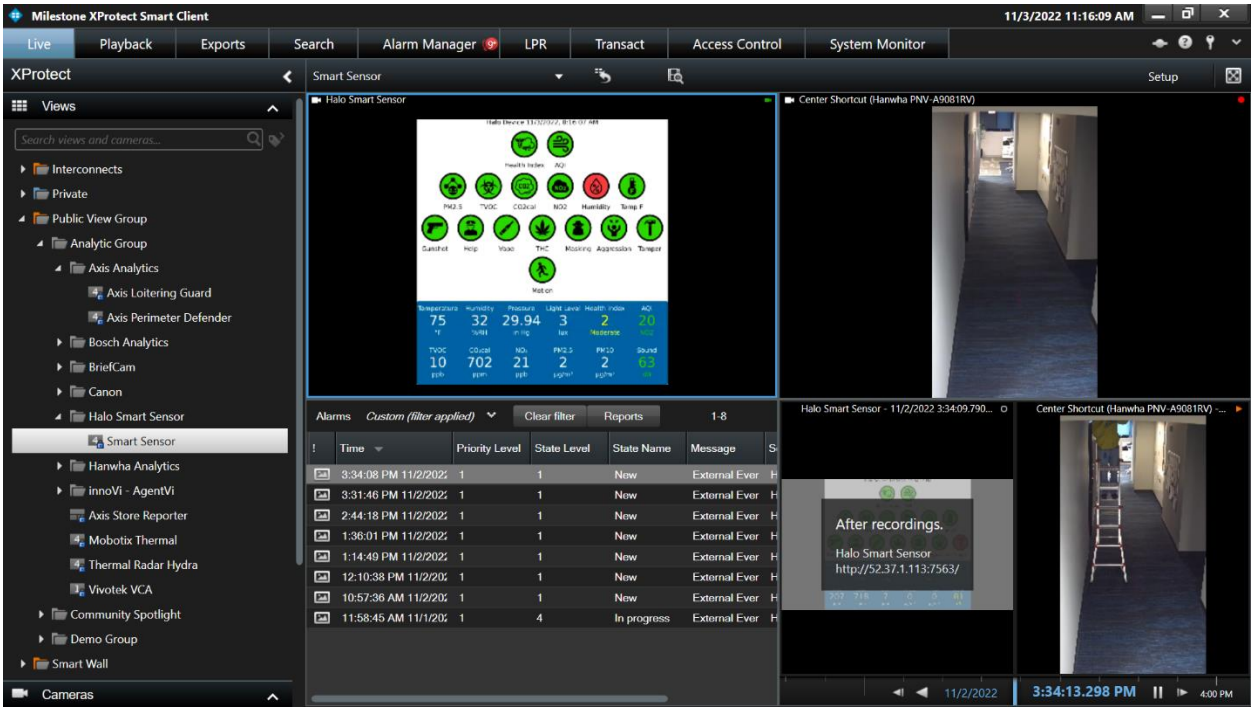
- Access control
- Audio
- Biometric
- Business Intelligence
- Cameras
- Event Handling
- Facial Recognition
- Fire Detection/Suppression
- HVAC
- Intercom
- Intrusion Panel
- License Plate Recognition
- Network
- Perimeter Protection
- Privacy Protection
- PSIM
- Server
- Storage
- Time Attendance
- Transactional Analysis
- Video Analytic
- Video Wall

For additional information, see the following website.
https://www.milestonesys.com/community/marketplace/start-exploring/

HALO Smart Sensor - The #1 Vape Detector and Indoor Air Quality Monitoring Device.

HALO IOT Smart Sensor is a multi-sensor capable of detecting vape, smoke, THC and shouting in areas a camera cannot be placed. Additional sensors give HALO the ability to monitor air quality for temperature, humidity, hazardous chemicals and more!

HALO helps those in education, healthcare, hospitality, real estate, manufacturing and more. HALO can detect staff and guest smoking and vaping, chemical spills in custodial closets and labs, and temperature, humidity, and moisture to prevent mold and illness.



HALO supplies Milestone VMS a MJPEG stream showing the current status/readings of its sensors. The XProtect Event Manager integration can discern the cause of the alarm and whether it is a set or reset of an alarm condition.

Email or text notifications can also be programmed. Notifications can include device name, IP address, event ID, threshold that was surpassed, sensor value, date of event, time of event.

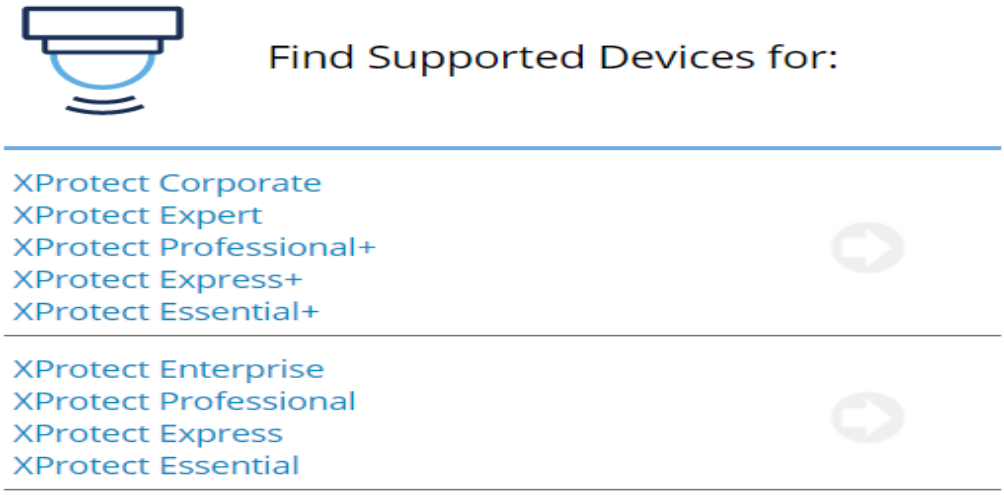
Key features that NMUSD operators can find value includes:

- HALO has 12 built in sensors and it is the only vape detector that detects THC oil.
- HALO connects directly to your security monitor and VMS - no need for separate applications. Uses Analytics in threshold levels and reporting.
- HALO can transmit alerts to Milestone when thresholds are exceeded using Generic Events, defined in the Milestone Management Client.
- Each of the unique sensors in HALO can have its own Event and Rules which can be executed when alerts match defined Generic Events.
- Sensors include: Vape, Smoke, Temperature, Humidity, Light, Chemicals, THC, Sound decibel levels, Air Quality, Pressure, and a Tamper alarm.

Camera Integrations

Milestone's XProtect Professional Plus VMS provides the ability to integrate with the newest cameras on the market as products are released. The Milestone open platform enables users to select best-in-class security solutions to its surveillance system as Milestone integrates with over 12,000 camera types.

As the open platform company Milestone is dedicated to ensuring that our XProtect® software works with the widest choice of devices. XProtect software supports IP cameras, encoders, and digital video recorders from over 150 manufacturers, and we are continually adding new products. With XProtect, Newport Mesa Unified School District has the freedom to choose the best hardware according to its specific budget and needs.



Elite Camera Partners Include:

- Axis Communication
- Bosch
- Hanwha Techwin

ONVIF Driver

Milestone is compatible with four ONVIF profiles – G, S, T and M – which means that Milestone XProtect customers can now benefit from a smoother integration between their ONVIF devices and the VMS – being able to use more device functions and bring more data on top of video and audio streams.

Universal Driver

The Universal driver is to be used when: (1) there is no dedicated driver for the device, or (2) the device is not ONVIF compatible. The Universal driver can be looked at as a stream media receiver/player. It does only receive multimedia streams and does not control the device in any way.

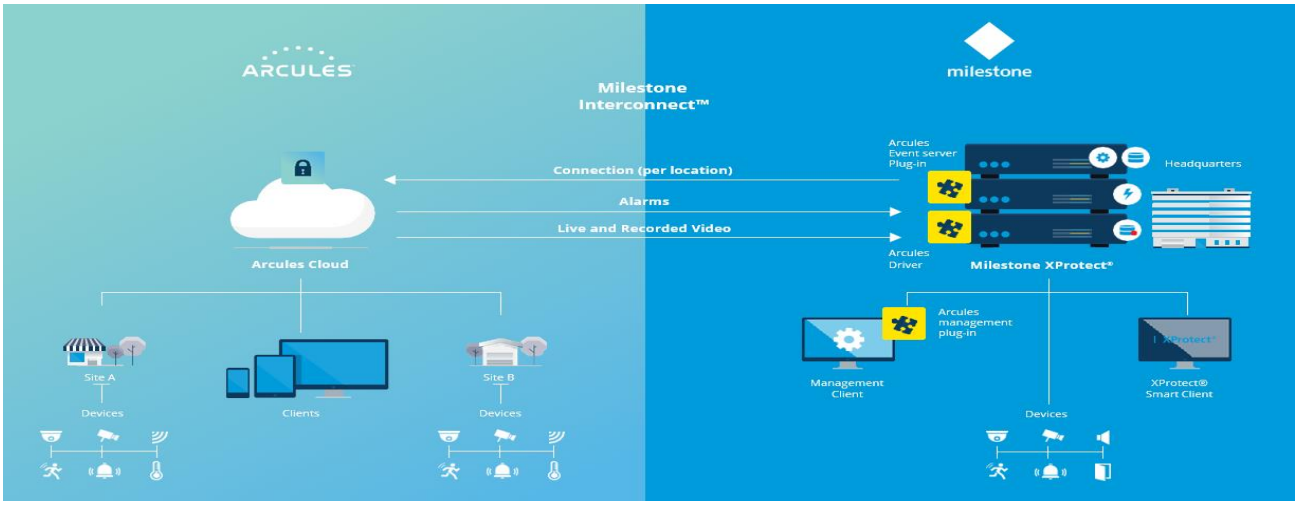
As no specifics of command API or protocols are known, the driver does not send any commands to the device. The Universal driver tries to receive a multimedia stream from a device using standard streaming methods (RTSP/RTP, HTTP streaming or JPEG snapshots). There are currently 3 variations of the Universal driver available in XProtect: 1 channel; 16 channels; 64 channels.

For additional information, see the following website https://www.milestonesys.com/community/business-partner-tools/supported-devices/xprotect-corporate-and-xprotect-expert/

Arcules Video Surveillance as a Service (VSaaS) ** Alternate Deployment Option

The Arcules Video Surveillance as a Service (VSaaS) integration with XProtect on-premise VMS is the first step in Milestone's journey to provide an answer to the increasing interest in cloud-based video solutions.

This joint solution harnesses the power of XProtect technology to help drive the adoption of cloud- based VMS solutions. It provides an ideal solution for organizations looking to centralize their dispersed video solution operations by using on-prem hardware and Milestone XProtect while growing their business with remote cloud monitoring.



With the dedicated Arcules driver, a XProtect VMS can connect to the Arcules Cloud and create a Hybrid Cloud service option. It is a SaaS and a Classic surveillance platform offering in one.

The solution combines the best of the worlds: the scalability of VSaaS and the functionality of on-premises VMS. It is designed to provide a fast way of deploying remote sites with minimum

IT resources and downtime. By using VSaaS to deploy remote sites, users can reduce their capital investment and better control their operational costs due to flexible pricing schemes and minimal hardware requirements. By using on-premises VMS at headquarters, users can benefit from the strong capabilities that XProtect has to offer.

Key Benefits include:

Reduce investment - reduce capital investment and better control operational costs at dispersed sites

- Leverage cloud architecture for remote/smaller sites instead of purchasing your own
- Reduce initial investment and better control operational costs with flexible VSaaS pricing schemes
- Shorter deployment and training times reduce investment and total system costs
- Eliminate the need for expensive hardware at dispersed sites
- Connect Arcules VSaaS cameras to your on-prem XProtect system with minimal need for additional server hardware – video is stored in the Arcules VSaaS service at all times
- No additional Arcules VSaaS service charge to connect cameras to an on-prem XProtect VMS system

Ease of use - deploy, configure and maintain distributed sites fast and with minimum IT resources

- Setup, configure and maintain smaller distributed sites quickly and remotely
- Connect Arcules sites and cameras seamlessly to a XProtect on-prem VMS system through a few simple steps with no duplicated configuration
- No additional training of operators as, Arcules VSaaS cameras and alarms have the same principal behavior as XProtect native cameras
- Automatic synchronization and propagation of alarms between Arcules VSaaS and XProtect
- Streamline training and maintenance with Arcules' cloud service automatic software updates and reduced need for onsite service visits
- Synchronize and enable propagation of Arcules VSaaS defined alarms in the on-prem XProtect system through a simple click
- Connect your VMS platform to customers using Arcules VSaaS easily (security companies, monitoring stations and law enforcement)

Newport-Mesa
Unified School District

NEWPORT-MESA UNIIFED SCHOOL DISTRICT

ADDENDUM NO. 1
Integrated Security Standards

RFP No. 104-23

NEWPORT MESA UNIFIED SCHOOL DISTRICT
2985 BEAR ST., BLDG.-A
COSTA MESA, CALIFORNIA 92626

October 17, 2022

The following revisions and/or clarifications shall be made to the RFP documents for the above-named work. All work described in the original RFP documents and all applicable Sections of the original RFP documents shall be included in the contract, except as herein modified:
Acknowledgement of this Addendum shall be made below and submitted with the RFP submission. If acknowledgement is not made the proposal may be considered non-responsive.

1. ***Change:*** Change RFP Submitters Meeting date to October 24, 2022, at 1:00 PM

All other provisions of the RFP remain unchanged.

BELOW, PLEASE ACKNOWLEDGE RECEIPT OF THIS ADDENDUM AND SUBMIT IT WITH YOUR PROPOSAL.

Name: Laurie Dickson

Signature: 

Firm Name: Milestone Systems, Inc

Address: 5300 Meadows Rd, Suite 400, Lake Oswego, OR 97035

Telephone #: 1 503 350 1100

Fax #: 1 503 662 7321

(END OF ADDENDUM NO.1)

The Following Pages Contain Supplemental Information that can be referenced as needed

Customer Study

Anaheim Union High School District Deploys Milestone VMS to Prevent Crime and Optimize Safety

For more Customer Studies:
milestonesys.com/news



As one of the largest school districts in California, the Anaheim Union High School District installed their first district-wide IP video surveillance system. Connected to five Orange County Police Departments, the system is designed to prevent petty crime and protect lives during an active shooter scenario.

Challenge: Proactively keeping students safe

The Anaheim Union High School District (AUHSD) lacked a centralized video security system that would allow administrators to prevent, monitor, and investigate incidents on campuses. Ongoing occurrences of theft and vandalism were financially impacting the district. In addition, parents and staff members were increasingly concerned about active shooter incidents happening at other schools across the country.

Solution: Consolidated district-wide monitoring

AUHSD expanded and upgraded its existing security infrastructure with a campus-wide solution using Hanwha Techwin America IP security cameras and DDN storage servers, plus new fencing at all schools with strategically placed perimeter sensors — all integrated with the Milestone XProtect Enterprise open platform video management system (VMS) for easy monitoring, prevention, and incident investigation. Local law enforcement and Orange Country Public Safety have direct access to all the cameras and the VMS during emergencies.

Result: Decrease in property loss and added crime prevention

The Milestone VMS was selected based on a range of included features, ease of use, devices supported, technical support, performance, and cost evaluation. The new video surveillance system has helped administrators monitor and address campus vandalism and graffiti, thefts, student fights, and other potential threats faster and with greater ease. When an incident occurs, administrators can quickly access the VMS and review the security footage to investigate the event. The use of Hanwha cameras has helped identify when and where vandalism and theft are occurring on campuses. With proper evidence, restitution may be possible.

“As we were installing cameras, the schools were getting images of vandalism and even images of golf carts being stolen. It was phenomenal to see how many issues

July 2021

Organization
Anaheim Union High School District

Location
Anaheim, California

Industry Segment
Education

Solution
Milestone Systems
XProtect Enterprise

Cameras:
Hanwha Techwin America

Servers:
DDN

milestone

MAKE THE WORLD SEE

Date: March 18, 2022

Video Management Software A&E Specification
Construction Specifications Institute (CSI) edition

A&E Specification for XProtect Professional+ 2022 R1

Prepared by:
Milestone Systems

milestone

Americas:

Milestone Systems, Inc.
5300 Meadows Rd # 400
Lake Oswego, OR 97035
U.S.A.
Phone: (503) 350-1100
Web: www.milestonesys.com

EMEA:

Milestone Systems A/S
Banemarksvej 50C
2605 Brøndby
Denmark
Phone: +45 88 300 300
Web: www.milestonesys.com

APAC:

Milestone Systems Singapore
10 Eunos Road 8
#12-03 North Lobby
Singapore Post Centre
Singapore 408600
Phone: +65 6742 0623
Web: www.milestonesys.com

© 2022 Milestone Systems A/S. All rights reserved.

Specifications

This Architectural and Engineering Specifications document utilizes MasterFormat™ Titles and Numbers April 2018 Edition and SectionFormat™/PageFormat™ December 2009 Edition standards by the Construction Specifications Institute (CSI).

This document specifies the architectural/engineering and bid criteria for a premises-based networked Video Management Software (VMS) .

Notes to Specifier

1. Where several alternative parameters or specifications exist, or where the Specifier has the option of inserting text, such choices are presented in **bold red text**.
2. Explanatory notes and comments are presented in red hidden text.
3. Delete any item or paragraph that is not applicable to this project, renumber the paragraphs. Insert additional provisions as required for this project.

Document Disclaimer and Restrictions

Information in this document was current as of the time of publication, and subject to change without notice. For the most up-to-date information, visit www.milestonesys.com.

SECTION 28 23 00
VIDEO MANAGEMENT SOFTWARE

[**Specifier Note:** Delete Specifier Notes and unused optional items in red.]

PART 1. GENERAL

1.1. SUMMARY

A. *Section Includes:* Description, architectural and functional requirements, data security requirements, operational capabilities, and computer equipment requirements for a single or multi-site on-premises Video Management Software (VMS) supporting an unrestricted number of users, devices, servers and sites.

B. *Compliance:* System equipment and installation shall comply with all provisions and requirements of this specification as well as all applicable national, state and local codes and standards.

C. Products Furnished **[OR]** Supplied But Not Installed Under This Section.

D. Products Installed But Not Furnished **[OR]** Supplied Under This Section.

E. *Related Requirements*:

1. Section 27 00 00 Communications (Division 27).
    a. Section 27 05 00 Common Work Results for Communications.
    [**SPECIFIER NOTE:** For general requirements that are common to more than one section in Division 27.]
        1) Section 27 05 28 – Pathways for Communication Systems.
    b. Section 27 10 00 – Structured Cabling.
        1) Section 27 13 00 – Communications Backbone Cabling.
        2) Section 27 15 00 – Communications Horizontal Cabling.
2. Section 28 00 00 Electronic Safety and Security (Division 28).
    a. Section 28 05 00 – Common Work Results for Electronic Safety and Security.
    [**SPECIFIER NOTE:** For general requirements that are common to more than one section in Division 28.]
    b. Section 28 08 00 Commissioning of Electronic Safety and Security.
    [**SPECIFIER NOTE:** For expanded requirements for commissioning, systems readiness checklists, and training.]
        1) 28 08 11 Testing for Baseline Performance Criteria.

1.2. REFERENCES

A. Trademarks Used in This Document:

1. *Apple*: Safari®
2. *Digital Living Network Alliance:* DLNA®
3. *Google*: Google Chrome™
4. *Immervision:* ImmerVision Enables®
5. *Intel:* Intel®, Core™, Xeon®
6. *Microsoft:* Microsoft®, Outlook®, Windows®, Active Directory®, Hyper-V®, SQL Server®
7. *Milestone:* XProtect®, Milestone Husky™, Milestone Husky IVO™, Milestone Federated Architecture™, Milestone Interconnect™, Scalable Video Quality Recording™
8. *Milestone:* XProtect®, Scalable Video Quality Recording™
9. *NVIDIA:* NVIDIA®
10. *Mozilla*: Mozilla®, Firefox®
11. *VMware:* VMware®

B. Abbreviations and Acronyms:

1. *ACC*: Advanced Audio Coding.
2. *AES*: Advanced Encryption Standard.
3. *API*: Application Programming Interface.
4. *CA*: Certificate Authority.
5. *DLNA*: Digital Living Network Alliance.
6. *EULA*: End User License Agreement.
7. *FIPS*: Federal Information Processing Standards.
8. *FPS*: Frames per Second.
9. *Full HD*: High Definition video resolution of 1920 x 1080 pixels.
10. *GB*: Gigabyte.
11. *GOP*: Group of Pictures.
12. *GraphQL*: Graph Query Language.
13. *H.264/H.265*: Video compression formats.
14. *HD*: High Definition video resolution of 1280 x 720 pixels.
15. *HTML*: Hyper Text Markup Language.
16. *HTTPS*: Hyper Text Transfer Protocol Secure.
17. *IDP*: Identity Provider.

18. *I/O*: Input/Output.
19. *IP*: Internet Protocol.
20. *JPEG*: Joint Photographic Experts Group (image format).
21. *LAN*: Local Area Network.
22. *LPR*: License Plate Recognition.
23. *MIP SDK*: Milestone Integration Platform Software Development Kit.
24. *MPEG*: Moving Picture Experts Group (video format).
25. *NAS*: Network Attached Storage.
26. *NAT*: Network Address Translation.
27. *ONVIF*: Open Network Video Interface Forum.
28. *PTZ*: Pan-Tilt-Zoom.
29. *RTSP*: Real Time Streaming Protocol.
30. *SDK*: Software Development Kit.
31. *SOAP*: Services Oriented Architecture Protocol.
32. *SVQR*: Scalable Video Quality Recording.
33. *UPnP*: Universal Plug and Play.
34. *UPS*: Uninterruptible Power Supply.
35. *VMS*: Video Management Software.
36. *WAN*: Wide Area Network.

C. Definitions:

1. *AAC Audio Codec*: Advanced Audio Coding is a proprietary audio coding standard for lossy digital audio compression.
2. *Active Media Storage:* High-performance media storage used for active video, audio and metadata recording.
3. *Application Programming Interface (API):* Set of clearly defined methods of communication between various software components.
4. *Archived Media Storage:* Secondary media storage used for storing video, audio and metadata beyond an initial retention period.
5. *Authentication:* Process that establishes the origin of information or determines an entity's identity.
6. *Authorization:* Process that associates permission to access a resource or asset with a person and the person's identifier(s) for the purpose of granting or denying access.
7. *Bit Rate:* Number of bits per time unit sent over a network.
8. *Contractor:* Firm selected by Owner and any of Contractor's subcontractors, vendors, suppliers or fabricators, to perform work specified in these contract documents and supporting documentation. Contractor shall supply all equipment, labor, material and

services necessary to complete the project construction in accordance with Contract Documents.

9. *Central Processing Unit (CPU):* General purpose electronic circuitry within a computer that carries out the instructions of a computer program, typically contained in a single integrated circuit chip.
10. *Digital Living Network Alliance:* Standards-making group for consumer electronics manufacturers establishing interoperability among consumer devices for picture and video display.
11. *Dwg-files*: Proprietary binary file format used for storing two- and three- dimensional design data and metadata.
12. *Dxf-files*: CAD data file format developed by Autodesk for enabling data interoperability between AutoCAD and other programs.
13. *Federal Information Processing Standards*: A set of U.S. government standards that define the critical security parameters that vendors must use for encryption before selling the software or hardware to U.S. government and regulated industries.
14. *G.711 Audio Codec*: ITU-T standard audio codec that provides toll-quality audio.
15. *G.726 Audio Codec*: ITU-T ADPCM speech codec standard covering the transmission of voice.
16. *Graphics Processing Unit (GPU):* Specialized electronic circuit designed to rapidly decode video, manipulate images and accelerate the creation of video images in a video frame buffer intended for output to a display device, much more efficiently than can be done by general purpose computer CPUs. GPUs are used in mobile phones, personal computers, workstations and game consoles.
17. *Group of Pictures (GOP):* In video coding, a group of pictures, or GOP structure, specifies the order in which intra- and inter-frames are arranged. The GOP is a collection of successive pictures within a coded video stream. Each coded video stream consists of successive GOPs, from which the visible frames are generated. Encountering a new GOP in a compressed video stream means that the decoder doesn't need any previous frames to decode the next ones and allows fast seeking through the video.
18. *Hardware Acceleration:* Use of computer hardware (such as a GPU) to perform some functions more efficiently than is possible in software running on a more general-purpose CPU.
19. *Kerberos:* Ticket-based network authentication protocol designed to provide strong authentication for client/server or server/server applications.
20. *Multi-site:* Reference to a VMS that spans multiple physical site locations.
21. *Open Network Video Interface Forum (ONVIF):* Global and open industry forum for the creation of standards for how IP-networked products within video surveillance and other physical security areas can communicate with each other.
22. *Pre-buffering:* Temporary storage of video and audio for pre-recording.
23. *Pre-recording:* Automatically recording video and audio starting a specified number of seconds just before the event or time condition that initiated the recording.

24. *Post-recording:* Automatically continuing the recording of video and audio for a specified number of seconds after the end of the event or time condition that initiated the recording.
25. *PTZ Patrolling or PTZ Tour:* Automatically moving a camera through a specified series of preset PTZ positions, dwelling on those positions for a specified amount of time, and transitioning between the preset positions at a specified speed.
26. *Reseller:* Contractor authorized by manufacturer to furnish, install and maintain manufacturer's VMS, who may be the primary contractor or a subcontractor for the provision of this project's VMS.
27. *Universal Plug and Play (UPnP):* Set of networking protocols that permits networked devices, such as personal computers, printers, Internet gateways, Wi-Fi access points, IP video cameras and mobile devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing and communications.

D. Brand Names Used in This Document:
   1. XProtect® LPR
   2. XProtect® Professional+
   3. XProtect® Retail
   4. XProtect® Transact

1.3. SUBMITTALS

A. *Submission:* Submit under provisions of Section 01 30 00 - Administrative Requirements.

B. *Product Data:* Provide manufacturer's data sheets and installation manuals on each product to be used, including:
   1. Preparation instructions and recommendations.
   2. Storage and handling requirements and recommendations.
   3. Installation methods.

C. *Shop Drawings:* Provide the following drawings.
   1. Schematic of system components with physical space requirements.
   2. System network topology diagram.
   3. Connecting riser diagrams for all interfacing equipment.
      a. List of all equipment with part numbers.
      b. Locations for all components to be installed under this scope of work.

1.4. CLOSEOUT SUBMITTALS

A. *As-Built Drawings:* Provide original shop drawings modified to reflect changes made to comply with installation/configuration requirements and actual field conditions.

B. *Maintenance Contracts:* Submit a maintenance service agreement, including cost and services for a two-year period for Owner's review.

C. *Warranty Documentation:* Submit manufacturer's standard VMS warranty.

1.5. QUALITY ASSURANCE

[**SPECIFIER NOTE**: Use this article to describe owner requirements for contractor experience, certifications and references. Delete if not applicable.]

A. *Qualifications*:

1. Manufacturer shall regularly and presently produce, as one of the manufacturer's principal products, material and services specified for this project for commercial, military or industrial use.

2. *Contractors / Installers*:

   a. *Licensure:* Contractor or security sub-contractors shall be licensed to perform security installations in the state/region where the work is to be performed if so required.

   b. *Experience:* Contractor or security sub-contractor shall have a minimum of three years of experience installing and servicing systems of similar scope and complexity**.**

   a. *References:* Contractor shall provide four current Milestone project references from clients with systems of similar scope and complexity which became operational in the past three years**.**

      1) At least three references shall be utilizing the same system components, in a similar configuration as the proposed system.

      2) References shall include a current point of contact, company or agency name, business address, telephone number, and if the contact agrees, include a basic system description and date of project completion. The owner reserves the option to visit the reference sites, with the site owner's permission and representative, to verify the quality of installation and the reference's level of satisfaction with the system.

   a. *Technician Certification:* Utilize only manufacturer-trained technicians to install, program, and service VMS equipment**.**

      1) Ensure technicians have a minimum of five continuous years of technical experience in electronic security systems including IP networking and VMS solutions**.**

   c. *Dealer Certification:* Provide evidence that installing service company is an authorized dealer in good standing for the product's manufacturer, and that it meets the manufacturer's technical certification requirements.

1.6. DELIVERY, STORAGE AND HANDLING

A. Deliver software installation packages via download directly from manufacturer's web site

B. Software installation packages must be digitally signed by the manufacturer.

1.7. SITE CONDITIONS

A. *Ambient Conditions*:

B. *Existing Conditions*:

1.8. WARRANTY AND SUPPPORT

A. *Manufacturer Warranty and Support*:

1. *Software Warranty*:

   a. Manufacturer's software warranty must be described in the manufacturer's EULA for the product.

2. *Software Support*:

   a. Provide free access to any software service updates or hot fixes released due to a material defect or error in the product.

   b. Provide new device driver packs, multiple times per year, to extend support for additional devices without the need for a new version of the product.

   c. Provide free access to self-paced interactive e-training.

3. *Software Updates and Upgrades*:

   a. Make software upgrades available for a period of one year from activation of the software license. Coverage options shall include:

      1) Free access to any new product versions for the purchased Milestone VMS software product.

      2) 100% credit on owners current Milestone VMS software products when upgrading to a more advanced Milestone VMS product.

      1) Prioritized handling of support phone call response times based upon criticality of issue, for questions submitted by email or that cannot be answered in initial phone call.

      2) Additional years of software upgrades available for purchase separately.

B. *Contractor Warranty*:

1. Fully warrant parts, materials and labor for a minimum of one year from date of the final acceptance of the VMS, including wiring, software, hardware and third-party products, including:

   a. Provision of all new software service releases during the warranty period.

   b. Provision of all new device driver packs.

C. *Maintenance and Service*:

1. *General Requirements*:
   a. Provide all services required and equipment necessary to maintain VMS in an operational state as specified for one year from formal written acceptance of system.
   b. Provide all necessary material required for performing scheduled adjustments or other non-scheduled work.
   c. Minimize impacts on facility operations when performing scheduled adjustments or other non-scheduled work.
2. *Description of Work:* Deployment of VMS includes installation and setup of new server hardware and software, plus any new and existing equipment specified in Article 2.1. OWNER-FURNISHED PRODUCTS.
3. *Personnel:* Service personnel shall be certified in the maintenance and repair of the selected type of equipment and integrations, and qualified to accomplish all work promptly and satisfactorily.
4. *Schedule of Work:* Work shall be performed during regular workweek working hours, as determined by the deployment facility's locale, excluding federal/public holidays.
5. *Emergency Service*:
   [**SPECIFIER NOTE:** Use this article to describe owner requirements for Support Level Agreements (SLA). Delete if not applicable.]
   a. Provide Owner with an emergency service center telephone number. Emergency service center shall be staffed 24 hours a day, 365 days a year and be located within 60 miles/kilometers of the deployment facility.
   b. Be a stocking contractor of the manufacturer's equipment.
   c. Owner shall initiate service calls whenever system is not functioning properly.
   d. *Service Response*:
      1) Owner has sole authority for determining catastrophic and non-catastrophic system failures.
      2) Catastrophic system failure is defined as any system failure that Owner determines will place a facility at increased risk.
      3) For catastrophic system failures, provide same-day four-hour service response with continued status updates at least every four hours.
      4) For non-catastrophic failures, provide service response within eight hours with continued status updates at least twice a week.
6. *Verification of Operation:* As part of scheduled adjustments and repairs, verify operation of system as demonstrated by performance verification testing.

PART 2. PRODUCTS

2.1. OWNER-FURNISHED PRODUCTS

[**SPECIFIER NOTE**: use this article to describe owner-furnished products to enable Contractor to correctly install and configure them for use with VMS. Delete if not applicable.]

A. *New Products*:

B. *Existing Products*:

2.2. MANUFACTURER

A. *Americas*:

1. Milestone Systems, Inc., 5300 Meadows Rd, # 400, Lake Oswego, OR 97035 U.S.A.
    a. Telephone: (503) 350-1100
    b. Website: www.milestonesys.com

B. *EMEA*:

1. Milestone Systems A/S, Banemarksvej 50C, 2605 Brøndby, Denmark
    a. Telephone: +45 88 300 300
    b. Website: www.milestonesys.com

C. *APAC*:

1. Milestone Systems Singapore, 10 Eunos Road 8, #12-03 North Lobby, Singapore Post Centre, Singapore 408600
    a. Telephone: +65 6742 0623
    b. Website: www.milestonesys.com

D. *Milestone Product Name*: XProtect Professional+.

E. *Substitution Limitations*: No Substitutions.

2.3. VIDEO MANAGEMENT SOFTWARE

A. *Description:* Video surveillance management software (referred to as “system” or “VMS”) supporting an unrestricted number of users, devices, servers and sites, with options for central surveillance operations and mobile devices.

B. *System Architecture:* The VMS shall consist of:

1. *Servers:* One or more VMS servers.
    a. Physical or virtualized Windows servers.
    b. Virtualized Windows servers, using:
        1) Microsoft Hyper-V.
        2) VMWare.
    c. UPS provided to physical servers, network infrastructure and devices such as cameras.

2. *Server Software Components:* One or more Milestone XProtect software components, or software components made by others as noted, per VMS server.
    a. *Management Server:* Central service component of the VMS responsible for handling system configuration, distributing the configuration to other system components, such as Recording Server services, and for facilitating user authentication.
    b. *Management Server Failover:* A second server shall take over the Management Server function if the first server fails.
        1) *Failover Management Server:* Installation of the Management Server service in a Microsoft Windows Failover Cluster, or similar compatible third-party software.
    c. *Recording Server:* Service responsible for communications, recording and event handling for all devices (cameras, video and audio encoders, I/O modules, metadata sources, etc.), including:
        1) Retrieving video, audio, metadata and I/O event streams from devices.
        2) Recording video, audio and metadata.
        3) Providing access to live and recorded video, audio and metadata.
        4) Transmit live audio from operator's microphone to one or more camera speakers or supported IP speakers.
        5) Providing access to device status.
        6) Triggering system and video events on device failures, events, etc.
        7) Writes video streams, audio streams and their metadata to a high-performance media database.
        8) Performing motion detection and generate smart search metadata.
    d. *Event Server:* Service that handles various tasks related to events, alarms, maps and third-party integrations via the Milestone Integration Platform Software Development Kit (MIP SDK).
    e. *Log Server*: Service that writes all system, audit and rule-triggered log messages to database.
    f. *Service Channel*: Service responsible for communicating the following:
        1) Service and configuration messages to XProtect Smart Client.
    g. *XProtect Mobile Server:* Service responsible for hosting the XProtect Web Client and for providing access to the VMS for XProtect Web Client and XProtect Mobile client users.
    h. *Milestone Open Network Bridge:* Optional server, including Milestone Open Network Bridge service, Milestone RTSP Bridge service, and the Milestone Open Network Bridge Manager, plus 64-bit plug-in for Management Client. This is to enable private-to-public video integration.

i. *DLNA Server*: Service to enable display of live video on any DLNA compliant TV or displays without the need for additional equipment.

j. *Microsoft SQL Server*: Microsoft database server service for the Management Server, Event Server and Log Server services.

k. *API Gateway:* Service that provides a front-end and common entry point for RESTful API services on other VMS server components. *Microsoft Active Directory:* Active Directory is not required for single-site systems but is recommended for cyber security purposes.

3. *PC or Laptop Workstations:* One or more PCs or laptops for Milestone XProtect client software applications intended to run on Windows-based PCs and laptops.

   a. *Management Client:* The administration interface for all parts of the VMS, designed to be run remotely from, for example, an administrator's computer.

   b. *XProtect Smart Client:* Designed for day-to-day use by dedicated operators, to be run remotely on the operator's computer. XProtect Smart Client provides dedicated task-oriented tabs for Live Video, Video Playback, Search, plus dockable tabs for Alarm Monitor. XProtect Smart Client supports definable keyboard and joystick button shortcuts for frequently used actions, including window or camera selection.

   c. *XProtect Web Client:* Browser-based application for the occasional or remote user that needs easy access to live video monitoring and audio listening with PTZ control including use of presets, and video and audio playback and export, with defined exports available for later usage or download.

4. *Tablets or Smartphones:* One or more tablets or smartphones using XProtect Web Client (see above) or XProtect Mobile client.

   a. *XProtect Mobile Client:* Native mobile app for smartphone or tablet users, for easy access to live and playback of cameras, and to activate system events and outputs. Additionally, for use as a remote recording device by using the mobile device's built-in camera, whereby video from the device's camera is streamed back to the VMS and recorded like a standard camera.

5. *Smart Walls:* Optionally one or more Smart Walls.

   a. See Section 28 51 19.13 VIDEO WALL.

6. *Networks*:

   a. *Multiple Network Segments*: The VMS must support network segmentation into separate device, server and internet-connected networks.

   b. *Device Network:* Local network whose capacity and configuration are suitable for the level of video, audio and metadata data transmission established by the system design and its intended usage.

   c. *Server Network:* Local network whose capacity and configuration are suitable for the level of video data transmission, systems integration, and user operations established by the system design and its intended usage.

   d. *Internet-Connected Network*: Internet-connected network providing connection to remote VMS sites and private-to-public connection via Milestone Open Network

Bridge. This network is also used for remote user access via the XProtect Mobile Server.

e. *Network Traversal*:

1) Enable software clients to access Recording Server services from outside a NAT firewall, by the use of public addresses and port forwarding.

2) Provide Remote Connect Services that enable secure remote connections to devices across different types of private and public networks.

C. *Multi-System Architectures:* Provide the following architecture option for multi-site deployments:

1. *Distributed Recording Server Services:* Intended for sites with stable network connections between the central site and any number of remote sites.

a. Management Server at central site is providing user authentication and authorization for all distributed Recording Server services.

b. Each site has at least one Recording Server.

2.4. SYSTEM DESIGN CRITERIA

A. *Scalability:* Provide component-based system architecture to support scaling of VMS from small systems (up to 100 devices) to very large systems (several thousand devices) for single-site or multi-site deployment, whereby:

1. *For Small Systems:* All software components can be installed on the same server if the server is able to handle the combined load.

2. *For Large Systems:* Software components can be installed on separate dedicated servers to scale and distribute the load.

B. *Availability and High Performance:* Provide the following capabilities to ensure high VMS availability and performance.

1. *Failover Recording Server:* Provide hot and cold Failover Recording Server capabilities.

2. *Management Server, Event Server, Log Server, API Gateway*: Support Windows Server Failover Clustering, or similar.

3. Storage solution shall be configured with RAID10 for Live database and RAID5 or RAID6 for archive database.

C. *Operating Systems:* Provide server and client software applications that are native 64-bit Microsoft Windows applications.

D. *Network Addressing:* Support both IPv4 and IPv6 addressing.

E. *Video Standards:* Provide simultaneous live streaming and recording of video from IP cameras and IP video encoders without any software limitations on the number of cameras per Recording Server, with support for the following codecs and options:

1. *Codecs*:

a. H.264 and H.265

b. MPEG-4 and MPEG-4 ASP

c. MJPEG

d. MxPEG

2. *Options*:

a. Toggling between recording key frames only or full video stream for MPEG-4, H.264 and H.265 video.

b. Adjustable GOP length for MPEG-4, H.264 and H.265 video.

c. Toggle between recording full framerate from the camera and any lower FPS for MJPEG video.

F. *Video De-Interlacing:* Provide live video views with an adaptive de-interlacing option, to improve the quality of interlaced video, based on the actual video content received, for example, to smooth area of an image where object lines would otherwise appear as jagged lines.

G. *Multi-Live Video Streaming:* Provide multiple streams for live viewing using any combination of supported standards, video resolutions and frame rates.

H. *Adaptive Streaming:* Depending on the requested resolution, provide automatic selection between the video streams configured for multi-live video streaming to these clients:

1. XProtect Smart Client: Live video streams from the Recording Server to the XProtect Smart Client or XProtect Smart Wall.

2. XProtect Web Client: Live video streams from the XProtect Mobile Server to the XProtect Web Client.

3. XProtect Mobile Client: Live video streams from the XProtect Mobile Server to the XProtect Mobile Client.

I. *Direct Streaming:* Provide live video streams in these codecs directly from the Mobile Server to clients without transcoding:

1. XProtect Web Client: Provide MJPEG and H.264 live video streams.

2. XProtect Mobile Client: Provide H.264 and H.265 live video streams.

J. *Audio Standards*: Provide simultaneous digital two-way audio streaming and recording of audio from IP speaker and IP microphone devices without any software limitations on the number of devices per Recording Server, with support for the following codecs and options:

1. *Codecs*:

a. AAC

b. G711

c. G726

2. *Options*:

a. Playback of audio files on rule.

K. *DLNA Support:* Provide the ability to easily display live video from the installed cameras directly onto any modern consumer-grade TV supporting DLNA functionality.

L. *Hardware Acceleration XProtect Smart Client:* Provide the following hardware acceleration capabilities to offload Smart Client video processing from the computer CPU to dedicated hardware video processing capabilities:

1. *NVIDIA GPU:* Automatically detect and use all available NVIDIA GPUs, for hardware accelerated decoding, color correction, and scaling.
2. *Intel Quick Sync:* Automatically detect and use Intel Quick Sync Video GPU integrated into select Intel processors for hardware accelerated decoding, color correction, and scaling.
3. Provide the ability to use both NVIDIA and Intel GPUs at the same time and automatically load balance the requests for optimal performance.
4. Provide the ability to show which GPU is used to decode which stream.

M. *Hardware Acceleration Recording Server:* Provide the following hardware acceleration capabilities to offload Recording Server video processing from the computer CPU to dedicated hardware video processing capabilities:

1. *Intel Quick Sync:* Automatically detect and use Intel Quick Sync Video GPU integrated into select Intel processors for hardware accelerated decoding to enable server-side motion detection.

N. *Hardware Acceleration Mobile Server:* Provide the following hardware acceleration capabilities to offload Mobile Server video processing from the computer CPU to dedicated hardware video processing capabilities:

1. *NVIDIA GPU:* Automatically detect and use all available NVIDIA GPUs, for hardware accelerated decoding to enable adaptive transcoding.
2. *Intel Quick Sync:* Automatically detect and use Intel Quick Sync Video GPU integrated into select Intel processors for hardware accelerated decoding to enable adaptive transcoding.
3. Provide the ability to use both NVIDIA and Intel GPUs at the same time and automatically load balance the requests for optimal performance.

O. *Open Network Bridge Functionality:* Provide access to live and recorded video, and the ability to control pan-tilt-zoom cameras in compliance with the relevant ONVIF Profile G and Profiles S standards.

P. *Camera-Independent Motion Detection:* Provide real-time, camera-independent motion detection with:

1. *Configurable Sensitivity:* Configurable and automatic motion-detection sensitivity per camera
2. *Searchable Metadata:* Searchable motion detection metadata created during motion detection.
3. *Exclusion Zones:* Multiple motion exclusion zones definable per camera to keep irrelevant motion from triggering recording.

Q. *PTZ Control Priorities*:

1. Provide 3 PTZ priority levels for control of rights between different operators and automatic scanning and patrolling schemes.
2. PTZ Scans and Patrols shall pause for higher-priority manual or event-based camera control, and resume after manual session timeout and completion of event camera control period.

R. *Configurable Pre-Buffering:* Provide pre-buffering with variable buffer length, with the ability to place buffer on disk or in memory.

S. *Device Video Quality Optimization:* Provide video quality optimized per available bandwidth, device screen resolution, and camera view window sizes in these clients:

1. *XProtect Smart Client Optimization*:
   a. Switch between all configured live video streams from the cameras to optimize bandwidth consumption and workstation performance.
   b. Optimize viewing performance for remote viewing according to the available bandwidth and view layouts, maximizing video stream quality per display capabilities of defined views.
2. *XProtect Web Client and XProtect Mobile Client Optimization:* Optimize transcoding by capping video stream resolution and frame rate for transmission to XProtect Web Client and XProtect Mobile client.

T. *Multiple Language Support:* Provide support for multiple languages in these XProtect clients:

1. *Management Client User Interface:* American English, Chinese (Simplified), Chinese (Traditional), Danish, French, German, Italian, Japanese, Korean, Portuguese (Brazilian), Russian, Spanish, Swedish and Turkish.
2. *Management Client Built-In Help:* American English, Chinese (Simplified), French, German, Japanese, Korean and Portuguese (Brazil).
3. *XProtect Smart Client, XProtect Web Client and XProtect Mobile Client User Interface:* American English, Arabic, Bulgarian, Chinese (Simplified), Chinese (Traditional), Croatian, Czech, Danish, Dutch, Farsi, Finnish, French, German, Hebrew, Hindi, Hungarian, Icelandic, Italian, Japanese, Korean, Norwegian (Bokmål), Polish, Portuguese (Brazilian), Russian, Serbian, Slovak, Spanish, Swedish, Thai, Turkish and Ukranian.
4. *XProtect Smart Client Built-In Help:* American English, Arabic, Chinese (Simplified), Chinese (Traditional), Czech, Danish, Dutch, French, German, Italian, Japanese, Korean, Polish, Portuguese (Brazilian), Russian, Spanish, Swedish and Turkish.
5. *XProtect Web Client and XProtect Mobile Client Built-In Help:* American English, Danish and Japanese.

U. *True Multi-Window Support:* Provide true multi-window support in XProtect Smart Client whereby secondary windows have full functionality and can be operated in independent mode or synchronized mode where they follow the control of the main window.

V. *System Capacities:* Provide the following maximum capacities, constrained only by the physical performance capabilities of installed server hardware and network infrastructure:

1. Unrestricted devices.
2. Unrestricted client software users.
3. Unrestricted mobile devices.
4. Unrestricted client PCs or laptops.
5. Unrestricted servers.
6. Unrestricted sites.
7. Unrestricted system rules.
8. Unrestricted time profiles.
9. Three software client profiles.
10. Unrestricted media storage.
11. Recording rates of at least 30 FPS per camera, limited only by hardware capabilities.

2.5. SYSTEM SECURITY

A. *Control and Information Security:* Provide the following data protection measures and user rights management capabilities in support of system confidentiality, integrity and availability:

1. *Data in Transit:* Encrypted communication between servers and clients using secure communication CA digital certificates.
    a. HTTPS connections from Recording Server to devices that support HTTPS connections.
    b. Encrypted communication between the Recording Server and services that retrieve streaming data using customer-provided CA digital certificates for connections to the Recording Server.
    c. Encrypted communication between the Management Server and the Recording Server using customer-provided CA digital certificates.
    d. HTTPS connections from VMS clients, SDK clients and services that support HTTPS connections to Recording Server.
2. *System Configuration Data*: Provide password protection of the system configuration backup.
3. *Off-Premises Live and Recorded Video in Transit*: HTTPS connections must use trusted CA certificates and support HTTPS connections from:
    a. Mobile Server to browser-based XProtect Web Client and XProtect Mobile client app.

b. Open Network Bridge to remote public systems.

4. *Data Integrity of Exported Video*:

a. Export video in XProtect format that can only be viewed in the XProtect Smart Client — Player.

b. Per-export password protection for playback.

c. 256-bit AES encryption.

d. Digitally signed media exports with SHA-2 algorithm to establish a means of detecting modification of exported video.

e. XProtect Smart Client — Player's Verify Signatures function to validate authenticity of exported video recording.

f. Option to prevent re-export of exported video.

5. *Digital Certificates:* Use of customer-provided CA digital certificates for connections to the Mobile Server.

6. *Data Access Control*: Provide:

a. User profiles restricting device access and video viewing, playback and export, including by day and time-of-day.

b. Timestamped audit log of who logged in, viewed live or recorded video, or exported video.

B. *User Authentication*:

1. *Log-in Options:* Log-in authentication via:

a. Microsoft Active Directory.

b. Local Windows user accounts.

c. External IDP using Open ID Connect to facilitate single sign-on.

d. Basic user system account (username and password credentials).

1) Ability for basic user to change password during login.

2) Ability for system administrator to enforce password change during login.

3) Ability to enforce password complexity.

e. Dual authentication, a.k.a. two-person rule, requiring two verified persons to gain access.

2. *Auto-Log-In:* Use of last used credentials for authentication, with Auto-log-in and auto-restore of camera views.

3. *Kerberos Authentication:* Provide strong authentication via Kerberos support.

C. *User Rights Management:* Provide common and central detailed management of user rights across all user and programmatic (SDK) interfaces, using roles, users, and user groups:

1. *User Rights:* Define roles, add and delete users, manage permissions for roles, user groups and users, generate user rights management reports.

2. *Roles:* Defining roles establishes permissions (also called “rights”) that determine which system features may be accessed by users and groups. Provide the following security settings for roles:
    a. *Role Info*:
        1) *General:* Smart Client profiles, dual authorization rights.
        2) *Applications:* Login to XProtect Smart Client, XProtect Web Client and XProtect Mobile client.
        3) *Anonymous PTZ Sessions*: Enabling anonymous user information for PTZ sessions.
    b. *Users and Groups*: Users and groups can be assigned to multiple roles.
    c. *Overall System Permissions:* Globally allow or deny permissions for servers, devices and functions (such as manage, read, edit and delete).
    d. *Specific System Permissions:* Allow permissions for specific individual devices and functions:
        1) *Cameras:* Visibility, live view (within time profile), playback (within time profile), search sequences, smart search, export, manual recording, bookmark functions, AUX commands.
        2) *Microphones and Speakers:* Visibility, listen to live audio (within time profile), playback audio (within time profile), search sequences, export, manual recording, bookmark functions.
        3) *Inputs and Outputs:* Visibility, activation.
        4) *PTZ Control:* Manual control, activate PTZ presets, PTZ priority, manage PTZ presets and patrolling.
        5) *Speech:* Speak to speakers, speak priority.
        6) *Remote Recordings:* Retrieve remote recordings.
        7) *External Events:* Visibility, edit, delete, trigger.
        8) *View Groups*: Visibility, edit, delete, operate.
        9) *Servers:* Professional server access and authentication details.
        10) *Matrix*: Visibility.
        11) *Alarms:* Manage, view, disable alarms, receive notifications.
        12) *MIP:* Milestone Integration Platform plug-in permissions.

D. *Client Authentication:* Provide Management Server authentication and authorization of connecting clients (XProtect Smart Client, Management Client and MIP SDK clients) and use a session-limited access token for controlling access to the Recording Server.

E. *System Hardening:* System hardening guide that:
    1. Describes data security, network security and physical security measures and best practices for securing the installed VMS against cyber-attacks. This includes security

considerations for the hardware and software of servers, clients and network device components of a video surveillance system.

2. Incorporates standards-based and best-practice-based security and privacy controls and maps them to each hardening recommendation.

F. *GDPR:* The system must facilitate compliance to GDPR:

1. *GDPR-Ready Certification*: The VMS must have a European Privacy Seal from GDPR ready certificate.
    a. The vendor shall provide comprehensive guides and templates to aid in configuring a GDPR compliant system.
    b. The vendor shall have a clear and concise privacy policy.
2. The system shall provide warnings when use of the system is at risk of going outside GDPR compliance.
3. *Privacy by default*: The VMS must have privacy settings set by default.
    a. The system shall have audio data processing disabled by default.
    b. The system shall have metadata, recording, transmission, and other processing disabled by default.
    c. The system shall have online map services disabled by default.

G. *FIPS 140-2 compliant mode*: The VMS has the ability to operate in a FIPS 140-2 compliant mode.

2.6. LOGGING

A. Provide logging of errors, warnings, system information, user activity, and logs about rules to a centralized database with time, date, and other related information. Logs provide multi-system support and configurable logging limits.

1. *System Logs:* Log all system related errors, warnings and system information, to be used for troubleshooting.
2. *Audit Logs:* Log user activity in client applications including, but not limited to, user system access, configuration changes and operator actions.
3. *Rule-Triggered Logs:* Log rules in which the system administrator has specified the “Make new log entry” action.
4. *Log Exporting:* Logs can be exported as comma-separated-values (.csv) files.
5. *Log Filtering:* Logs can be filtered based on time frame, source name, source type, user, user location, rule name, etc.
6. *Log-Related Options:* Settings can be changed about:
    a. Log retention time.
    b. Which levels (error, warning, and system information) are logged.
    c. Log security.

2.7. SYSTEM FUNCTIONALITY

A. *Configuration Management*:

1. *Real-Time Configuration Change Application:* Immediately apply authorized changes of system configuration data for all sites, including, but not limited to licenses, devices, rules, schedules, users, maps, alarms, recording, client views, including while recording is in operation.
2. *Configuration Data Caching for Continued Operation:* Cached Recording Server configuration data shall ensure continuous operation of Recording Server during periods where the Management Server is inaccessible.
3. *Backup and Restore:* Built-in backup and restore support for manual system backup of all configuration data, including but not limited to:
    a. All system configuration data.
    b. Full device configuration data.
    c. Maps.
    d. Alarm settings and definitions.
    e. Software client views.
    f. User-defined rules and events. Defined video bookmarks.
4. *Configuration Reporting:* Provide complete or partial documentation of system configuration, including custom and site-specific free-text information, contractor's notes and option for logo inclusion.

B. *Application Workspace Optimization*:

1. Options for optimizing application workspaces in the Management Client software:
    a. *Application Layout*: Rearranging layout via drag-and-drop.
2. Options for optimizing application workspaces in the XProtect Smart Client software:
    a. *General*: Control general look and feel and navigation properties, such as color mode, camera title bar, grid sizes.
    b. *Personal or Centrally Enforced*: Optimization can either be made as individual personalization managed by each operator, or centrally enforced using Smart Client profiles.
    c. *View Layouts:* Availability of specific view layouts enforced using Smart Client profiles.
    d. *Themes:* User interface color schemes enabling user choice of dark or light themes.
    e. *Control Panes Availability*: Control availability of control panes and functions in live and playback tabs, and in setup mode.
    f. *Timeline Information*: Control information included in timeline in playback tab.
    g. *Export Behavior*: Control behavior and availability of export function.
    h. *Keyboard and Joystick Setup*: Setup of keyboard short cuts and joystick controls.

i. *Alarm and Access Control Notifications*: Control behavior of alarms and access control notifications.

j. *Application Language*: Control application language.

k. *Advanced Application Settings*: Control advanced application settings such as use of hardware acceleration, videos diagnostics overlay and time zone settings.

C. *Device Discovery and Management*:

1. Add Hardware wizard to automatically discover and upon approval add devices to system using Universal Plug and Play (UPnP) discovery, IP network range scanning, or manual device detection. User ability to perform initial setup of credentials on devices without factory default credentials detected. Must be supported for Axis, Bosch, Hanwha Techwin, and for ONVIF profile Q conformant devices.

2. Replace Hardware wizard for swift replacement of malfunctioning devices with preservation of configuration settings and recordings, including those for attached cameras, microphones, speakers, inputs, outputs and metadata devices.

3. Move Hardware wizard for moving devices and related devices from one Recording Server to another during runtime with no loss of settings, recordings, rules, permissions etc.

4. User ability to enable and disable devices for purposes of maintenance or temporary deactivation.

5. User ability to change the password of one or multiple devices based on a pre-configured time interval. Must be supported for Axis, Bosch, Canon, Hanwha Techwin, Hikvision, Panasonic, Sony and ONVIF-compliant devices.

6. User ability to see the firmware version of each device.

7. User ability to update information about the firmware and features available for a device.

8. User ability to upgrade the firmware of single devices. Must be supported for Axis, Bosh, Hanwha, Techwin and ONVIF.

1. For ONVIF Profile T & Q compliant devices. User ability to manage a VMS user account that communicates with a device. Add a user, list an existing user, and delete a user.

2. For ONVIF Profile T & Q compliant devices. User ability to manage network configuration. Change IP address, subnet mask, and default gateway.

D. *Camera Image and Video Stream Management:* Adjustment of per-camera and per-video stream settings, with each camera allowed one or more streams for live viewing and one stream for recording, including an optional per-camera or per-camera-group preview window:

1. *Per Camera*:

a. *General Settings*: Change all camera specific general settings such as brightness, color level, compression, maximum bit rate, resolution and image rotation.

b. *Camera Video Stream Settings*: Define as many different streams as specific camera support. Change individual stream settings such as FPS, resolution, image quality, video encoding format and resolution.

2. *Per Camera Group*:

   a. *General Settings*: Change all common camera specific general settings for the camera group such as brightness, color level, compression, maximum bit rate, resolution and image rotation.

   b. *Camera Video Stream Settings*: Define as many different streams as specific camera support for the camera group. Change individual stream settings such as FPS, resolution, image quality, video encoding format and resolution.

   c. One camera can be associated to multiple camera groups.

1. *Video Streams:* Define one camera video stream used for recording and one camera video stream to be used for live viewing.

3. *Recording*: Manage recording functionality including:

   a. Related device recording.

   b. Manual recording timer.

   c. Pre-buffer use.

   d. Recording framerate.

   e. Media storage assignment.

   f. Automatic retrieval of edge recordings.

4. *Fisheye Lens Viewing:* Capability for fisheye lens camera views provided through utilization of the ImmerVision Enables panomorph lens technology. Other lenses than ImmerVision can be supported by using a generic dewarping lens profile or a third-party plug-in.

5. *Motion Detection*: Manage motion detection functionality including:

   a. Motion sensitivity.

   b. Processing all frames or keyframes only.

   c. Generation of motion metadata for smart search.

   d. Exclusion zones.

6. *Camera Events*: Define which camera events will be forwarded to the VMS.

7. *Client Settings*: Define client related functionality including:

   a. Related devices.

   b. Keyboard shortcut.

8. *Privacy Masks:* Permanent and liftable system-defined camera image privacy masks hide certain areas in the camera image for live view, recording, and video export.

   a. Permanent Masks: Allow a system admin to mask areas in cameras at all times and for all users. Permanently masked areas cannot be revealed once recorded.

b. *Liftable Masks:* Allows a system admin to establish default mask areas in cameras at all times and for all users, but with the option to sufficiently privileged operators to temporarily remove the masks for authorized users if needed – such as during investigation.

c. *Masking Level:* When establishing a privacy mask, system admins may select a mask level on a scale between 'light blur' to 'solid grey'.

E. *PTZ Camera Control:* Camera-based and system-based PTZ camera control including the following capabilities.

1. *Camera PTZ preset positions:* Camera-based PTZ presets may be imported from the camera and renamed for use in system-based manual and automatic PTZ control.

2. *Automated Use of PTZ Presets:* Scheduled and event-based rules capability to move PTZ cameras to pre-set positions.

3. *System-Based PTZ Preset Positions:* System-based PTZ presets are definable for use in system-based manual and automatic PTZ control.

4. *PTZ Patrolling:* Multiple per-camera PTZ patrolling schemes may be defined with the following options:

a. Adjustable wait times between preset position changes.

b. Disabling of motion detection to avoid false detection alarms.

c. Multiple patrolling schedules per camera per day, with different schedule for days, nights and weekends.

2.8. EVENT AND ALARM MANAGEMENT

A. *Rules Engine:* Provide rules for automating of different aspects of the system, including camera control, system behavior and external devices, based on events or time profiles, or a combination of events and time profiles.

1. *Trigger Events:* Provide a Microsoft-Outlook-style configuration dialog where pre-defined and custom-defined events are used in rules to trigger actions.

a. *Event Categories:* Organize events into the following categories:

1) *Hardware:* Physical hardware devices connected to the system.

2) *Devices:* Certain functions and states of devices available via connected hardware devices.

3) *External:* Relating to VMS integrations.

4) *Recording Server: A*rchivingand database functions.

5) *Analytics:* From integrated analytics applications and systems.

6) *User-Defined:* Custom-configured events enabling users to manually trigger actions and events in the system.

2. *Start Actions:* Triggering events may initiate a wide set of system actions, including, but not limited to:

a. Control start and stop of recording, including scheduled and event-based recording.

b. Change camera stream properties.

c. PTZ camera preset positions and patrols.

d. Event-based notifications, including email notifications to single or multiple recipients with optional attachment of a camera still image or AVI video clip.

e. External system interactions.

f. Play pre-recorded audio.

g. Retrieve video and audio from edge storage devices.

h. Single rule allows for executing multiple system actions.

i. Rule actions shall be triggered by event, time interval or a combination of event and time.

j. Rules shall be optionally stopped by event or after a specified time.

k. Unrestricted number of rules.

B. *Time Profiles:* Provide the following time profile functionality for use with profiles, rules and triggers:

1. Time profiles contain one, or more, single or recurring periods of time.

2. A single time period may span one or more days, defined by a starting date and time and an ending date and time.

3. A recurring period of time is defined as a time range with recurrence pattern and range:

a. Time range is a starting and ending time within a day.

b. Recurrence pattern may be Daily, Weekly, Monthly or Yearly.

c. Recurrent range is a starting and ending date, or a starting date with a duration in days.

4. Unrestricted number of time profiles.

C. *Single-Point Event/Alarm Management:* Provide central management of all internal system alarms and external security alarms. Events are pre-defined or user-specified incidents on the VMS that can be set up to trigger an alarm, including analytics events and manual control actions. Event and alarm management capabilities shall include but not be limited to:

1. *Alarm Data Settings*:

a. Customizable alarm priorities, statuses and categories to enable alignment of the alarm handling workflow with existing workflows and security systems.

b. Optional sound notifications for different alarm priorities for notification of new incoming alarms.

c. Manage which alarm priorities trigger desktop notifications for alarms.

d. Manage which alarm data are shown in the Alarm Manager, including but not limited to:

1) ID.

2) Image.

3) Location.
4) Message.
5) Owner.
6) Priority Level.
7) Source.
8) State Level.
9) State Name.
10) Time.

e. Optional Reasons for Closing to be chosen when an alarm is closed.
f. Add audio files in wav-format to be used as alarm notification sounds.
g. Manage how long alarms instances are kept in the system before being automatically deleted.

2. *Alarm Configuration*:
   a. User-definable alarm descriptions and work instructions.
   b. Select triggering event and source.
   c. Alarm time profiles specifying that response actions must take place within the specified time profile.
   d. Select start and stop events specifying that response actions must take place within the specified event window.
   e. Select a user defined event to be triggered if an alarm is not acknowledged within a defined time limit.
   f. Association of alarms with one or more cameras, with automatic display of camera video in the alarm preview window, with a minimum of 15 cameras showing simultaneously in the alarm preview window.
   g. Association of alarms to maps.
   h. Association of initial alarm owner (individual user or group) and priority.
   i. Association of alarm category.
   j. Select user defined event to be triggered by the alarm.
   k. Enable or disable desktop notifications for alarms.
3. *Alarm Manager*:
   a. Alarm list with extensive sorting and filtering capabilities.
   b. Instant preview of recorded video from primary and related cameras, at the time of the incident.
   c. Thumbnail image from primary camera, at the time of the incident.
   d. Alarm disabling option shall enable users to suppress alarms from a given device for a specified time period.

e. Alarm handling reports providing information about alarm inflow and alarm handling performance.

4. *Alarm Handling*:
   a. Instant preview live video of primary camera.
   b. Instant preview of recorded video from primary and related cameras, at the time of the incident.
   c. Option to select any related cameras to be displayed in the live and playback view items.
   d. Present the alarm work instructions.
   e. Change priority and status of the alarm.
   f. Alarm escalation with option to forward alarms to operators with appropriate skills to handle specific types of alarms.
   g. Present time logged alarm activities.
   h. Add time logged comments to the alarm incident.
   i. Desktop notifications shall allow immediate access to alarm handling.
5. *Map Integration*:
   a. Present incident location automatically on the map allowing operators to view and acknowledge active alarms.
6. All other map functionality must be available when viewing maps in the Alarm Manager. *XProtect Web Client*: Provide the following alarm list, alarm handling and investigation functionality:
   a. *Alarm List*:
      1) Alarm list with filtering capabilities:
         a) All or personal alarms.
         b) All or specific alarm states.
         c) All or specific alarm priorities.
      2) Thumbnail image from primary camera, at the time of the incident.
      3) Click to handle alarm.
   b. *Alarm Handling*:
      1) Instant preview of recorded video from primary and related cameras, at the time of the incident. Available incoming audio for cameras that have related microphones.
      2) Present the alarm work instructions.
      3) Change priority and status of the alarm.
      4) Alarm escalation with option to forward alarms to operators with appropriate skills to handle specific types of alarms.

7. *XProtect Mobile Client*: Provide the following alarm notification, alarm list, alarm handling and investigation functionality:
    a. *Alarm Notification*: Receive alarm notifications using Push Notifications. Notifications include access to:
        1) Video.
        2) Alarm information.
        3) Work instructions.
    b. *Alarm List*:
        1) Alarm list with filtering capabilities:
            a) All or personal alarms.
            b) All or specific alarm states.
            c) All or specific alarm priorities.
        2) Thumbnail image from primary camera, at the time of the incident.
        3) Click to handle alarm.
    c. *Alarm Handling*:
        1) Instant preview of recorded video from primary and related cameras, at the time of the incident.
        2) Present the alarm work instructions.
        3) Change priority and status of the alarm.
        4) Alarm escalation with option to forward alarms to operators with appropriate skills to handle specific types of alarms.

2.9. VIDEO PROCESSING AND VIEWING

A. *Multiple Monitor Support*: Support multiple monitors where each monitor shall show multiple floating or full-screen windows for display of views or individual view items.

B. *View Window Aspect Ratios:* Support multiple views optimized for 4:3 and 16:9 display settings in both landscape and portrait orientations.

C. *Private or Shared Views:* Private views can only be access by the user who created them. Views may be shared generally and available to all roles or restricted to specific roles.

Viewing of a content item in a shared view is subject to the viewer's permissions relating to the content item.

D. *View Groups:* View groups facilitate view navigation and simplify searching across multiple views by narrowing search scope.

E. *View Layout Persistence*: Same view layout in both live and playback modes.

F. *View Arrange and Restore:* Support simple drag-and-drop re-arrangement of cameras in views for optimized monitoring of incidents, including replacement of individual cameras with different cameras, with single-click restore of original view layout.

G. *View Creation:* Views that display up to 100 view items including cameras, web pages, still images, text and interactive items. View capabilities include, but are not limited to:

1. *Camera View Item:* Live and recorded camera video displayed in resizable view windows, utilized in several workspaces within the application. Each camera view item contains the following:

a. *Video Status Indicator:* A round dot indicating one of four states:

1) *Green:* A connection to the camera is established.

2) *Red:* Video from the camera is being recorded.

3) *Yellow:* Playing back recorded video.

4) *Gray:* The video has not changed for more than two seconds.

b. *Motion Indicator:* An icon of a moving person that appears only when motion is detected since it was last cleared.

c. *Bounding-Box Display:* Display of metadata bounding boxes as provided by supported cameras and integrated analytics in live and playback views.

d. *Update on motion only:* Optimizes CPU use by allowing motion detection to control whether the image should be decoded and displayed.

e. *PTZ Camera View Item:* PTZ camera view item can be configured to provide virtual joystick camera control and PTZ navigation overlay buttons on the video image.

f. *Overlay Buttons:* Used to add manually controlled speakers, events, outputs, PTZ cameras and to start/stop recording.

2. *Carousel:* Allow a specific view item to automatically sequence rotate through pre-defined set of cameras that are not necessarily present in the view at the same time. Operators may select default or custom display times for each camera, and they are able to manually switch to the next or previous camera in the carousel list.

3. *Hotspot:* Global hotspot function shall allow users to work in detail with any camera selected from any view. Local hotspot function shall allow users to work in detail with a camera selected from the same view.

4. *HTML Page*: Show interactive HTML page.

5. *Image:* Show a still image.

6. *Matrix:* Shows live video from multiple cameras in any view layout with customizable rotation paths, remotely controlled by the computers sending matrix remote commands.
7. *Navigable Map Pages:* Static or active map pages may be used to provide a good overview of premises, and for switching between different views, such as map page displaying a floor plan.
8. *Text*: Add text.
9. *3rd party plug-ins*: Add 3rd party plug-ins to extend the behavior of XProtect Smart Client.

H. *Live Video*: Views provide camera live viewing capabilities including, but not limited to:

1. *Live Viewing:* View live video of camera view items on the Live tab.
2. *Manual PTZ Control:* Manual PTZ control options:
    a. Video overlaid PTZ control.
    b. Joystick.
    c. Virtual joystick function.
    d. PTZ point-and-click control.
    e. PTZ preset positions.
    f. Overlay buttons to activate PTZ preset positions.
    g. PTZ zoom to a defined rectangle.
    h. Start, stop, and pause patrolling.
    i. View who have PTZ control and time to automatic release, including anonymous users.
3. *Send Video to Destination*: Option to send current camera to the following destinations:
    a. View item in an existing window.
    b. New floating window.
4. *Digital Zoom:* Magnification of video to facilitate detail viewing.
5. *Bookmarks:* Create quick or detailed bookmarks, to facilitate incident review and documentation.
    a. System generated headline for quick bookmark.
    b. Optional headline and description information for detailed bookmark.
6. *Independent Video Playback*:
    a. Playback of video in multiple camera view items, each on its own independent timeline.
    b. Option to initiate playback mode and synchronizing playback timeline with current time in independent playback.

7. *Instant Change of Camera:* Drag-and-drop placement of a different camera in a camera view item, instantly changes the content to video from the new camera, according to the camera view item's current timeline position.
8. *Centralized Search*: Initiate Centralized Search for the camera in a new window.
9. *Manual Recording*: Start and stop manual recording with automatic stop of recording after a configurable number of minutes.

I. *Video Playback:* Views provide additional camera playback capabilities including, but not limited to:

1. *Playback:* Time synchronized play back video of camera view items on the Playback tab.
2. *Navigation:* Advanced video navigation includes:
   a. Forward and backwards playback at different speeds:
      1) *Playback Speeds*: ¼x, ½x, 1x, 2x, 4x, 8x, 16x.
      2) *Instant Realtime Speed*: Toggle 1x playback speed or selected playback speed.
   b. Forward and backwards frame-by-frame.
   c. Skip to next or previous recorded sequence.
   d. Skip to beginning or end of recordings.
   e. Jump to date/time.
3. *Timeline:* An overview of recorded sequences and bookmarks via integrated video timeline with time navigation and playback controls, including the following functionality:
   a. *Timeline Video Playback:* Video from multiple camera view items integrated to a common video timeline, with common timeline control from any of the integrated camera view item.
   b. *Single and Consolidated Timeline*: Two timelines with the first showing overview of selected camera view item and second showing a consolidated overview of all camera view items in the view.
   c. *Timeline Period*: Select which period timeline covers.
      1) 5, 10, 20 minutes.
      2) 1, 2, 4, 8, 12, 16, 20 hours.
      3) 1, 2, 4 days.
      4) 1, 2, 4 weeks.
   d. *Recorded Sequences Overview*: Recorded sequences of video and audio are shown in the timeline. The timeline displaying light-red to indicate recording, red for motion, light-green for incoming audio, and green for outgoing audio. If there are additional sources of data available, these are displayed as other colors.
   e. *Bookmarks Overview*: Bookmarks are shown in the timeline with instant preview of the recorded video.

f. *Integrated Time Interval Selection*: Integrated function to select a time interval for export or video and audio retrieval from edge storage devices.

1) Visual selection on timeline.

2) Select start and end date/time.

3) Loop selected period on playback.

g. *Multi-Window Timeline*: Ability to use one timeline to control playback of cameras in multiple view windows.

4. *Recording Search:* Search listing of camera sequences or bookmarks.

a. *Preview*: Search results may be previewed.

b. *Print*: Print of still image from the selected video clip may be initiated.

c. *Export:* Export of selected video clips may be initiated, reducing time needed to prepare forensic video material.

J. *Two-Way Audio:* Audio from cameras with built-in or attached microphones can be configured for listening. Camera built-in or attached speakers can be configured for use to talk to individuals near speakers. Additional capabilities include:

1. *Broadcast:* Broad announcements can be made by selecting the All Speakers option when talking.

2. *Lock to Selected Audio Devices:* Enables continued use of microphones and speakers from selected cameras, while viewing video from a different set of cameras. This enables, for example, informing an individual at risk about the safety status of nearby areas.

3. *Level Meter:* Level meter indicates the volume of the speaking operator's voice, to indicate whether the operator is at a correct distance from the microphone.

K. *Centralized Search:* Shall enable users to apply search categories and filters to find recording sequences, recordings with motion and bookmarks. From the search results, users shall be able to preview video and perform various actions, e.g. by exporting the search results or sending the search results to PDF. The search results shall be presented instantly as thumbnail images:

1. *Sequence Search:* Search in recording sequences on one or more cameras.

2. *Motion Search:* Search for sequences with motion, or Smart Search for motion in selected areas on one or more cameras.

3. *Bookmark Search:* Search for bookmark headlines or descriptions.

4. *Navigation:* Ability to jump to search results through a clickable timeline, or the ability to scroll through the search results.

5. *Preview:* Selected sequence previews with auto play and direct export support.

L. *Video Export and Documentation:* Smart Client options for video export and documentation include, but are not limited to:

1. *Snapshot:* Produce instant visual documentation of a camera by saving the camera image to a file.

2. *Print:* Produce instant visual documentation of a camera by sending it directly to a printer.
3. *Storyboarding:* The storyboarding function makes it possible to include video sequences from different or overlapping time intervals from different cameras in the one and the same export.
4. *Export XProtect Format:* Export in XProtect format; including the standalone XProtect Smart Client — Player application for simple instant viewing by authorities.
5. *Export Preview:* Review video just prior to export, with looped playback option.
6. *Export Other Formats:* Create evidence material in media player format (AVI files), MKV format, or still image format (JPEG images).
7. *Re-Export:* Re-Export allows an authorized individual to export a digitally signed selection from the original video exported. Option to disable re-export, during initial export to XProtect format, prevents undesirable re-distribution of sensitive video recordings.
8. *Bulk Export:* In a single step, export in multiple formats to multiple destinations, including direct export to optical media, to ensure consistency across exported video sequences in various formats, and reduce human error possibilities.
9. *Export of Comments:* Two video formats support inclusion of comments in exported video:
    a. *XProtect Format:* Include general and/or camera-specific comments to a video export file.
    b. *Media Player Format:* Include comments as pre/post slides.
10. *Video Incident Report Printing:* Utilize still images rather than clips to print incident reports including images, surveillance details and free-text user comments.

2.10. MAPS

A. *Maps:* Provide multi-layered physical overview of surveillance video coverage, with interactive access to and control of the VMS and related devices, including the following elements:
    1. *Map Images:* Illustrated maps or photographs. Supported image file formats are: BMP, GIF, JPEG, JPG, PNG, TIF, TIFF, and WMP.
    2. *Camera Icons:* Indicate camera locations on the map. Fixed camera icons show camera view as colored angle radiating from the camera. PTZ camera icons show preset camera views as colored angles radiating from the camera.
        a. *Live Preview:* Hover mouse pointer over camera icon to display a live preview in a resizable window.
        b. *PTZ Preset Navigation:* Click on PTZ preset view zone moves camera to the preset position.
    3. *Microphone Icons:* Microphone icons show microphone locations on the map.

a. *Live Listening:* Place mouse over microphone icon; press and hold left mouse button to listen to incoming audio from microphone.

4. *Speaker Icons:* Indicate speaker locations on the map.
   a. *Live Speaking:* Place mouse over speaker icon; press and hold left mouse button to talk through speaker.
5. *Control Icons:* Icons to use for control of objects such as doors, gates, and lights.
6. *Hot Zones:* Hot zones to provide vertical navigation through a hierarchy of maps by clicking on a hot zone.
7. *Map Overview Window:* Navigable overview of map hierarchy set up in XProtect Smart Client.
8. *Map Image Updates:* When map images are replaced by an updated version of the map image of the same scale, map icons and other elements are kept in their original locations.
9. *Map Display Information:* Information display options include but are not limited to:
   a. Real-time status monitoring indication from all system components including cameras, I/O devices and system servers.
   b. Graphical visualization of the system status through color coding.
   c. Hierarchical propagation of status indications to higher ordered maps.
   d. Different levels of status indications available (alarm, warning and errors).
   e. System performance data for cameras and servers including camera resolution, FPS, network use and disk space.
   f. Ability to suppress status indications (such as alarms and operational status) for a given device.
   g. Editable device names in map and map-specific names and references assignable to devices in Map, subject to user permissions.

2.11. MEDIA STORAGE MANAGEMENT

A. Provide multiple media storage containers definable with the following characteristics:
   1. *Container:* Each container consists of a live database and optionally one archive database, with container-specific archiving scheme and retention times. Archive database can reside on the same disk as the live database or on secondary disk or network drive.
   2. *Capacity:* Maximum recording capacity shall be limited only by available disk space or configured container storage limit.
   3. *Device Assignment:* Recording of each device is assigned to a specific storage container. The assigned storage container for a device or group of devices may be changed from one container to another.

4. *Archiving:* Recorded video data may be automatically moved from a container's live database storage to its archived storage. Archived data is still online and available to client software.
5. *Maximum Recording Times:* Maximum recording times may be set for manual recordings, with VMS deleting older video to free up storage for newer video.

B. *Edge Video Storage:* Provide utilization of camera-based storage including the following capabilities:

1. *Video and Audio Retrieval:* Retrieving video and audio recordings across low-bandwidth connections based on time profiles, events or manual requests.
2. *Video and Audio Consolidation:* Consolidating video and audio from multiple storage mechanisms:
    a. Seamless merging of video and audio stored centrally in media database, and video and audio retrieved from associated camera edge storage, or from an interconnected system.
    b. Optionally consolidate pre-event images recorded locally in camera or video encoder.
3. *Scalable Video Quality Recording (SVQR):* Capability to record high quality video using edge storage and record low quality video centrally, to minimize network bandwidth utilization, using the capabilities described above. High quality video can be retrieved when needed, on an event-driven, scheduled or manual basis.

2.12. XPROTECT MOBILE SERVER

A. *User Authentication:* Facilitate the following methods of user authentication:

1. *Basic Authentication:* Basic user VMS account.
2. *Windows Authentication:* Via Active Directory or local Windows user account. Possible to use current Windows user to facilitate single sign-on.

B. *Direct Streaming:* Configure the use of client requested live video streams without server transcoding.

C. *Adaptive Streaming:* Configure the use of automatic live video streams selection depending on the resolution requested by the client.

D. *Dynamic Bandwidth Optimization:* Optimize camera video stream from server to client to make optimum use of bandwidth.

E. *Bookmarks:* Enable the use of bookmarks in live video and recorded video.

F. *Smart Connect:* Easy configuration of internet access to the Mobile Server by automatic configuration of firewalls and internet routers via UPnP, with verification of configuration

and operation of internet connection, with option to email connection details to XProtect Mobile client users. Includes automatic Mobile Server on LAN via UPnP.

2.13. XPROTECT WEB CLIENT

A. Provide the following browser-based capabilities:

1. *User Authentication*:
    a. Require only username and password.
    b. Enable basic users to change password during login.
    c. User authentication and authorization is handled by XProtect Mobile Server.
2. *Inherit System Views:* Automatically obtain the user's private and shared views configuration from the system.
3. *All-Camera View:* Automatically generate a view for all cameras when no views are set up.
4. *Two-Way Audio:* Audio from cameras with built-in or attached microphones can be configured for listening. Camera built-in or attached speakers can be configured for use to talk to individuals near speakers. Audio playback shall be available for investigations, video exports and alarms. Additional capabilities include:
    a. *Broadcast:* Broad announcements can be made by selecting a microphone icon on the view level when talking.
    b. *Use the Push-to-talk (PTT) Feature:* Communicate via the VMS system, through a PC microphone and while watching live video from one camera, with people near a video camera with audio equipment. Push-to-talk (PTT) is also available in Actions.
5. *Live Video Monitoring:* View live video with PTZ control including use of presets, video playback, and triggering of camera-related outputs and events from within the camera's view.
6. *Search:* Search function to find cameras, types of camera, cameras with related microphones, cameras with related speakers and camera views.
7. *Video Export:* Provide video export, with the option to preview and store exported video on the server, and make it available for later usage or download, for example, when a higher-bandwidth connection is in use:
    a. *AVI, MKV, XProtect Format files:* Ability to create AVI, MKV or XProtect format export files.
    b. *Still Image Export:* Provide camera view JPEG image export.
    c. *Audio:* Option to include audio in the export package.
    d. *Export On Server:* Ability to export on the server to avoid moving large files.
    e. *Exceed Retention Time:* Ability to store video recordings for a period that is longer than the retention time.

f. *Play Back Deleted Recordings:* Ability to play back the recordings even if the recordings have been deleted from the media database.

g. *Reduced Download:* Ability to download only needed files or save them for downloading when on a faster connection.

h. *Preview On Server:* Preview exports on the server without downloading them.

8. *Data Integrity Of Exported Video:*

a. *Encryption And Password Protection:* Option to encrypt and password protect any of the available export formats.

b. *256-bit AES Encryption*: Ability to encrypt exports using 256-bit AES algorithm.

c. *Digital Signature:* Digitally signed media exports with SHA-2 algorithm to establish a means of detecting modification of exported video.

9. *Bookmarks:* Bookmarks shall be applicable for live video and recorded video:

a. Ability to create quick or detailed bookmarks to facilitate incident review and documentation.

b. Ability to edit and delete bookmarks and to use filtering to find bookmarked video.

10. *Secure Connection:* Connect to XProtect Mobile Server through trusted CA certificates for HTTPS encryption.

11. *Supported Browsers*:

a. Microsoft Edge

b. Safari

c. Google Chrome

d. Mozilla Firefox

12. *Browser Plug-Ins or Extensions*: No plug-ins or extensions to be installed.

2.14. XPROTECT MOBILE CLIENT

A. Provide the following native-app mobile client capabilities:

1. *User Authentication*:

a. Require only user name and password.

b. Enable basic users to change password during login.

c. User authentication and authorization is handled by XProtect Mobile Server.

2. *Multiple Server Profiles:* Select between multiple server profiles to facilitate easily switching between sites or different connection addresses.

3. *Views and View Groups:* Automatically obtain the user's private and shared views from the system to be used as camera lists.

a. *View Groups:* Views shall be organized in view group folders. View groups shall also have the capability of organizing subordinate view groups.

b. *All-Camera View:* Automatically generate a view for all cameras when no views are set up.

4. *Two-Way Audio:* Audio from cameras with built-in or attached microphones can be configured for listening. Camera built-in or attached speakers can be configured for use to talk to individuals near speakers. Audio playback shall be available for investigations and alarms. Additional capabilities include:

   a. *Use the Push-to-talk (PTT) Feature:* Communicate via the VMS system, through the microphone of the mobile device and while watching live video from one camera, with people near a video camera with audio equipment. Push-to-talk (PTT) is also available in access control.

5. *Full-Screen View:* Display cameras in full screen to take better advantage of the mobile device's screen, with camera view navigation in full screen by swiping left or right.

6. *Pinch-To-Zoom:* Digital pinch-to-zoom shall enable mobile users to enlarge a part of the image for closer review and conduct detailed investigation of video.

7. *Picture-In-Picture*: Provide the following functionality for Picture-In-Picture:

   a. Display a live picture-in-picture frame of the same camera when in playback mode.

   b. The picture-in-picture shall be movable by dragging.

   c. Double-tapping and will return to live view.

   d. Hide live picture-in-picture frame.

8. *Search:* Search function to find cameras, types of camera, cameras with related microphones, cameras with related speakers, and camera views.

9. *Navigation:* Ability to navigate recorded video using a time picker and to adjust the start time by dragging a timeline scroller.

10. *Bookmarks:* Bookmarks shall be applicable for live video and recorded video.

   a. Ability to create quick or detailed bookmarks to facilitate incident review and documentation.

   b. Ability to edit and delete bookmarks and to use filtering to find bookmarked video.

11. *Mobile Video Push:* Provide XProtect Mobile client capability for mobile device users to use their mobile device cameras as cameras in the VMS, including the following characteristics:

   a. *No Mobile Setup:* No mobile device setup shall be required for mobile video push. Provide central server-side configuration.

   b. *Metadata Support:* Mobile users shall be able to include metadata in the video submitted.

   c. *Audio*: Mobile users shall be able to include audio in the video submitted.

12. *Investigation*: Provide access to investigations created in the XProtect Web Client.

13. *Secure Connection:* Connect to XProtect Mobile server through trusted CA certificates for HTTPS encryption.

14. *Supported Mobile Operating Systems*:
    a. Android
    b. iOS

2.15. SDK-BASED INTEGRATION

A. *Milestone Integration Platform Software Development Kit (MIP SDK)*: The VMS shall support a software development kit (*MIP SDK*) that allows integrating the video management system with third-party applications, for example access control and video analytics.

B. *Integration Types and Functionalities*: Integration of third-party applications and plug-ins shall be possible in three different ways:

1. Integration through network protocols shall allow for the possibility to choose coding platform. Protocol integration shall make it possible to:
    a. Retrieve, save, and change the configuration of the VMS through a SOAP or RESTful API.
    b. Retrieve live or recorded video, audio, and metadata.
    c. Send control commands and events to the VMS.
    d. Receive VMS status information, for example if a camera is down or a server is running out of space.
    e. Implement protocols on Windows, Java® and Linux® systems.
2. Integration through the .NET libraries which shall allow for using software components to integrate with the VMS. .NET integration shall make it possible to:
    a. Retrieve, save, and change the configuration of the VMS.
    b. Retrieve live and recorded audio and metadata.
    c. Display live and recorded video with optional overlay of graphics.
    d. Issue control commands to the VMS or related device, for example a camera with PTZ and outputs.
    e. Send and receive events to the VMS.
3. Integration through a plug-in embedded directly into the VMS environment that shall run as part of the VMS and client applications. Plug-in integration shall make it possible to:
    a. Be integrated with the event server, enabling the event server to use plug-in functionality. This shall allow event-based functionality to be executed without the need for an open user interface.
    b. Be integrated with XProtect Smart Client, enabling the application to use plug-in functionality.
    c. Be integrated with XProtect Management Client, enabling the application to use plug-in functionality.

d. Plug-ins shall be able to run across all products and versions of the VMS.

e. Plug-ins shall be able to listen for events from other plug-ins.

f. It shall be possible to activate licenses for third party plug-ins in XProtect Management Client.

C. *Integration Capabilities*: Third party applications shall be able to integrate with the VMS to access a variety of functionalities:

1. *Video, Audio, and Metadata Functionality:*

a. Retrieve and play live and recorded video.

b. Retrieve and play live and recorded audio.

c. Retrieve and access live and recorded metadata.

d. Retrieve and display single images (JPEG).

e. Export video and audio in AVI, MKV and native database format.

f. Place overlay information on live and recorded video in component-based implementation and in plug-ins for XProtect Smart Client.

g. Create, find, and delete bookmarks.

2. *Configuration:*

a. Retrieve and change VMS configuration, including camera, user and alarm information.

b. Enable third party applications to save and retrieve their own configuration.

3. *Authentication and Authorization*. Logins and authorization of third-party plug-ins, applications and protocol integrations:

a. Manage user rights on plug-in functionality.

b. A framework for system access and security token handling.

4. *Event and Alarms:*

a. Trigger internal (system-related) and external (integrated) events and alarms.

b. A specific event can trigger start or stop recording.

c. Search for existing alarms and events.

d. Update and acknowledge alarms.

5. *Licensing*. Read licenses and add own plug-in license:

a. Licensing of third-party integrations

b. Integration with online registration

6. *System status:*

a. Receive all status messages from the VMS, including server disk, CPU usage, and triggered events.

7. *Control*. Trigger output, control PTZ, start/stop recordings:

a. Send PTZ commands to cameras.

b. Retrieve PTZ position from absolute PTZ cameras.

c. Send a start or stop recording event from a specific event.

d. Set bookmarks in recording.

e. Activate external output.

f. Control video wall application functionality.

g. Send camera to a video-sharing monitor.

h. Send commands to third party-developed plug-ins.

i. Playback time controller.

j. Support for displaying plug-in items on smart map in XProtect Smart Client.

k. Change XProtect Smart Client theme

8. *System and Audit logs*. Generate log entries and reads logs:

a. Write and read systems and audit logs.

D. Use cases:

1. Compatibility with XProtect Transact, which integrate video surveillance with automatic teller machines (ATM), point-of-sale (POS) and enterprise resource planning (ERP) systems for managing loss prevention and fraud.

2. Compatibility with XProtect LPR for automatic reading and tracking of vehicle license plates.

3. Event integration via a simple message-based socket communication interface enabling external applications to trigger events in the VMS.

4. Functionality for external applications to trigger user-defined events in the VMS.

2.16. COMPUTER EQUIPMENT

A. *Computer Requirements:* Consult with VMS manufacturer to determine current computer requirements appropriate for system design, intended use and desired level of performance. Optimize server computer count, and server application distribution across servers, to account for likely system expansion. The following are minimum requirements.

1. *Computer Running XProtect VMS*:

a. *CPU:* Intel® Core™ i3 or better.

b. *RAM:* 16 GB or more.

c. *Network:* Ethernet 2 x 1 Gbit or better.

d. *Graphics Adapter:* Onboard GFX, AGP or PCI-Express, minimum 1024×768, 16-bit color or better.

e. *Hard Disk Space:* 50 GB free or more (depends on number of servers, devices, rules, and logging settings).

f. *Operating System*:

1) *For Individual Servers*:
   a) Microsoft Windows 8.1 Pro (64 bit).
   b) Microsoft Windows 8.1 Enterprise (64 bit).
   c) Microsoft Windows 10 Pro (64 bit).
   d) Microsoft Windows 10 Enterprise (64 bit).
   e) Microsoft Windows 10 Enterprise LTSB (Long-Term Servicing Branch) 2016 (version 1607 or later).
   f) Microsoft Windows 10 IoT Enterprise, version 1803 or later (64 bit), IoT Core.
   g) Microsoft Windows Server 2012 (64 bit): Standard and Datacenter.
   h) Microsoft Windows Server 2012 R2 (64 bit): Standard and Datacenter.
   i) Microsoft Windows Server 2016 (64 bit): Essentials, Standard and Datacenter.
   j) Microsoft Windows Server 2019 (64 bit): Essentials, Standard or Datacenter.
2) *To Run Clustering/Failover Management Server*:

g. *Software*:
   1) Microsoft .NET 4.7.2 Framework.
   2) Microsoft .NET Core 3.1.13.
   3) DirextX 11 or newer.

2.17. LICENSING

A. *License Activation:* VMS shall offer easy-to-use automatic or manual online activation via the Internet and alternatively, offline activation via email and web for closed surveillance networks.

B. *Server Base License*:
   1. Require one mandatory XProtect Professional+ server base license for installing the product.
   2. Server base license shall permit the following deployments within the legal entity purchasing the base license:
      a. Unrestricted number of Management Server services.
      b. Unrestricted number of Recording Server services.
      c. Unrestricted number of XProtect Smart Client, XProtect Web Client and XProtect Mobile client applications.

C. *Hardware Device License*:
   1. Require one license per hardware IP address to connect:
      a. Cameras.

b. Audio devices.

c. Video encoders.

d. Other devices.

2. Support an unlimited number of hardware device licenses.

D. *License Overview Information:* License overview shall include add-on products.

E. *License Administration:* Provide license information presenting the license use.

F. *Changes Without Activation:* A "Changes without activation" function shall allow additions and replacements of limited number of devices without requiring license device activation or reactivation.

PART 3. EXECUTION

3.1. EXAMINATION

A. *Verification of Conditions*:

1. Visit site and verify that site conditions are in agreement with design package. Report all changes to the site or conditions which will affect performance of the system to the Owner. Do not take any corrective action without written permission from the Owner.

2. *General*:

a. Verify that existing site conditions are acceptable for product installation in accordance with manufacturer's instructions.

b. Verify that wire runs, related items, and conditions are ready to receive work of this Section.

3. *Cable and Wiring*:

a. Examine pathway elements intended for cables. Check raceways, cable trays, and other elements for compliance with space allocations, installation tolerances, hazards to cable installation, and other conditions affecting installation.

b. Examine roughing-in for LAN and control cable conduit systems to PCs and other cable-connected devices to verify actual locations of conduit and back boxes before device installation.

4. *LAN / WAN*:

a. Verify LAN connections for server and workstation computers.

b. Provide access to the internet for the Mobile Server.

5. *Power Connections*:

a. Verify power circuits which are existing or have been previously installed under other sections are acceptable for product installation in accordance with manufacturer's instructions.

3.2. PREPARATION

A. Review configurable features of the VMS with the Owner's Representative and document the results of the meeting in the Project planning documents. The following configuration topics shall be resolved prior to configuring equipment and services:

1. Internet Service Provider, firewall, and IP schema for VMS devices.
2. Time server synchronization scheme for overall security system.
3. Plan for system testing, startup, and demonstration.
4. Acceptance test concept and, on approval, develop specifics of the test.
5. List of default user IDs and passwords (factory defaults) for VMS application, servers and workstations.
6. Prepare root certificate and necessary child certificates for secure connection between system components.

B. Provide a schedule with a list of participants to attend monthly coordination and progress update meeting until job completion. Attendees shall include:

1. Owner's Representative of Facilities Management, Information Services, Security Management.
2. Contractor Project Manager.
3. Manufacturer(s) Employed Representative.
4. Architect / Engineer / Security Consultant.

C. At all coordination meetings with Owner's Representative, present Project planning documents and review, adjust, and prepare final setup documents. Use final documents to set up system software.

D. Owner's Representative and Owner shall assist in establishing procedural guidelines and in defining terminology and conditions unique to the Owner's operation.

E. Supervise installation to appraise ongoing progress of other trades and contracts, make allowances for all ongoing work, and coordinate the requirements of the installation of the VMS.

F. Coordinate Owner installation or update of workstation operating system software and web browser software to a version as specified by the VMS provider.

G. Coordinate Owner-managed computer and network security practices as specified by the VMS provider.

3.3. INSTALLATION

A. Deploy VMS in accordance with manufacturer's Deployment Best Practice Guide, including workstation and integration instructions and requirements.

B. Collaborate with Owner's Representative on the application of manufacturer's hardening guide recommendations.

C. Supervise installation to appraise ongoing progress of other trades and contracts, make allowances for all ongoing work, and coordinate the requirements of the VMS installation.

D. *Drawings and Diagrams*:

1. System devices identified on building drawings are intended to generally indicate areas where such devices are to be located. Determine final location of these devices in accordance with Owner's requirements.

2. Riser diagrams are schematic and do not show every conduit, wire box, fitting, or other accessories. Provide such materials as necessary for a complete and functioning installation.

E. Comply with manufacturer's written data, including product technical bulletins, product catalog installation instructions and product carton installation instructions.

F. All firmware in products shall be the latest and most up-to-date provided by the manufacturer, or of a version as specified by the provider of the VMS to ensure approved integration compatibility.

G. Install, configure, and test VMS for complete and proper operation.

3.4. SITE QUALITY CONTROL

A. *Site Tests and Inspections*:

1. Submit documented test plan to Owner at least 14 days in advance of final acceptance test, inspection and check-off.

2. Perform acceptance reviews with Owner's representative of device and system configurations and their documentation.

3. Perform final acceptance testing in the presence of Owner's representative, executing a point by point inspection against a documented test plan that demonstrates compliance with system requirements as designed and specified, including response times for control actions and sequences, and rules-based actions. Tests shall demonstrate the functionality of each individual device control item, including as camera alarm outputs and control relays.
4. Conduct acceptance tests in presence of Owner's representative, verifying that each device point and sequence is operating correctly and properly reporting back to control panel and control center, and provide Owner's Representative with written report of test results.
5. Specific tests shall be witnessed by Authorities Having Jurisdiction if necessary.
6. Consider VMS accepted only after all acceptance test items have been successfully checked-off.
    a. Beneficial use of part or all of the system shall not be considered as acceptance.
7. As required to sufficiently demonstrate the VMS functionality, request the console operator on duty and his/her superior to perform certain daily operations using the VMS.
8. Complete all required training prior to initiation of the final acceptance test.
9. Inspect the installation of all field computers and devices.
    a. Point out general neatness and quality of installation, test the full functionality of each individual device, and show that mounting, backbox and conduit meet compliance requirements.
10. Owner's Representative shall, upon successful completion of the final acceptance test (or subsequent punch list retest), issue a letter of final acceptance.
11. Owner's Representative retains right to suspend and/or terminate testing at any time when the system fails to perform as specified.
    a. Collaborate with Owner's Representative prior to start of testing, to establish criteria pass/fail criteria and classification of test execution problems, such as:
        1) *Pass/fail:* Criteria determining what constitutes a test pass or failure.
        2) *Suspension and resumption:* Criteria determining when testing must be suspended and resulted later.
        3) *Show Stopper:* Stop test, fix problem and restart test from beginning.
        4) *Major Problem:* Fix problem before test can be resumed or concluded.
        5) *Minor Problem:* Add problem to "punch list", complete test.
        6) *Special Issue:* Investigate to determine which problem category above category applies.
    b. If it becomes necessary to suspend testing or inspections, work diligently to complete/repair all outstanding items to the condition specified in Specification and as indicated on related drawings.

c. Supply Owner's Representative with detailed completion schedule outlining phase by phase completion dates and a tentative date for a subsequent punch list retest.

d. During final acceptance test, make no adjustments, repairs or modifications to system without permission of Owner's Representative.

3.5. ADJUSTING

A. Perform field software changes after the initial programming session to "fine tune" operating parameters and sequence of operations based on any revisions to the Owner's operating requirements.

B. *Installer/Factory User Accounts*:

1. Remove all default, installer, or temporary user accounts and passwords used during installation that are not part of End-user's final operational requirements.

2. Assign new passwords that are substantially different from factory default passwords to user accounts that match factory-default user accounts.

3. Apply appropriate measures from manufacturer's system hardening guide.

3.6. CLOSEOUT ACTIVITIES

A. *Training*:

1. *General*:

a. Submit training plans and instructor qualifications to Owner's Representative for approval.

b. Coordinate with Owner's Representative to accommodate owner shift schedules to reduce impact to regular operations.

B. Provide training as scheduled.

C. Deliver printed or electronic reference materials that cover the entire training presentation.

3.7. PROTECTION

A. Maintain strict site security during the installation of equipment and software.

1. *Equipment Rooms:* Lock and secure rooms housing accessible equipment that has been powered up.

2. *Dedicated Workstations:* Shut down, lock and secure rooms containing workstations during periods when a qualified operator in Contractor's employ is not present.

B. Protect installed work of other trades when working in the same location, protecting all completed work prior to acceptance by Owner, unless Owner has specifically relieved Contractor from this responsibility.

C. *Incremental and As-built Configuration Backup*:

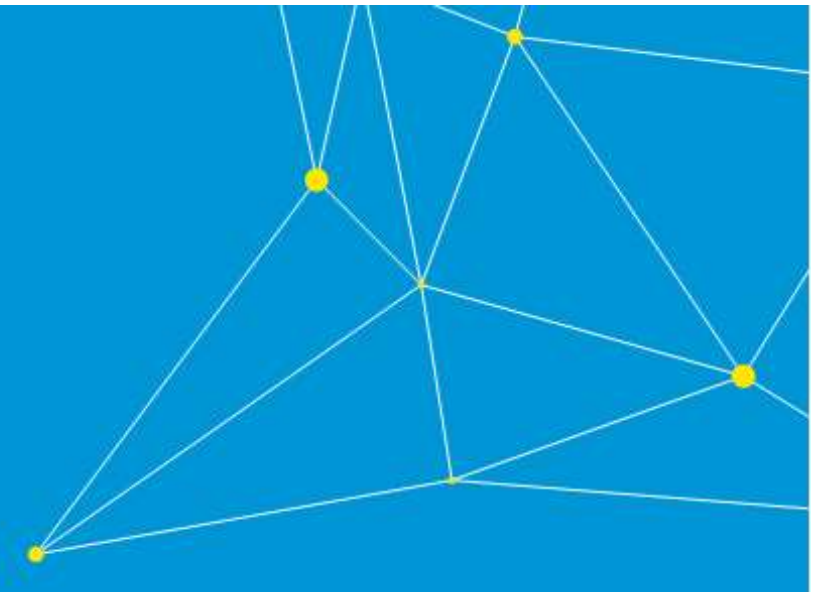
1. Perform full back-up of all configuration settings and system data from VMS at the completion of critical installation milestones, immediately prior to start of acceptance testing, and immediately after acceptance testing is completed.

2. Deliver instructions for restoration of the VMS backups upon completion of acceptance testing.

3.8. MAINTENANCE

A. Provide maintenance updates by VMS manufacturer per agreed schedule.

END OF SECTION



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 150,000 sites worldwide. Founded in 1998, Milestone is a stand-alone company in the Canon Group.

MAKE THE
WORLD SEE

Milestone Systems

XProtect® VMS 2022 R3

System architecture document

XProtect Corporate
XProtect Expert
XProtect Professional+
XProtect Express+
XProtect Essential+

milestone

Contents

Copyright, trademarks, and disclaimer **5**

Introduction **6**

Target audience and purpose **7**

Overall system architecture **8**

Server components **9**

Management server 9

Recording server 9

Media database 10

Event server 10

Log server 11

SQL Server 11

Mobile server 11

API Gateway 12

Client components **13**

XProtect Management Client 13

XProtect Smart Client 13

XProtect Web Client 13

XProtect Mobile client 13

Encryption **15**

Introduction to certificates 16

Identity Provider (explained) **18**

Additional products and components **19**

MIP SDK 19

Milestone Software Manager 20

XProtect Smart Wall 20

XProtect Incident Manager 20

XProtect Access 21

XProtect Transact 21

XProtect LPR ... 22
Milestone Interconnect ... 22
XProtect DLNA Server ... 23
Milestone Open Network Bridge ... 24
System communication and data flow ... 25
Server communication ... 25
Login from XProtect Smart Client as an AD user ... 26
Login from XProtect Smart Client as a basic user ... 27
Login from XProtect Smart Client with an external IDP ... 28
Live video and audio ... 29
Live video multicasting ... 30
Matrix ... 31
Management server – view update ... 32
XProtect Smart Wall ... 33
Play back video and audio ... 34
Login from XProtect Web Client and XProtect Mobile as an AD user ... 35
Login from XProtect Web Client and XProtect Mobile as a basic user ... 36
Login from XProtect Web Client and the XProtect Mobile client with an external IDP ... 37
Live video for XProtect Web Client and XProtect Mobile ... 38
Recording and playback video for XProtect Web Client and XProtect Mobile ... 39
Video push ... 40
Milestone Interconnect live ... 41
Milestone Interconnect recording options ... 42
Milestone Interconnect play back ... 43
XProtect DLNA Server ... 44
Milestone Open Network Bridge ... 45
Management Client configuration update ... 46
Log server ... 47
Event server ... 47
XProtect Transact ... 48

XProtect LPR 49
View and manage alarms 50
Data collector 51
Recording server failover 52
Evidence lock 53
XProtect Incident Manager 54
Move hardware 55
Ports used by the system **56**

Copyright, trademarks, and disclaimer

Copyright © 2022 Milestone Systems A/S

Trademarks

XProtect is a registered trademark of Milestone Systems A/S.

Microsoft and Windows are registered trademarks of Microsoft Corporation. App Store is a service mark of Apple Inc. Android is a trademark of Google Inc.

All other trademarks mentioned in this document are trademarks of their respective owners.

Disclaimer

This text is intended for general information purposes only, and due care has been taken in its preparation.

Any risk arising from the use of this information rests with the recipient, and nothing herein should be construed as constituting any kind of warranty.

Milestone Systems A/S reserves the right to make adjustments without prior notification.

All names of people and organizations used in the examples in this text are fictitious. Any resemblance to any actual organization or person, living or dead, is purely coincidental and unintended.

This product may make use of third-party software for which specific terms and conditions may apply. When that is the case, you can find more information in the file 3rd_party_software_terms_and_conditions.txt located in your Milestone system installation folder.

Introduction

This document contains illustrations and descriptions of communication and dataflow between the most common system components in a distributed system.

The document shows a range of scenarios with a supporting illustration and a description of actions supplemented by information about port numbers, protocols and bandwidth usage.

The illustrations are simplified and primarily focus on the general dataflow between system components. This means that less important flows may have been omitted in order to reduce the level of complexity.

Target audience and purpose

This document is primarily aimed at system integrators and IT administrators. It gives insight on the benefits and simplicity of using Milestone XProtect as a VMS and you can use it for assistance in the process of selecting, deploying, administrating, maintaining, and expanding a Milestone XProtect VMS.

Read the document for guidance on the following subjects:

- Overall system architecture
- Primary system components and their functions
- Data flow and communication through the system
- Basic system design

To benefit from the information in this document, you should have a general experience with administrating an IT installation.

Overall system architecture

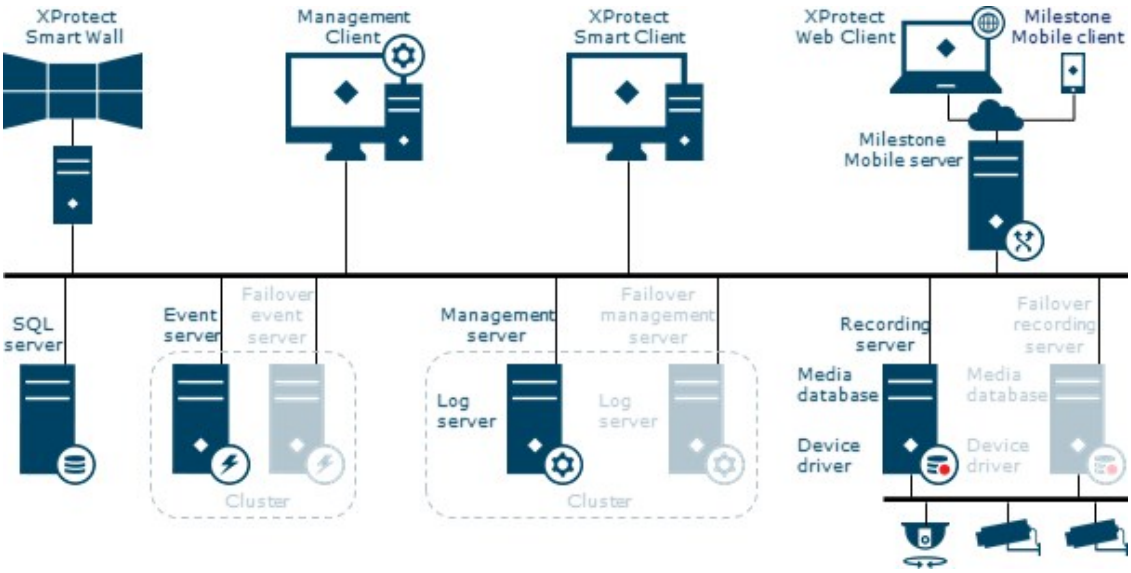
To enable scaling of thousands of cameras across multiple sites, the system consists of several components that handle specific tasks. You can install all components on a single server if the server can handle the load, or you can install the components on separate, dedicated servers to scale and distribute the load.

Depending on hardware and configuration, smaller systems with 50 to100 cameras can run on a single server.

For systems with more than 100 cameras, Milestone recommends that you use dedicated servers for all or some of the components.

As a starting point, all components need not be available in all installations. Components such as failover recording servers or mobile servers can be added if the functionality they offer is needed at a later time for hosting and providing access to both XProtect Web Client and XProtect Mobile.

The components of the XProtect VMS



Server components

Management server

The management server is the central VMS component. It stores the configuration of the surveillance system in a SQL database, either on a SQL Server on the management server computer itself or on a separate SQL Server on the network. It also handles user authentication, user rights, the rule system and more.

To improve system performance, you can run several management servers as a Milestone Federated Architecture™. The management server runs as a service and is typically installed on a dedicated server.

Failover management server

You can get failover support on the management server by installing the management server in a Microsoft Windows cluster. The cluster ensures that another server takes over the management server function in case the first server fails.

Recording server

Recording servers are computers where you have installed the Recording Server software, and configured it to communicate with the management server. A surveillance system typically consists of several recording servers.

The recording server is responsible for all communication, recording, and event handling related to devices such as cameras, video and audio encoders, I/O modules, and metadata sources. Examples of actions the recording server handles:

- Retrieve video, audio, metadata and I/O event streams from the devices
- Record video, audio and metadata from devices
- Provide operators with access to live and recorded video, audio and metadata
- Provide operators with access to device status
- Trigger system and video events on device failures or events
- Perform motion detection and generate smart search metadata

The recording server is also responsible for communicating with other Milestone products when using the Milestone Interconnect™ technology. For more information, see Milestone Interconnect on page 22.

The recording server supports encryption of data streams to the clients and services as well as encryption of the connection with the management server.For more information, see the certificates guide about how to secure your XProtect VMS installations.

Failover recording server

The failover recording server is responsible for taking over the recording task in case a recording server fails.

The failover recording server operates in two modes:

Cold standby, for monitoring multiple recording servers

In a cold standby failover recording server setup, you group multiple failover recording servers in a failover group. The entire failover group is dedicated to take over from any of several preselected recording servers, if one of these becomes unavailable. You can also specify a secondary failover server group that takes over from the primary group if all the recording servers in the primary group are busy

Hot standby, for monitoring a single recording server

In a hot standby failover recording server setup, you dedicate a failover recording server to take over from one recording server only. With this approach, the failover recording server is continuously synchronized with the correct/current configuration of the recording server it is dedicated to and it can take over much faster than a cold standby failover recording server.

Media database

The system stores the retrieved video, audio and metadata in the customized high performance Milestone media database which is optimized for recording and storing audio and video data.

The media database supports various unique features including multistage archiving, video grooming, encryption and adding a digital signature to the recordings.

Event server

The event server handles the tasks related to events, alarms, and maps and also third-party integrations via the Milestone Integration Platform.

Events:

- All system events are consolidated in the event server so there is a single place and interface for partners to make integrations that use system events
- The event server offers third-party access for sending events to the system via the Generic events or Analytics events interface

Alarms:

- The event server hosts the alarm feature, alarm logic, alarm state and handling of the alarm database. The alarm database is stored in the same SQL database as the management server uses

Maps:

- The event server also hosts maps. You configure and use maps in the XProtect Smart Client

Milestone Integration Platform:

- You can install third-party developed plug-ins on the event server and utilize access to system events

You can get failover support on the event server by installing the event server in a Microsoft Windows cluster. The cluster ensures that another server takes over the event server function in case the first server fails.

Log server

The log server stores all log messages for the entire system. The log server typically uses the same SQL Server as the management server but has its own SQL database. The log server is also typically installed on the same server as the management server. If you need to increase the performance of the management server or log server, you can install the log server on a separate server and use a separate SQL Server.

The system can through the log server write three types of log messages:

- System logs: the system administrator can choose to log errors, warnings, and information, or a combination of these. The default is to log errors only
- Audit logs: the system administrator can choose to log user activity in clients in addition to login and administration logs
- Rule-triggered logs: the system administrator can use the rule log to create logs on specific events

SQL Server

The management server, the event server and the log server use SQL databases on one or two SQL Server installations to store, for example, configuration, alarms, events and log messages.

The Milestone XProtect installer includes Microsoft SQL Server Express which is free edition of SQL Server.

For very large systems or systems with many transactions to and from the SQL databases, Milestone recommends that you use a Microsoft® SQL Server® Standard or Microsoft® SQL Server® Enterprise edition of the SQL Server on a dedicated computer on the network and on a dedicated hard disk drive that is not used for other purposes. Installing the SQL Server on its own drive improves the entire system performance.

Mobile server

XProtect Mobile server handles logins to the system from XProtect Mobile client or XProtect Web Client.

A XProtect Mobile server distributes video streams from recording servers to XProtect Mobile client or XProtect Web Client. This offers a secure setup where recording servers are never connected to the Internet. When a XProtect Mobile server receives video streams from recording servers, it also handles the complex conversion of codecs and formats allowing streaming of video on the mobile device.

API Gateway

The MIP VMS API provides a unified RESTful API, based on industry standard protocols such as OpenAPI, for accessing XProtect VMS functionality, simplifying integration projects and serving as a basis for cloud connected communication.

The XProtect VMS API Gateway supports these integration options through the Milestone Integration Platform VMS API (MIP VMS API).

The API Gateway is installed on-premise and is intended to serve as a front-end and common entry point for RESTful API services on all the current VMS server components (management server, event server, recording servers, log server, etc). An API Gateway service can be installed on the same host as the management server or separately, and more than one can be installed (each on their own host).

The RESTful API is implemented in part by each specific VMS server component, and the API Gateway can simply pass-through these requests and responses, while for other requests, the API Gateway will convert requests and responses as appropriate.

Currently, the configuration API, hosted by the management server, is available as a RESTful API.

For more information, see the API Gateway administrator manual and the Milestone Integration Platform VMS API reference documentation.

Client components

XProtect Management Client

The Management Client is the administration interface for all parts of the system.

The VMS is designed for large-scale operation so the Management Client is designed to run remotely from, for example, the administrator's computer.

You can access the settings in the Management Client from a tree structure where you can open items and sub items.

For more information, see the administrator manual for XProtect VMS.

XProtect Smart Client

XProtect Smart Client is the main client for the VMS. It is designed to run remotely from the operators' computer for day-to-day use in order to manage IP surveillance cameras. It provides instant control of cameras and connected security devices and quick access to live and recorded video and metadata.

XProtect Smart Client has an adaptable user interface that can be optimized for individual operators' tasks and adjusted according to specific skills and authority levels.

For more information, see the user manual for XProtect Smart Client.

XProtect Web Client

XProtect Web Client is a client designed for the occasional or remote user that needs easy access to live monitoring, playback and export. XProtect Web Client also provides access to activating system events and outputs.

For more information, see the user manual for XProtect Web Client.

On the System Requirements web page, you can find information about compatible browsers under XProtect Web Client.

XProtect Mobile client

The XProtect Mobile client is a mobile surveillance solution and it offers easy access to cameras, views and other functionality that is set up in the management clients.

It runs on an Android tablet or smartphone or on an Apple® tablet, smartphone or portable music player.

You can use the XProtect Mobile client as a remote recording device by using the device's built-in camera and the Milestone Video Push feature. With Video Push activated, video from the device's camera is streamed back to the VMS and recorded as if it was from a standard camera.

For more information, see the XProtect Mobile webpage and user manual.

On the System Requirements web page, you can find information about which operating systems are compatible with XProtect Mobile.

Encryption

This section gives you an introduction to encryption and certificates.

XProtect systems support secure communication:

From	To
Recording Server	Management Server
Management Server	Recording Server
Clients, servers, and integrations that retrieve data streams from the recording server	Recording Server
Mobile devices	Mobile Server
Management Server	Data Collector servers affiliated with remote servers
Data Collector servers affiliated with remote servers	Management Server

When do you need to install certificates?

First, decide whether your system actually needs encrypted communication.

Don't use certificates with recording server encryption if you are using one or more integrations that don't support HTTPS communication. This is, for example, third-part MIP SDK integrations that don't support HTTPS.

Unless your installation is made in a physically isolated network, it's recommended that you secure the communication by using certificates.

This document describes when to use certificates:

- If your XProtect VMS system is set up in a Windows Workgroup environment
- Before you install or upgrade to XProtect VMS 2019 R1 or newer, if you want to enable encryption during the installation
- Before you enable encryption, if you installed XProtect VMS 2019 R1 or newer without encryption
- When you renew or replace certificates due to expiry

Introduction to certificates

Hypertext Transfer Protocol Secure (HTTPS) is an extension of the Hypertext Transfer Protocol (HTTP) for secure communication over a computer network. In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS), or its predecessor, Secure Sockets Layer (SSL).

In XProtect VMS, secure communication is obtained by using TLS/SSL with asymmetric encryption (RSA).

TLS/SSL uses a pair of keys—one private, one public—to authenticate, secure, and manage secure connections.

A certificate authority (CA) is anyone who can issue root certificates. This can be an internet service that issues root certificates, or anyone who manually generates and distributes a certificate. A CA can issue certificates to web services, that is to any software using https communication. This certificate contains two keys, a private key and a public key. The public key is installed on the clients of a web service (service clients) by installing a public certificate. The private key is used for signing server certificates that must be installed on the server. Whenever a service client calls the web service, the web service sends the server certificate, including the public key, to the client. The service client can validate the server certificate using the already installed public CA certificate. The client and the server can now use the public and private server certificates to exchange a secret key and thereby establish a secure TLS/SSL connection.

For manually distributed certificates, certificates must be installed before the client can make such a verification.

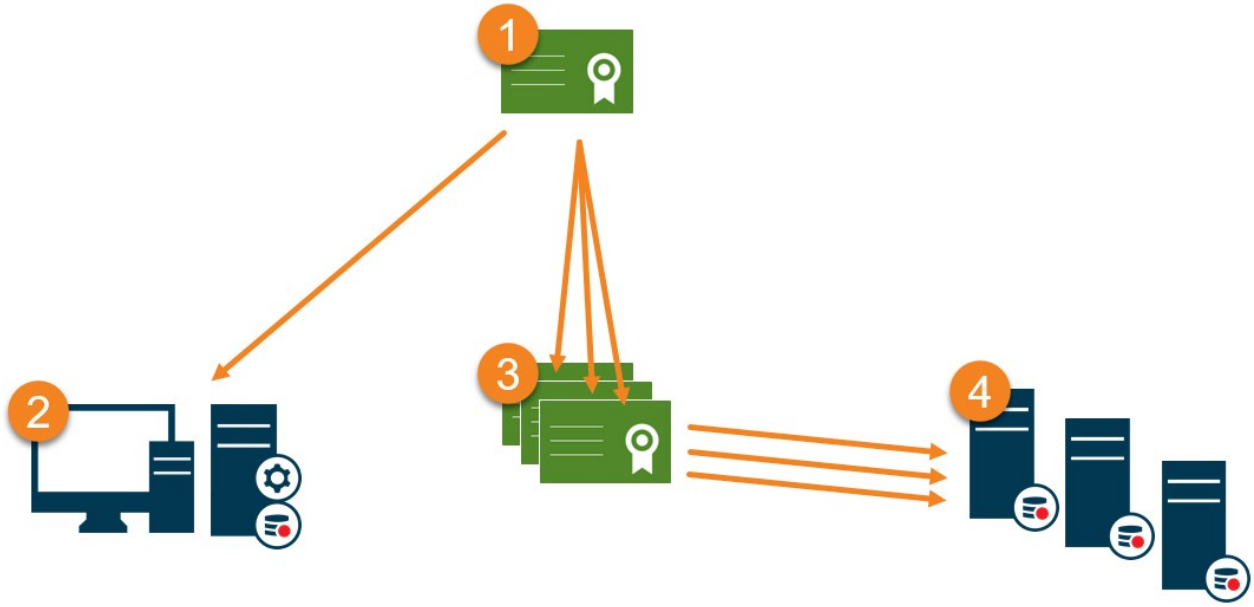
See Transport Layer Security for more information about TLS.

In XProtect VMS, the following locations are where you can enable TLS/SSL encryption:

- In the communication between the management server and the recording servers, event servers, and mobile servers
- On the recording server in the communication with clients, servers, and integrations that retrieve data streams from the recording server
- In the communication between clients and the mobile server

Certificate distribution

The graphic illustrates the basic concept of how certificates are signed, trusted, and distributed in XProtect VMS.



❶ A CA certificate acts as a trusted third-party, trusted by both the Subject/owner (server) and by the party that verifies the certificate (clients).

❷ The public CA certificate must be trusted on all client computers. In this way the clients can verify the validity of the certificates issued by the CA.

❸ The CA certificate is used to issue private server authentication certificates to the servers.

❹ The created private SSL certificates must be imported to the Windows Certificate Store on all servers.

Requirements for the private SSL certificate:

- Issued to the server so that the server's host name is included in the certificate, either as subject (owner) or in the list of DNS names that the certificate is issued to
- Trusted on all computers running services or applications that communicate with the service on the servers, by trusting the CA certificate that was used to issue the SSL certificate
- The service account that runs the server must have access to the private key of the certificate on the server.

> Certificates have an expiry date. XProtect VMS will not warn you when a certificate is about to expire. If a certificate expires, the clients will no longer trust the server with the expired certificate and thus cannot communicate with it.
> To renew the certificates, follow the steps in this guide as you did when you created certificates.

For more information, see the certificates guide about how to secure your XProtect VMS installations.

Identity Provider (explained)

Identity Provider app pool (IDP) is a system entity that creates, maintains, and manages identity information for basic users.

Identity Provider also provides authentication and registration services to relying applications or services, in this case: Recording Server, Management Server, Data Collector, and Report Server.

When you log in to XProtect clients and services as a basic user, your request goes to the Identity Provider. When authenticated the user can call the management server.

Identity Provider runs in the IIS as a part of the management server using the same SQL Server with a separate database and is responsible for creating and handling OAuth communication tokens that services use when communicating (Surveillance_IDP).

Identity Provider logs can be found at: \\ProgramData\Milestone\IDP\Logs.

Additional products and components

Available functionality depends on the system you are using. See the complete feature list, which is available on the product overview page on the Milestone website (https://www.milestonesys.com/solutions/platform/product-index/).

MIP SDK

The Milestone Integration Platform Software Development Kit (MIP SDK) is a comprehensive tool that makes it easy to create applications, plug-ins or integrations for Milestone's XProtect products.

MIP

The open platform is integrated in the following Milestone XProtect system components and applications:

- XProtect Smart Client
- XProtect Management Client
- Management Application
- Management Server
- Event Server

MIP SDK

To have a truly open platform and a community around it Milestone provides the SDK that contains:

- The tools for developing integrations
- Documentation of a set of interfaces
- A set of wrapper .NET DLLs providing an easy interface to a variety of functionality
- A large collection of samples demonstrating different ways of using the MIP SDK
- Short descriptions and how-to guides
- A small application to display links to this information
- Libraries

The MIP SDK is also used internally by Milestone software development teams.

For more information, see the MIP SDK and Develop Forum webpages.

Milestone Software Manager

Milestone Software Manager is a tool that you, from a central point, can use to remotely install and upgrade recording servers, recording server device packs and XProtect Smart Clients on servers or PCs in the network.

For larger installations, the tool makes it easy and fast to remotely upgrade the components that are installed on servers and client PCs.

For more information, see the XProtect Smart Wall webpage and manual.

XProtect Smart Wall

XProtect Smart Wall is designed for control centers to display live video from selected cameras on one or more video wall displays.

There are several ways you can select the cameras:

- Manually using the XProtect Smart Client
- Via the VMS' rule system on events and/or time schedule
- Via MIP SDK integrations

XProtect Smart Wall does not require a dedicated XProtect software component itself, nor does it use a dedicated XProtect client - all the required components are included in the standard XProtect Corporate management server and XProtect Smart Client. It just needs a PC running XProtect Smart Client to show the Smart Wall views.



XProtect Smart Wall is included in XProtect Corporate. You can purchase it as an add-on for XProtect Expert.

For more information, see the XProtect Smart Wall webpage and manual.

XProtect Incident Manager

XProtect Incident Manager is a Milestone add-on that enables organizations to document incidents and combine them with sequence evidence (video and, potentially, audio) from their XProtect VMS.

You can store the following information about the incidents in incident projects:

- Sequences with video and, potentially, audio from the XProtect VMS
- Incident properties like type, status, categories, and data elements
- Free text information like comments, descriptions, and information about calls.

All the required components for XProtect Incident Manager are included in the standard XProtect VMS management server and XProtect Smart Client.

XProtect Incident Manager is included in XProtect Corporate version 2022 R2 and later.

See also the manual for XProtect Incident Manager.

XProtect Access

The access control integration feature introduces new functionality that makes it simple to integrate customers' access control systems with XProtect. You get:

- A common operator user interface for multiple access control systems in XProtect Smart Client
- Faster and more powerful integration of access control systems
- More functionality for the operator (see below)

In XProtect Smart Client, the operator gets:

- Live monitoring of events at access points
- Operator aided passage for access requests
- Map integration
- Alarm definitions for access control events
- Investigation of events at access points
- Centralized overview and control of door states
- Cardholder information and management

The use of XProtect Access requires that you have purchased a base license that allows you to access this feature within your XProtect system. You also need an access control door license for each door you want to control.

You can use XProtect Access with access control systems from vendors where a vendor-specific plug-in for XProtect Access exists. You must install this plug-in on the event server before you can start an integration.

For more information, see the XProtect Access webpage and administrator manual.

XProtect Transact

XProtect Transact is an add-on to Milestone's IP video surveillance solutions XProtect VMS and XProtect Professional VMS.

XProtect Transact is a tool for observing ongoing transactions and investigating transactions in the past. The transactions are linked with the digital surveillance video monitoring the transactions, for example to help you prove fraud or provide evidence against a perpetrator. There is a 1-to-1 relationship between the transaction lines and video images.

The transaction data may originate from different types of transaction sources, typically point of sales (PoS) systems or automated teller machines (ATM).

For more information, see the XProtect Transact webpage and administrator manual.

XProtect LPR

XProtect LPR offers video-based content analysis (VCA) and recognition of vehicle license plates that interacts with your surveillance system and your XProtect Smart Client.

To read the characters on a plate, XProtect LPR uses optical character recognition on images aided by specialized camera settings.

You can combine LPR (license plate recognition) with other surveillance features such as recording and event-based activation of outputs.

Examples of events in XProtect LPR:

- Trigger surveillance system recordings in a particular quality
- Activate alarms
- Match against positive/negative match lists
- Open gates
- Switch on lights
- Push video of incidents to computer screens of particular security staff members
- Send mobile phone text messages

With an event, you can activate alarms in XProtect Smart Client.

For more information, see the XProtect LPR webpage and administrator manual.

Milestone Interconnect

Milestone Interconnect allows you to integrate several XProtect or Milestone Husky™ installations with one XProtect Corporate central site. You can also install these sites, called remote sites, on mobile units, for example, boats, busses or trains. This means that such sites do not need to be permanently connected to a network.

The central site considers the remote site as an advanced camera or multi-channel encoder with edge storage capabilities.

Each remote site runs independently and can perform surveillance tasks as configured. Depending on the network connections and appropriate user rights, Milestone Interconnect offers you direct live viewing of remote site cameras and play back of remote site recordings on the central site.

It also offers you the possibility to transfer remote site recordings to the central site based on either system-defined events, rules, schedules or by manual requests from XProtect Smart Client users.

The central site can only see and access devices that the user account specified on the remote site has access to. This allows local system administrators on the remote sites to control which devices should be made available to the central site and its users.

On the central site, you can view the status for the interconnected cameras, but not the entire status of the remote site. Instead, to monitor the remote site, you can use remote site events to trigger alarms or other notifications on the central site.

Only XProtect Corporate systems can work as central sites. All other products can act as remote sites including XProtect Corporate. How specific the products interact in a Milestone Interconnect setup depends on the version of the XProtect or Milestone Husky installations, the number of cameras and how devices and events are configured on the remote site.

For more information, see the Milestone Interconnect webpage and documentation.



It is not possible to add systems with free XProtect installation as remote sites.

XProtect DLNA Server

DLNA (Digital Living Network Alliance) is a standard for connecting multimedia devices. Electronic manufactures get their products DLNA certified to ensure interoperability between different vendors and devices and thereby enable them to distribute multimedia content such as audio, video, and photos.

Public displays and TVs are often DLNA certified and connected to a network. They are able to scan the network for media content, connect to the device, and request a media stream to their built-in media player. XProtect DLNA Server can be discovered by certain DLNA certified devices and deliver live video streams from selected cameras to DLNA certified devices with a media player.



The DLNA devices have a live video delay of 1-10 seconds. This is caused by different buffer sizes in the devices.

XProtect DLNA Server must be connected to the same network as the XProtect system and the DLNA device must be connected to the same network as XProtect DLNA Server.

For more information, see the XProtect DLNA Server feature brief and administrator manual.

Milestone Open Network Bridge

The ONVIF standard facilitates full video interoperability in multivendor installations and ensures information exchange by defining a common protocol. The protocol contains ONVIF profiles, which are collections of specifications for interoperability between ONVIF compliant devices.

Milestone Open Network Bridge is compliant with the parts of ONVIF Profile G and Profile S that provide access to live and recorded video, and the ability to control pan-tilt-zoom cameras:

- Profile G - Provides support for video recording, storage, search, and retrieval. For more information, see ONVIF Profile G Specification (https://www.onvif.org/profiles/profile-g/).
- Profile S - Provides support for streaming live video using the H.264 codec, audio streaming, and pan-tilt-zoom (PTZ) controls. For more information, see ONVIF Profile S Specification (https://www.onvif.org/profiles/profile-s/).

For more information about the ONVIF standard, see the ONVIF® website (https://www.onvif.org/).

ONVIF Profiles support “get” functions that retrieve data, and “set” functions that configure settings. Each function is either mandatory, conditional, or optional. For security reasons, Milestone Open Network Bridge supports only the mandatory, conditional, and optional “get” functions that do the following:

- Request video
- Authenticate users
- Stream video
- Play recorded video

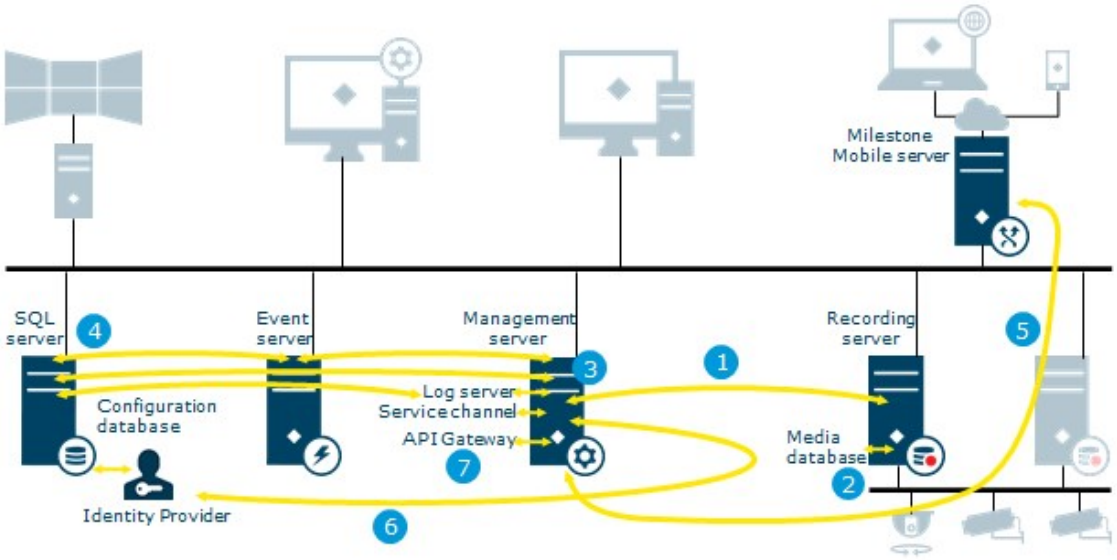
For more information, see the Ecosystem webpage and administrator manual for Milestone Open Network Bridge.

System communication and data flow

The following illustrations provide an overview of the flow of data between XProtect components.

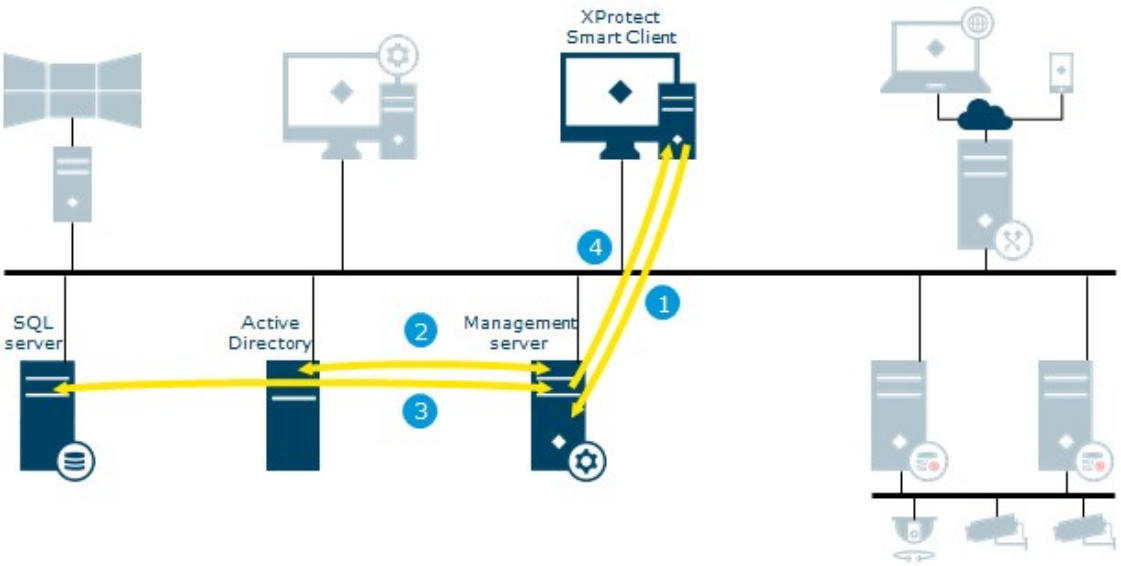
For a complete list of the ports that must be enabled for communication between components, see Ports used by the system.

Server communication



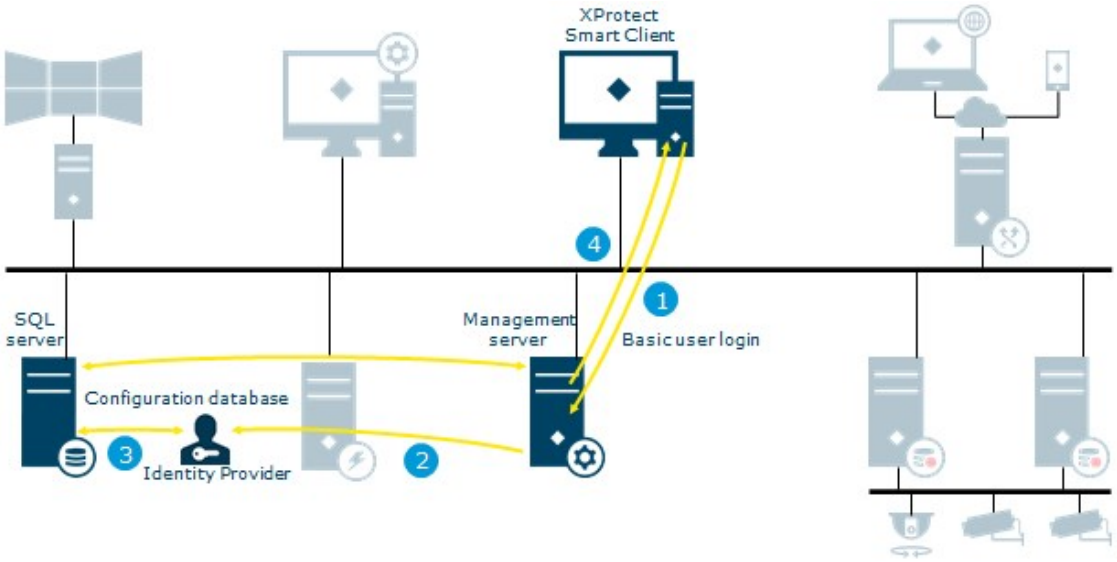
1. Management server - Recording server
2. Recording server - Media database
3. Management server - Internal
4. SQL database communication
5. Management server - Mobile server
6. Authentication of basic users by the Identity Provider
7. API Gateway - Management server

Login from XProtect Smart Client as an AD user



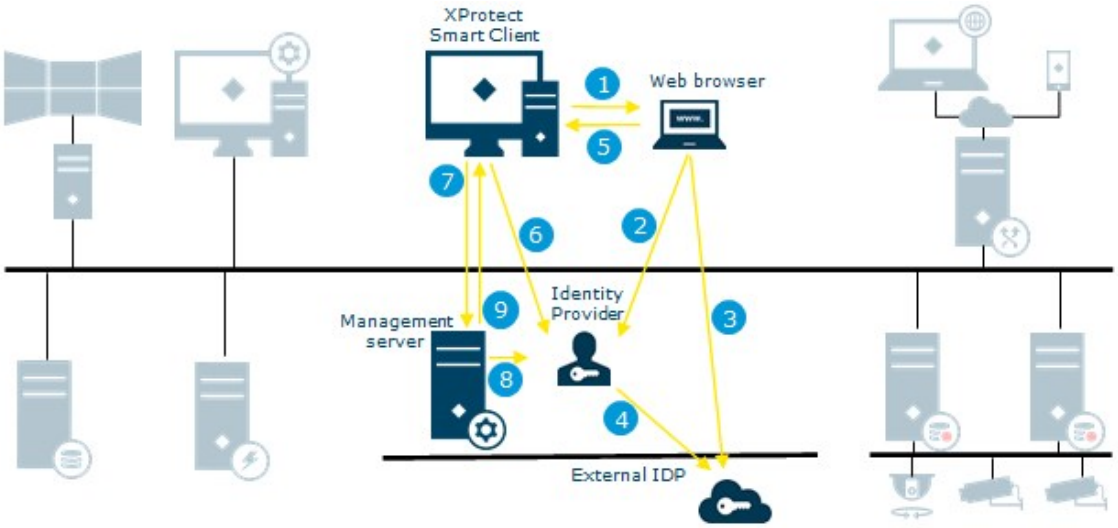
1. XProtect Smart Client connects to the management server and attempts to log in
2. The management server contacts Active Directory to authenticate the user
3. User-specific configuration is retrieved from the SQL database
4. Login is granted and the configuration is sent to XProtect Smart Client

Login from XProtect Smart Client as a basic user



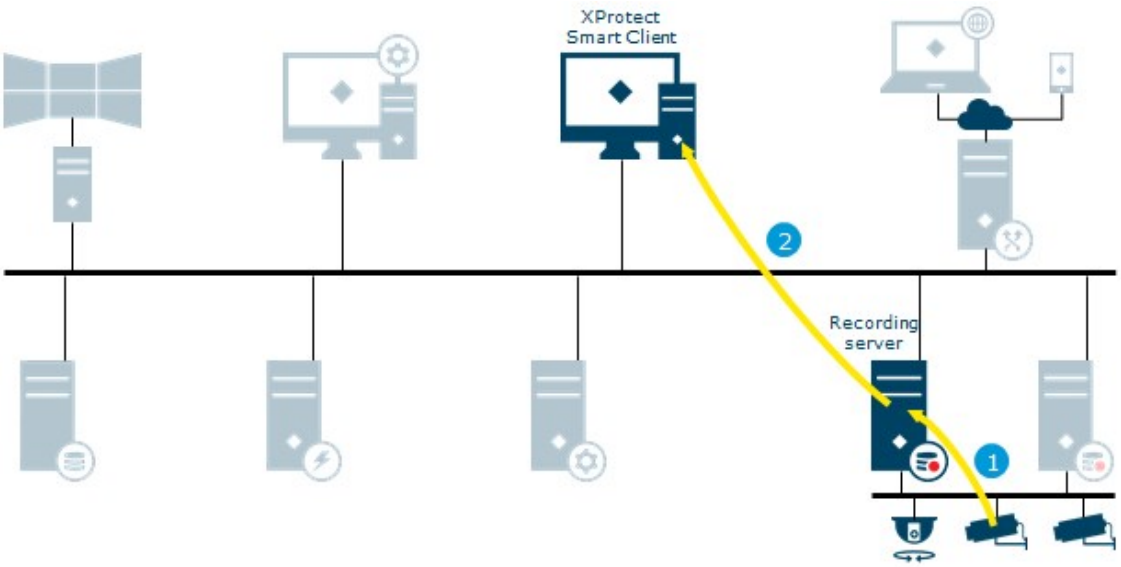
1. XProtect Smart Client attempts to connect to the management server as a basic user
2. The login request goes to the Identity Provider for authentication
3. User-specific configuration is retrieved from the SQL database
4. Login is granted and the configuration is sent to XProtect Smart Client

Login from XProtect Smart Client with an external IDP



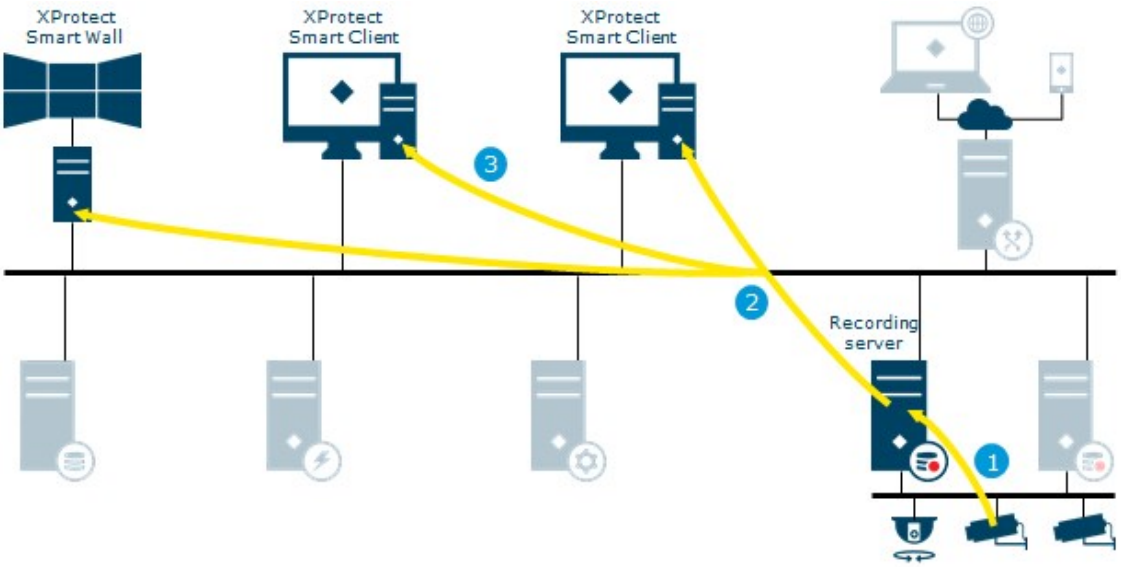
1. Login from XProtect Smart Client launches a web browser on the client computer.
2. The login request goes from the web browser to the Identity Provider for authentication.
3. The web browser is redirected to the external IDP login page where the user enters credentials and the browser receives an authorization code.
4. The Identity Provider requests information about the user from the external IDP and receives a list of claims. If a new user logs in to the VMS, the user is created in the VMS.
5. The web browser is redirected to XProtect Smart Client with the authorization code from the Identity Provider.
6. XProtect Smart Client gets an access token from the Identity Provider.
7. XProtect Smart Client login to the management server using the access token.
8. Verification of user rights permissions according to claims to role mapping.
9. The user logs in to XProtect Smart Client upon successful authorization.

Live video and audio



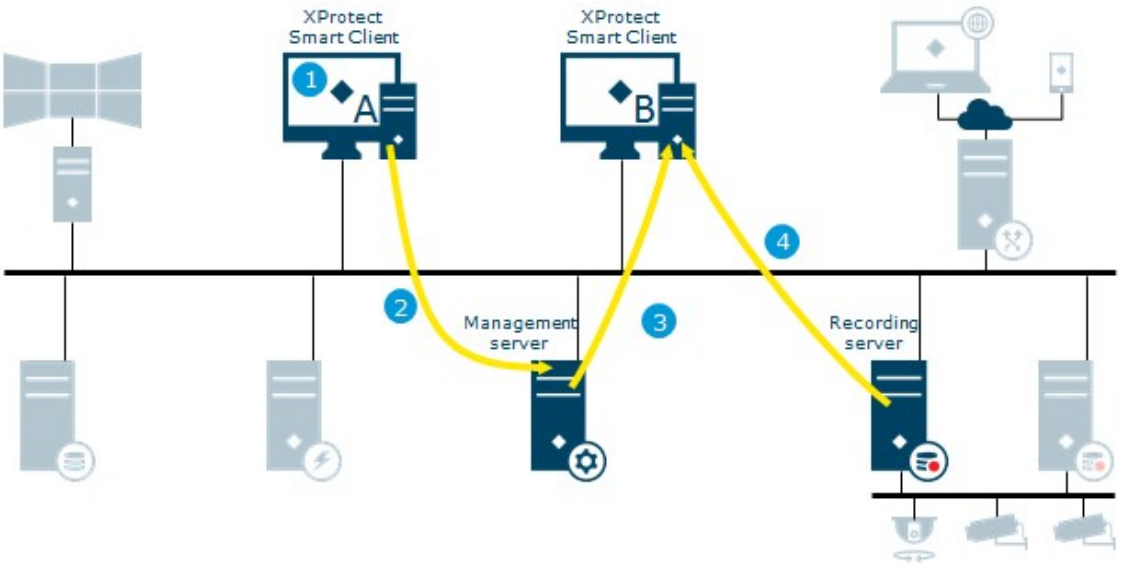
1. Live streams from cameras retrieved by the recording server
2. Streams are sent to XProtect Smart Client on request

Live video multicasting



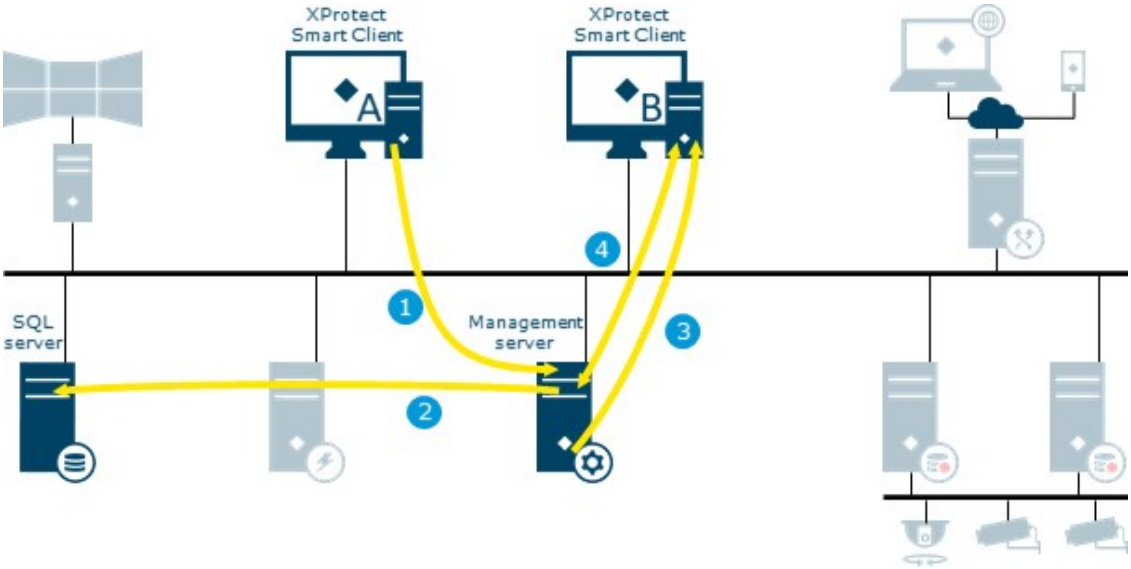
1. Live streams from cameras retrieved by the recording server
2. Recording server sends multicast stream to the multicast enabled network. This requires that all switches handling the data traffic between the XProtect Smart Client and the recording server must be configured for multicast
3. The multicast stream is received by all XProtect Smart Clients on request

Matrix



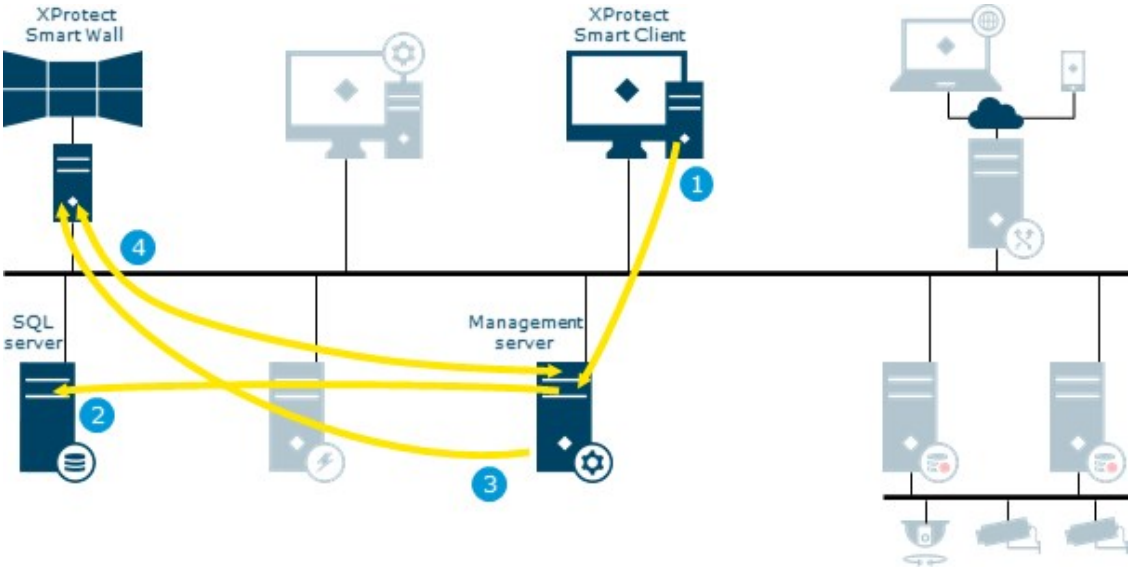
1. XProtect Smart Client user selects to send a camera to a Matrix-recipient
2. Information is sent to management server
3. Management server sends request to Matrix-recipient on specified IP address and port (XProtect Smart Client B)
4. Streams are sent to XProtect Smart Client from recording server on request

Management server – view update



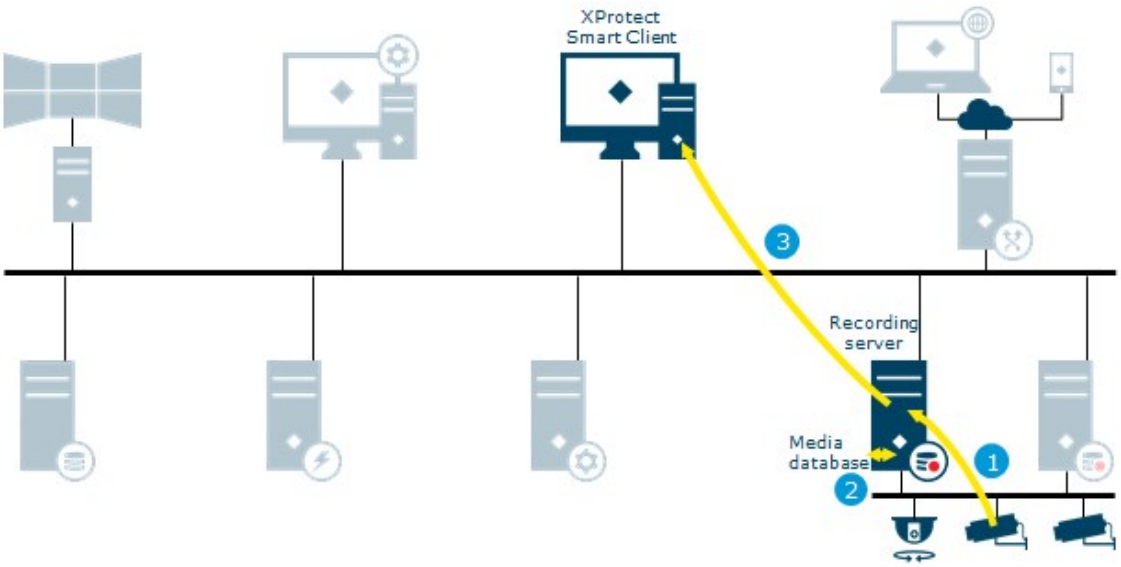
1. View updated on XProtect Smart Client
2. The system configuration is stored in the SQL database
3. The management server sends notification about view update to XProtect Smart Clients
4. XProtect Smart Clients retrieves and applies the new view

XProtect Smart Wall



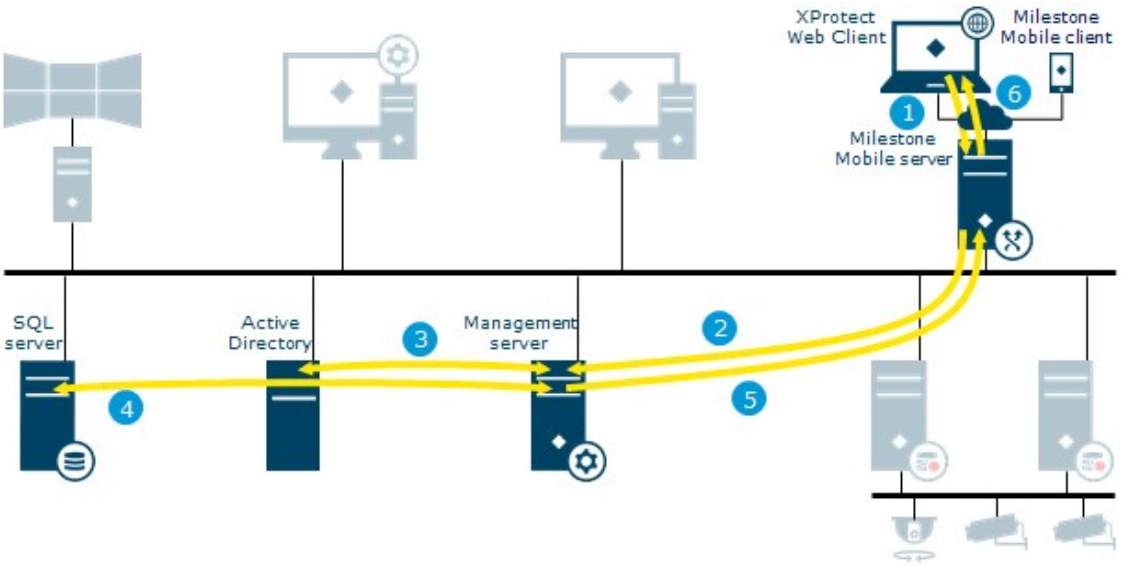
1. An XProtect Smart Client user updates the XProtect Smart Wall view
2. The XProtect Smart Wall view configuration is updated and stored in the SQL database
3. The management server sends a notification to the XProtect Smart Client running the XProtect Smart Wall
4. The XProtect Smart Client running the XProtect Smart Wall retrieves and applies new layout

Play back video and audio



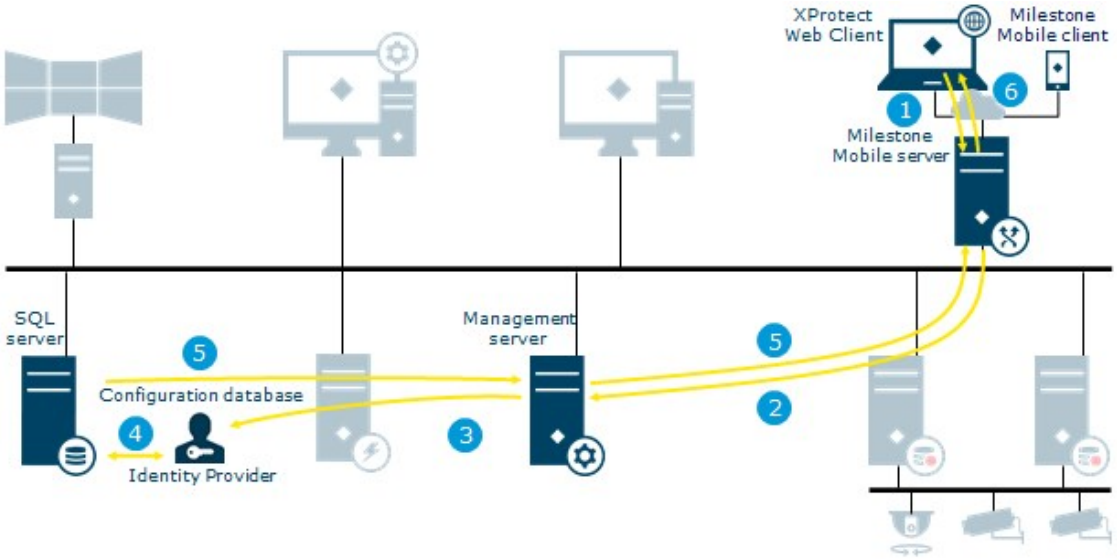
1. Recording stream from cameras retrieved by the recording server
2. The stream is recorded in the recording server database based on rules
3. The recorded stream is retrieved by XProtect Smart Client on playback request

Login from XProtect Web Client and XProtect Mobile as an AD user



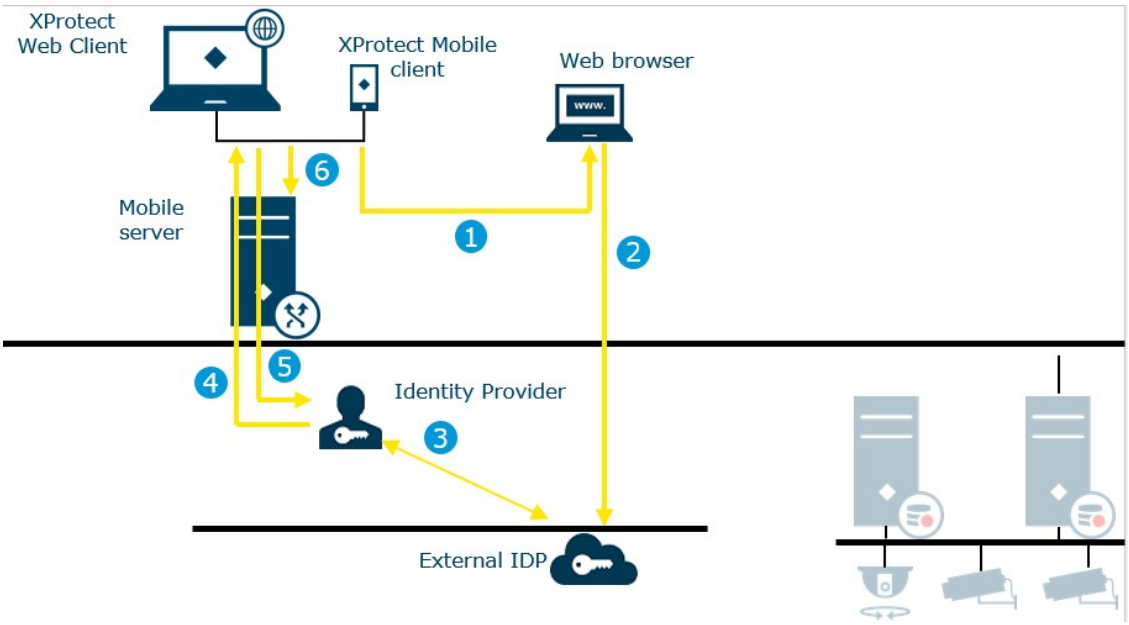
1. Login request from XProtect Web Client or XProtect Mobile received on the mobile server
2. The mobile server forwards request to the management server
3. The management server contacts Active Directory to authenticate the user
4. User-specific configuration is retrieved from the SQL database
5. Information returned to the mobile server
6. The login is granted and configuration is sent to XProtect Web Client or XProtect Mobile

Login from XProtect Web Client and XProtect Mobile as a basic user



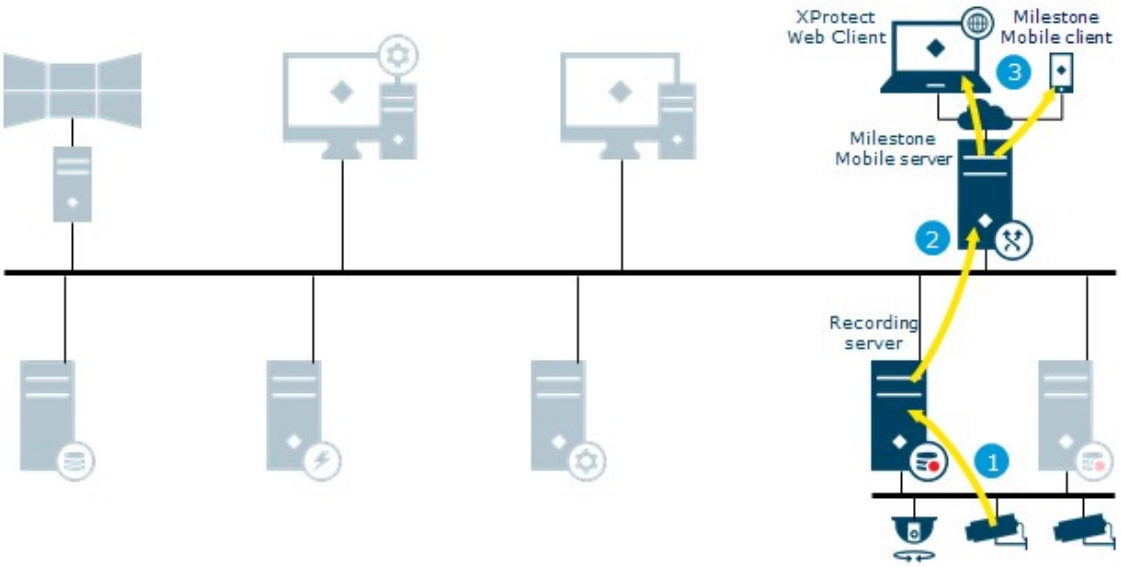
1. Login request from XProtect Web Client or XProtect Mobile received on the mobile server
2. The mobile server forwards a request to the management server
3. The login request goes to the Identity Provider for authentication
4. User-specific configuration is retrieved from the SQL database
5. Information returned to the mobile server
6. The login is granted and configuration is sent to XProtect Web Client or XProtect Mobile

Login from XProtect Web Client and the XProtect Mobile client with an external IDP



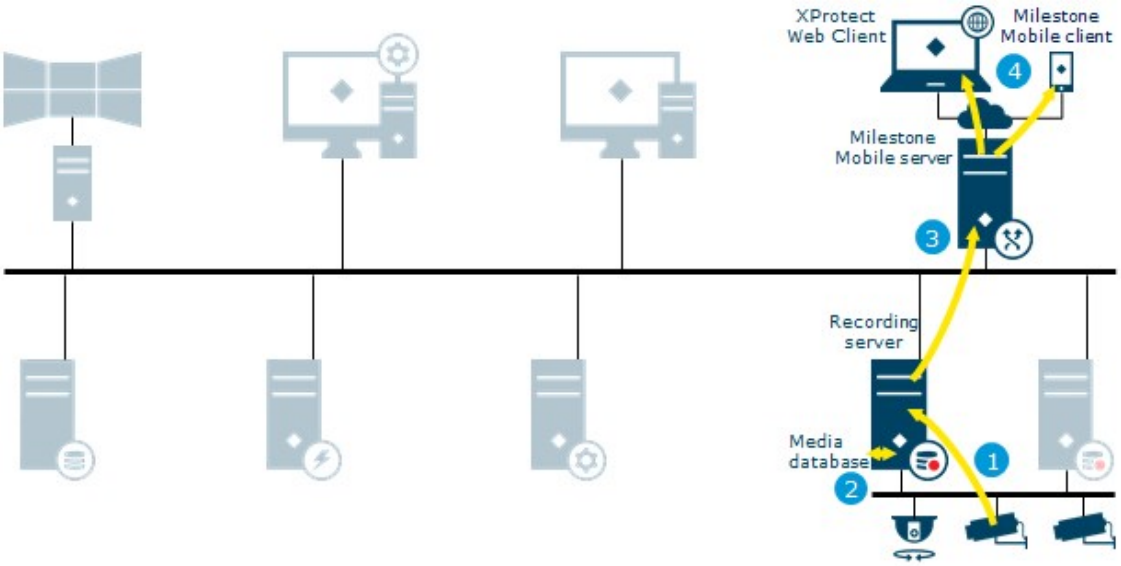
1. In XProtect Web Client or in the XProtect Mobile client, the user selects to log in via an external IDP. The login request launches a web browser.
2. The web browser is redirected to the external IDP login page where the user enters credentials.
3. The Identity Provider receives an authorization code from the external IDP to be exchanged for an access token. Then the Identity Provider requests information about the user from the external IDP and gets a list of claims. If a new user logs in to the VMS, the user is created in the VMS.
4. The Identity Provider returns an authorization code to XProtect Web Client or the XProtect Mobile client.
5. XProtect Web Client or the XProtect Mobile client requests an access token from the Identity Provider.
6. XProtect Web Client or the XProtect Mobile client logs in to the mobile server using the access token.

Live video for XProtect Web Client and XProtect Mobile



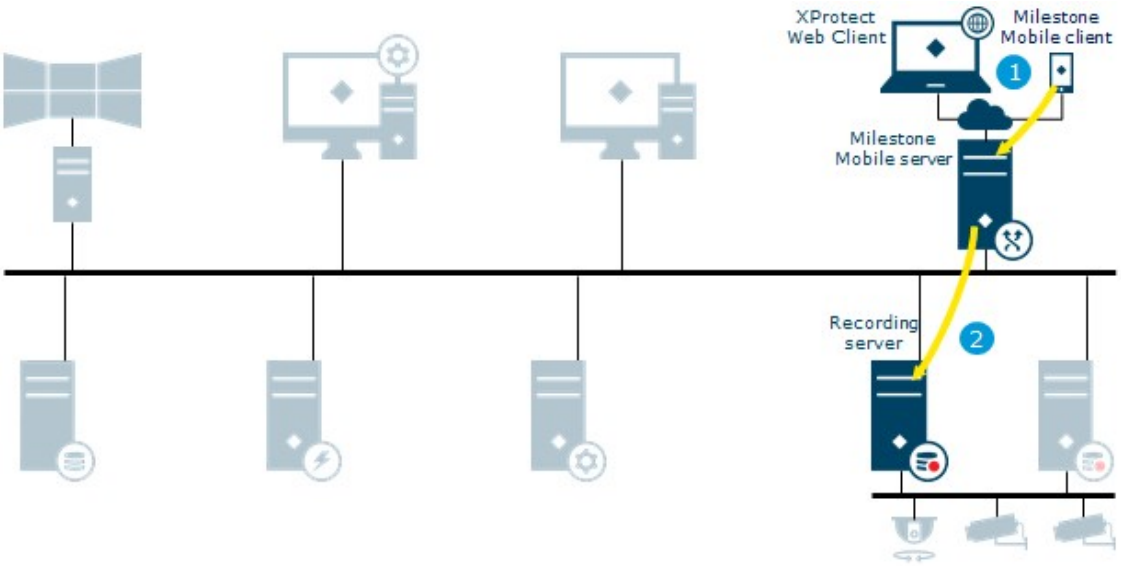
1. Live stream(s) from cameras retrieved on the recording server
2. Streams are sent to the mobile server for transcoding or as direct streaming
3. Video is streamed to the clients

Recording and playback video for XProtect Web Client and XProtect Mobile



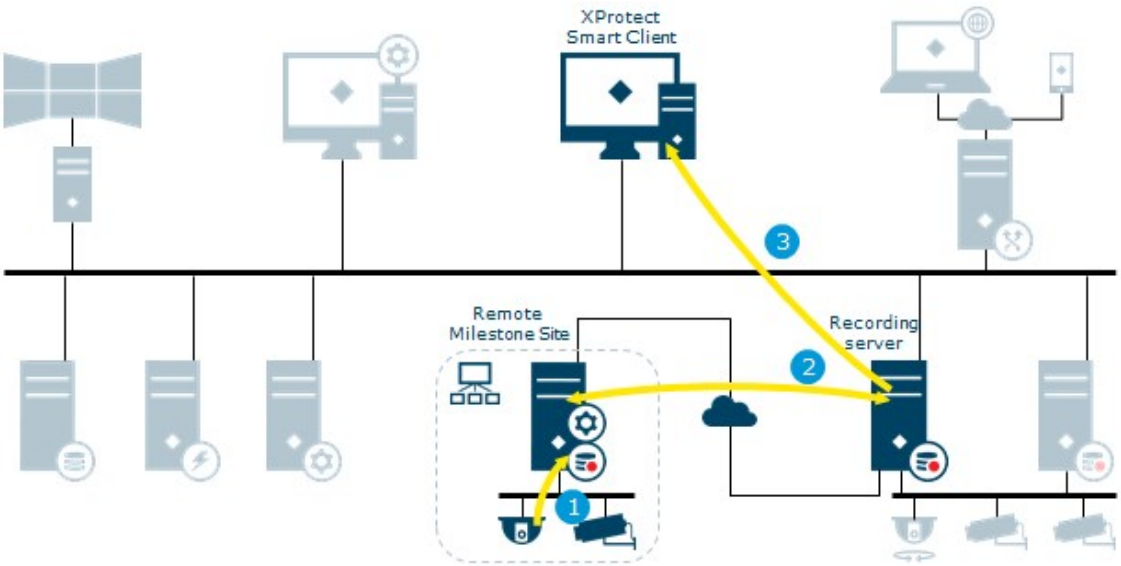
1. Recording stream from cameras retrieved on the recording server
2. The stream is recorded in the recording server database based on rules
3. Recordings are sent to the mobile server for transcoding or as direct streaming
4. Video is streamed to clients

Video push



1. Video push stream from a device running XProtect Mobile is sent instantly to the mobile server
2. The video push stream is retrieved by recording server using the specific video push device driver

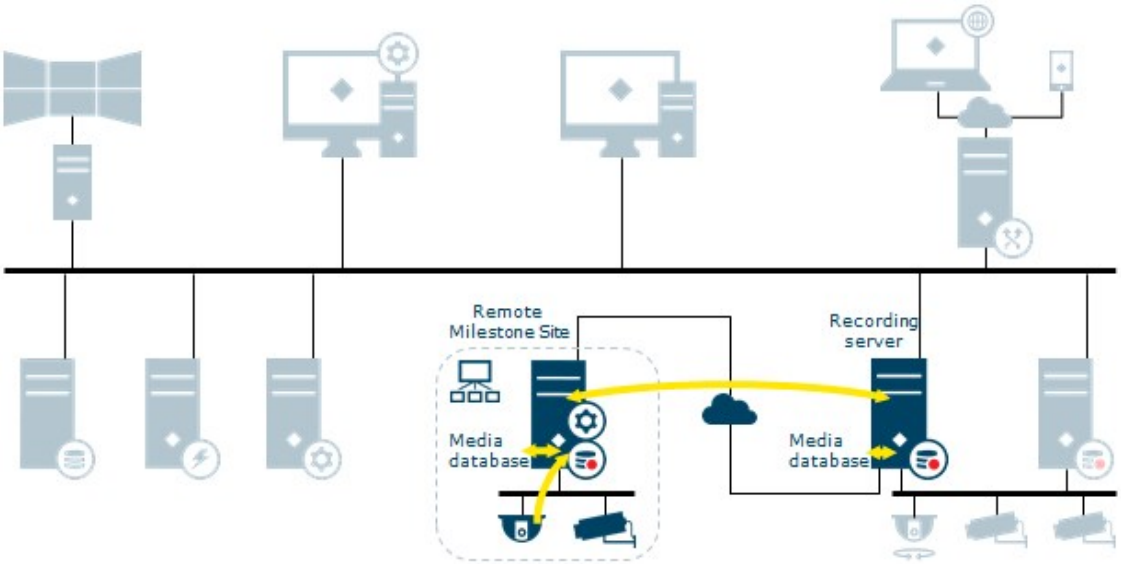
Milestone Interconnect live



Illustrates how XProtect Smart Client users, specified for the interconnected system, only need to log into the management server on the central site to view video.

1. Live stream(s) from the remote site cameras retrieved by the remote site recording server
2. Live streams from the remote site recording server retrieved by the central site recording server
3. Stream(s) are sent to XProtect Smart Client on request

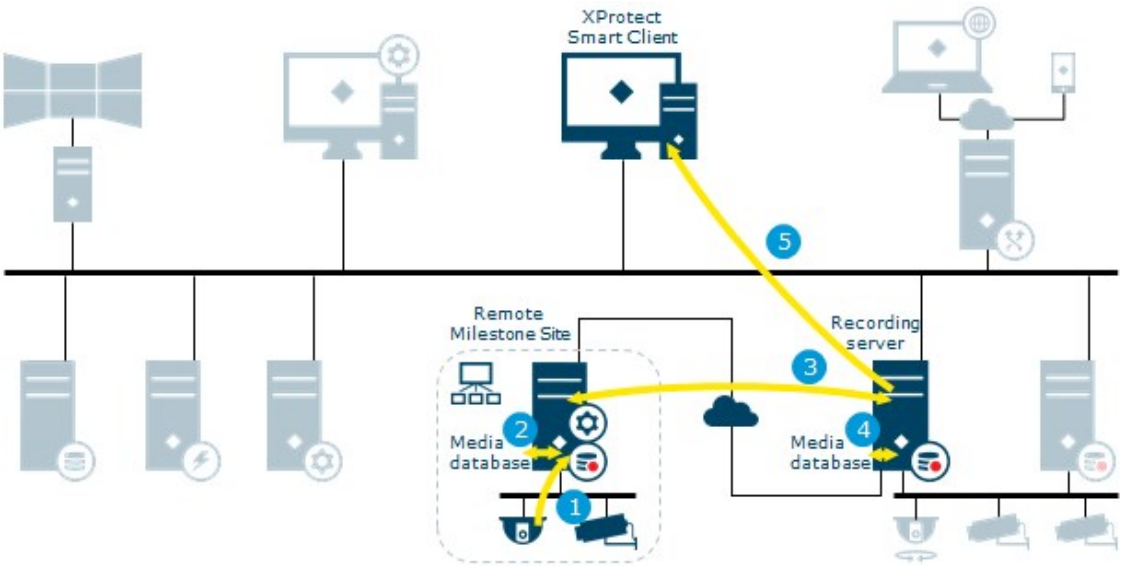
Milestone Interconnect recording options



Some of the different options when configuring your system recording settings:

- No recording
- Record at remote site only
- Retrieve recordings from remote site on request
- Retrieve recordings from remote site based on rule (time profile)
- Record at central site only
- Retrieve recordings from remote site after site link down
- Record at both sites
- Combinations of above and other options

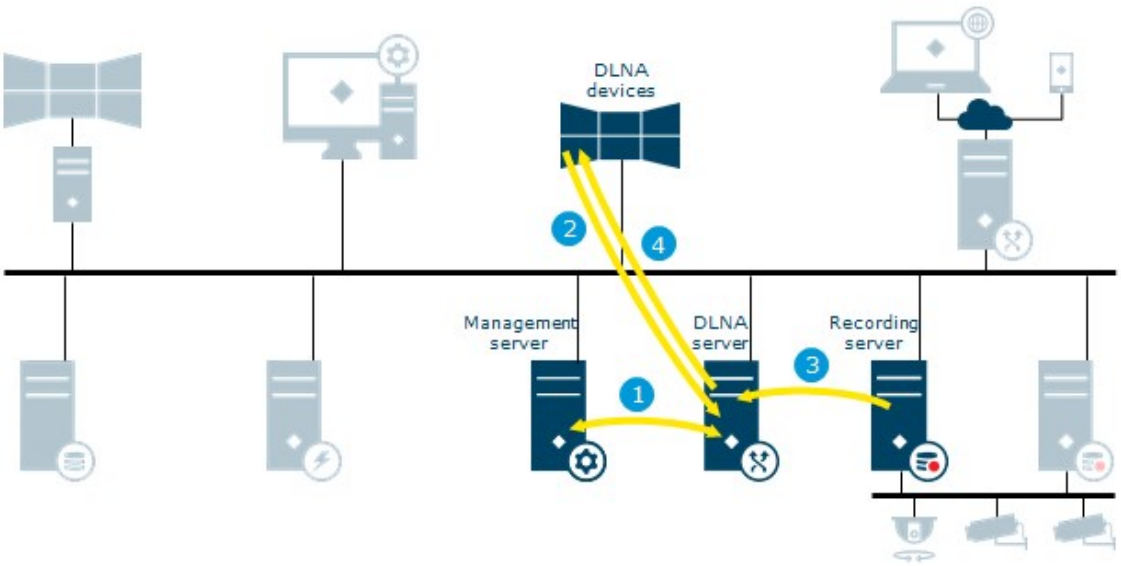
Milestone Interconnect play back



Illustrates when recording is done on both sites. Recordings can be retrieved to the central site based on schedule, event or request. XProtect Smart Client users, specified for the interconnected system, only need to log into the management server on the central site to view video.

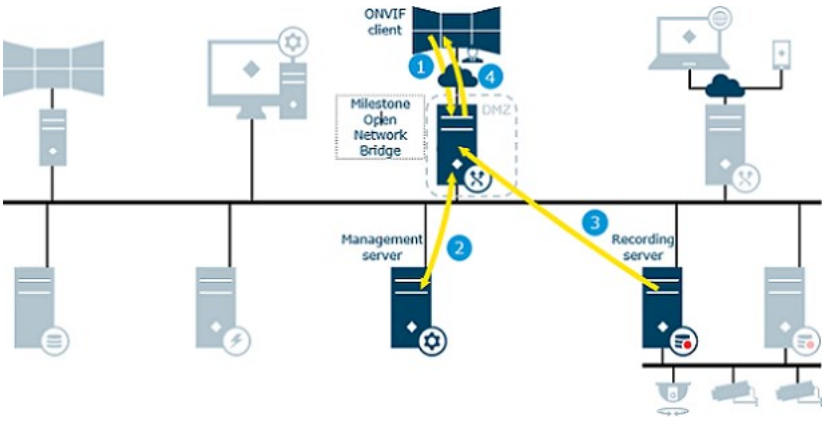
1. Recording stream from the remote site cameras retrieved by the remote site recording server
2. The stream is recorded in the remote site recording server database based on rules
3. Recording stream from the remote site recording server retrieved by the central site recording server
4. The stream is recorded in the central site recording server database based on rules. Recordings not available due to remote site link downtime can be retrieved automatically or based on schedule, event or request
5. The recorded stream(s) are retrieved by XProtect Smart Client on playback request

XProtect DLNA Server



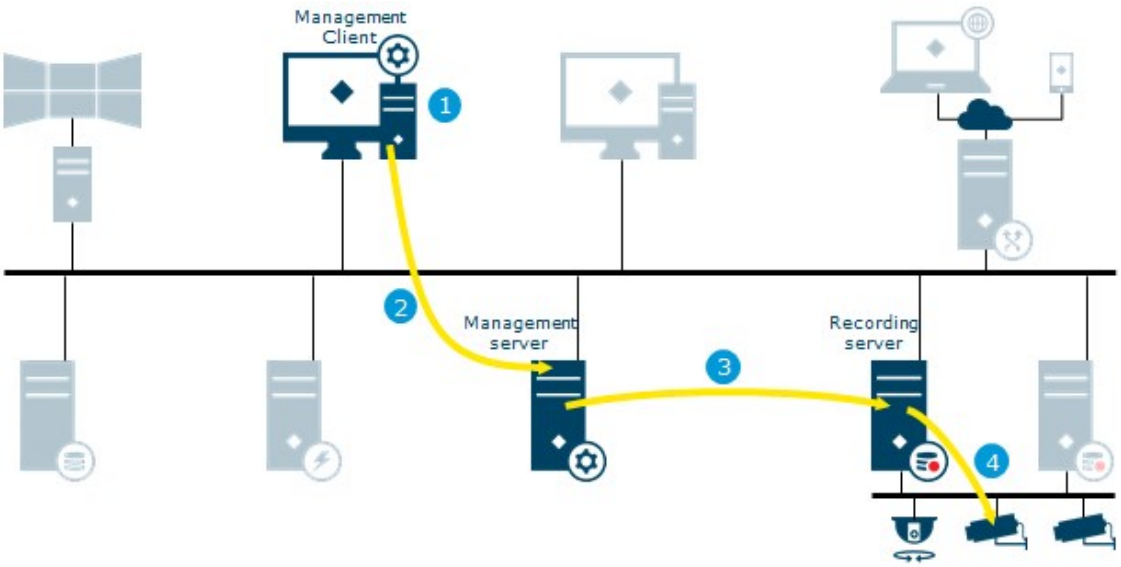
1. The XProtect DLNA Server connects to the management server to authorize itself with the provided credentials
2. A DLNA device scans the network and connects to the XProtect system via the XProtect DLNA Server and requests a live camera video stream
3. XProtect DLNA Server retrieves the requested camera video stream from the recording server
4. XProtect DLNA Server sends the live video stream from the requested camera to the DLNA device

Milestone Open Network Bridge



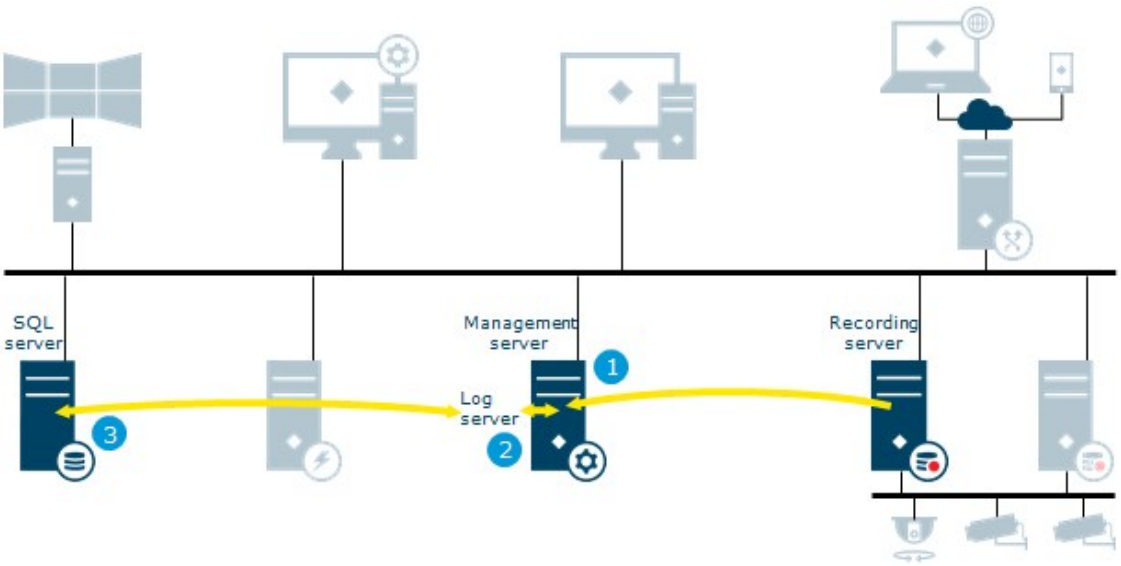
1. Login, stream or PTZ request from ONVIF client received on the Milestone Open Network Bridge server. The Milestone Open Network Bridge is a gateway for non-Milestone clients to the Milestone VMS
2. The Milestone Open Network Bridge forwards the login request to the management server to authenticate the user.
   Access to the Milestone VMS is granted and sent to the Milestone Open Network Bridge server
3. Requested live or playback stream from the recording server is retrieved by the Milestone Open Network Bridge server
4. Video is streamed to the ONVIF client

Management Client configuration update



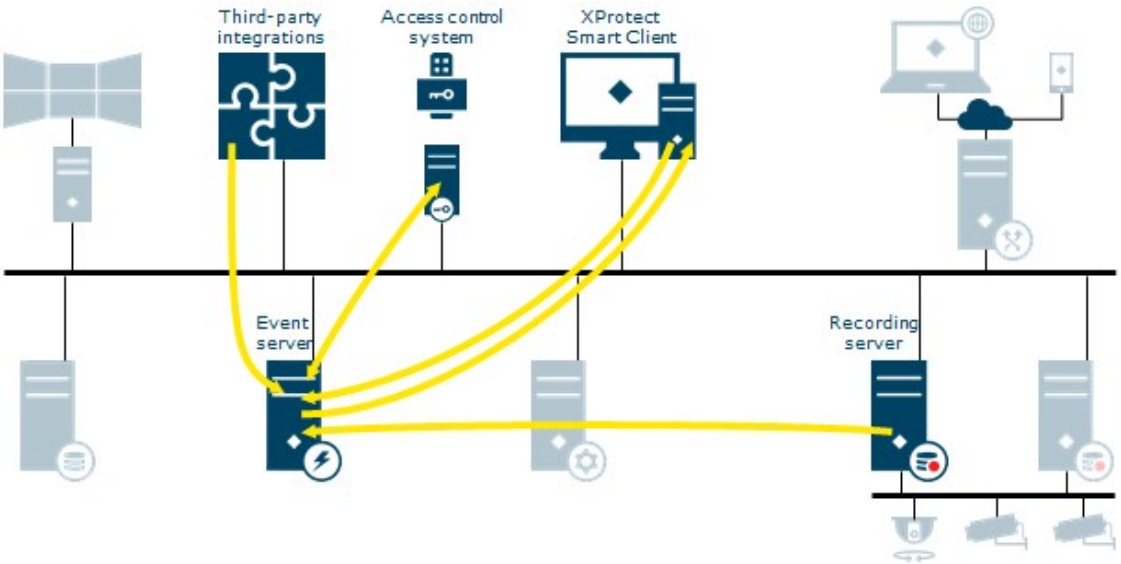
1. Configuration updated on the Management Client
2. Changes are stored on the management server
3. Configuration update sent to relevant components. In this case, the recording server
4. If updates concern cameras, the recording server applies new settings

Log server



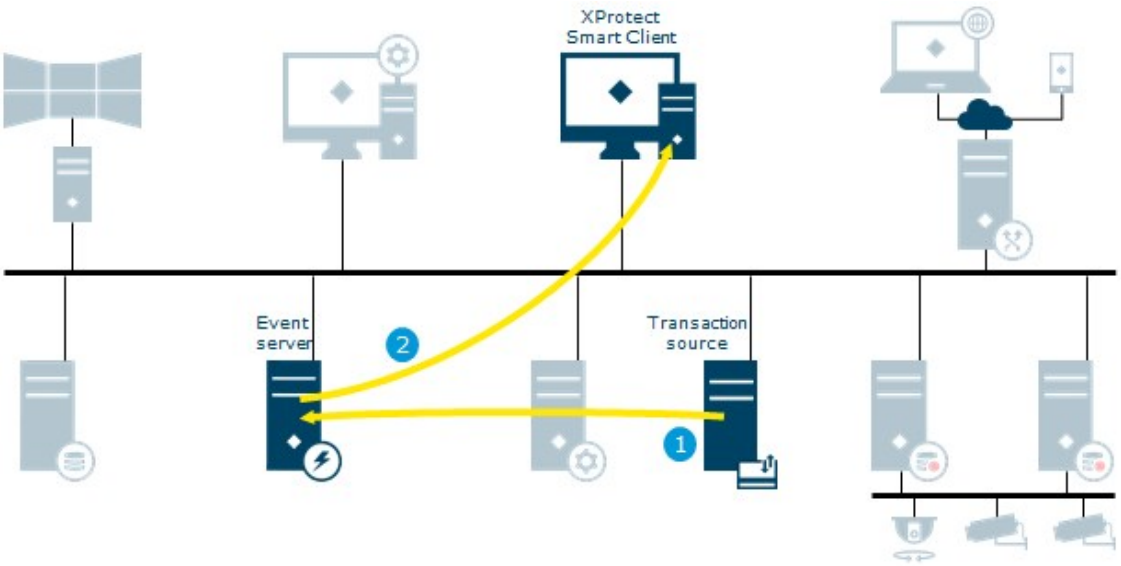
1. The Management server or recording server creates a log message
2. The log message is forwarded to the log server
3. The log message is stored in the log server's SQL database

Event server



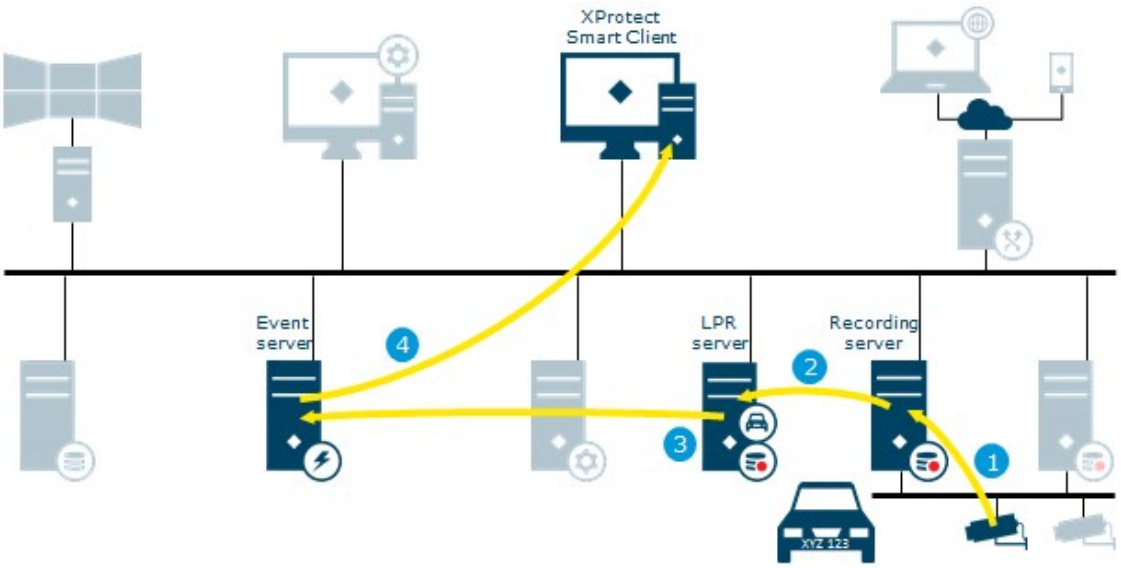
The event server sends data to XProtect Smart Client to show in alarm list, XProtect Access or the map overview.
The event server Plug-in is a client to the access control system.
The XProtect Smart Client user responds to the notification and returns data to event server.

XProtect Transact



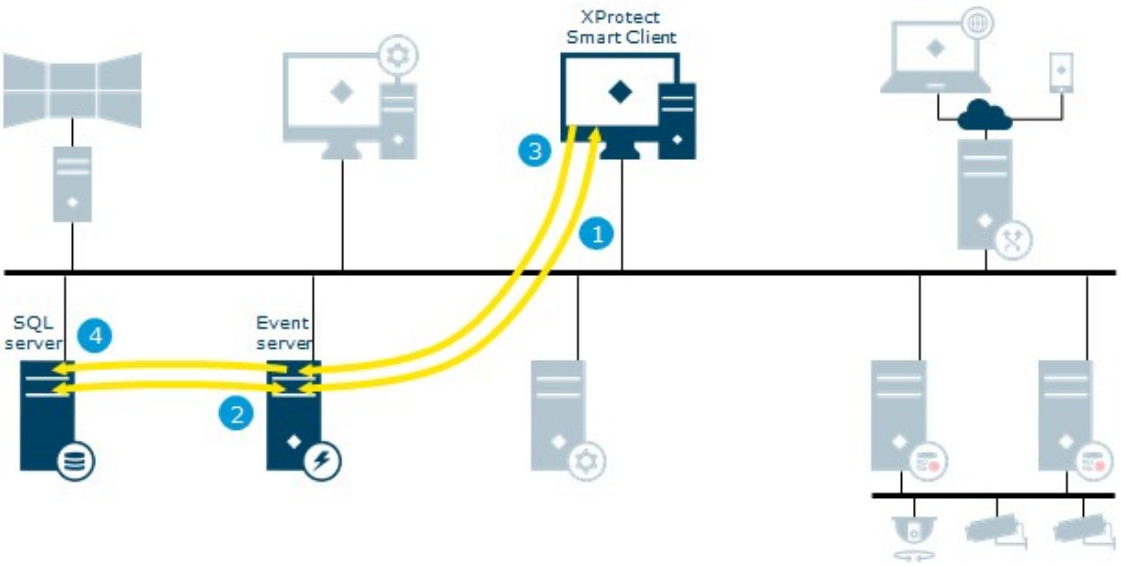
1. Transaction data generated by the transaction source is sent to the event server and stored
2. The event server sends transaction data to XProtect Smart Client. View items containing transaction data and the associated video is updated

XProtect LPR



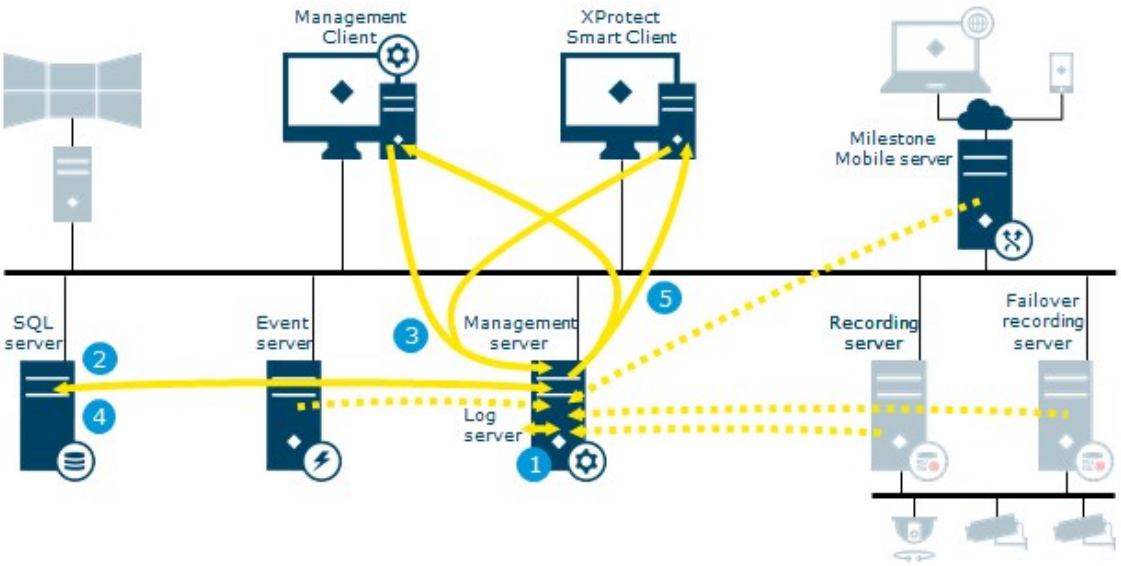
1. Live streams from cameras configured for LPR (License Plate Recognition) retrieved by the recording server
2. Streams from the recording server retrieved by the LPR server
3. The LPR server recognizes license plates by comparing them with the license plate styles of the installed country modules. Found license plates are compared with the match list requests from the event server LPR plug-in
4. The event server sends events and alarms to XProtect Smart Client when there is a match

View and manage alarms



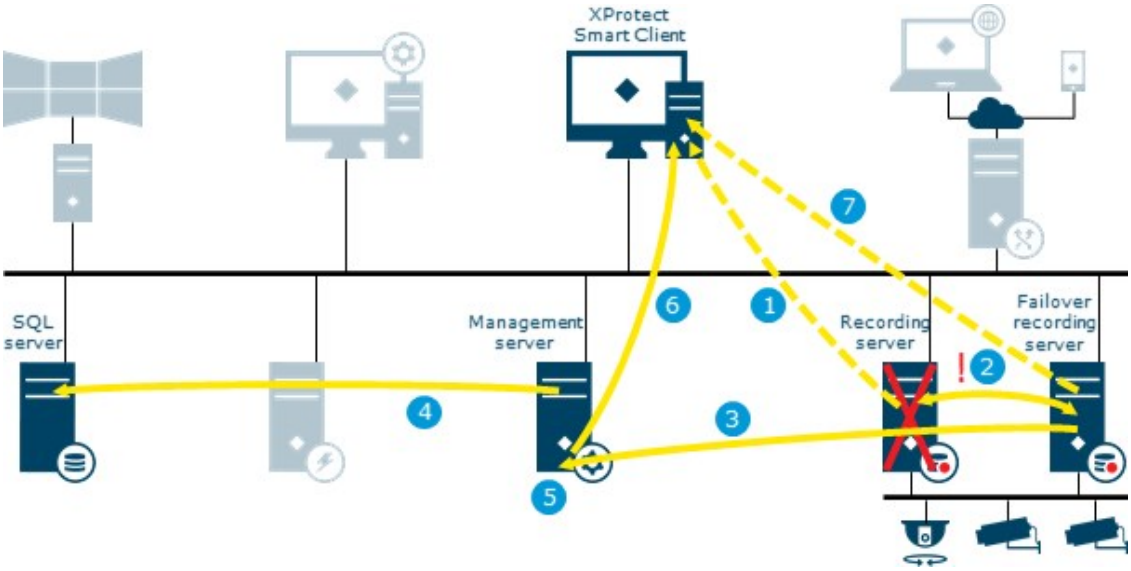
1. XProtect Smart Client requests an alarm list from event server
2. The alarm list is retrieved from the SQL database and returned to XProtect Smart Client
3. The alarm is handled and its state/details is updated by the user
4. New state/details stored in the SQL database

Data collector



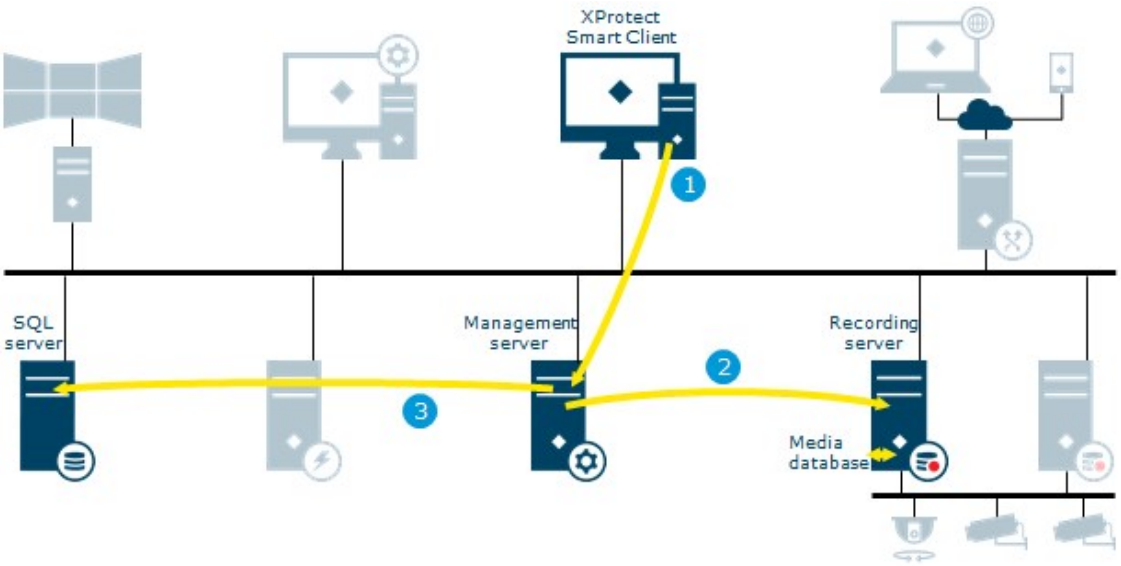
1. System status received on management server delivered by: log server, event server, recording server, failover recording server and mobile server
2. The collected data is stored in an SQL database on a SQL Server
3. XProtect Smart Client or the Management Client requests status via System Monitor
4. Requested data is collected from an SQL database on a SQL Server
5. Data returned to clients

Recording server failover



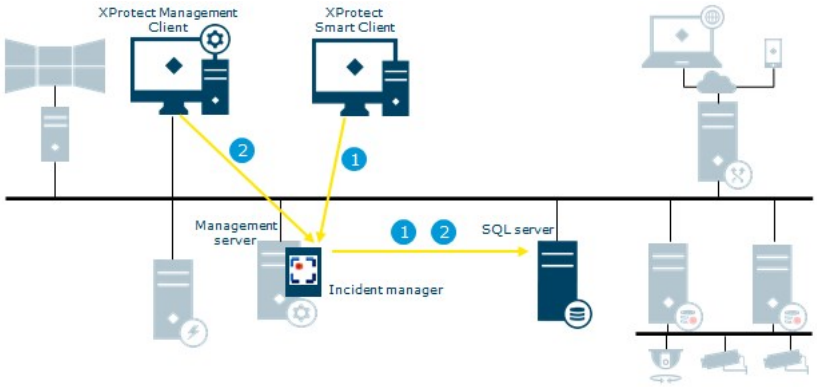
1. Video streamed from the recording server
2. Alive messages exchanged between recording and failover recording server
3. Cold standby: failover message sent, configuration retrieved, start failover
   Hot standby: failover message sent, start failover
4. Configuration updated with active failover recording server
5. Update configuration message sent to the management server
6. Update message distributed to all clients
7. Video streamed from failover recording server

Evidence lock



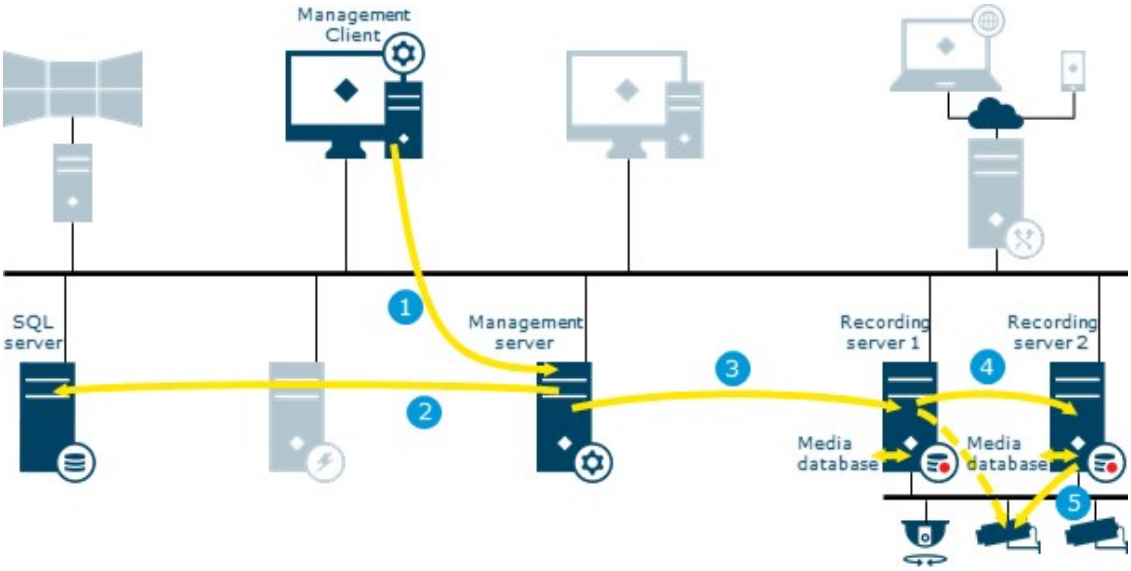
1. The user creates an evidence lock in XProtect Smart Client. XProtect Smart Client sends the information to the management server
2. The management server informs the recording server to store and protect the locked recordings in the Media database
3. The management server stores information about the evidence lock in the SQL database

XProtect Incident Manager



1. An operator of XProtect Smart Client starts, saves, edits, or deletes an incident project. Information about the incident project and its data is saved in the add-on's own SQL database Surveillance_IM. The activities related to incident projects are - depending on the activity - logged in the add-on's own SQL database Surveillance_IM, in the Log Server service's SQL database SurveillanceLogServerV2, or in both.
2. A Management Client administrator creates, edits, or deletes an incident property. The incident property definition is saved in the add-on's own SQL database Surveillance_IM. The user activity is logged in the Log Server service's SQL database SurveillanceLogServerV2.

Move hardware



1. The user moves hardware from recording server 1 to recording server 2 in Management Client
2. The management server receives the update in the system configuration and stores it in the SQL database
3. The management server sends update to recording server 1
4. The management server sends update to recording server 2
5. Recording server 2 connects to Hardware. All new recordings are stored in the recording server 2 database

Old recordings are still available on recording server 1. The system deletes them when the retention time expires. Recordings marked with evidence lock are not deleted until the evidence lock's retention time expires.

Clients connect to recording server 2

Ports used by the system

All XProtect components and the ports needed by them are listed below. To ensure, for example, that the firewall blocks only unwanted traffic, you need to specify the ports that the system uses. You should only enable these ports. The lists also include the ports used for local processes.

They are arranged in two groups:

- **Server components** (services) offer their service on particular ports which is why they need to listen for client requests on these ports. Therefore, these ports need to be opened in the Windows Firewall for inbound and outbound connections
- **Client components** (clients) initiate connections to particular ports on server components. Therefore, these ports need to be opened for outbound connections. Outbound connections are typically open by default in the Windows Firewall

If nothing else is mentioned, ports for server components must be opened for inbound connections, and ports for client components must be opened for outbound connections.

Do keep in mind that server components can act as clients to other server components. These are not explicitly listed in this doc.

The port numbers are the default numbers, but this can be changed. Contact Milestone support, if you need to change ports that are not configurable through the Management Client.

Server components (inbound connections)

Each of the following sections list the ports that need to be opened for a particular service. To figure out which ports need to be opened on a particular computer, you need to consider all services running on the computer.

Management Server service and related processes

Port number	Protocol	Process	Connections from...	Purpose
80	HTTP	IIS	All servers and the XProtect Smart Client and the Management Client	The purpose of port 80 and port 443 is the same. However, which port the VMS uses depends on whether you have used certificates to secure the communication. • When you have not secured the communication with certificates, the VMS uses port 80. • When you have secured the communication with certificates, the VMS uses port 443 except for communication from the event server to the management server. The communication from the event server to the management server uses Windows Secured Framework (WCF) and Windows authentication on port 80.
443	HTTPS	IIS		
6473	TCP	Management Server service	Management Server Manager tray icon, local connection only.	Showing status and managing the service.
8080	TCP	Management server	Local connection only.	Communication between internal processes on the server.
9000	HTTP	Management server	Recording Server services	Web service for internal communication between servers.
12345	TCP	Management Server service	XProtect Smart Client	Communication between the system and Matrix recipients. You can change the port number in the Management Client.

Port number	Protocol	Process	Connections from...	Purpose
12974	TCP	Management Server service	Windows SNMP Service	Communication with the SNMP extension agent. Do not use the port for other purposes even if your system does not apply SNMP. In XProtect 2014 systems or older, the port number was 6475. In XProtect 2019 R2 systems and older, the port number was 7475.

SQL Server service

Port number	Protocol	Process	Connections from...	Purpose
1433	TCP	SQL Server	Management Server service	Storing and retrieving configurations via the Identity Provider.
1433	TCP	SQL Server	Event Server service	Storing and retrieving events via the Identity Provider.
1433	TCP	SQL Server	Log Server service	Storing and retrieving log entries via the Identity Provider.

Data Collector service

Port number	Protocol	Process	Connections from...	Purpose
7609	HTTP	IIS	On the management server computer: Data Collector services on all other servers. On other computers: Data Collector service on the Management Server.	System Monitor.

Event Server service

Port number	Protocol	Process	Connections from...	Purpose
1234	TCP/UDP	Event Server Service	Any server sending generic events to your XProtect system.	Listening for generic events from external systems or devices. Only if the relevant data source is enabled.
1235	TCP	Event Server service	Any server sending generic events to your XProtect system.	Listening for generic events from external systems or devices. Only if the relevant data source is enabled.
9090	TCP	Event Server service	Any system or device that sends analytics events to your XProtect system.	Listening for analytics events from external systems or devices. Only relevant if the Analytics Events feature is enabled.
22331	TCP	Event Server service	XProtect Smart Client and the Management Client	Configuration, events, alarms, and map data.
22333	TCP	Event Server service	MIP Plug-ins and applications.	MIP messaging.

Recording Server service

Port number	Protocol	Process	Connections from...	Purpose
25	SMTP	Recording Server Service	Cameras, encoders, and I/O devices.	Listening for event messages from devices. The port is disabled by default. (Deprecated) Enabling this will open a port for non-encrypted connections and is not recommended.
5210	TCP	Recording Server Service	Failover recording servers.	Merging of databases after a failover recording server had been running.
5432	TCP	Recording Server Service	Cameras, encoders, and I/O devices.	Listening for event messages from devices. The port is disabled by default.
7563	TCP	Recording Server Service	XProtect Smart Client, Management Client	Retrieving video and audio streams, PTZ commands.
8966	TCP	Recording Server Service	Recording Server Manager tray icon, local connection only.	Showing status and managing the service.
9001	HTTP	Recording Server Service	Management server	Web service for internal communication between servers. If multiple Recording Server instances are in use, every instance needs its own port. Additional ports will be 9002, 9003, etc.

Port number	Protocol	Process	Connections from...	Purpose
11000	TCP	Recording Server Service	Failover recording servers	Polling the state of recording servers.
12975	TCP	Recording Server Service	Windows SNMP service	Communication with the SNMP extension agent. Do not use the port for other purposes even if your system does not apply SNMP. In XProtect 2014 systems or older, the port number was 6474. In XProtect 2019 R2 systems and older, the port number was 7474.
65101	UDP	Recording Server service	Local connection only	Listening for event notifications from the drivers.

In addition to the inbound connections to the Recording Server service listed above, the Recording Server service establishes outbound connections to:

- Cameras
- NVRs
- Remote interconnected sites (Milestone Interconnect ICP)

Failover Server service and Failover Recording Server service

Port number	Protocol	Process	Connections from...	Purpose
25	SMTP	Failover	Cameras, encoders, and	Listening for event messages from

Port number	Protocol	Process	Connections from...	Purpose
		Recording Server Service	I/O devices.	devices. The port is disabled by default. (Deprecated) Enabling this will open a port for non-encrypted connections and is not recommended.
5210	TCP	Failover Recording Server Service	Failover recording servers	Merging of databases after a failover recording server had been running.
5432	TCP	Failover Recording Server Service	Cameras, encoders, and I/O devices.	Listening for event messages from devices. The port is disabled by default.
7474	TCP	Failover Recording Server Service	Windows SNMP service	Communication with the SNMP extension agent. Do not use the port for other purposes even if your system does not apply SNMP.
7563	TCP	Failover Recording Server Service	XProtect Smart Client	Retrieving video and audio streams, PTZ commands.
8844	UDP	Failover Recording Server Service	Local connection only.	Communication between the servers.
8966	TCP	Failover Recording Server Service	Failover Recording Server Manager tray icon, local connection only.	Showing status and managing the service.

Port number	Protocol	Process	Connections from...	Purpose
8967	TCP	Failover Server Service	Failover Server Manager tray icon, local connection only.	Showing status and managing the service.
8990	TCP	Failover Server Service	Management Server service	Monitoring the status of the Failover Server service.
9001	HTTP	Failover Server Service	Management server	Web service for internal communication between servers.



In addition to the inbound connections to the Failover Server / Failover Recording Server service listed above, the Failover Server / Failover Recording Server service establishes outbound connections to the regular recorders, cameras, and for Video Push.

Log Server service

Port number	Protocol	Process	Connections from...	Purpose
22337	HTTP	Log Server service	All XProtect components except for Management Client and the recording server.	Write to, read from, and configure the log server.

Mobile Server service

Port number	Protocol	Process	Connections from...	Purpose
8000	TCP	Mobile Server service	Mobile Server Manager tray icon, local connection only.	SysTray application.
8081	HTTP	Mobile Server service	Mobile clients, Web clients, and Management Client.	Sending data streams; video and audio.
8082	HTTPS	Mobile Server service	Mobile clients and Web clients.	Sending data streams; video and audio.
40001 - 40099	HTTP	Mobile Server service	Recording server service	Mobile Server Video Push. This port range is disabled by default.

LPR Server service

Port number	Protocol	Process	Connections from...	Purpose
22334	TCP	LPR Server Service	Event server	Retrieving recognized license plates and server status. In order to connect, the Event server must have the LPR plug-in installed.
22334	TCP	LPR Server Service	LPR Server Manager tray icon, local connection only.	SysTray application

Milestone Open Network Bridge service

Port number	Protocol	Process	Connections from...	Purpose
580	TCP	Milestone Open Network Bridge Service	ONVIF clients	Authentication and requests for video stream configuration.
554	RTSP	RTSP Service	ONVIF clients	Streaming of requested video to ONVIF clients.

XProtect DLNA Server service

Port number	Protocol	Process	Connections from...	Purpose
9100	HTTP	DLNA Server Service	DLNA device	Device discovery and providing DLNA channels configuration. Requests for video streams.
9200	HTTP	DLNA Server Service	DLNA device	Streaming of requested video to DLNA devices.

XProtect Screen Recorder service

Port number	Protocol	Process	Connections from...	Purpose
52111	TCP	XProtect Screen Recorder	Recording Server Service	Provides video from a monitor. It appears and acts in the same way as a camera on the recording server. You can change the port number in the Management Client.

XProtect Incident Manager service

Port number	Protocol	Process	Connections from...	Purpose
80	HTTP	IIS	XProtect Smart Client and the Management Client	The purpose of port 80 and port 443 is the same. However, which port the VMS uses depends on whether you have used certificates to secure the communication. • When you have not secured the communication with certificates, the VMS uses port 80. • When you have secured the communication with certificates, the VMS uses port 443.
443	HTTPS	IIS		

Server components (outbound connections)

Management Server service

Port number	Protocol	Connections to...	Purpose
443	HTTPS	The License server that hosts the License Management service. Communication is via https://www.milestonesys.com/OnlineActivation/LicenseManagementService.asmx	Activating licenses.

Recording Server service

Port number	Protocol	Connections to...	Purpose
80	HTTP	Cameras, NVRs, encoders	Authentication, configuration, data streams, video, and audio.

Port number	Protocol	Connections to...	Purpose
		Interconnected sites	Login
443	HTTPS	Cameras, NVRs, encoders	Authentication, configuration, data streams, video, and audio.
554	RTSP	Cameras, NVRs, encoders	Data streams, video, and audio.
7563	TCP	Interconnected sites	Data streams and events.
11000	TCP	Failover recording servers	Polling the state of recording servers.
40001 – 40099	HTTP	Mobile Server service	Mobile Server Video Push. This port range is disabled by default.

Failover Server service and Failover Recording Server service

Port number	Protocol	Connections to...	Purpose
11000	TCP	Failover recording servers	Polling the state of recording servers.

Event Server service

Port number	Protocol	Connections to...	Purpose
443	HTTPS	Milestone Customer Dashboard via https://service.milestonesys.com/	Send status, events and error messages from the XProtect system to Milestone Customer Dashboard.

Log Server service

Port number	Protocol	Connections to...	Purpose
443	HTTP	Log server	Forwarding messages to the log server.

API Gateway

Port number	Protocol	Connections to...	Purpose
443	HTTPS	Management sever	RESTful API

Cameras, encoders, and I/O devices (inbound connections)

Port number	Protocol	Connections from...	Purpose
80	TCP	Recording servers and failover recording servers	Authentication, configuration, and data streams; video and audio.
443	HTTPS	Recording servers and failover recording servers	Authentication, configuration, and data streams; video and audio.
554	RTSP	Recording servers and failover recording servers	Data streams; video and audio.

Cameras, encoders, and I/O devices (outbound connections)

Port number	Protocol	Connections to...	Purpose
25	SMTP	Recording servers and failover recording servers	Sending event notifications (deprecated).
5432	TCP	Recording servers and failover recording servers	Sending event notifications. The port is disabled by default.
22337	HTTP	Log server	Forwarding messages to the log server.



Only a few camera models are able to establish outbound connections.

Client components (outbound connections)

XProtect Smart Client, XProtect Management Client, XProtect Mobile server

Port number	Protocol	Connections to...	Purpose
80	HTTP	Management Server service	Authentication
443	HTTPS	Management Server service	Authentication of basic users when encryption is enabled.
443	HTTPS	Milestone Systems A/S (doc.milestonesys.com at 52.178.114.226)	Management Client and Smart Client occasionally check if the online help is available by accessing the help URL.
7563	TCP	Recording Server service	Retrieving video and audio streams, PTZ commands.
22331	TCP	Event Server service	Alarms.

XProtect Web Client, XProtect Mobile client

Port number	Protocol	Connections to...	Purpose
8081	HTTP	XProtect Mobile server	Retrieving video and audio streams.
8082	HTTPS	XProtect Mobile server	Retrieving video and audio streams.

API Gateway

Port number	Protocol	Connections to...	Purpose
80	HTTP	Management Server	RESTful API
443	HTTPS	Management Server	RESTful API



helpfeedback@milestone.dk

About Milestone

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 Systems 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 150,000 sites worldwide. Founded in 1998, Milestone Systems is a stand-alone company in the Canon Group. For more information, visit https://www.milestonesys.com/.

Milestone Systems
Learning & Performance Catalog



The mission of the Learning & Performance team is to empower the people in the Milestone community to successfully perform on the job by delivering effective learning and performance support solutions. Our vision is to grow the number of people globally who have proven expertise in the design and implementation of Milestone community solutions.

We offer both instructor-led training classes and free online eLearning courses to help learners build the knowledge and skills needed to perform on the job. Our online certification assessments allow individuals to prove their expertise in design, installation, and configuration of Milestone products and to fulfill Channel Partner Program (CPP) requirements.

It is important that learners receive recognition and documentation of their successes! Completion certificates are available for learners after attending our instructor-led training classes or completing many of our eLearning courses. Certification diplomas are issued to individuals who pass the certification assessments.

In support of our global community, our Learning Portal, training, and certifications are available in multiple languages.

milestone

Contents

eLearning 3
Partner Courses 3
Getting Started with XProtect® Smart Client * 3
Milestone Fundamentals of IP Surveillance Systems 3
Getting Started with XProtect® Professional * 3
Installing and Configuring the Milestone Husky™ M30/M50 4
Using the Customer Dashboard 4
New Feature Series 4
End-User Courses 4
Getting Started with XProtect® Smart Client * 4
Configuring and Using the Milestone Husky™ M10 5

Instructor-led training 6
Milestone Professional 6
Milestone Solution Design 6
Milestone Technical Configuration Level 1 7
Milestone Technical Configuration Level 2 8

Certifications 9
Professional Certification 9
Milestone Certified Design Engineer (MCDE) 9
Milestone Certified Integration Technician (MCIT) 10
Milestone Certified Integration Engineer (MCIE) 10

Register today! 10

Contact Us 10



eLearning

Our eLearning is a convenient way of getting immediate access to free training online! We offer an ever-increasing number of eLearning courses for integrators and reseller partners, as well as end-user customers. These courses are free, available 24/7 from your computer or tablet, and are localized in several languages.

Partner Courses

These eLearning courses are designed for our integrators and reseller partners. To access these courses, partners must be logged into their MyMilestone account.

Getting Started with XProtect® Smart Client *

The XProtect Smart Client is a powerful application used to view and manage the daily operations of a surveillance installation. In this eLearning course, the learner acts as a consultant and helps virtual team members get started setting up and using the Milestone XProtect Smart Client. Designed for end-user administrators and operators, the course covers how to:

- Install and navigate through the XProtect Smart Client.
- Create views in the XProtect Smart Client.
- Monitor events by viewing and adjusting live video.
- Investigate incidents by searching through and playing back recorded video.
- Export evidence via video and still images.

This eLearning course is available to both Partners and End-Users.

Milestone Fundamentals of IP Surveillance Systems

The *Milestone Fundamentals of IP Surveillance System* helps build foundational knowledge and skills with digital video management systems (VMS). The course covers how to:

- Describe the types of devices in IP surveillance installations and list the characteristics of a VMS.
- Select appropriate cameras and lenses by considering the surveillance objective, field of view, resolution standards, exposure, codecs, and other characteristics.
- Describe the main network components and protocols that support IP surveillance systems.
- Perform network bandwidth calculations and identify limitations or critical points in a network design that may lead to choke points.
- Describe the main types of storage and the recommendations for storing video in a VMS.

Getting Started with XProtect® Professional *

XProtect Professional is IP video management software (VMS) designed for mid-sized security installations of more than 45 cameras and is typically used in institutions such as schools, museums, and hospitals. In this eLearning course, the learner acts as a consultant to help a virtual team member install and configure XProtect Professional video management systems (VMS). The course covers how to:

- Download and install the XProtect Professional VMS.
- Automatically and manually connect devices.

- Configure storage and archive settings.
- Adjust motion detection.
- Add and manage users.
- Manage licenses.
- Smart Connect.
- Push notifications.
- Configuring and using maps.

Installing and Configuring the Milestone Husky™ M30/M50

The Milestone Husky products are customizable workstation appliances embedded with XProtect video management software (VMS). This eLearning course uses hands-on simulations to teach the basic installation and configuration of Milestone Husky M30s and M50s. The course covers how to:

- Prepare and connect a Milestone Husky M30 or M50 to the network.
- Configure a surveillance server using the Husky M30 or M50 Management Application.
- Configure the XProtect Smart Client.

Using the Customer Dashboard

The Customer Dashboard is an online service used to monitor the health of a customer's security system in real-time. This eLearning course covers how to use the dashboard to:

- Activate Milestone software.
- Manage SLCs and customers.
- Monitor customer installations.
- Stay updated with system uptime reports.

New Feature Series

Milestone product releases occur three times a year and include a number of new features. These releases are supported by both printable reference guides and eLearning modules covering use of the new features. The modules in the XProtect 2016 series include:

- XProtect® Smart Wall 2016
- Access Control
- Enhanced Web Client (Investigation Mode)
- Extended System Monitor
- PTZ Presets and Patrolling
- Push Notifications
- Move Hardware
- Smart Connect

End-User Courses

Getting Started with XProtect® Smart Client *

The XProtect Smart Client is a powerful application used to view and manage the daily operations of a surveillance installation. In this eLearning course, the learner acts as a consultant and helps virtual team members get started setting up and using the Milestone XProtect Smart Client. Designed for end-user administrators and operators, the course covers how to:

- Install and navigate through the XProtect Smart Client.
- Create views in the XProtect Smart Client.
- Monitor events by viewing and adjusting live video.
- Investigate incidents by searching through and playing back recorded video.
- Export evidence via video and still images.

This eLearning course is available to both Partners and End-Users.

Configuring and Using the Milestone Husky™ M10

The Milestone Husky products are customizable workstation appliances embedded with XProtect video management software (VMS). The Milestone Husky M10 supports all Milestone clients and is recommended for entry-level surveillance. This eLearning course covers the basic installation, configuration, and usage of the Milestone Husky M10. This eLearning course uses hands-on simulations to teach the basic installation and configuration of Milestone Husky M10. The course covers how to:

- Prepare and connect the Milestone Husky M10 to the network.
- Configure the Husky M10 by adding users and cameras.
- Configure the camera settings.
- View live video.
- Play back and exporting recorded video.

** Recommended for the Channel Partner Program.*



Instructor-led training

Milestone's expert trainers teach classes all over the globe in a number of different languages. Our instructor-led training workshops use a combination of real-world scenarios and hands-on exercises to build the knowledge and skills necessary to successfully design, install, and configure Milestone Advanced products to meet customer needs. These workshops support the transfer of knowledge to on-the-job performance through the use of checklists and job aids that learners take with them into the field.

Individuals who are looking to build their capabilities with Milestone products are encouraged to attend our instructor-led training workshops. These workshops also help attendees prepare for the corresponding certification tests, which prove expertise with Milestone products and fulfil certification requirements for various levels in the Channel Partner Program.

After attending a class, a completion certificate will be available.

BICSI CEC credit hours are available for many classes.

Milestone Professional

This one-day training and certification class uses presentations and hands-on exercises to guide students through installing, configuring, and using XProtect Professional.

This class includes a certification test at the end.

Target Audience

Field technicians who are responsible for installing and configuring Milestone's Business Ready line of video surveillance systems.

Milestone Solution Design

This two-day training workshop is designed to empower our partners to consistently meet their customers' needs and exceed their expectations. During this workshop, attendees will concentrate on best practices in customer needs identification, information collection, and making video surveillance design decisions.

Attendees use the Milestone Solution Design Model, job aids, and additional tools provided in class to design effective solutions for real-life scenarios. A professional facilitator guides attendees to meet stated requirements and provides expertise in Milestone best practices.

Target Audience

Individuals responsible for working with customers and designing security systems using Milestone products.

Individuals with limited system design experience will benefit most from attending this workshop.

This training workshop is not required prior to taking the Milestone Certified Design Engineer (MCDE) online certification assessment but is recommended as preparation.

**For learners looking to earn the MCDE certification and who have experience in system design, we recommend attempting the online assessment prior to enrolling in the class. We also recommend reviewing the MCDE Study Guide, as it provides insight into the knowledge and skills required and how to best prepare for the certification assessment.*

Prerequisites

We require attendees to complete the following eLearning courses:

1. Milestone Fundamentals of IP Surveillance Systems
2. Getting Started with Design Decisions

These eLearning courses are available on the Milestone Partner Learning Portal.

Milestone Technical Configuration Level 1

This three-day training workshop is designed to develop participant ability to install and configure moderately complex XProtect® Advanced VMS installations.

The workshop consists of a series of hands-on exercises where learners practice configuring the XProtect® Corporate VMS to specifications from realistic scenarios. Step-by-step instructions and a professional facilitator guide the learner as they configure systems according to sample specs.

A final project allows learners to practice and demonstrate their skills in a more independent environment, but with continued support from the facilitator.

Participants leave with a detailed sequential checklist and annotated notes to help transfer their knowledge to the field.

Target Audience

Field technicians who are responsible for installing and configuring Milestone's Advanced product line of video surveillance systems.

Content Areas Covered:

- Configure the Network and Server
- Install Milestone XProtect Advanced Components
- Configure the Recording and Storage Settings
- Add Devices to the Recording Server
- Configure Cameras
- Rules introduction
- Create Profiles
- Configure and using events
- Configure a Smart Wall
- Set Security
- Set Options
- Define alarms
- System monitoring
- Configure Mobile Server
- Interconnect

This training workshop is not required prior to taking the Milestone Certified Integration Technician (MCIT) online certification assessment but is recommended as preparation.

**For learners looking to earn the MCIT online assessment after attending class, we recommend first reviewing MCIT Study Guide, as it provides insight into the knowledge and skills required and how to best prepare for the certification assessment.*

Prerequisites

Fundamental knowledge and skills with cameras, network and storage devices, as well as installing and configuring the XProtect Smart Client.

We also require attendees to complete the following FREE eLearning courses, as these topics are not covered during the workshop:

1. Milestone Fundamentals of IP Surveillance Systems
2. Getting Started with XProtect Professional
3. Getting Started with XProtect Smart Client

These eLearning courses are available on the Milestone Partner Learning Portal.

Milestone Technical Configuration Level 2

This three-day training workshop is designed to further develop the ability to install and configure more complex XProtect® Advanced VMS installations.

During this workshop, participants work in small teams to modify and expand existing XProtect® Corporate VMS configurations to accommodate evolving customer business needs, as well as demonstrate what each modification accomplishes. New requirements and requests introduce layers of complexity into the surveillance installations and increase their skills in handling challenging scenarios.

A final project allows learners to practice and demonstrate their skills in a more independent environment, but with continued support from the facilitator.

Participants leave with a detailed sequential checklist and annotated notes to help transfer their knowledge to the field.

Target Audience

Milestone Certified Integration Technicians who are responsible for installing and configuring advanced features of Milestone XProtect Corporate for high-complexity surveillance systems.

Content Areas Covered

- Fine-tuning Mobile Server performing
- Advanced user security settings
- Automate Smart Client installation and startup behavior
- Working with advanced camera settings and unsupported cameras
- Complex event support
- Hot and cold failover
- Domain support
- Configuring Milestone Federated Architecture™
- Clustering servers

This training workshop is not required prior to taking the Milestone Certified Integration Engineer (MCIE) online certification assessment but is recommended as preparation.

**For learners looking to earn the MCIE online assessment after attending class, we recommend first reviewing the MCIE Study Guide, as it provides insight into the knowledge and skills required and how to best prepare for the certification assessment.*

Prerequisites

To be eligible to attend, you must be a Milestone Certified Integration Technician.



Certifications

Earning a Milestone certification proves expertise with our products and is a promise to end customers of the certificate holder's ability to design, install, and configure surveillance solutions that meet their needs. Certifications are also required to progress in the Milestone Channel Partner Program.

Our online certification assessments are available 24/7 from your computer or tablet and are available in several languages. Each certification is valid for two years. Partners can register for and complete the online certification assessments on the Partner Learning Portal. Please note, If you are not logged into the Partner Learning Portal, the available certification assessments will not be visible.

We also have several tools available to help prepare for the online certification assessments, including instructor-led training workshops, free eLearning courses, white papers, and Study Guides. These tools are available to anyone who is interested in becoming Milestone certified.

Upon successfully passing a certification assessment, a diploma is made available in the learner's profile. The diplomas are printable and can be accessed when logged into the Partner Learning Portal.

Professional Certification

The Milestone Professional certification assessment tests an individual's knowledge and skills in installing, configuring, and using XProtect Professional.

Prerequisites

We do not require any certifications prior to taking the Professional certification assessment. However, we do recommend completing the *Milestone Fundamentals of IP Surveillance Systems* and *Getting Started with XProtect Professional* eLearning courses.



Milestone Certified Design Engineer (MCDE)

The Milestone Certified Design Engineer (MCDE) assessment tests knowledge and skills in designing IP surveillance systems using the Milestone XProtect VMS product suite. An MCDE has proven capability in designing a security system using Milestone products following best practices in technical architecture and meeting customer needs.

**The MCDE is required for Gold and Platinum levels in the Channel Partner Program.*

Prerequisites

We do not require any certifications or classes prior to taking the MCDE assessment. However, going through the MCDE Study Guide is required and we highly recommend that people new to design also attend the Milestone Solution Design training workshop when preparing to take the assessment.



Milestone Certified Integration Technician (MCIT)

The Milestone Certified Integration Technician (MCIT) assessment tests the ability to install and configure moderately complex XProtect Advanced VMS installations with camera counts between 100-500 cameras, a single Management Server, and features like a Milestone Interconnect™ connection to a remote site.

**The MCIT is required for the Gold and Platinum levels in the Channel Partner Program.*

Prerequisites

We do not require any classes or certifications prior to taking the MCIT assessment. However, going through the MCIT Study Guide is required and, for new installers, we highly recommend attending the Milestone Technical Configuration Level 1 training workshop when preparing to take the assessment.



Milestone Certified Integration Engineer (MCIE)

The Milestone Certified Integration Engineer (MCIE) assessment tests your ability to install and configure a complex XProtect Advanced VMS installation with a camera count of approximately 100-10,000 cameras, including features such as multiple Management Servers, multiple Mobile Servers, edge storage, multicast, clustering, and other advanced configuration options.

**The MCIE is required for the Platinum level in the Channel Partner Program.*

Prerequisites

An MCIT certification is required to be eligible to take the MCIE assessment. We also require going through the MCIE Study Guide. While it is not required, we highly recommend attending the Milestone Technical Configuration Level 2 training workshop before taking the test.

Register today!

The Milestone Learning Portal makes it easy to find what you need—whether it is an eLearning course, an upcoming training workshop in your area, or a certification assessment. The portal allows you to self-register, pay, and even complete training and certification assessments.

Visit the Milestone Learning & Performance homepage for more information and to access the portal.

Be sure to review the "How to Use This Portal" guide when first using the portal. This guide is available on the portal's Home page, is available in several languages, and is a great tool in learning how to navigate the portal.

Contact Us

Milestone has team members all over the world available to assist you.

For questions regarding our Learning Portal and our Training and Certification program, please contact your region's Learning and Performance team.

Americas: Milestonetrainingamericas@milestonesys.com

EMEA: MilestonetrainingEMEA@milestonesys.com

APAC: MilestonetrainingAPAC@milestonesys.com



© 2016 Milestone Systems
Milestone Systems Inc.
8905 SW Nimbus Avenue
Suite 400
Beaverton, OR 97008
Tel: +1 503 350 1100 Fax: +1 503 350 1199
www.milestonesys.com

No portion of this material may be reproduced in any form without permission.

MAKE THE
WORLD SEE

Milestone Care Policy

Prepared by:

Line Byssing, Senior Product Marketing Manager, Milestone Systems 2021

milestone

Milestone Care Program

Milestone Care is a complete software maintenance and support program that takes care of your product throughout its lifetime. It delivers on our commitment to your business that you can take full advantage of your product and get the most out of your investment.

Designed to give you peace of mind, the Care program has two distinct packages. Whether you need recurring software updates or 24/7 access to Milestone Support — or both — there is a package to suit your needs.

Milestone Care™ Plus

When you want to protect your investment.
XProtect® video management software (VMS) products are updated on a recurring basis to become safer and more efficient and powerful. Milestone Care Plus is designed as a software maintenance service. It ensures you have instant access to the product updates. This helps to protect your initial investment and ensure the solidity of your system.



Here is what you get with Care Plus:

- Recurring product updates that make your product safer and more efficient and powerful
- Full return on your initial XProtect investment if upgrading to a more advanced XProtect solution.

Recurring product updates

Customers with active Milestone Care Plus coverage can instantly update their software to the latest version. Customers who want to upgrade to a more advanced product, or customers without Milestone Care Plus coverage who wish to update their present Milestone product need to do that as an order transaction via Milestone Store.

Full return on your initial XProtect investment if upgrading to a more advanced XProtect solution

Milestone offers a unique trade-in policy for our software products, allowing customers to protect investments made in Milestone software. The trade-in policy provides:

- Software update to a newer version of the same product

- Software upgrade to a more advanced product, for example, upgrade from XProtect Expert to XProtect Corporate

The present Milestone trade-in policy grants the customer a refund on the old product to be updated/upgraded, where the amount credited is dependent on the Milestone Care service level.

- Customers with active Milestone Care Plus are entitled to a 100 percent refund of the current recommended retail price when trading-in licenses for their existing XProtect products.
- Customers without Milestone Care Plus coverage are entitled to 30 percent refund of the current recommended retail price of their existing product.

A refund from trading in software products cannot be converted to a cash payout, voucher etc., but will instead have to be used to purchase other Milestone products.

Customers with Milestone Care Plus can instantly update their software to the latest version via the Customer Dashboard. Customers who want to upgrade to a more advanced product or customers without Milestone Care Plus coverage who wish to update their present Milestone product need to do that as an order transaction via Milestone Store.

Please note that end customers should consult with Milestone resellers for pricing. The terms outlined above reflect our current trade-in policy, which may be subject to change.

+ If you need more support coverage, Care Premium expands the benefits of Care Plus:

Milestone Care™ Premium

When you need 24/7 direct access to the Milestone Support Team.
When support can't wait until Monday, Milestone Care Premium provides you with direct, personalized and prioritized access to the experts in the global Milestone technical support team round-the-clock.



Here is what you get with Care Premium:

- 24/7 access to the Milestone Support Team.
- Prioritized support to ensure critical issues are dealt with quickly.
- Support in selected languages based on availability.

Committed first response time for Milestone Care Premium

All severities have a first response within 15 minutes if reported by phone and within four hours if reported online. In addition to these initial response times, there are service objectives for progress status reporting.

Support entry point	First response time (FRT)
Phone	15 minutes (callback if needed)
Online web-form & email	Four hours

Committed Progress Status time for Milestone Care Premium

The Progress Status Time (PST) is the time it takes Milestone to report back to you the progress of the issue, current thoughts as to the cause of the issue, requests for additional information from the client, a decision of the actual severity level (if that needs to move up or down), as well as possible support activities moving forward.

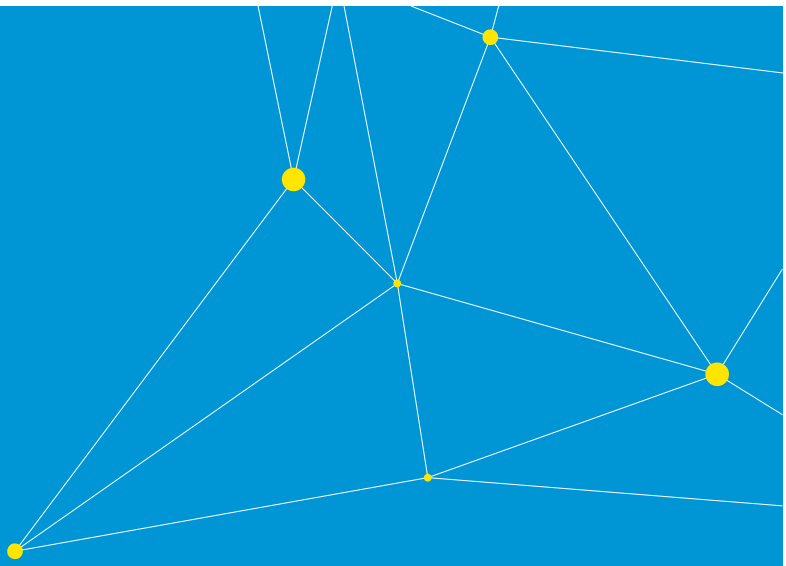
Severity Level	Progress status time (PST)
A Catastrophic	Every 4 hours
B Severe	Semi-weekly
C Moderate	Every second week
D Minor	Every second week

Technical Phone Support

The primary support language is English. Based on availability, local language support in Europe, the Middle East and Africa include Danish, Dutch, German, French, Italian, Russian, and Spanish. Based on availability, local language support in the Americas includes Spanish.

Local language support is delivered during regular business hours and subject to availability. Outside-office hours will always only be in English, as we serve that need using follow-the-sun model, from Melbourne, Bangalore, Dubai, Sofia, Barcelona, Mexico, and Portland offices.

Click here to see the local dial-in numbers.



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.

Milestone System Professional Services

Milestone Professional Services is a portfolio of system deployment and optimization services designed to unlock the full potential of Milestone installations while optimizing the system performance for a problem-free and stable operation.

Quick Start-Up Service: The Quick Start-Up service is a remote installation and configuration service for new Milestone installations. Drawing on Milestone's broad system experience, the service ensures that the implementation is in according to best practices and that the system is tuned to ensure optimal performance for the specific customer application.

System Start-Up Services: The System Start-Up service is an onsite installation and configuration services for new Milestone installations. Drawing on Milestones broad system experience the service ensures that the implementation is executed according to best practices and that the system is tuning for optimal performance for the specific customer application. During the on-site service execution, the Milestone Engineer work together with the Milestone Partner and the end-customer, which not only ensures that everything is installed and configured properly, but also that competence about the installation is transferred.

Upgrade Assistance Services: The Upgrade Assistance service is designed to assist end-customers who want to upgrade their existing Milestone XProtect software to the newest version, and gain access to the latest functions and capabilities. The service is relevant to end-customers that subscribe to the Milestone Care Plus service.

System Health Check Services: The System Health Check service is an audit of installed software and hardware configurations. This service ensures that the configuration of the installation is aligned with Milestone's best practices and ensures optimal performance. Observed deficiencies and system optimization recommendations will be documented in a service report and delivered upon completion of the service.

System Design Services: The System Design Service is an onsite demo-to-win installation and configuration service. The implementation is executed with test licenses and replicates fully the network, CPU and storage load for the camera count and video feeds specified for the proof of concept.

System Troubleshooting: Troubleshooting complex XProtect systems especially when outside Milestone Technical Support framework, is not always easy. With extensive experience in this area Milestone Professional Services team is ready to assist you.

Installation and configuration of Milestone VMS: Get a functional and properly configured XProtect system meant to last with help from Milestone Professional Services team.

Basic Installation without configuration of Milestone VMS: You want to spare some time or learn new skills; Milestone Professional Services team is ready to assist you.

Full installation and configuration of Milestone VMS: You need to install and configure a complex XProtect VMS on your own, or the task may take too long? Choose our team of experts to get a functional and properly configured XProtect system meant to last.

Upgrade and system migration: Milestone Professional Services team can onsite or remotely upgrade your XProtect software to the latest purchased version or assist with its migration from E-Code to C-Code or C-Code to C-Code, as requested.

Customized Services: At customer's request, Milestone can provide tailored and customer-specific solutions. All concluded service engagements are fully documented.

For additional information, see the following website https://www.milestonesys.com/video-technology/services/professional-services/

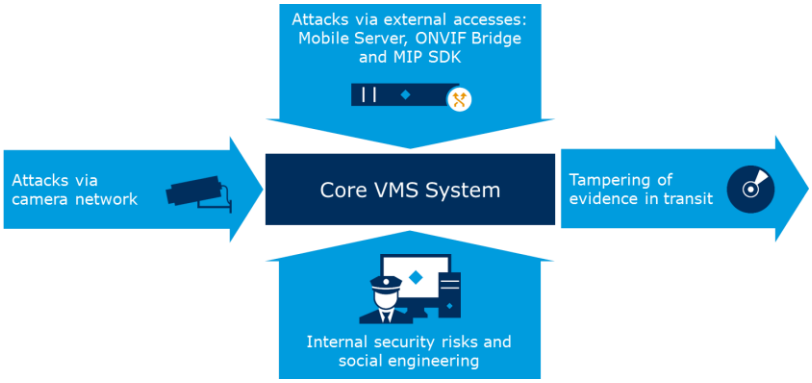
Milestone XProtect VMS - secure by design

- providing high protection resilience against cyber attacks

Milestone XProtect VMS products are designed to provide the highest security protection against external and internal security threats. Tiered administrator and user rights, enforced on the server side, combined with the use of standard IT security procedures, make XProtect VMS the perfect choice for organizations with focus on cybersecurity.

Video surveillance systems are one of several ways organizations safeguard assets and people. As with other protection systems, video surveillance systems can be exposed to attacks in conjunction with criminal activities. However, unlike the physical protection systems, the attacks on IT and video surveillance systems are more refined and subtler, and often difficult to detect as there often are no visible traces.

Video surveillance systems are, like any other IT infrastructure, exposed to both internal and external security threats. Potential threats include: distributed denial-of-service (DDoS) attacks, hacking, social engineering, port scanning and general software vulnerabilities, among others.



Principal risk exposures in a VMS system

The exposure to cyberattack depends on three primary parameters: the overall risk profile of the company or organization in question, the cybersecurity maturity level of the organization and the degree of attention on cybersecurity when designing and installing the system.

Key benefits

- Protects the system integrity from cybersecurity attacks
- Secure end-to-end handling of exported forensic material
- Secure access for web and mobile users
- Secure integration of third-party applications and systems

Key features

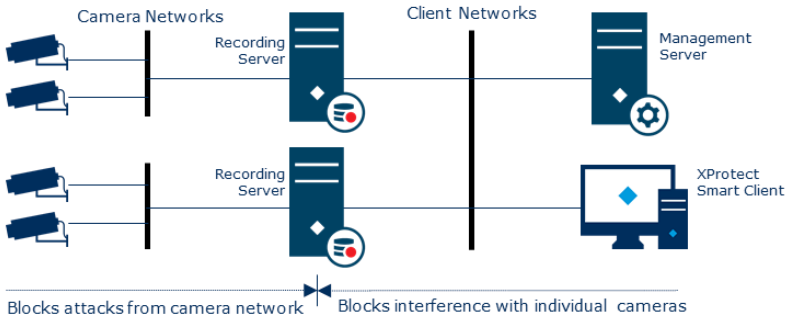
- Possibility for physical separation of camera networks and client network
- HTTPS – secure camera connectivity
- Encryption and password protection of video databases and exports
- Digital signing of video databases and exports
- Option for Windows AD user authentication via Microsoft NTLM or Kerberos authentication
- Strict and time-controlled user rights management, enforced server side
- Secure and encrypted (HTTPS) access for web and mobile client users
- Audit log provides full tractability of user actions
- Full authentication and authorization of third-party applications integrated via Milestone Integration Platform SDK (MIP SDK)

The solution dilemma

Designing a modern IP video surveillance solution is often a compromise between security on one hand, and flexibility and user friendliness, on the other. Milestone XProtect VMS software offers an array of security mechanisms described in this feature brief. Using these capabilities, it is possible to protect the system from both internal and external security threats, without compromising the system's flexibility or usability.

Security through network separation

Milestone's VMS architecture builds on a tiered system architecture, which makes it possible to separate the camera network and the core server/client network. With the recording server as a gateway between the camera and the system networks, there is no direct routing between the two network segments.



Network separation protects the system integrity

This means that a cyberattack potentially may reach the recording server on a particular network segment but will have difficulties penetrating beyond this point. Likewise, the recording server will prevent internal hacker attempts on the camera network.

HTTPS – secure camera connection

Milestone XProtect VMS products support HTTPS communication between the recording servers and the connected cameras and other security devices. HTTPS provides bidirectional encryption of communication and prevents eavesdropping and tampering with the contents of the communication.

Secure video storage

To protect recorded video, audio and metadata while stored in the recording servers and the associated storage, XProtect Corporate offers the ability to encrypt and password-protect the media data. This means that the recorded data is protected even if someone gains access to the database files

Cameras with support for HTTPS

Visit the Milestone website for information about which cameras support HTTPS:

Video encryption

The video database encryption is made in real-time as data is stored in the databases. The encryption is available in two levels:

- Light encryption
  Encrypts the data header information which prevents the media data from being decoded. The light encryption is recommended for minimizing the impact on CPU load
- Full encryption
  Encrypts all data and is stronger but slightly more CPU intensive

System hardening

Read more about how to protect surveillance installations based on Milestone XProtect VMS software against cybersecurity threats.

The guide outlines best practices for system design, operating system configuration, servers, workstations and the Milestone XProtect VMS software. It also contains input on cybersecurity policies, risk evaluation and mitigation.

on the storage system, a network share or in conjunction with an actual system hacker attack.

In addition to media data encryption, XProtect Corporate supports a digital signature on the recorded media data in the system. The signature can be used to prove that the video has not been altered or manipulated while stored in the system.

Strict server-side authentication and authorization

Milestone XProtect VMS products use consistent user authentication and authorization across all clients and integration interfaces that are enforced on the server side. This authentication and authorization process applies to both human users, and system services accessing the VMS system via the Milestone Integration Platform (MIP) SDK or Milestone ONVIF Bridge.

Building on user role definitions, it is possible to apply strict and granular user rights to specific roles (individual or groups of users) in terms of:

- Client interfaces the user may use
- Cameras and other security devices and device functions the user can access
- System functions the user has the right to use
- System configuration data the user can see/edit

The user rights can be defined to be both static and time conditioned. This, for example, makes it possible to block a user from accessing the system outside normal working hours, or limiting access rights to cameras and functions during certain time periods. The time-conditioned user rights also make it possible to block access to recordings older than a given time.

Certificate-based encryption

To secure the communication of data (video, audio, metadata) originated in the Recording Server and retrieved by connected components such as the Management, Mobile and Event servers as well as the Management, Mobile and Smart clients, XProtect uses SSL/TLS certificate-based encryption forced on both ends.

Builds on Windows security infrastructure

Milestone XProtect VMS products support Windows Active Directory (AD) based authentication, where both native Microsoft NTLM and Kerberos authentication may be used.

Audit logging

Milestone XProtect VMS products maintain an audit log, which makes it possible to perform detailed user activity monitoring. The audit log tracks all user accesses and activities, including changes to the system configuration. This enables system administrators to detect and investigate potential attempts to intercept the system.

Kerberos

Kerberos (RFC 3244) is a security authentication protocol that offers a more secure way to authenticate users than NTLM. Kerberos builds on symmetric key cryptography and requires a trusted third party. Milestone supports Kerberos authentication as a complement to Microsoft NTLM authentication.

Dual authentication

Dual authentication offers an additional level of system security for customers operating high-security installations. The dual authentication only grants a user access to the system when a second user (for example a supervisor) has confirmed the login with a successful authorization by the second user.

The dual authentication may optionally be applied to users accessing the VMS system via the XProtect Smart Client or the Management Client.

Secure remote user access

To facilitate remote system access via the XProtect Web Client and the Milestone Mobile application, the XProtect VMS products use a dedicated mobile server as a gateway to the system. Apart from being responsible for the connection management for web and mobile users, the mobile server plays an important role in protecting the integrity when used by remote users.
The communication between the mobile server and the two clients support HTTPS, which provides secure authentication and bidirectional encryption of all information exchanged, including user credentials, configuration and media data. This prevents eavesdropping and tampering of the communication.
To protect the VMS system from attacks via the Internet, Milestone recommends placing the mobile server in a demilitarized zone with two separate network connections.

Secure systems integration via MIP SDK

To address potential security threats imposed by third-party applications integrated via the MIP SDK, the XProtect VMS applies the same strict authentication, authorization and certification policies on integrated applications as on the client interfaces.

External video access using Milestone ONVIF Bridge

External systems and applications can access live and recorded video in Milestone XProtect VMS systems via an ONVIF-based RTSP interface using the Milestone ONVIF Bridge. As with internal VMS users, external systems using the Milestone ONVIF Bridge must run under a registered account. This makes it possible to apply the same strict authentication and authorization policies on integrated applications and users. Similar to the mobile server (see above), Milestone recommends placing the Milestone ONVIF Bridge in a DMZ with two separate network connections.

Protection of evidence material

The ultimate output of any video surveillance installation is the evidence material it can provide. When exporting forensic material using the XProtect Smart Client, the video material can be password protected, encrypted and digitally signed. These security measures can be applied in addition to signing recorded data in the recording server.

Encryption and password protection ensure that the forensic material can be viewed by the authorized receiver only, while the digital signature proves that the video has not been altered or manipulated while in transit.

Two-step verification

To protect the VMS system from attacks via the remote web and mobile interfaces, it is possible to apply a two-step verification process for users accessing the VMS system via the XProtect Web Client or the Milestone Mobile application. In addition to the normal username and password-based verification, with two-step verification the VMS system sends a random one-time code to the user via email or SMS. The user is only permitted access to the system if the correct one-time access code is provided.

Want to know more

Read more about the benefits of advanced management rights and the use of inherited device permissions in the Advanced Security Management white paper:

Feature availability

The security capabilities described in this brief are fully available in XProtect Corporate, and partially available in rest of the VMS products. For details please refer to the specification sheets of the individual products.

MAKE THE
WORLD SEE

Milestone Systems

XProtect® VMS

Hardening guide

milestone

Changes to this document

Version history

Document version	Release	Comments
Version 20	2022 R2	Added information on Disable IIS header information on the Identity Provider on page 74. Warning removed stating that the Mobile Server is not configurable when the Management Server is in a cluster from Use a "demilitarized zone" (DMZ) to provide external access on page 77.
Version 19	2022 R1	Added information about Encryption of communication with the Event Server on page 35.
Version 18	2021 R2	Added new section CIS Microsoft IIS 10 benchmark on page 118.
Version 17	2021 R1	Updated reference to *Microsoft Security Update Guide* to https://msrc.microsoft.com/update-guide. Added new section Configure the Content Security Policy (CSP) on page 82. Updated restrictions to Mobile Server in a DMZ in Use a "demilitarized zone" (DMZ) to provide external access on page 77.
Version 16	2020 R3	Updated new supported FIPS compliant drivers in Supported drivers on page 108.
Version 15	2020 R3	Added new sections FIPS 140-2 compliance on page 97 and Drivers and FIPS 140-2 on page 108. Added information on Disable the IIS Default Page on page 74. Updated information on Disable IIS HTTP TRACE / TRACK verbs on page 73. Port 25 for the recording server and failover recording server is deprecated. See Use firewalls to limit IP access to servers and computers on page 49.
Version 14	2020 R2	Added information to deny access to X-Frames in Manage IIS header information on page 72.

Document version	Release	Comments
Version 13	2020 R2	Added information about encryption between the management server and the data collector (see Encryption between the management server and the Data Collector server (explained) on page 32 Added information on Disable IIS HTTP TRACE / TRACK verbs on page 73.
Version 12	2020 R1	Microsoft Internet Explorer no longer supported. Microsoft Edge is supported. See Use only supported browsers with the latest security updates on page 94.
Version 11	2019 R3	Port 5432 is disabled by default. See Use firewalls to limit IP access to servers and computers on page 49. Added information on Manage IIS header information on page 72.
Version 10	2019 R2	Added section Secure communication (explained) on page 29 • Management server encryption (explained) on page 29 • Encryption from the management server to the recording server (explained) on page 31 • Mobile server data encryption (explained) on page 36 Added hardening information for the SQL Server and database connection in Connection to the SQL Server and database on page 69. Added hardening information for Recording Server in Harden Network Attached Storage (NAS) to store recorded media data on page 76.
Version 9	2019 R1	Added encryption from the recording server to all clients, described here: Encryption from the management server to the recording server (explained) on page 31
Version 8	2018 R3	Added design recommendations, described here: Privacy by design on page 21. Log Server uses port number 22337, described here: Use firewalls to limit IP access to servers and computers on page 49 and Limit the IP access to Log Server on page 83. Mobile server no longer uses port 8000 for communication with Tray Manager. This was removed from Use firewalls to limit IP access to servers and computers

Document version	Release	Comments
		on page 49. New recommendation for scanning for devices, described in Scanning for devices on page 48.
Version 7	2018 R2	No changes to this document
Version 6	2018 R1	Clarified the need to add specific firewall rules to the Management Server, described here: Use firewalls to limit IP access to servers and computers on page 49.
Version 5	2018 R1	No changes to this document
Version 4	2017 R3	No changes to this document
Version 3	2017 R2	This document applies to XProtect VMS versions 2017 R2 and before. These are the changes to the document: • Added Two-step verification for XProtect Mobile (see Set up users for two-step verification via email on page 78) • Storage and Recording Settings properties on page 74
Version 2	2016 R3	This document applies to XProtect VMS versions 2016 R3 and before. These are the changes to the document: • Added Changes to this document topic • Added Kerberos support (see Kerberos authentication (explained) on page 38) • Updated port numbers in Use firewalls to limit IP access to servers and computers on page 49
Version 1	2016 R2	This document applies to XProtect VMS versions 2016 R3 and before.

Contents

Changes to this document **2**
Version history 2
Copyright, trademarks, and disclaimer **11**
Introduction **12**
Introduction 12
What is "hardening?" 12
Target audience 12
Resources and references 13
Hardware and device components 14
Cyber threats and cyber risks 14
Cyber Risk Management Framework 15
Hardening system components 19
General setup **20**
Overview 20
Privacy by design 21
Servers, Workstations, Clients and Applications **25**
Servers, Workstations, Clients and Applications 25
Basic steps – Servers, Workstations, Clients and Applications 25
Establish surveillance and security objectives 26
Establish a formal security policy and response plan 26
Use Windows users with Active Directory 27
Secure communication (explained) 29
Management server encryption (explained) 29
Encryption from the management server to the recording server (explained) 31
Encryption between the management server and the Data Collector server (explained) 32
Encryption to clients and servers that retrieve data from the recording server (explained) 33
Encryption of communication with the Event Server 35
Mobile server data encryption (explained) 36

Mobile server encryption requirements for clients ... 37
Kerberos authentication (explained) ... 38
Use Windows update ... 39
Keep software and device firmware updated ... 40
Use antivirus on all servers and computers ... 40
Monitor logs in the VMS for signs of suspicious activity ... 41
Advanced steps – Servers, Workstations, Clients and Applications ... 43
Adopt standards for secure network and VMS implementations ... 43
Establish an incident response plan ... 43
Protect sensitive VMS components ... 44
Follow Microsoft OS Security best practices ... 45
Use tools to automate or implement the security policy ... 45
Follow established network security best practices ... 45
Devices and network ... 46
Devices and network ... 46
Basic steps – Devices ... 46
Use strong passwords instead of default passwords ... 46
Stop unused services and protocols ... 46
Create dedicated user accounts on each device ... 47
Scanning for devices ... 48
Basic steps – Network ... 48
Use secure and trusted networks connection ... 48
Use firewalls to limit IP access to servers and computers ... 49
Use a firewall between the VMS and the Internet ... 63
Connect the camera subnet to the recording server subnet only ... 64
Advanced steps – Devices ... 64
Use Simple Network Management Protocol to monitor events ... 64
Advanced steps – Network ... 65
Use secure wireless protocols ... 65
Use port-based access control ... 65

Run the VMS on a dedicated network 66

Milestone Servers **67**

Basic steps – Milestone servers 67

Use physical access controls and monitor the server room 67

Use encrypted communication channels 67

Advanced steps – Milestone servers 67

Run services with service accounts 68

Run components on dedicated virtual or physical servers 68

Restrict the use of removable media on computers and servers 68

Use individual administrator accounts for better auditing 68

Use subnets or VLANs to limit server access 69

Enable only the ports used by Event Server 69

SQL Server 69

Connection to the SQL Server and database 69

Run the SQL Server and database on a separate server 70

Management Server 70

Adjust the token time-out 71

Enable only the ports used by the management server 71

Disable non-secure protocols 71

Disable legacy remoting channel 72

Manage IIS header information 72

Disable IIS header information 72

Set X-Frame Options 73

Disable IIS HTTP TRACE / TRACK verbs 73

Disable the IIS Default Page 74

Identity Provider 74

Disable IIS header information on the Identity Provider 74

Recording Server 74

Storage and Recording Settings properties 74

Use separate network interface cards 76

Harden Network Attached Storage (NAS) to store recorded media data ... 76
XProtect Mobile Server ... 76
Only enable ports that Mobile Server uses ... 77
Use a "demilitarized zone" (DMZ) to provide external access ... 77
Disable non-secure protocols ... 77
Set up users for two-step verification via email ... 78
Requirements ... 78
Two-step verification tab ... 79
Configure the Content Security Policy (CSP) ... 82
Log Server ... 82
Install Log Server on a separate server with SQL Server ... 82
Limit the IP access to Log Server ... 83
Client programs ... 84
Client programs ... 84
Basic steps (all client programs) ... 84
Use Windows users with AD ... 84
Restrict permissions for client users ... 84
Always run clients on trusted hardware on trusted networks ... 86
Advanced steps – XProtect Smart Client ... 86
Restrict physical access to any computer running XProtect Smart Client ... 86
Always use a secure connection by default, particularly over public networks ... 87
Activate login authorization ... 87
Do not store passwords ... 90
Turn on only required client features ... 91
Use separate names for user accounts ... 91
Prohibit the use of removable media ... 92
Advanced steps – XProtect Mobile client ... 92
Always use the XProtect Mobile client on secure devices ... 92
Download the XProtect Mobile client from authorized sources ... 93
Mobile devices should be secured ... 93

Advanced steps – XProtect Web Client 93
Always run XProtect Web Client on trusted client computers 93
Use certificates to confirm the identity of XProtect Mobile server 94
Use only supported browsers with the latest security updates 94
Advanced steps – Management Client 95
Use Management Client profiles to limit what administrators can view 95
Allow administrators to access relevant parts of the VMS 95
Run the Management Client on trusted and secure networks 96
Compliance 97
FIPS 140-2 compliance 97
What is FIPS? 97
What is FIPS 140-2? 98
Which XProtect VMS applications can operate in a FIPS 140-2 compliant mode? 98
Is XProtect VMS always FIPS compliant? 98
Should you enable FIPS 140–2 mode? 98
How to ensure XProtect VMS can operate in FIPS 140-2 compliant mode? 98
Considerations regarding upgrade 99
Recommended upgrade process for customers running XProtect VMS 99
Verify third-party integrations 100
Connect devices: background 100
Device connectivity requirements 100
Effects of operating in FIPS 140-2 compliant mode 101
Devices running over Milestone Open Network Bridge 101
Media database: Considerations regarding backward compatibility 101
Media upgrade depending on XProtect VMS version 102
Media upgrade details 102
Media database data upgrade: XProtect VMS 2017 R1 and earlier 105
Media database upgrade: XProtect VMS 2017 R2 to XProtect VMS 2019 R3 105
What is the media conversion tool? 105
Media conversion tool workflow 106

Media database upgrade: XProtect VMS 2020 R1 or XProtect VMS 2020 R2 ... 106
FIPS Group Policy on the Windows operating system ... 106
FIPS Group Policy and Milestone Federated Architecture ... 107
Install XProtect VMS ... 107
Encrypt hardware detection passwords ... 107
Drivers and FIPS 140-2 ... 108
Requirements for FIPS 140-2 compliant mode ... 108
Device requirements ... 108
Supported drivers ... 108
Effects of running in FIPS 140-2 compliant mode ... 109
How to configure the device and the driver for FIPS 140-2 ... 109
Axis drivers ... 110
Canon drivers ... 111
Bosch drivers ... 111
Hanwha drivers ... 112
ONVIF drivers ... 112
Universal drivers ... 113
VideoPush driver ... 114
Example of FIPS 140-2 compliant cipher suites ... 114
FIPS resources ... 116
Center for Internet Security (CIS) Benchmarks ... 118
CIS Microsoft IIS 10 benchmark ... 118
Controls that do not impact XProtect VMS functionality ... 118
Controls that impact XProtect VMS functionality ... 118
Product comparision chart ... 120
Product comparison ... 120
Appendix ... 121
Appendix 1 - Resources ... 121
Appendix 2 - Acronyms ... 122

Copyright, trademarks, and disclaimer

Copyright © 2022 Milestone Systems A/S

Trademarks

XProtect is a registered trademark of Milestone Systems A/S.

Microsoft and Windows are registered trademarks of Microsoft Corporation. App Store is a service mark of Apple Inc. Android is a trademark of Google Inc.

All other trademarks mentioned in this document are trademarks of their respective owners.

Disclaimer

This text is intended for general information purposes only, and due care has been taken in its preparation.

Any risk arising from the use of this information rests with the recipient, and nothing herein should be construed as constituting any kind of warranty.

Milestone Systems A/S reserves the right to make adjustments without prior notification.

All names of people and organizations used in the examples in this text are fictitious. Any resemblance to any actual organization or person, living or dead, is purely coincidental and unintended.

This product may make use of third-party software for which specific terms and conditions may apply. When that is the case, you can find more information in the file 3rd_party_software_terms_and_conditions.txt located in your Milestone system installation folder.

Introduction

Introduction

This guide describes security and physical security measures and best practices that can help secure your XProtect video management software (VMS) against cyber-attacks. This includes security considerations for the hardware and software of servers, clients and network device components of a video surveillance system.

This guide adopts standard security and privacy controls and maps them to each of the recommendations. That makes this guide a resource for compliance across industry and government security, and network security requirements.

What is "hardening?"

Developing and implementing security measures and best practices is known as "hardening." Hardening is a continuous process of identifying and understanding security risks, and taking appropriate steps to counter them. The process is dynamic because threats, and the systems they target, are continuously evolving.

Most of the information in this guide focuses on IT settings and techniques, but it's important to remember that physical security is also a vital part of hardening. For example, use physical barriers to servers and client computers, and make sure that things like camera enclosures, locks, tamper alarms, and access controls are secure.

The following are the actionable steps for hardening a VMS:

1. Understand the components to protect
2. Harden the surveillance system components:
    1. Harden the servers (physical and virtual) and client computers and devices
    2. Harden the network
    3. Harden the cameras
3. Document and maintain security settings on each system
4. Train and invest in people and skills, including your supply chain

Target audience

Everyone in an organization must understand at least the basics about network and software security. Attempts to compromise critical IT infrastructure are becoming more frequent, so everyone must take hardening and security seriously.

This guide provides basic and advanced information for end users, system integrators, consultants, and component manufacturers.

- Basic descriptions give general insight into security
- Advanced descriptions give IT-specific guidance for hardening XProtect VMS products. In addition to software, it also describes security considerations for the hardware and device components of the system.

Resources and references

The following organizations provide resources and information about best practices for security:

- International Standards Organization (ISO),
- United States (US) National Institute of Standards and Technology (NIST)
- Security Technical Implementation Guidelines (STIGs) from the US Defense Information Systems Administration (DISA)
- Center for Internet Security
- SANS Institute
- Cloud Security Alliance (CSA)
- Internet Engineering Task Force (IETF)
- British Standards

Additionally, camera manufacturers provide guidance for their hardware devices.



See Appendix 1 - Resources on page 121 for a list of references and Appendix 2 - Acronyms on page 122 for a list of acronyms.

This guide leverages country, international, and industry standards and specifications. In particular, it refers to the United States Department of Commerce National Institute of Standards and Technology Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations (http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf).



The NIST document is written for the US Federal government; however, it is generally accepted in the security industry as the current set of best practices.

This guide refers and links to additional information about security controls. The guidance can be cross-referenced to industry-specific requirements and other international security and risk management standard and frameworks. For example, the current NIST Cybersecurity Framework uses SP 800-53 Rev4 as a basis for the controls and guidance. Another example is Appendix H in SP 800-53 Rev 4, which contains a reference to ISO/IEC 15408 requirements, such as Common Criteria.

Hardware and device components

In addition to software, the components of an XProtect VMS installation typically include hardware devices, such as:

- Cameras
- Encoders
- Networking products
- Storage systems
- Servers and client computers (physical or virtual machines)
- Mobile devices, such as smartphones

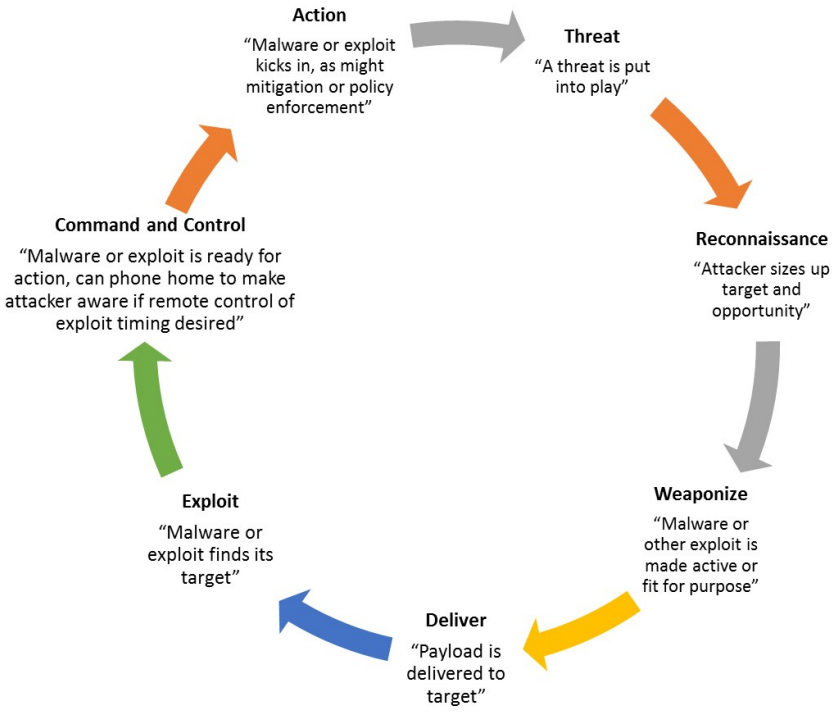
It is important to include hardware devices in your efforts to harden your XProtect VMS installation. For example, cameras often have default passwords. Some manufacturers publish these passwords online so that they're easy for customers to find. Unfortunately, that means the passwords are also available to attackers.

This document provides recommendations for hardware devices.

Cyber threats and cyber risks

There are many sources of threats to a VMS, including business, technology, process and human attacks or failures. Threats take place over a lifecycle. The threat lifecycle, sometimes called the "cyber kill" or "cyber threat chain," was developed to describe the stages of advanced cyber threats.

Each stage in the threat lifecycle takes time. The amount of time for each stage is particular to the threat, or combination of threats, and its actors and targets.



The threat lifecycle is important for risk assessment because it shows where you can mitigate threats. The goal is to reduce the number of vulnerabilities, and to address them as early as possible. For example, discouraging an attacker who is probing a system for vulnerabilities can eliminate a threat.

Hardening puts in place actions that mitigate threats for each phase in the threat lifecycle. For example, during the reconnaissance phase an attacker scans to find open ports and determine the status of services that are related to the network and the VMS. To mitigate this, hardening guidance is to close unnecessary system ports in XProtect VMS and Windows configurations.

The risk and threat assessment process includes the following steps:

- Identify information and security risks
- Assess and prioritize risks
- Implement policy, procedures, and technical solutions to mitigate these risks

The overall process of risk and threat assessment, and the implementation of security controls, is referred to as a risk management framework. This document refers to NIST security and privacy controls and other publications about risk management frameworks.

Cyber Risk Management Framework

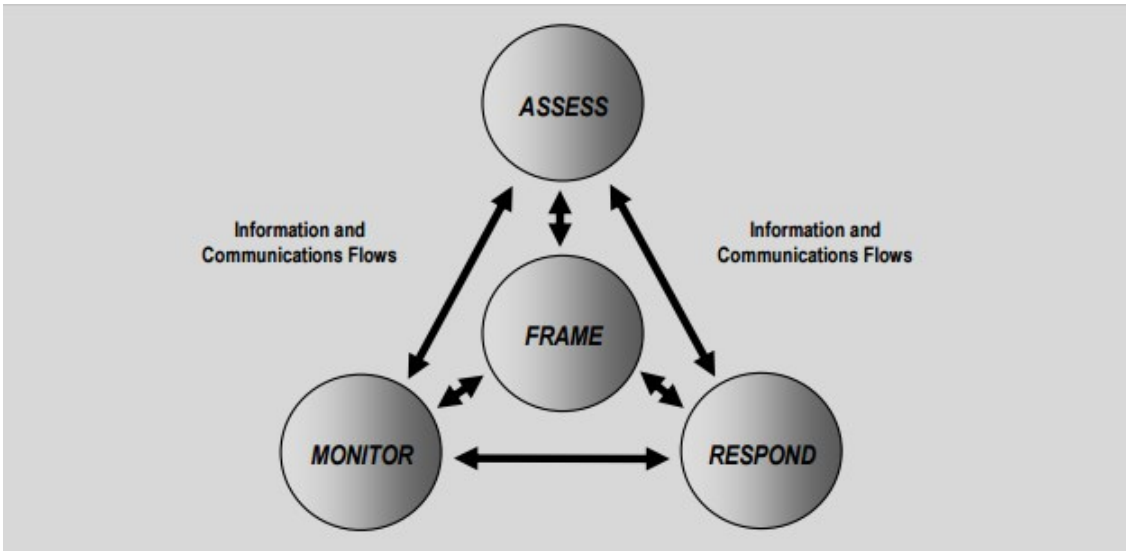
The security and privacy controls in SP 800-53 Revision 4 (http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf) are part of an overall risk management framework from NIST. The NIST document SP800-39

(http://csrc.nist.gov/publications/nistpubs/800-39/sp800-39-final.pdf) is a guide to applying a risk management framework. SP800-36 is a foundational document for the NIST Cybersecurity Framework, which is described in Cybersecurity Framework (http://www.nist.gov/cyberframework/).

The figures here show:

- An overview of the risk management process. It shows a high-level, overall approach.
- Risk management at a business level, taking strategic and tactical considerations into account.
- The lifecycle of a risk management framework, and the NIST documents that provides details for each of the steps in the lifecycle.

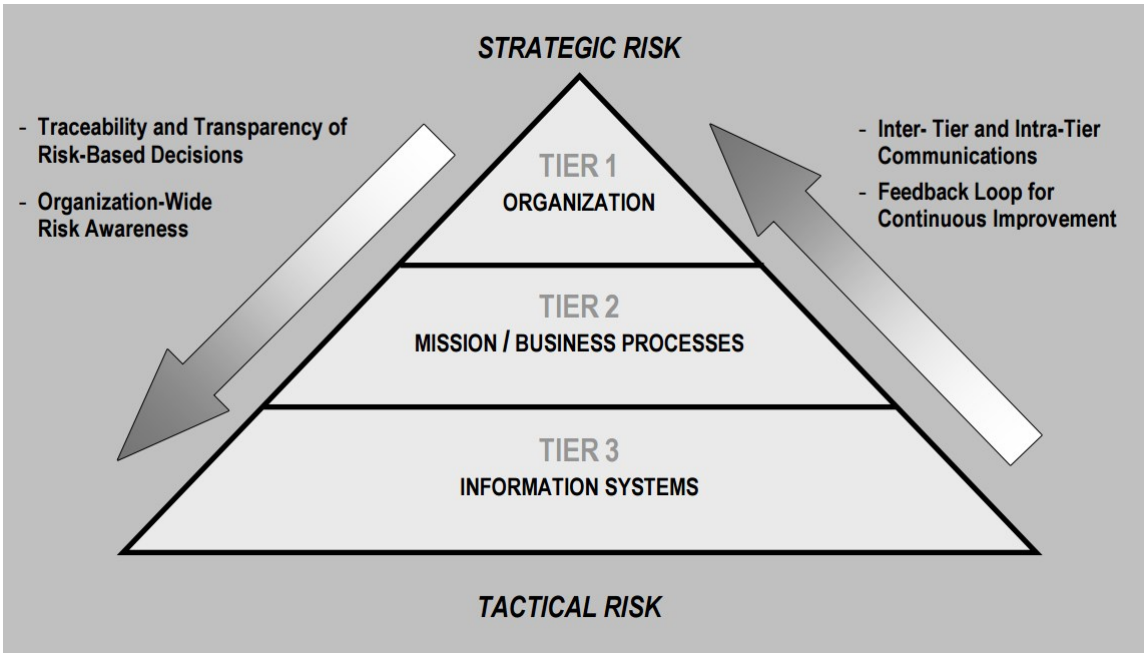
Security and privacy controls represent specific actions and recommendations to implement as part of a risk management process. It's important that the process includes the assessment of the organization, the particular requirements of a given deployment, and the aggregation of these activities into a security plan. SP 800-18 Revision 1 (http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf) provides references for detailed security plans.



High-level view of risk management (SP 800-39, page 8 (http://csrc.nist.gov/publications/nistpubs/800-39/sp800-39-final.pdf))

The process is interactive, and responses and their outcomes are iterative. Security threats, risks, responses and results are dynamic and adapt, and as a result so must a security plan.

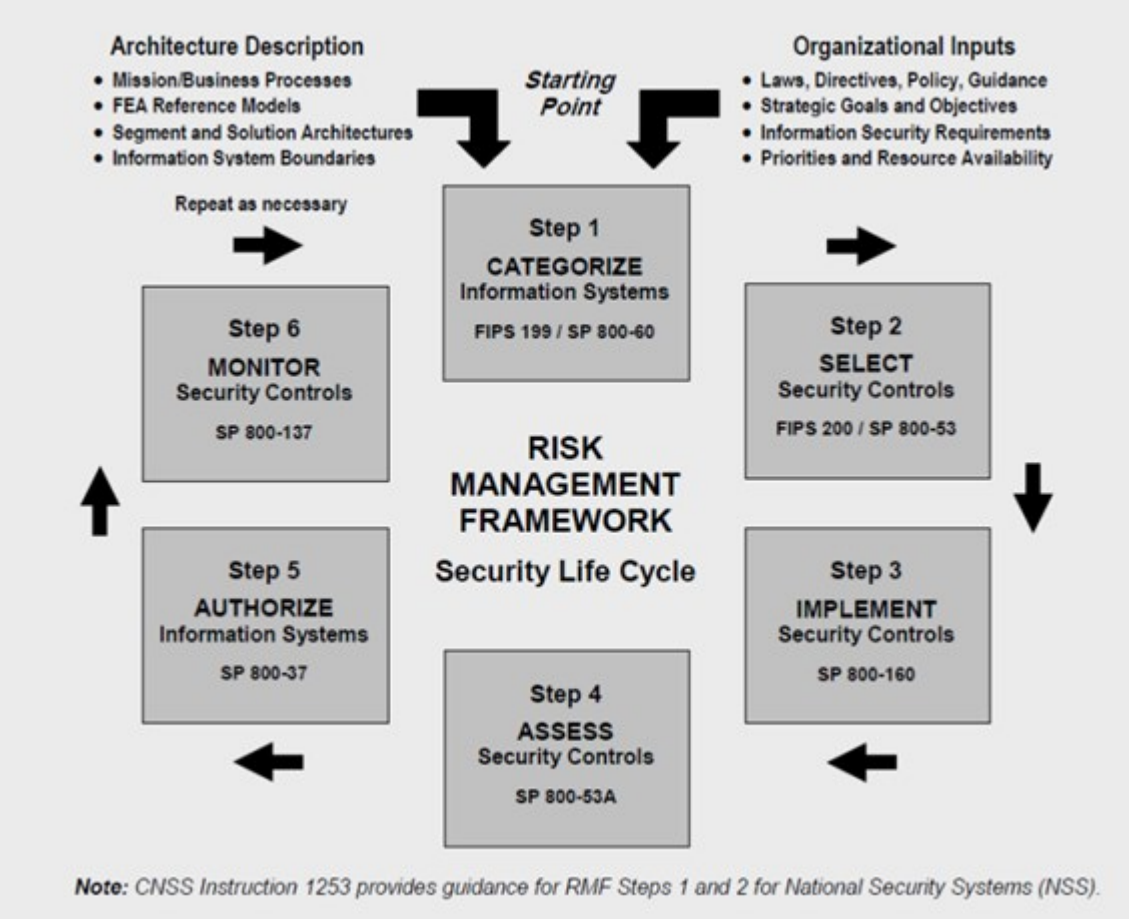
This diagram shows how a risk management framework considers IT systems, business processes, and the organization as a whole to find a balance for the security plan.



Balancing security and business goals (SP 800-39, page 9 (http://csrc.nist.gov/publications/nistpubs/800-39/sp800-39-final.pdf))

When hardening a system, you balance the impact on business productivity and usability for the sake of security, and vice versa, in the context of the services you deliver. Security guidance is not isolated from other business and IT activities.

For example, when a user enters their password incorrectly on three consecutive attempts, the password is blocked and they cannot access the system. The system is secure from brute-force attacks, but the unlucky user cannot use the device to do their work. A strong password policy that requires 30 character passwords, and changing passwords every 30 days is a best practice, but it's also difficult to use.



Example of a risk management framework (SP 800-53 Rev 4, page 8 (http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf))

To document its risk management framework, NIST produced multiple special publications. It includes the following components:

1. Categorization (identification of risk level)
2. Selection of security and privacy controls
3. Implementation
4. Assessment of the effectiveness of security controls
5. Creating an improved system security profile, and what's called an Authority to Operate (ATO)
6. Monitoring and evaluating through iterations

The risk management framework helps put a security plan and guidance in a security context.

Hardening system components

To harden system components, you change configurations to reduce the risk of a successful attack. Attackers look for a way in, and look for vulnerabilities in exposed parts of the system. Surveillance systems can involve 100s or even 1000s of components. Failure to secure any one component can compromise the system.

The need to maintain configuration information is sometimes overlooked. XProtect VMS provides features for managing configurations, but organizations must have a policy and process in place, and commit to doing the work.

Hardening requires that you keep your knowledge about security up-to-date:

- Be aware of issues that affect software and hardware, including operating systems, mobile devices, cameras, storage devices, and network devices. Establish a point-of-contact for all of the components in the system. Ideally, use reporting procedures to track bugs and vulnerabilities for all components.
- Keep current on Common Vulnerabilities and Exposures (CVEs) (described in Common Vulnerabilities and Exposures (https://cve.mitre.org/)) for all system components. These can relate to the operating systems, devices that have hard-coded maintenance passwords, and so on. Address vulnerabilities for each component, and alert manufacturers to vulnerabilities.
- Review Milestone Knowledge Base (KB) articles, and regularly review logs for signs of suspicious activity. For more information, see the *Milestone Knowledge Base* (https://force.milestonesys.com/support/MccKnowledgeBase).
- Maintain up-to-date configuration and system documentation for the system. Use change-control procedures for the work you perform, and follow best practices for configuration management, as described in SP 800-128 (http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf).

The following sections provide basic and advanced hardening and security recommendations for each system component. The sections also contain examples of how these relate to specific security controls described in the NIST Special Publication 800-53 Revision 4, titled *Security and Privacy Controls for Federal Information Systems and Organizations*.

In addition to the NIST document, the following sources are referenced:

- Center for Internet Security
- SP 800-53
- ISO 27001
- ISO/IEC 15408 (also known as Common Criteria, ISO/IEC 15408-1:2009 (http://www.iso.org/iso/catalogue_detail.htm?csnumber=50341)) .

Appendix 1 - Resources on page 121 in this document provides recommendations from camera manufacturers. This is a relatively new effort from manufacturers, so limited resources are available. For the most part, the recommendations can be generalized across camera manufacturers.

General setup

Overview

To help secure your surveillance system, Milestone recommends the following:

- Restrict access to servers. Keep servers in locked rooms, and make it difficult for intruders to access network and power cables.

  (PE2 and PE3 in Appendices D and F in NIST SP 800-53 Rev4 (http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf) (PE Physical and Environment Protection).)

- Design a network infrastructure that uses physical network or VLAN segmentation as much as possible.

  (SC3 in Appendices D and F in NIST SP 800-53 Rev4 (http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf) (SC System and Communication Protection).)

  - Separate the camera network from the server network by having two network interfaces in each recording server: one for the camera network, and one for the server network.
  - Put the mobile server in a "demilitarized zone" (DMZ) with one network interface for public access, and one for private communication to other servers.

    (SC7 in Appendices D and F NIST SP 800-53 Rev4 (http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf).)

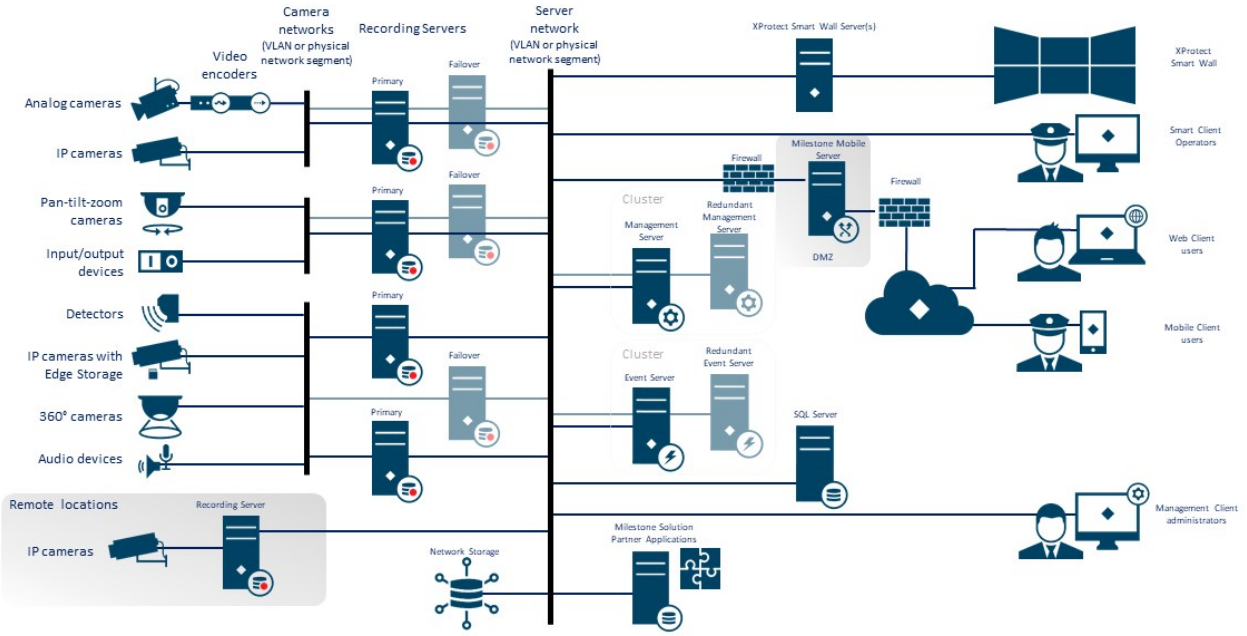
  - Many precautions can be taken when it comes to general set up. In addition to firewalls, these include techniques to segment the network and control access to the servers, clients and applications.

    (AC3, AC4, AC6, CA3, CM3, CM6, CM7, IR4, SA9, SC7, SC28, SI3, SI 8 in Appendices D and F in NIST SP 800-53 Rev4 (http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf) (AC Access Controls), (CM Configuration Management) (IR Incident Response) (SA System and Service Acquisition) (SI Systems and Information Integrity).)

- Configure the VMS with roles that control access to the system, and designate tasks and responsibilities.

  (AC2, AC3, AC6, AC16, AC25, AU6, AU9, CM5, CM11, IA5, PL8, PS5, PS7, SC2, SI7, in Appendices D and F in NIST SP 800-53 Rev4 (http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf) (AU Audit and Accountability) (IA Identification and Authentication) (PL Planning).)

The figure shows an example of a general setup.



Privacy by design

Milestone products are designed to deliver secure, end-to-end communication. Milestone products are designed to protect privacy and to secure data. Data protection is always important, but especially if you intend to be General Data Protection Regulation (GDPR) compliant in the EU.

According to GDPR, the controller of personal data, when processing such data, has an obligation to implement technical or organizational measures which are designed to implement the data protection principles set out in GDPR. GDPR refers to this as privacy by design.

In the context of a surveillance camera, a relevant example of privacy by design would be a feature that digitally allows the user to restrict image capture to a certain perimeter, preventing the camera from capturing any imagery outside this perimeter that would otherwise be captured.

In XProtect, there is support for privacy masking in two forms – permanent masks that cannot be removed, and liftable masks that (with the appropriate permissions) can be lifted to reveal the image behind the mask.

The controller also has an obligation to implement technical or organizational measures which by default ensure the least privacy intrusive processing of the personal data in question. GDPR refers to this as privacy by default. In the context of a camera, a relevant example of privacy by default could be using privacy masking to keep a sensitive area within the view of the camera private.

What should you do to ensure privacy by design?

- Consider the resolution of different points in the camera scene and document these settings

  Different purposes require different image qualities. When identification is not necessary, the camera resolution and other modifiable factors should be chosen to ensure that no recognizable facial images are captured.

- Encrypt your recordings

  Milestone recommends that you secure your recordings by enabling at least Light encryption on your recording servers' storage and archives. Milestone uses the AES-256 algorithm for encryption. When you select Light encryption, only a part of the recording is encrypted. When you select Strong encryption, the entire recording is encrypted.

- Secure the network

  Milestone recommends that you select cameras that support HTTPS. It is recommended that you set the cameras on separate VLANs and use HTTPS for your camera to recording server communication.

  It is recommended that XProtect Smart Clients and XProtect Smart Walls are on the same VLAN as the servers.

  Use a VPN encrypted network or similar if using Smart Client or Smart Wall from a remote location.

- Enable and document the intended retention time

  According to Article 4(1)(e) of the GDPR, recordings must not be retained longer than necessary for the specific purposes for which they were made. Milestone recommends that you set the retention time according to regional laws and requirements, and in any case, to set the retention time to a maximum of 30 days.

- Secure exports

  Milestone recommends that you only allow access to export functionality for a select set of users that need this permission.

  Milestone also recommends that the Smart Client profile is changed to only allow export in XProtect Format with encryption enabled. AVI and JPEG exports should not be allowed, because they can not be made secure. This makes export of any evidence material password protected, encrypted and digitally signed, making sure forensic material is genuine, untampered with and viewed by the authorized receiver only.

- Enable privacy masking – permanent or liftable

  Use privacy masking to help eliminate surveillance of areas irrelevant to your surveillance target.

  Milestone recommends that you set a liftable blurring mask for sensitive areas and in places where person identification is not allowed. Create then a second role that can authorize the mask to be lifted.

- Restrict access permissions with roles

  Apply the principle of least privilege (PoLP).

  Milestone recommends that you only allow access to functionality for a select set of users that need this permission. By default, only the system administrator can access the system and perform tasks. All new roles and users that are created have no access to any functions until they are deliberately configured by an administrator.

  Set up permissions for all functionality, including: viewing live video and recordings, listening to audio, accessing metadata, controlling PTZ cameras, accessing and configuring Smart Wall, lifting privacy masks, working with exports, saving snapshots, and so on.

  Grant access to only the cameras that the specific operator needs to access, and restrict access to recorded video, audio, and metadata for operators, either completely, or grant access to only the video, audio, or metadata recorded in the past few hours or less.

  Regularly assess and review roles and responsibilities for operators, investigators, system administrators and others with access to the system. Does the principle of least privilege still apply?

- Enable and use two-step verification

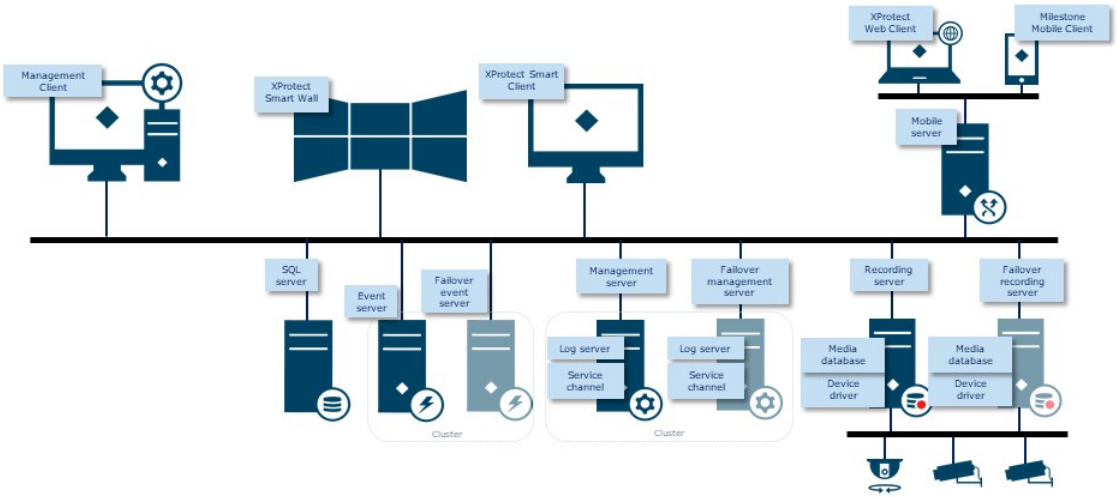
  Milestone recommends that you specify an additional login step for users of XProtect Mobile or XProtect Web Client by enabling two-step verification.

- Restrict administrator permissions

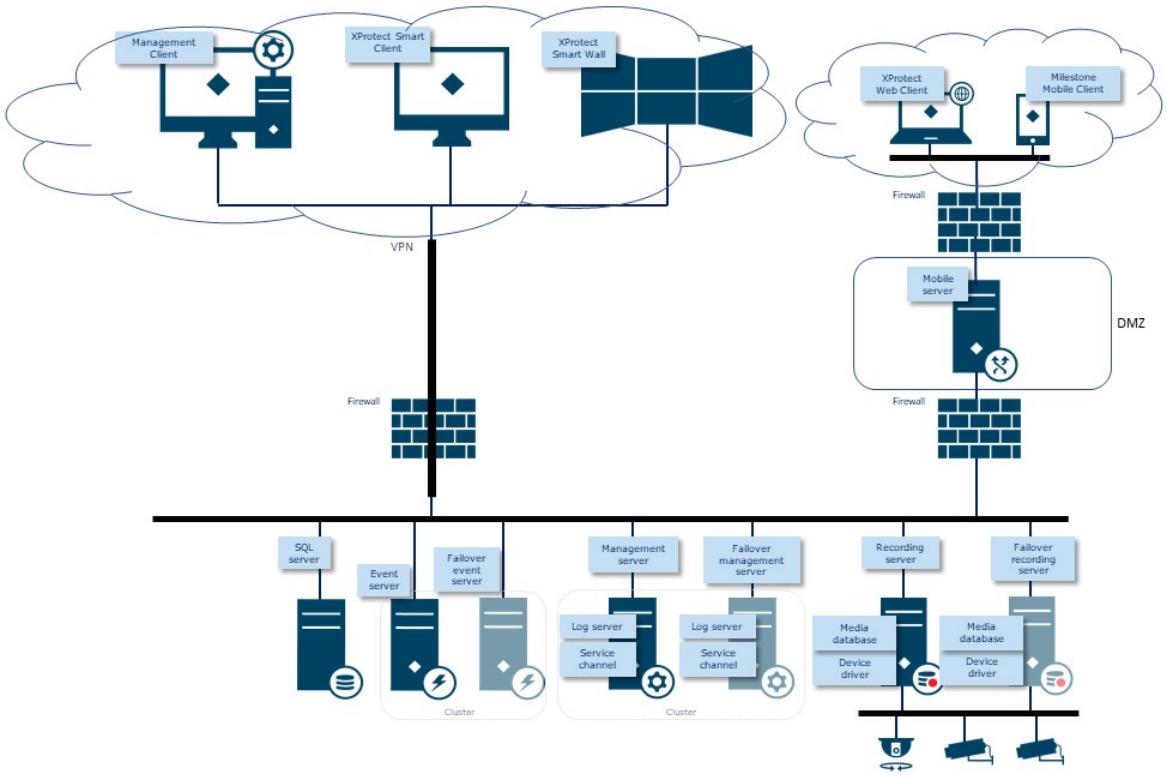
  Milestone recommends that you limit the number of users that have an Administrator role. If you need to create multiple Administrator roles, you can restrict their access by creating Administrator roles that can manage only select parts of the system, such as certain devices or functions.

  Milestone also recommends that the VMS administrator does not have full administrator permissions on the storage that contains recorded video, and the storage administrator should not have access to the VMS or backup administration.

For security, segment the network so there is a client/management network, and camera networks behind the recording servers:



For greater security, put the mobile server in a "demilitarized zone" (DMZ) with one network interface for public access, and one for private communication to other servers, and use VPN encrypted networks for external connections or to increase security for less secure internal networks:



Servers, Workstations, Clients and Applications

Servers, Workstations, Clients and Applications

This section provides hardening guidance based on Microsoft Windows and the services that XProtect VMS uses. This includes:

- The XProtect VMS product, for example XProtect® Corporate or XProtect® Enterprise running on Windows Servers
- The device pack installed on the recording servers
- The server hardware or virtual platforms, and operating systems and services
- The client computers for XProtect® Smart Client and XProtect® Web Client
- Mobile devices and their operating systems and applications

Basic steps – Servers, Workstations, Clients and Applications

Establish surveillance and security objectives **26**

Establish a formal security policy and response plan **26**

Use Windows users with Active Directory **27**

Secure communication (explained) **29**

Management server encryption (explained) **29**

Encryption from the management server to the recording server (explained) **31**

Encryption between the management server and the Data Collector server (explained) **32**

Encryption to clients and servers that retrieve data from the recording server (explained) **33**

Encryption of communication with the Event Server **35**

Mobile server data encryption (explained) **36**

Kerberos authentication (explained) **38**

Use Windows update **39**

Keep software and device firmware updated **40**

Use antivirus on all servers and computers **40**

Monitor logs in the VMS for signs of suspicious activity **41**

Establish surveillance and security objectives

Before implementing the VMS, Milestone recommends that you establish surveillance objectives. Define goals and expectations related to capturing and using video data and related metadata. All stakeholders should understand the surveillance objectives.



Specifics of surveillance objectives can be found in other documents, for example BS EN 62676-1-1: *Video surveillance systems for use in security applications.System requirements. General*.

When surveillance objectives are in place, you can establish the security objectives. Security objectives support the surveillance objectives by addressing what to protect in the VMS. A shared understanding of security objectives makes it easier to secure the VMS and maintain data integrity.

With the surveillance and security objectives in place, you can more easily address the operational aspects of securing the VMS, such as how to:

- Prevent data from being compromised
- Respond to threats and incidents when they occur, including roles and responsibilities.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 PL-2 *System Security Plan*
- NIST SP 800-53 SA-4 *Acquisition Process*

Establish a formal security policy and response plan

In compliance with NIST SP 800-100 Information Security Handbook: A Guide for Managers (http://csrc.nist.gov/publications/nistpubs/800-100/sp800-100-mar07-2007.pdf), Milestone recommends that you establish a formal security policy and a response plan that describe how your organization addresses security issues, in terms of practical procedures and guidelines. For example, a security policy can include:

- A password policy defined by the internal IT department
- Access control with ID badges
- Restrictions for smartphones from connecting to the network

Adopt existing IT policies and plans if they adhere to security best practices.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 IR-1 *Incident Response Policy and Procedures*
- NIST SP 800-53 PM-1 *Information Security Program Plan*

Use Windows users with Active Directory

There are two types of users in XProtect VMS:

- Basic user: a dedicated VMS user account authenticated by a combination of username and password using a password policy. Basic users connect to the VMS using a secure socket layer (SSL) with current Transport Layer (TLS) security protocol session (https://datatracker.ietf.org/wg/tls/charter/) for login, encrypting the traffic contents and username and password.
- Windows user: the user account is specific to a machine or a domain, and it is authenticated based on the Windows login. Windows users connecting to the VMS can use Microsoft Windows Challenge/Response (NTML) for login, Kerberos (see Kerberos authentication (explained) on page 38), or other SSP options from Microsoft (https://msdn.microsoft.com/en-us/library/windows/desktop/aa380502(v=vs.85).aspx).

Milestone recommends that, whenever possible, you use Windows users in combination with Active Directory (AD) to authorize access to the VMS. This allows you to enforce:

- A password policy that requires users to change their password regularly
- Brute force protection, so that the Windows AD account is blocked after a number of failed authentication attempts, again in line with the organization password policy
- Multi-factor authentication in the VMS, particularly for administrators
- Role-based permissions, so you can apply access controls across your domain

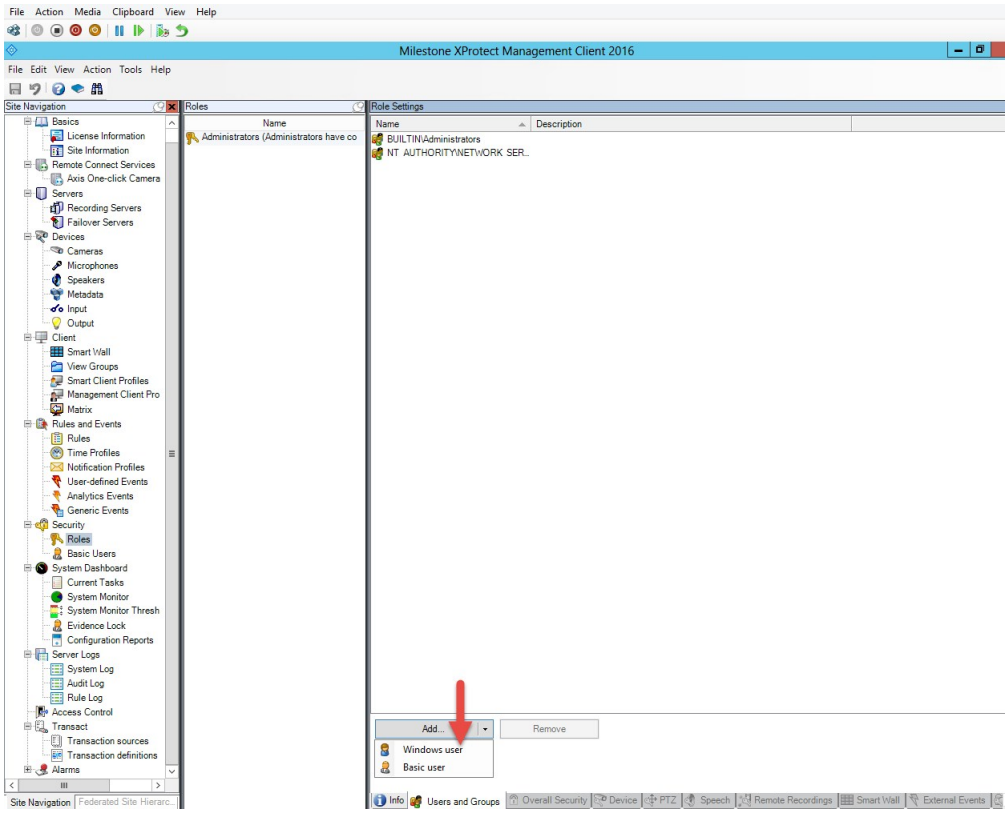
If your organization does not use AD, you can add Windows users to workgroups on the management server instead. Workgroups give you some of the same advantages as Windows users with AD. You can enforce a password policy, which helps protect against brute force attacks, but Milestone recommends that you use a Windows Domain because this gives you central control over user accounts.

Windows users have the advantage of being authenticated via the directory as a single authoritative source and enterprise service for the network and not ad hoc for their local machine. This lets you use role based access controls to assign permissions to users and groups consistently across the domain and the computers on the network.

If you use local Windows users, the user must create a local user name and password on each machine, which is problematic from security and usability perspectives.

To add Windows users or groups to roles in Management Client, follow these steps:

1. Open Management Client.
2. Expand the **Security** node.



3. Select the role to which you want to add the Windows users.
4. On the **Users** and **Groups** tab, click **Add**, and select **Windows user**. A pop-up window appears.
5. If the domain name does not appear in the **From this location** field, click **Locations**.
6. Specify the Windows user, and then click **OK**.

To verify that the Windows user is an AD user, the domain name must appear as a prefix, for example "Domain\John".

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 CM-6 *Configuration Settings*
- NIST SP 800-53 SA-5 *Information System Documentation*
- NIST SP 800-53 SA-13 *Trustworthiness*

Secure communication (explained)

Hypertext Transfer Protocol Secure (HTTPS) is an extension of the Hypertext Transfer Protocol (HTTP) for secure communication over a computer network. In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS), or its predecessor, Secure Sockets Layer (SSL).

In XProtect VMS, secure communication is obtained by using TLS/SSL with asymmetric encryption (RSA).

TLS/SSL uses a pair of keys—one private, one public—to authenticate, secure, and manage secure connections.

A certificate authority (CA) is anyone who can issue root certificates. This can be an internet service that issues root certificates, or anyone who manually generates and distributes a certificate. A CA can issue certificates to web services, that is to any software using https communication. This certificate contains two keys, a private key and a public key. The public key is installed on the clients of a web service (service clients) by installing a public certificate. The private key is used for signing server certificates that must be installed on the server. Whenever a service client calls the web service, the web service sends the server certificate, including the public key, to the client. The service client can validate the server certificate using the already installed public CA certificate. The client and the server can now use the public and private server certificates to exchange a secret key and thereby establish a secure TLS/SSL connection.

For manually distributed certificates, certificates must be installed before the client can make such a verification.

For more information about TLS: https://en.wikipedia.org/wiki/Transport_Layer_Security



Certificates have an expiry date. XProtect VMS will not warn you when a certificate is about to expire. If a certificate expires:
• The clients will no longer trust the recording server with the expired certificate and thus cannot communicate with it
• The recording servers will no longer trust the management server with the expired certificate and thus cannot communicate with it
• The mobile devices will no longer trust the mobile server with the expired certificate and thus cannot communicate with it

To renew the certificates, follow the steps in this guide as you did when you created certificates.

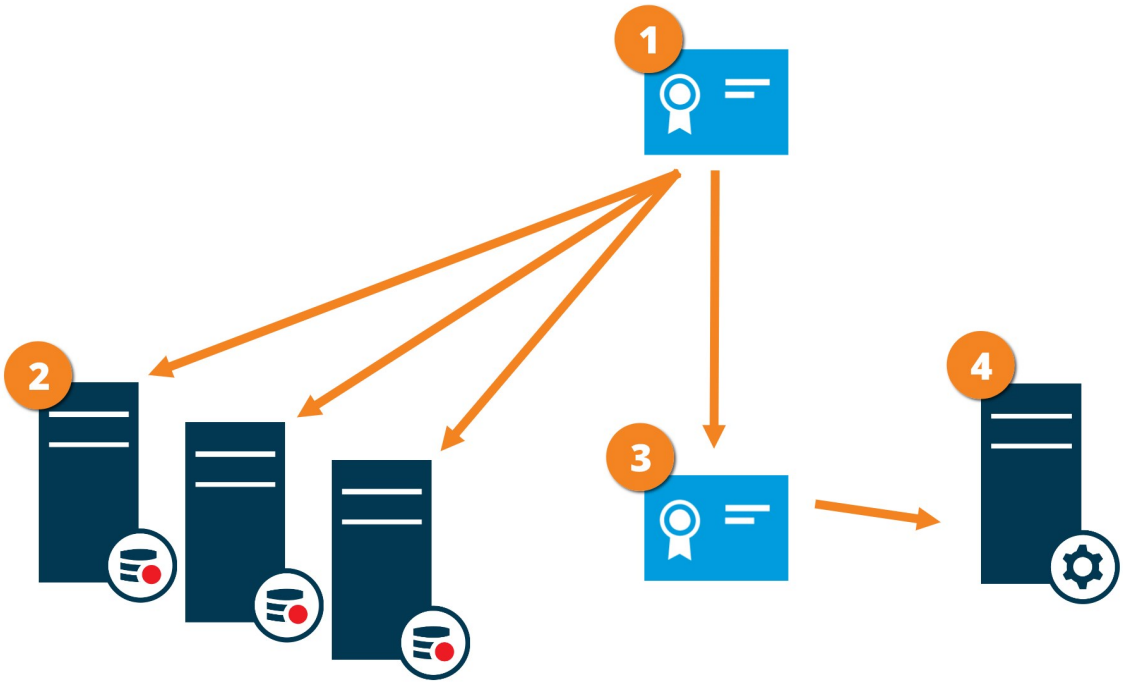
For more information, see the certificates guide about how to secure your XProtect VMS installations.

Management server encryption (explained)

You can encrypt the two-way connection between the management server and the recording server. When you enable encryption on the management server, it applies to connections from all the recording servers that connect to the management server. If you enable encryption on the management server, you must also enable encryption on all of the recording servers. Before you enable encryption, you must install security certificates on the management server and all recording servers.

Certificate distribution for management servers

The graphic illustrates the basic concept of how certificates are signed, trusted, and distributed in XProtect VMS to secure the communication to the management server.



❶ A CA certificate acts as a trusted third party, trusted by both the subject/owner (management server) and by the party that verifies the certificate (recording servers)

❷ The CA certificate must be trusted on all recording servers. In this way, the recording servers can verify the validity of the certificates issued by the CA

❸ The CA certificate is used to establish a secure connection between the management server and the recording servers

❹ The CA certificate must be installed on the computer on which the management server is running

Requirements for the private management server certificate:

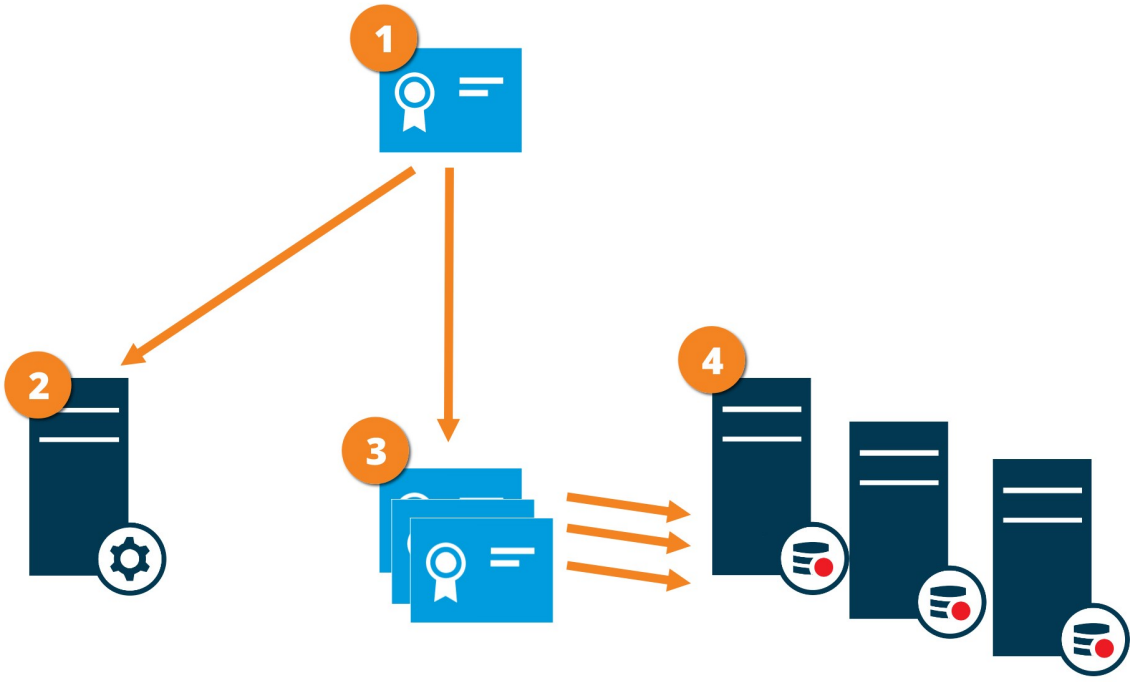
- Issued to the management server so that the management server's host name is included in the certificate, either as subject (owner) or in the list of DNS names that the certificate is issued to
- Trusted on the management server itself, by trusting the CA certificate that was used to issue the management server certificate
- Trusted on all recording servers connected to the management server by trusting the CA certificate that was used to issue the management server certificate

Encryption from the management server to the recording server (explained)

You can encrypt the two-way connection between the management server and the recording server. When you enable encryption on the management server, it applies to connections from all the recording servers that connect to the management server. Encryption of this communication must follow the encryption setting on the management server. So, if management server encryption is enabled, this must also be enabled on the recording servers and vice-versa. Before you enable encryption, you must install security certificates on the management server and all recording servers, including failover recording servers.

Certificate distribution

The graphic illustrates the basic concept of how certificates are signed, trusted, and distributed in XProtect VMS to secure the communication from the management server.



❶ A CA certificate acts as a trusted third party, trusted by both the subject/owner (recording server) and by the party that verifies the certificate (management server)

❷ The CA certificate must be trusted on the management server. In this way, the management server can verify the validity of the certificates issued by the CA

❸ The CA certificate is used to establish a secure connection between the recording servers and the management server

❹ The CA certificate must be installed on the computers on which the recording servers are running

Requirements for the private recording server certificate:

- Issued to the recording server so that the recording server's host name is included in the certificate, either as subject (owner) or in the list of DNS names that the certificate is issued to
- Trusted on the management server by trusting the CA certificate that was used to issue the recording server certificate

Encryption between the management server and the Data Collector server (explained)

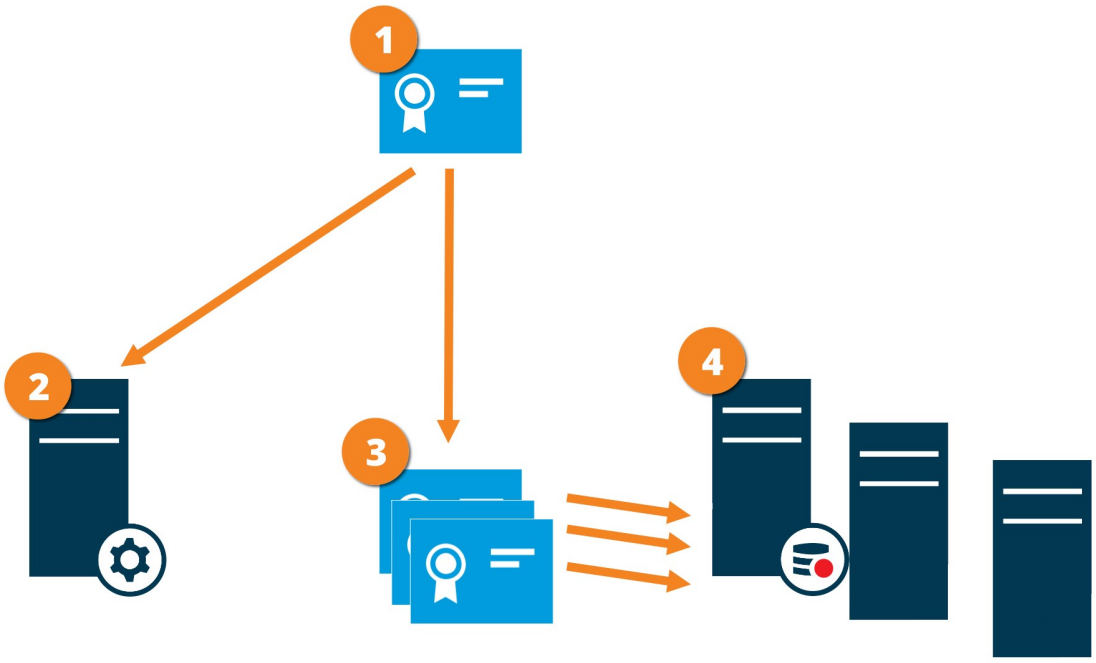
You can encrypt the two-way connection between the management server and the Data Collector affiliated when you have a remote server of the following type:

- Recording Server
- Event Server
- Log Server
- LPR Server
- Mobile Server

When you enable encryption on the management server, it applies to connections from all the Data Collector servers that connect to the management server. Encryption of this communication must follow the encryption setting on the management server. So, if management server encryption is enabled, this must also be enabled on the Data Collector servers affiliated with each remote server and vice-versa. Before you enable encryption, you must install security certificates on the management server and all Data Collector servers affiliated with the remote servers.

Certificate distribution

The graphic illustrates the basic concept of how certificates are signed, trusted, and distributed in XProtect VMS to secure the communication from the management server.



1. A CA certificate acts as a trusted third party, trusted by both the subject/owner (data collector server) and by the party that verifies the certificate (management server)
2. The CA certificate must be trusted on the management server. In this way, the management server can verify the validity of the certificates issued by the CA
3. The CA certificate is used to establish a secure connection between the data collector servers and the management server
4. The CA certificate must be installed on the computers on which the data collector servers are running

Requirements for the private data collector server certificate:

- Issued to the data collector server so that the data collector server's host name is included in the certificate, either as subject (owner) or in the list of DNS names that the certificate is issued to
- Trusted on the management server by trusting the CA certificate that was used to issue the data collector server certificate

Encryption to clients and servers that retrieve data from the recording server (explained)

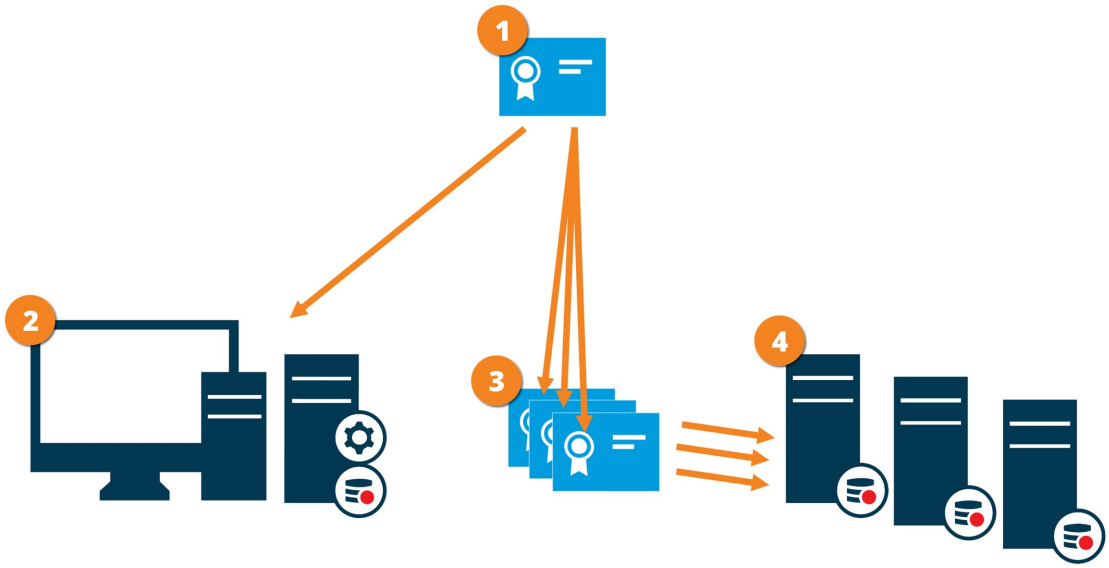
When you enable encryption on a recording server, communication to all clients, servers, and integrations that retrieve data streams from the recording server are encrypted. In this document referred to as 'clients':

- XProtect Smart Client
- Management Client
- Management Server (for System Monitor and for images and AVI video clips in email notifications)
- XProtect Mobile Server
- XProtect Event Server
- XProtect LPR
- Milestone Open Network Bridge
- XProtect DLNA Server
- Sites that retrieve data streams from the recording server through Milestone Interconnect
- Some third-party MIP SDK integrations

For solutions built with MIP SDK 2018 R3 or earlier that accesses recording servers: If the integrations are made using MIP SDK libraries, they need to be rebuilt with MIP SDK 2019 R1; if the integrations communicate directly with the Recording Server APIs without using MIP SDK libraries, the integrators must add HTTPS support themselves.

Certificate distribution

The graphic illustrates the basic concept of how certificates are signed, trusted, and distributed in XProtect VMS to secure the communication to the recording server.



❶ A CA certificate acts as a trusted third-party, trusted by both the subject/owner (recording server) and by the party that verifies the certificate (all clients)

❷ The CA certificate must be trusted on all clients. In this way, the clients can verify the validity of the certificates issued by the CA

❸ The CA certificate is used to establish a secure connection between the recording servers and all clients and services

❹ The CA certificate must be installed on the computers on which the recording servers are running

Requirements for the private recording server certificate:

- Issued to the recording server so that the recording server's host name is included in the certificate, either as subject (owner) or in the list of DNS names that the certificate is issued to
- Trusted on all computers running services that retrieve data streams from the recording servers by trusting the CA certificate that was used to issue the recording server certificate
- The service account that runs the recording server must have access to the private key of the certificate on the recording server.



If you enable encryption on the recording servers and your system applies failover recording servers, Milestone recommends that you also prepare the failover recording servers for encryption.

Encryption of communication with the Event Server

You can encrypt the two-way connection between the Event Server and the components that communicate with the Event Server, including the LPR Server. When you enable encryption on the Event Server, it applies to connections from all the components that connect to the Event Server. Before you enable encryption, you must install security certificates on the Event Server and all connecting components.



When the Event Server communication is encrypted, this applies to all communication with that Event Server. That is, only one mode is supported at a time, either http or https, but not at the same time.

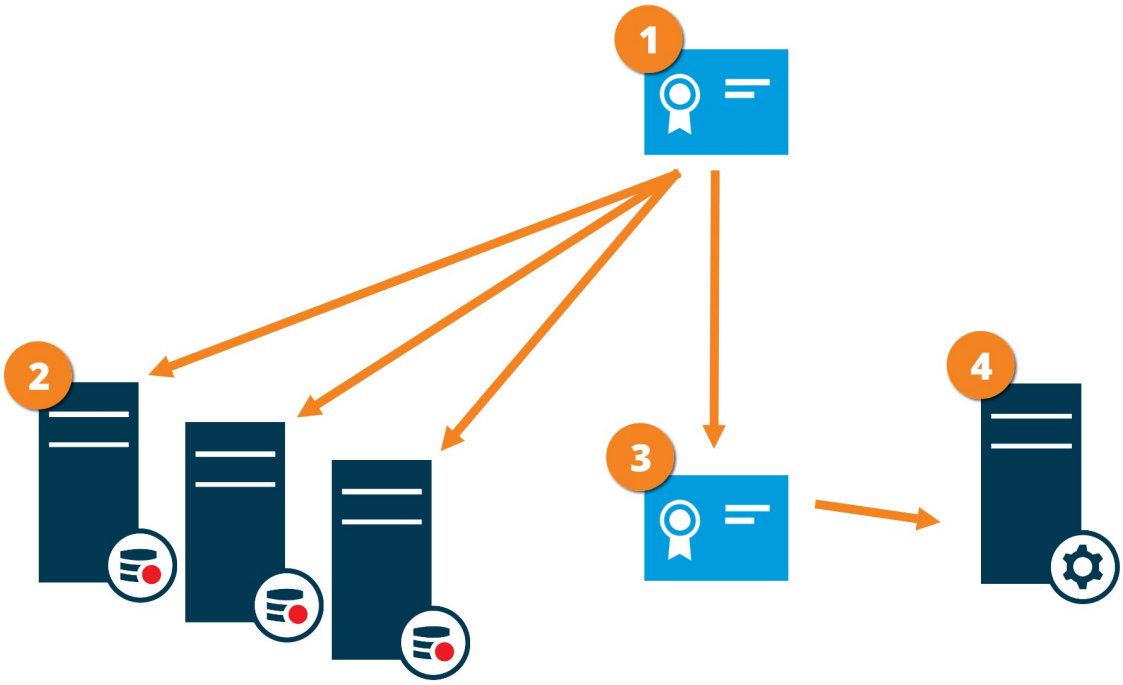
Encryption applies to every service hosted in the Event Server, including Transact, Maps, GisMap, and Intercommunication.



Before you enable encryption in the Event Server, all clients (Smart Client and Management Client) and the XProtect LPR plug-in must be updated to at least version 2022 R1.
HTTPS is only supported if every component is updated to at least version 2022 R1.

Certificate distribution

The graphic illustrates the basic concept of how certificates are signed, trusted, and distributed in XProtect VMS to secure the communication to the event server.



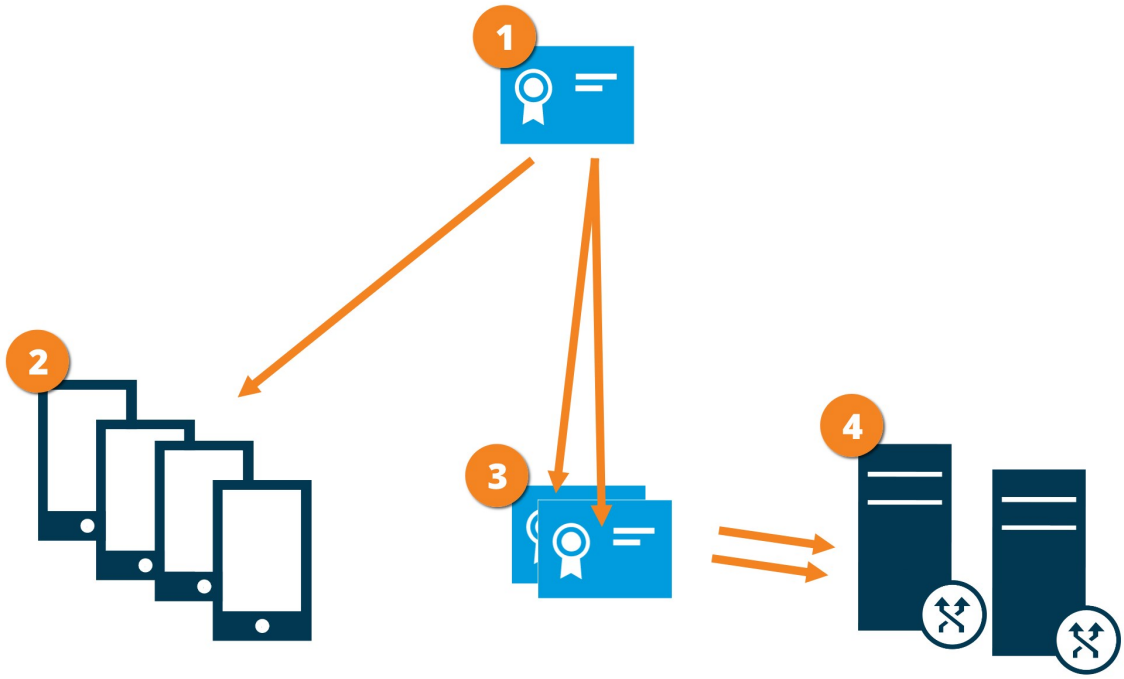
1. A CA certificate acts as a trusted third party, trusted by both the subject/owner (event server) and by the party that verifies the certificate
2. The CA certificate must be trusted on all clients. In this way, the clients can verify the validity of the certificates issued by the CA
3. The CA certificate is used to establish a secure connection between the event server and the clients
4. The CA certificate must be installed on the computer on which the event server is running

Mobile server data encryption (explained)

In XProtect VMS, encryption is enabled or disabled per mobile server. When you enable encryption on a mobile server, you will have the option to use encrypted communication with all clients, services, and integrations that retrieve data streams.

Certificate distribution for mobile servers

The graphic illustrates the basic concept of how certificates are signed, trusted, and distributed in XProtect VMS to secure the communication with the mobile server.



❶ A CA certificate acts as a trusted third party, trusted by both the subject/owner (mobile server) and by the party that verifies the certificate (all clients)

❷ The CA certificate must be trusted on all clients. In this way, clients can verify the validity of the certificates issued by the CA

❸ The CA certificate is used to establish a secure connection between the mobile server and clients and services

❹ The CA certificate must be installed on the computer on which the mobile server is running

Requirements for the CA certificate:

- The mobile server's host name must be included in the certificate, either as subject/owner or in the list of DNS names that the certificate is issued to
- The certificate must be trusted on all devices that are running services that retrieve data streams from the mobile server
- The service account that runs the mobile server must have access to the private key of the CA certificate

Mobile server encryption requirements for clients

For security reasons, Milestone recommends that you use secure communication between the mobile server and clients when you manage user account settings.

If you do not enable encryption and use an HTTP connection, the push-to-talk feature in XProtect Web Client will not be available.

Kerberos authentication (explained)

Kerberos is a ticket-based network authentication protocol. It is designed to provide strong authentication for client/server or server/server applications.

Use Kerberos authentication as an alternative to the older Microsoft NT LAN (NTLM) authentication protocol.

Kerberos authentication requires mutual authentication, where the client authenticates to the service and the service authenticates to the client. This way you can authenticate more securely from XProtect clients to XProtect servers without exposing your password.

To make mutual authentication possible in your XProtect VMS you must register Service Principal Names (SPN) in the active directory. An SPN is an alias that uniquely identifies an entity such as a XProtect server service. Every service that uses mutual authentication must have an SPN registered so that clients can identify the service on the network. Without correctly registered SPNs, mutual authentication is not possible.

The table below lists the different Milestone services with corresponding port numbers you need to register:

Service	Port number
Management server - IIS	80 - Configurable
Management server - Internal	8080
Recording server - Data Collector	7609
Failover Server	8990
Event Server	22331
LPR Server	22334



The number of services you need to register in the active directory depends on your current installation. Data Collector is installed automatically when installing Management Server, Recording Server, Event Server, LPR Server or Failover Server.

You must register two SPNs for the user running the service: one with the host name and one with the fully qualified domain name.

If you are running the service under a network user service account, you must register the two SPNs for each computer running this service.

This is the Milestone SPN naming scheme:

```
VideoOS/[DNS Host Name]:[Port]
VideoOS/[Fully qualified domain name]:[Port]
```

The following is an example of SPNs for the recording server service running on a computer with the following details:

```
Hostname: Record-Server1
Domain: Surveillance.com
```

SPNs to register:

```
VideoOS/Record-Server1:7609
VideoOS/Record-Server1.Surveillance.com:7609
```

Use Windows update

Milestone recommends that you use Windows Update to protect your VMS against vulnerabilities in the operating system by making sure that the latest updates are installed.XProtect VMS is Windows-based, so security updates from Windows Update are important.

Updates can require a connection to the Internet, so Milestone recommends that this connection is open only as required, and that it is monitored for unusual traffic patterns.

Windows Updates often require a restart. This can be a problem if high-availability is required, because the server cannot receive data from devices while it restarts.

There are several ways to avoid this, or minimize the impact. For example, you can download updates to the server, and then apply them at a time when a restart will disrupt surveillance as little as possible.

If high availability is a concern, Milestone recommends that you run management server and event servers in clusters that include one or more failover servers. The failover server will take over while the recording server restarts, and surveillance is not interrupted. Do not include recording servers in the cluster. For recording servers, use a failover recording server.



Before implementing Windows updates across the organization, Milestone recommends that you verify the updates in a test environment. See NIST 800-53 CM-8 *Information system component inventory and sandboxing and SC-44 Detonation Chambers*.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 SI-2 *Flaw Remediation*

Keep software and device firmware updated

Milestone recommends that you use the latest version of XProtect VMS and firmware for the hardware devices, for example the cameras. This will ensure that your system includes the latest security fixes.

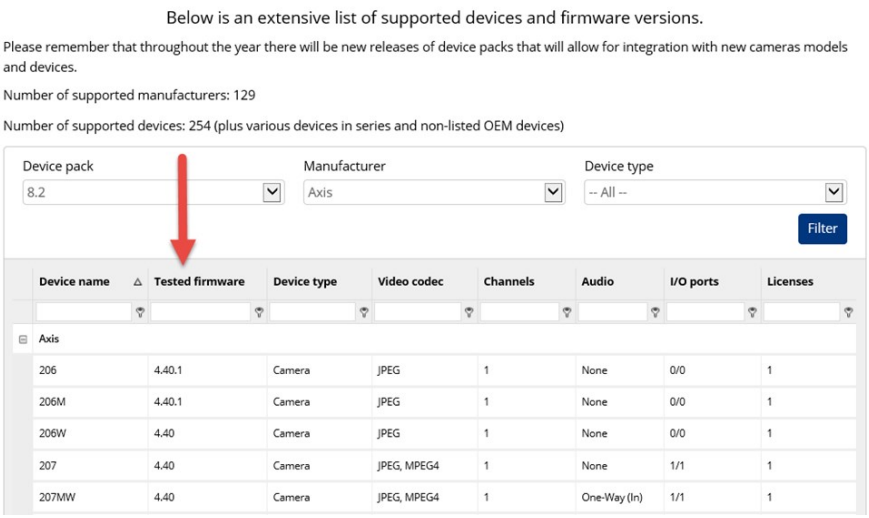
For hardware, network components, and operating systems, check the CVE database as well as any updates pushed out by manufacturers.

Before you upgrade the device firmware, verify that XProtect VMS supports it. Also, make sure that the device pack installed on the recording servers supports the device firmware.

Do this in a test environment for configuration, integration and testing before putting it into the production environment.

To verify that the VMS supports a device, follow these steps:

1. Open this link (https://www.milestonesys.com/da/community/business-partner-tools/supported-devices/).
2. Click the link that matches your XProtect VMS product.
3. In the **Device pack** column, select the version of the current device pack.
4. Select the manufacturer of your device, and then click **Filter**. The version of the firmware that the device pack supports is listed in the **Tested Firmware** column.



Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 SI-2 *Flaw Remediation*

Use antivirus on all servers and computers

Milestone recommends that you deploy anti-virus software on all servers and computers that connect to the VMS. Malware that gets inside your system can lock, encrypt, or otherwise compromise data on the servers and other devices on the network.

If mobile devices connect to the VMS, this includes ensuring that the devices have the latest operating systems and patches (though not directly anti-virus) installed.

When you do virus scanning, do not scan recording server directories and subdirectories that contain recording databases. In addition, do not scan for viruses on archive storage directories. Scanning for viruses on these directories can impact system performance.

For more information, see the section about how to exclude file types, folders, ports, and network traffic from virus scanning in the administrator manual for your XProtect VMS product.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 PL-8 *Information Security Architecture*
- NIST SP 800-53 SI-2 *Flaw remediation*
- NIST SP 800-53 SI-3 *Malicious Code Protection*
- NIST SP 800-53 SI *Information Systems Monitoring*

Monitor logs in the VMS for signs of suspicious activity

XProtect VMS provides features for generating and viewing logs that provide information about patterns of use, system performance, and other issues.Milestone recommends that you monitor the logs for signs of suspicious activities.

There are tools that leverage logs for operational and security purposes. Many businesses use syslog servers to consolidate logs. You can use syslog to note activities at a Windows level, however, XProtect VMS does not support syslog.

Milestone recommends that you use the Audit Log in XProtect VMS, and enable user access logging in Management Client. By default, the Audit Log notes only user logins. However, you can turn on user access logging so that the Audit Log notes all user activities in all of the client components of XProtect VMS products. This includes the times of the activities and the source IP addresses.

The client components are XProtect Smart Client, Web Client, and the XProtect Management Client component, and also integrations made by using the MIP SDK. Examples of activities are exports, activating outputs, viewing cameras live or in playback, and so on.



The Audit log does not note unsuccessful login attempts, or when the user logs out.

Logging all user activities in all clients increases the load on the system, and can affect performance.

You can adjust the load by specifying the following criteria that controls when the system will generate a log entry:

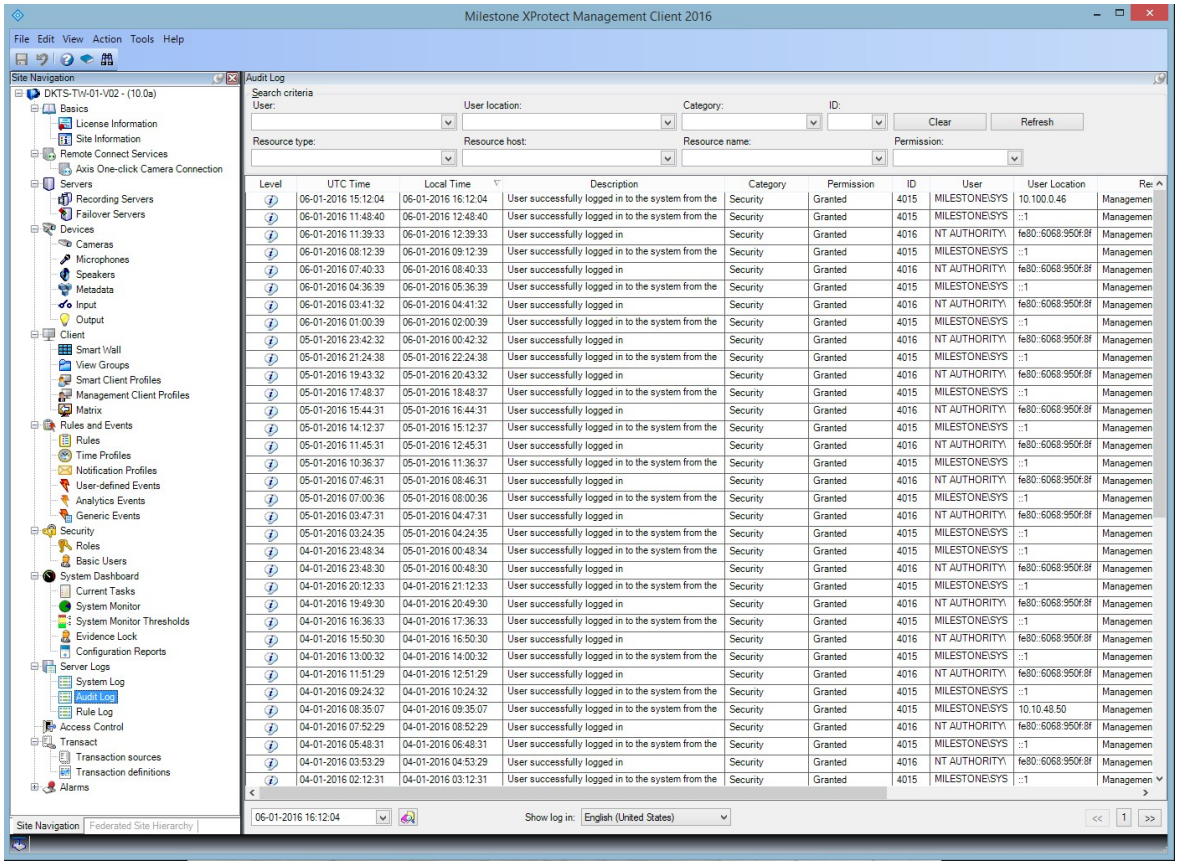
- The number of seconds that comprise one sequence. The VMS generates one log entry when a user plays video within the sequence.
- The number of frames that a user must view when playing back video before the VMS generates a log entry.

To turn on and configure extended user access logging, follow these steps:

1. In Management Client, click **Tools**, and select **Options**.
2. On the **Server Logs** tab, under **Log settings**, select **Audit Log**.
3. Under **Settings**, select the **Enable user access logging** check box.
4. Optional: To specify limitations for the information that is noted, and reduce impact on performance, make selections in the **Playback sequence logging length** and **Records seen before logging** fields.

To view the Audit Log in XProtect VMS, follow these steps:

1. Open Management Client.
2. Expand the **Server Logs** node.
3. Click **Audit Log**.



Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 AU-3 *Content of Audit Records*
- NIST SP 800-53 RA-5 *Vulnerability Scanning*
- NIST SP 800-53 AU-6 *Audit Review, Analysis and Reporting*

Advanced steps – Servers, Workstations, Clients and Applications

Adopt standards for secure network and VMS implementations **43**

Establish an incident response plan **43**

Protect sensitive VMS components **44**

Follow Microsoft OS Security best practices **45**

Use tools to automate or implement the security policy **45**

Follow established network security best practices **45**

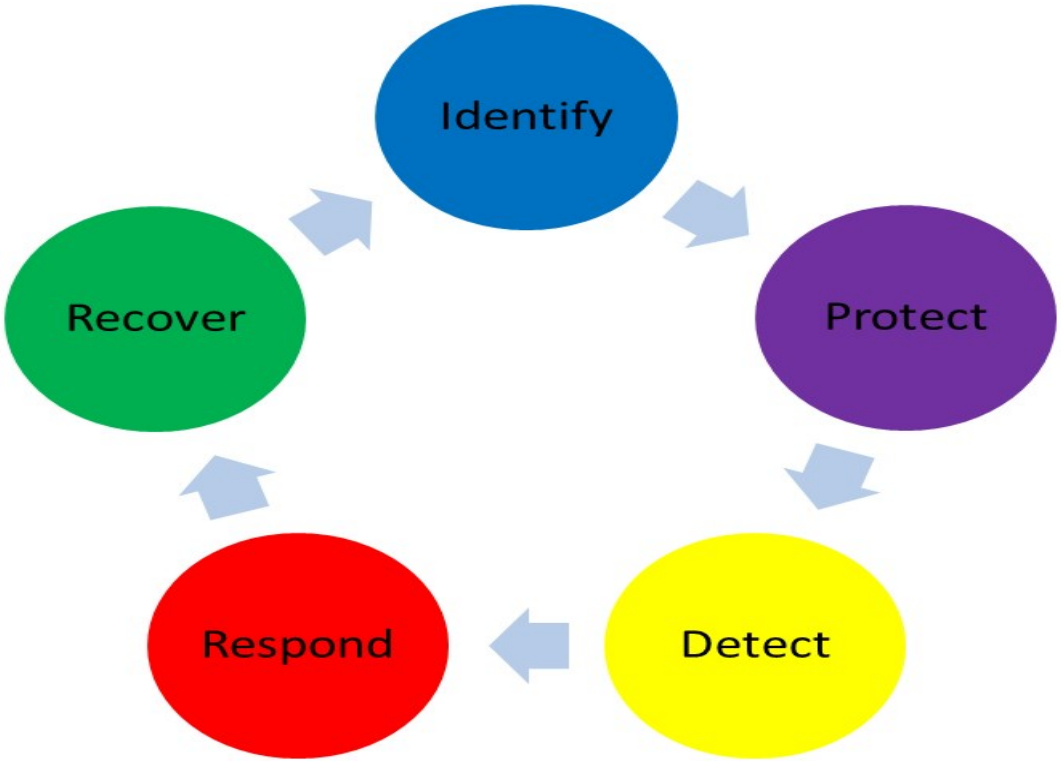
Adopt standards for secure network and VMS implementations

Milestone recommends that you adopt standards for secure networking and XProtect VMS implementations. The use of standards is a basic component of Internet and network engineering, and the basis of interoperability and system conformance. This also applies to the use of cryptographic solutions, where standards-based cryptography is the most commonly accepted approach.

Establish an incident response plan

Milestone recommends you start with a set of policies and procedures and establish an incident response plan. Designate staff to monitor the status of the system and respond to suspicious events. For example, activities that happen at unusual times. Establish a security Point of Contact (POC) with each of your vendors, including Milestone.

The following image is adapted from the NIST Cybersecurity Framework (http://www.nist.gov/cyberframework/). It shows the lifecycle that needs to be considered when creating a plan. The supporting material in the framework provide details about the lifecycle and security controls for incident response plans.



Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 IR 1-13 *Incident Response*

Protect sensitive VMS components

Milestone recommends that you use physical access control, and use the VMS to monitor and protect its sensitive VMS components. Physical restriction and role-based physical access control are countermeasures that keep servers and workstations secure.

Administrators and users should only have access to the information they need in order to fulfill their responsibilities. If all internal users have the same access level to critical data, it's easier for attackers to access the network.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 PE-1 *Physical and Environmental Protection Policy and Procedures*
- NIST SP 800-53 PE-2 *Physical Access Authorizations*
- NIST SP 800-53 PE-3 *Physical Access Control*
- NIST SP 800-53 AC-4 *Least Privilege*

Follow Microsoft OS Security best practices

Milestone recommends that you follow the security best practices for Microsoft operating systems (OS) to mitigate OS risks and maintain security. This will help you keep the Microsoft servers and client computers secure.

For more information, see *Microsoft Security Update Guide* (https://msrc.microsoft.com/update-guide).

Use tools to automate or implement the security policy

Milestone recommends that you find one or more tools to help you automate and implement the security policy. Automation reduces the risk of human error and makes it easier to manage the policy. For example, you can automate the installation of security patches and updates on servers and client computers.

One way to implement this recommendation is to combine the Microsoft Security Configuration Manager (SCCM) with the Security Content Automation Protocol (SCAP).(See for example, *Geek of All Trades: Automate Baseline Security Settings* (https://technet.microsoft.com/en-us/magazine/ff721825.aspx) and *Security Content Automation Protocol (SCAP) Validation Program* (http://scap.nist.gov/validation/).) This gives you a framework to create, distribute, and validate security settings on computers across your network.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 CM-1 *Configuration Management Policy and Procedures*
- NIST SP 800-53 CM-2 *Baseline Configuration*
- NIST SP 800-53 CM-3 *Configuration Change Control*

Follow established network security best practices

Milestone recommends that you follow IT and vendor best practices to ensure that devices on your network are securely configured. Ask your vendors to provide this information. It is important to open and maintain a security dialogue, and a discussion of best practices is a good place to start.

It is important to deny access to the VMS by not using vulnerable network settings. For more information, see *SP 800-128* (http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf), *SP 800-41-rev1* (http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf) (specific to firewalls), and *ICS-CERT Standards and References* (https://ics-cert.us-cert.gov/Standards-and-References) (general list).

Learn more

The following control(s) provide additional guidance:

- NIST 800-53 CM-6 *Configuration Settings*
- NIST 800-53 MA-3 *Maintenance Tools*

Devices and network

Devices and network

This section provides guidance for hardening the devices and network components related to XProtect VMS. This includes key parts of the system such as the cameras, storage, and the network.

Surveillance systems often include cameras at the edge of the network. Cameras and their network connections, if left unprotected, represent a significant risk of compromise, potentially giving intruders further access to the system.

Basic steps – Devices

Use strong passwords instead of default passwords **46**

Stop unused services and protocols **46**

Create dedicated user accounts on each device **47**

Scanning for devices **48**

Use strong passwords instead of default passwords

Milestone recommends that you change the default passwords on devices, for example, on a camera. Do not use default passwords because they are often published to the Internet and are readily available.

Instead, use strong passwords for devices. Strong passwords include eight or more alpha-numeric characters, use upper and lower cases, and special characters.

Learn more

The following control(s) provide additional guidance:

- NIST 800-53 IA-4 *Authenticator Management*
- NIST 800-53 IA-8 *Authenticator Feedback*
- NIST 800-53 SI-11 *Error Handling*

Stop unused services and protocols

To help avoid unauthorized access or information disclosure, Milestone recommends that you stop unused services and protocols on devices. For example, Telnet, SSH, FTP, UPnP, Ipv6, and Bonjour.

It is also important to use strong authentication on any services that access the VMS, network, or devices. For example, use SSH keys instead of user names and passwords, and use certificates from a Certificate Authority for HTTPS. For more information, see the hardening guides and other guidance from the device manufacturer.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 AC-17 *Remote Access (Disable Unused Protocols)*
- NIST SP 800-53 CM-6 *Configuration Settings*
- NIST SP 800-53 CM-7 *Least Functionality*
- NIST SP 800-53 IA-2 *Identification and Authentication*
- NIST SP 800-53 SA-9 *External Information Services*

Create dedicated user accounts on each device

All cameras have a default user account with a user name and password that the VMS uses to access the device. For auditing purposes, Milestone recommends that you change the default user name and password.

Create a user account specifically for use by the VMS, and use this user account and password when you add the camera to the VMS. When a recording server connects to the camera, it uses the user name and password you have created. If the camera has a log, this log shows that the recording server has connected to the camera.

With a dedicated user name and password, the device logs can help you determine whether a recording server or a person accessed the camera. This is relevant when investigating potential security issues affecting devices.

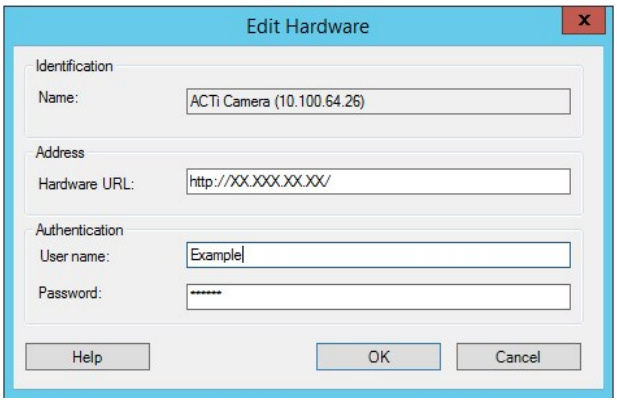
You can change the user name and password for a device before or after you add it in Management Client.

To change the user name and password before you add the device, follow these steps:

1. Go to the device's web interface, and change the default user name and password.
2. In Management Client, add the device, and specify the user name and password.

To change the user name and passwords of devices that are already added, follow these steps:

1. In Management Client, in the Site Navigation pane, expand the **Servers** node and select **Recording Servers**.
2. In the Recording Server pane, expand the recording server that contains the device, and then right-click the device and select **Edit hardware**.



3. Under **Authentication**, enter the new user name and password.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 AC-2 *Account Management*
- NIST SP 800-53 AC-4 *Least Privilege*

Scanning for devices

Scanning for devices (for example, **Express** scan or **Address range scanning** when adding hardware) is done using broadcasts that may contain user names and passwords in plain text.

Unless this is an initial setup, this functionality should not be used for adding devices to the system. Use the **Manual** option instead and manually select the driver.

Basic steps – Network

Use secure and trusted networks connection **48**

Use firewalls to limit IP access to servers and computers **49**

Use a firewall between the VMS and the Internet **63**

Connect the camera subnet to the recording server subnet only **64**

Use secure and trusted networks connection

Network communications must be secure, whether or not you are on a closed network. By default, secure communications should be used when accessing the VMS. For example:

- VPN tunnels or HTTPS by default
- Latest version of the Transport Layer Security (https://datatracker.ietf.org/wg/tls/charter/) (TLS, currently 1.2) with valid certificates that meet industry best practices, such as from Public-Key Infrastructure (X.509) (https://datatracker.ietf.org/wg/ipsec/documents/) and CA/Browser Forum (https://cabforum.org/).

Otherwise, credentials may be compromised and intruders might use them to access the VMS.

Configure the network to allow client computers to establish secure HTTPS sessions or VPN tunnels between the client devices and the VMS servers.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 SI-2 *Flaw remediation*
- NIST SP 800-53 CM-6 *Configuration Settings*
- NIST SP 800-53 SC-23 *Session Authenticity*

Use firewalls to limit IP access to servers and computers

Milestone recommends that you use secure connections, and the following additional steps:

- Use secure device authentication
- Use TLS
- Use device whitelisting to authenticate devices
- Use firewalls to limit network communication between servers and client computers and programs.

All XProtect components and the ports needed by them are listed in individual sections below. To ensure, for example, that the firewall blocks only unwanted traffic, you need to specify the ports that the XProtect VMS uses. You should only enable these ports. The lists also include the ports used for local processes.

They are arranged in two groups:

- Server components (services)—Offer their service on particular ports which is why they need to listen for client requests on these ports. Therefore, these ports need to be opened in the Windows Firewall for inbound connections.
- Client components (clients)—Initiate connections to particular ports on server components. Therefore, these ports need to be opened for outbound connections. Outbound connections are typically open by default in the Windows Firewall.

If nothing else is mentioned, ports for server components must be opened for inbound connections, and ports for client components must be opened for outbound connections.

Do keep in mind that server components can act as clients to other server components as well.

The port numbers are the default numbers, but this can be changed. Contact Milestone Support, if you need to change ports that are not configurable through the Management Client.

Server components (inbound connections)

Each of the following sections list the ports which need to be opened for a particular service. In order to figure out which ports need to be opened on a particular computer, you need to consider all services running on this computer.



Restrict remote access to the Management Server by adding firewall rules to only allow Recording Servers to connect to TCP port 9000.

Management Server service and related processes

Port number	Protocol	Process	Connections from...	Purpose
80	HTTP	IIS	All XProtect components • Management Server service • Recording Server services • API Gateway	Main communication, for example, authentication and configurations. Registration of recording servers and management servers by the Identity Provider.
443	HTTPS	IIS	XProtect Smart Client and the Management Client	Authentication of basic users by the Identity Provider.
6473	TCP	Management Server service	Management Server Manager tray icon, local connection only.	Showing status and managing the service.
8080	TCP	Management server	Local connection only.	Communication between internal processes on the server.
9000	HTTP	Management server	Recording Server services	Web service for internal communication between servers.
12345	TCP	Management Server service	XProtect Smart Client	Communication between the system and Matrix recipients. You can change the port number in the Management Client.
12974	TCP	Management Server service	Windows SNMP Service	Communication with the SNMP extension agent. Do not use the port for other purposes even if your system does not apply SNMP. In XProtect 2014 systems or older, the port number was 6475. In XProtect 2019 R2 systems and older, the port number was 7475.

SQL Server service

Port number	Protocol	Process	Connections from...	Purpose
1433	TCP	SQL Server	Management Server service	Storing and retrieving configurations via the Identity Provider.
1433	TCP	SQL Server	Event Server service	Storing and retrieving events via the Identity Provider.
1433	TCP	SQL Server	Log Server service	Storing and retrieving log entries via the Identity Provider.

Data Collector service

Port number	Protocol	Process	Connections from...	Purpose
7609	HTTP	IIS	On the management server computer: Data Collector services on all other servers. On other computers: Data Collector service on the Management Server.	System Monitor.

Event Server service

Port number	Protocol	Process	Connections from...	Purpose
1234	TCP/UDP	Event Server Service	Any server sending generic events to your XProtect system.	Listening for generic events from external systems or devices. Only if the relevant data

Port number	Protocol	Process	Connections from...	Purpose
				source is enabled.
1235	TCP	Event Server service	Any server sending generic events to your XProtect system.	Listening for generic events from external systems or devices. Only if the relevant data source is enabled.
9090	TCP	Event Server service	Any system or device that sends analytics events to your XProtect system.	Listening for analytics events from external systems or devices. Only relevant if the Analytics Events feature is enabled.
22331	TCP	Event Server service	XProtect Smart Client and the Management Client	Configuration, events, alarms, and map data.
22333	TCP	Event Server service	MIP Plug-ins and applications.	MIP messaging.

Recording Server service

Port number	Protocol	Process	Connections from...	Purpose
25	SMTP	Recording Server Service	Cameras, encoders, and I/O devices.	Listening for event messages from devices. The port is disabled by default. (Deprecated) Enabling this will open a port for non-encrypted

Port number	Protocol	Process	Connections from...	Purpose
				connections and is not recommended.
5210	TCP	Recording Server Service	Failover recording servers.	Merging of databases after a failover recording server had been running.
5432	TCP	Recording Server Service	Cameras, encoders, and I/O devices.	Listening for event messages from devices. The port is disabled by default.
7563	TCP	Recording Server Service	XProtect Smart Client, Management Client	Retrieving video and audio streams, PTZ commands.
8966	TCP	Recording Server Service	Recording Server Manager tray icon, local connection only.	Showing status and managing the service.
9001	HTTP	Recording Server Service	Management server	Web service for internal communication between servers. If multiple Recording Server instances are in use, every instance needs its own port. Additional ports will be 9002, 9003, etc.
11000	TCP	Recording Server Service	Failover recording servers	Polling the state of recording servers.

Port number	Protocol	Process	Connections from...	Purpose
12975	TCP	Recording Server Service	Windows SNMP service	Communication with the SNMP extension agent. Do not use the port for other purposes even if your system does not apply SNMP. In XProtect 2014 systems or older, the port number was 6474. In XProtect 2019 R2 systems and older, the port number was 7474.
65101	UDP	Recording Server service	Local connection only	Listening for event notifications from the drivers.



In addition to the inbound connections to the Recording Server service listed above, the Recording Server service establishes outbound connections to:

- Cameras
- NVRs
- Remote interconnected sites (Milestone Interconnect ICP)

Failover Server service and Failover Recording Server service

Port number	Protocol	Process	Connections from...	Purpose
25	SMTP	Failover Recording Server Service	Cameras, encoders, and I/O devices.	Listening for event messages from devices. The port is disabled by default. (Deprecated) Enabling this will open a

Port number	Protocol	Process	Connections from...	Purpose
				port for non-encrypted connections and is not recommended.
5210	TCP	Failover Recording Server Service	Failover recording servers	Merging of databases after a failover recording server had been running.
5432	TCP	Failover Recording Server Service	Cameras, encoders, and I/O devices.	Listening for event messages from devices. The port is disabled by default.
7474	TCP	Failover Recording Server Service	Windows SNMP service	Communication with the SNMP extension agent. Do not use the port for other purposes even if your system does not apply SNMP.
7563	TCP	Failover Recording Server Service	XProtect Smart Client	Retrieving video and audio streams, PTZ commands.
8844	UDP	Failover Recording Server Service	Local connection only.	Communication between the servers.
8966	TCP	Failover Recording Server Service	Failover Recording Server Manager tray icon, local connection only.	Showing status and managing the service.
8967	TCP	Failover Server	Failover Server Manager tray icon, local	Showing status and managing the service.

Port number	Protocol	Process	Connections from...	Purpose
		Service	connection only.	
8990	TCP	Failover Server Service	Management Server service	Monitoring the status of the Failover Server service.
9001	HTTP	Failover Server Service	Management server	Web service for internal communication between servers.



In addition to the inbound connections to the Failover Server / Failover Recording Server service listed above, the Failover Server / Failover Recording Server service establishes outbound connections to the regular recorders, cameras, and for Video Push.

Log Server service

Port number	Protocol	Process	Connections from...	Purpose
22337	HTTP	Log Server service	All XProtect components except for Management Client and the recording server.	Write to, read from, and configure the log server.

Mobile Server service

Port number	Protocol	Process	Connections from...	Purpose
8000	TCP	Mobile	Mobile Server Manager tray icon,	SysTray application.

Port number	Protocol	Process	Connections from...	Purpose
		Server service	local connection only.	
8081	HTTP	Mobile Server service	Mobile clients, Web clients, and Management Client.	Sending data streams; video and audio.
8082	HTTPS	Mobile Server service	Mobile clients and Web clients.	Sending data streams; video and audio.
40001 - 40099	HTTP	Mobile Server service	Recording server service	Mobile Server Video Push. This port range is disabled by default.

LPR Server service

Port number	Protocol	Process	Connections from...	Purpose
22334	TCP	LPR Server Service	Event server	Retrieving recognized license plates and server status. In order to connect, the Event server must have the LPR plug-in installed.
22334	TCP	LPR Server Service	LPR Server Manager tray icon, local connection only.	SysTray application

Milestone Open Network Bridge service

Port number	Protocol	Process	Connections from...	Purpose
580	TCP	Milestone Open Network Bridge Service	ONVIF clients	Authentication and requests for video stream configuration.
554	RTSP	RTSP Service	ONVIF clients	Streaming of requested video to ONVIF clients.

XProtect DLNA Server service

Port number	Protocol	Process	Connections from...	Purpose
9100	HTTP	DLNA Server Service	DLNA device	Device discovery and providing DLNA channels configuration. Requests for video streams.
9200	HTTP	DLNA Server Service	DLNA device	Streaming of requested video to DLNA devices.

XProtect Screen Recorder service

Port number	Protocol	Process	Connections from...	Purpose
52111	TCP	XProtect Screen Recorder	Recording Server Service	Provides video from a monitor. It appears and acts in the same way as a camera on the recording server. You can change the port number in the Management Client.

XProtect Incident Manager service

Port number	Protocol	Process	Connections from...	Purpose
80	HTTP	IIS	XProtect Smart Client and the Management Client	Main communication in non-secured installations
443	HTTPS	IIS	XProtect Smart Client and the Management Client	Main communication in installations secured by use of certificates

Server components (outbound connections)

Management Server service

Port number	Protocol	Connections to...	Purpose
443	HTTPS	The License server that hosts the License Management service. Communication is via https://www.milestonesys.com/OnlineActivation/LicenseManagementService.asmx	Activating licenses.

Recording Server service

Port number	Protocol	Connections to...	Purpose
80	HTTP	Cameras, NVRs, encoders Interconnected sites	Authentication, configuration, data streams, video, and audio. Login
443	HTTPS	Cameras, NVRs, encoders	Authentication, configuration, data streams, video, and audio.

Port number	Protocol	Connections to...	Purpose
554	RTSP	Cameras, NVRs, encoders	Data streams, video, and audio.
7563	TCP	Interconnected sites	Data streams and events.
11000	TCP	Failover recording servers	Polling the state of recording servers.
40001 – 40099	HTTP	Mobile Server service	Mobile Server Video Push. This port range is disabled by default.

Failover Server service and Failover Recording Server service

Port number	Protocol	Connections to...	Purpose
11000	TCP	Failover recording servers	Polling the state of recording servers.

Event Server service

Port number	Protocol	Connections to...	Purpose
443	HTTPS	Milestone Customer Dashboard via https://service.milestonesys.com/	Send status, events and error messages from the XProtect system to Milestone Customer Dashboard.

Log Server service

Port number	Protocol	Connections to...	Purpose
443	HTTP	Log server	Forwarding messages to the log server.

API Gateway

Port number	Protocol	Connections to...	Purpose
443	HTTPS	Management sever	RESTful API

Cameras, encoders, and I/O devices (inbound connections)

Port number	Protocol	Connections from...	Purpose
80	TCP	Recording servers and failover recording servers	Authentication, configuration, and data streams; video and audio.
443	HTTPS	Recording servers and failover recording servers	Authentication, configuration, and data streams; video and audio.
554	RTSP	Recording servers and failover recording servers	Data streams; video and audio.

Cameras, encoders, and I/O devices (outbound connections)

Port number	Protocol	Connections to...	Purpose
25	SMTP	Recording servers and failover recording servers	Sending event notifications (deprecated).

Port number	Protocol	Connections to...	Purpose
5432	TCP	Recording servers and failover recording servers	Sending event notifications. The port is disabled by default.
22337	HTTP	Log server	Forwarding messages to the log server.



Only a few camera models are able to establish outbound connections.

Client components (outbound connections)

XProtect Smart Client, XProtect Management Client, XProtect Mobile server

Port number	Protocol	Connections to...	Purpose
80	HTTP	Management Server service	Authentication
443	HTTPS	Management Server service	Authentication of basic users when encryption is enabled.
443	HTTPS	Milestone Systems A/S (doc.milestonesys.com at 52.178.114.226)	Management Client and Smart Client occasionally check if the online help is available by accessing the help URL.
7563	TCP	Recording Server service	Retrieving video and audio streams, PTZ commands.
22331	TCP	Event Server service	Alarms.

XProtect Web Client, XProtect Mobile client

Port number	Protocol	Connections to...	Purpose
8081	HTTP	XProtect Mobile server	Retrieving video and audio streams.
8082	HTTPS	XProtect Mobile server	Retrieving video and audio streams.

API Gateway

Port number	Protocol	Connections to...	Purpose
80	HTTP	Management Server	RESTful API
443	HTTPS	Management Server	RESTful API

Learn more

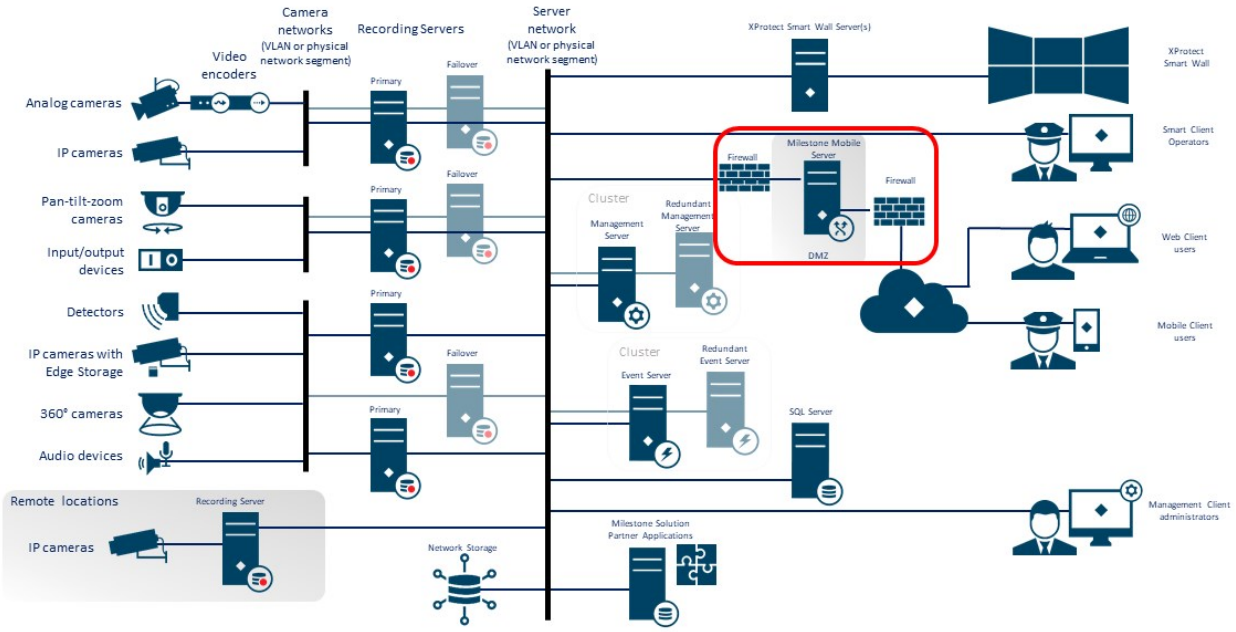
The following control(s) provide additional guidance:

- NIST SP 800-53 CA-3 *System Interconnections*
- NIST SP 800-53 CM-6 *Configuration Settings*
- NIST SP 800-53 SC-7 *Boundary Protection*

Use a firewall between the VMS and the Internet

The VMS should not connect directly to the Internet. If you expose parts of the VMS to the Internet, Milestone recommends that you use an appropriately configured firewall between the VMS and the Internet.

If possible, expose only the XProtect Mobile server component to the Internet, and locate it in a demilitarize zone (DMZ) with firewalls on both sides. This is illustrated in the following figure.



Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 CA-3 *System Interconnections*

Connect the camera subnet to the recording server subnet only

Milestone recommends that you connect the camera subnet only to the recording server subnet. The cameras and other devices need to communicate only with the recording servers. For more information, see Recording Server on page 74.

Learn more

The following control(s) provide additional guidance:

- NIST 800-53 SC-7 *Boundary Protection*

Advanced steps – Devices

Use Simple Network Management Protocol to monitor events

Milestone recommends that you use Simple Network Management Protocol (SNMP) to monitor events on the devices on the network. You can use SNMP as a supplement for syslog. SNMP works in real-time with many types of events that can trigger alerts, for example if a device is restarted.

For this to work, the devices must support logging via SNMP.

There are multiple versions of SNMP protocols available. Versions 2c and 3 are the most current. Implementation involves a suite of standards. A good overview can be found on the SNMP reference site (http://www.snmp.com/protocol/snmp_rfcs.shtml).

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 SI-4 *Event Monitoring*

Advanced steps – Network

Use secure wireless protocols **65**

Use port-based access control **65**

Run the VMS on a dedicated network **66**

Use secure wireless protocols

If you use wireless networks, Milestone recommends that you use a secure wireless protocol to prevent unauthorized access to devices and computers. For example, use standardized configurations. The NIST guidance on wireless local area networks provides specific details on network management and configuration. For more information, see *SP 800-48 revision 1, Guide to Securing Legacy IEEE 802.11 Wireless Networks* (http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf).

Additionally, Milestone recommends that you do not use wireless cameras in mission-critical locations. Wireless cameras are easy to jam, which can lead to loss of video.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 AC-18 *Wireless Access*
- NIST SP 800-53 SC-40 *Wireless Link Protection*

Use port-based access control

Use port-based access control to prevent unauthorized access to the camera network. If an unauthorized device connects to a switch or router port, the port should become blocked. Information about how to configure switches and routers is available from the manufacturers. See *SP 800-128, Guide for Security-Focused Configuration Management of Information Systems* (http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf), for information about configuration management of information systems.

Learn more

The following control(s) provide additional guidance:

- NIST 800-53 CM-1 *Configuration Management Policy and Procedures*
- NIST 800-53 CM-2 *Baseline Configuration*
- NIST 800-53 AC-4 *Least Privilege*
- NIST 800-53 CM-6 *Configuration Settings*
- NIST 800-53 CM-7 *Least Functionality*

Run the VMS on a dedicated network

Milestone recommends that, whenever possible, you separate the network where the VMS is running from networks with other purposes. For example, a shared network such as the printer network should be isolated from the VMS network. In addition, XProtect VMS deployments should follow a general set of best practices for system interconnections.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 CA-3 *System Interconnections*

Milestone Servers

Basic steps – Milestone servers

Use physical access controls and monitor the server room **67**

Use encrypted communication channels **67**

Use physical access controls and monitor the server room

Milestone recommends that you place the hardware with the servers installed in a designated server room, and that you use physical access controls. In addition, you should maintain access logs to document who has had physical access to the servers. Surveillance of the server room is also a preventive precaution.

Milestone supports integration of access control systems and their information. For example, you can view access logs in XProtect Smart Client.

Learn more

The following control(s) provide additional guidance:

- NIST 800-53 PE-3 *Physical Access Control*

Use encrypted communication channels

Milestone recommends that you use a VPN for communication channels for installations where servers are distributed across untrusted networks. This is to prevent attackers from intercepting communications between the servers. Even for trusted networks, Milestone recommends that you use HTTPS for configuration of cameras and other system components.

Learn more

The following control(s) provide additional guidance:

- NIST 800-53 AC-4 *Information Flow Enforcement*
- NIST 800-53 AC-17 *Remote Access*

Advanced steps – Milestone servers

Run services with service accounts **68**

Run components on dedicated virtual or physical servers **68**

Restrict the use of removable media on computers and servers **68**

Use individual administrator accounts for better auditing **68**

Use subnets or VLANs to limit server access **69**

Enable only the ports used by Event Server **69**

Run services with service accounts

Milestone recommends that you create service accounts for services related to XProtect VMS, instead of using a regular user account. Set up the service accounts as domain users, and only give them the permissions required to run the relevant services. See Kerberos authentication (explained) on page 38. For example, the service account should not be able to log on to the Windows desktop.

Learn more

The following control(s) provide additional guidance:

- NIST 800-53 AC-5 *Separation of Duties*
- NIST 800-53 AC-6 *Least Privilege*

Run components on dedicated virtual or physical servers

Milestone recommends that you run the components of XProtect VMS only on dedicated virtual or physical servers without any other software or services installed.

Learn more

The following control(s) provide additional guidance:

- NIST 800-53 CM-9 *Configuration Management Plan*

Restrict the use of removable media on computers and servers

Milestone recommends that you restrict the use of removable media, for example USB keys, SD cards, and smartphones on computers and servers where components of XProtect VMS are installed. This helps prevent malware from entering the network. For example, allow only authorized users to connect removable media when you need to transfer video evidence.

Learn more

The following control(s) provide additional guidance:

- NIST 800-53 MP-7 *Media Use*

Use individual administrator accounts for better auditing

As opposed to shared administrator accounts, Milestone recommends using individual accounts for administrators. This lets you track who does what in XProtect VMS. This helps prevent malware from entering the network. You can then use an authoritative directory such as Active Directory to manage the administrator accounts.

You assign administrator accounts to roles in Management Client under **Roles**.

Learn more

The following control(s) provide additional guidance:

- NIST 800-53 AC-5 *Separation of Duties*
- NIST 800-53 CM-9 *Configuration Management Plan*

Use subnets or VLANs to limit server access

Milestone recommends that you logically group different types of hosts and users into separate subnets. This can have benefits in managing privileges for these hosts and users as members of a group with a given function or role. Design the network so that there is a subnet or VLAN for each function. For example, one subnet or VLAN for surveillance operators and one for administrators. This allows you to define firewall rules by group instead of for individual hosts.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 AC-2 *Account Management*
- NIST SP 800-53 CSC 11: *Secure Configurations for Network Devices such as Firewalls, Routers, and Switches*
- NIST SP 800-53 SC-7 *Boundary Protection*

Enable only the ports used by Event Server

Milestone recommends that you enable only the ports used by event server, and block all other ports, including the default Windows ports.

The event server ports used in XProtect VMS are: 22331, 22333, 9090, 1234, and 1235.



The ports used depend on the deployment. If in doubt, contact Milestone Support.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 CSC 11: *Secure Configurations for Network Devices such as Firewalls, Routers, and Switches*

SQL Server

Connection to the SQL Server and database

Communication between the Milestone XProtect VMS and the SQL Server and database can potentially be tampered by an attacker because the certificate is not validated.

To mitigate this, you must first set up verifiable server certificates. After the certificates are set up, you must modify the ConnestionString in the Windows registry by removing trustServerCertificate=true, as follows:

Registry key: Computer\HKEY_LOCAL_MACHINE\SOFTWARE\VideoOS\Server\Common\ConnectionString

- Current

  connection string: Data Source=localhost;initial catalog='Surveillance';Integrated Security=SSPI;encrypt=true;trustServerCertificate=true

- Hardened

  connection string: Data Source=localhost;initial catalog='Surveillance';Integrated Security=SSPI;encrypt=true

This results in encryption occurring only if there is a verifiable server certificate, otherwise the connection attempt fails.

This issue is described in detail in the article Using Encryption Without Validation.

Run the SQL Server and database on a separate server

Milestone recommends that you make the SQL Server and database redundant. This reduces the risk of real or perceived downtime.

To support Windows Server Failover Clustering (WSFC), Milestone recommends that you run the SQL Server and database on a separate server, and not on the management server.

SQL Server must run in WSFC setup, and the management and event servers must run in a Microsoft Cluster setup (or similar technology). For more information about WSFC, see *Windows Server Failover Clustering (WSFC) with SQL Server* (https://msdn.microsoft.com/en-us/library/hh270278.aspx).

Learn more

The following control(s) provide additional guidance:

- NIST 800-53 SC-7 *Boundary Protection*
- NIST 800-53 CM-9 *Configuration Management Plan*

Management Server

Adjust the token time-out **71**

Enable only the ports used by the management server **71**

Disable non-secure protocols **71**

Disable legacy remoting channel **72**

Manage IIS header information **72**

Disable IIS HTTP TRACE / TRACK verbs **73**

Disable the IIS Default Page **74**

Adjust the token time-out

XProtect VMS uses session tokens when it logs in to the management server using SSL (basic users) or NTLM (Windows users) protocols. A token is retrieved from the management server and used on the secondary servers, for example the recording server and sometimes also the event server. This is to avoid that NTLM and AD lookup is performed on every server component.

By default, a token is valid for 240 minutes. You can adjust this down to 1 minute intervals. This value can also be adjusted over time. Short intervals increase security, however, the system generates additional communication when it renews the token.

The best interval to use depends on the deployment. This communication increases the system load and can impact performance.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 IA-5 *Authenticator Management*

Enable only the ports used by the management server

Milestone recommends that you enable only the ports used by the management server, and that you block all other ports, including the default Windows ports. This guidance is consistent for the server components of XProtect VMS.

The management server ports used in XProtect VMS are: 80, 443, 1433, 7475, 8080, 8990, 9000, 12345.



The ports used depend on the deployment. If in doubt, contact Milestone Support.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 AC-2 *Account Management*
- NIST SP 800-53 SC-7 *Boundary Protection*

Disable non-secure protocols

When a basic user logs in to the management server through IIS, the Management Client will use any protocol available.Milestone recommends that you always implement the latest version of the Transport Layer Security (TLS, currently 1.2) (https://datatracker.ietf.org/wg/tls/charter/), and disable all improper cipher suites and obsolete versions of TLS/SSL protocols. Perform actions to block non-secure protocols at the OS level. This prevents the Management Client from using protocols that are not secure. The OS determines the protocol to use.



The protocols used depend on the deployment. If in doubt, contact Milestone Support.

Learn more

The following control(s) provide additional guidance:

- NIST 800-53 AC-17 *Remote Access (Disable Unused Protocols)*
- NIST 800-53 CM-6 *Configuration Settings*
- NIST 800-53 CM-7 *Least Functionality*

Disable legacy remoting channel

Communication between the recording servers and the management server has become more secure with the solution implemented in 2019 R2. If you upgrade from a previous XProtect VMS release, the management server still starts the legacy 3rd party technology to be able to communicate with recording servers on older releases.

When all recording servers in your system are upgraded to version 2019 R2 or later, you can configure the management server to not start the legacy remoting channel, to make your system less vulnerable, Milestone recommends that you set **UseRemoting** to **False** in the management server configuration file.

Learn more

The following control(s) provide additional guidance:

- NIST 800-53 AC-17 *Remote Access (Disable Unused Protocols)*
- NIST 800-53 CM-6 *Configuration Settings*

Manage IIS header information

Disable IIS header information

For security purposes, Milestone recommends that you disable the X-Powered-By HTTP and X-AspNet-Version headers.

The HTTP header X-Powered-By reveals the version of IIS being used on the server. Disable this header by doing the following:

1. Open the IIS Manager.
2. Select the Default website.
3. Select **HTTP Response Headers**.
4. Select the **X-Powered-By** HTTP header and select **Remove**.

The HTTP header X-AspNet-Version reveals the version of ASP.NET being used by the Management Server application pool. Disable this header by doing the following:

1. Open the web.config file located in %windir%\Microsoft.NET\Framework\v4.0.30319\CONFIG.
2. After the `<system.web>` tag, add this: `<httpRuntime enableVersionHeader="false" />`
3. Save the file.

The SERVER header variable should not be removed, because it will cause functionality within Management Server to break.

Set X-Frame Options

For security purposes, Milestone recommends that you set the X-Frame-Options to **deny**.

When you set the HTTP header X-Frame-Options to deny, this disables the loading of the page in a frame, regardless of what site is trying to gain access.

Change this header by doing the following:

1. Open the IIS Manager.
2. Select the Default website > **Installation**.
3. Select **HTTP Response Headers**.
4. Right-click and select **Add...** from the menu.
5. In the **Name** field write **X-Frame-Options**, and in the **Value** field write **deny**.

Disable IIS HTTP TRACE / TRACK verbs

For security purposes, Milestone recommends that you disable the HTTP TRACE verb in your IIS installation. Disable the HTTP TRACE verb by doing the following:

1. Open the IIS manager.
2. Select the Default website.
3. Double-click **Request filtering**.

   If **Request filtering** is not available, install it by following the instructions here: https://docs.microsoft.com/en-us/iis/configuration/system.webserver/security/requestfiltering/

4. Select the **HTTP Verbs** tab.
5. Select **Deny Verb** from the **Actions** menu.
6. Type **TRACE** and click **OK**.
7. Select **Deny Verb** from the **Actions** menu.
8. Type **TRACK** and click **OK**.
9. Select **Deny Verb** from the **Options** menu.
10. Type **OPTIONS** and click **OK**.

Disable the IIS Default Page

For security purposes, Milestone recommends that you disable the IIS Default Page. By doing this, you remove information that could be used to discover what technologies are used in your installation, and you align with IIS Best Practices as defined by Microsoft. Disable the default page by doing the following:

1. Open the IIS manager.
2. Select the Default website.
3. Double-click **Default Document**.
4. Select **Disable** in the **Actions** menu.

Identity Provider

Disable IIS header information on the Identity Provider

For security purposes, Milestone recommends that you disable the server header on the Identity Provider application.

The server header describes the software used by the server of original that handles a request. Disable this header by doing the following.



Note: This is only applicable for IIS 10 and above.

1. Open the IIS Manager.
2. Under the Default website, select **IDP**.
3. Open the **Configuration Editor**.
4. Select the section **system.webServer/security/requestFiltering**.
5. Set **removeServerHeader** to **True**.

Recording Server

Storage and Recording Settings properties **74**

Use separate network interface cards **76**

Harden Network Attached Storage (NAS) to store recorded media data **76**

Storage and Recording Settings properties

Available functionality depends on the system you are using. See the complete feature list, which is available on the product overview page on the Milestone website (https://www.milestonesys.com/solutions/platform/product-index/).

In the **Storage and Recording Settings** dialog box, specify the following:

Name	Description
Name	Rename the storage if needed. Names must be unique.
Path	Specify the path to the directory to which you save recordings in this storage. The storage does not necessarily have to be located on the recording server computer. If the directory does not exist, you can create it. Network drives must be specified by using UNC (Universal Naming Convention) format, example: \\ server\volume\directory\.
Retention time	Specify for how long recordings should stay in the archive before they are deleted or moved to the next archive (depending on archive settings). The retention time must always be longer than the retention time of the previous archive or the default recording database. This is because the number of retention days specified for an archive includes all the retention periods stated earlier in the process.
Maximum size	Select the maximum number of gigabytes of recording data to save in the recording database. Recording data in excess of the specified number of gigabytes is auto-moved to the first archive in the list - if any is specified - or deleted. ⚠ When less than 5GB of space is free, the system always auto-archives (or deletes if no next archive is defined) the oldest data in a database. If less than 1GB space is free, data is deleted. A database always requires 250MB of free space. If you reach this limit (if data is not deleted fast enough), no more data is written to the database until you have freed enough space. The actual maximum size of your database is the amount of gigabytes you specify, minus 5GB.
Signing	Enables a digital signature to the recordings. This means, for example, that the system confirms that exported video has not been modified or tampered with when played back. The system uses the SHA-2 algorithm for digital signing.
Encryption	Select the encryption level of the recordings: • **None**

Name	Description
	• **Light (Less CPU usage)** • **Strong (More CPU usage)** The system uses the AES-256 algorithm for encryption. If you select **Light**, a part of the recording is encrypted. If you select **Strong**, the whole recording is encrypted. If you choose to enable encryption, you must also specify a password below.
Password	Enter a password for the users allowed to view encrypted data. Milestone recommends that you use strong passwords. Strong passwords do not contain words that can be found in a dictionary or are part of the user's name. They include eight or more alpha-numeric characters, upper and lower cases, and special characters.

Use separate network interface cards

Milestone recommends that you use multiple network interface cards (NICs) to separate the communication between recording servers and devices from the communication between recording servers and client programs. Client programs do not need to communicate directly with devices.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 SC-7 *Boundary Protection*

Harden Network Attached Storage (NAS) to store recorded media data

The Recording Server can use Network Attached Storage (NAS) to store recorded media data.

If you choose to use NAS, it can be hardened by using SMB 3.0 security enhancements, as described in this document on SMB security enhancements.

XProtect Mobile Server

Only enable ports that Mobile Server uses **77**

Use a "demilitarized zone" (DMZ) to provide external access **77**

Disable non-secure protocols **77**

Set up users for two-step verification via email **78**

Configure the Content Security Policy (CSP) **82**

Only enable ports that Mobile Server uses

Milestone recommends that you enable only the ports that Mobile Server uses, and block all other ports, including the default Windows ports.

By default, the XProtect Mobile Server uses ports 8081 and 8082.



The ports used depend on the deployment. If in doubt, contact Milestone Support.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 AC-2 *Account Management*
- NIST SP 800-53 SC-7 *Boundary Protection*

Use a "demilitarized zone" (DMZ) to provide external access

Milestone recommends that you install Mobile Server in a DMZ, and on a computer with two network interfaces:

- One for internal communication
- One for public Internet access

This allows mobile client users to connect to Mobile Server with a public IP address, without compromising the security or availability of the VMS network.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 SC-7 *Boundary Protection*

Disable non-secure protocols

Milestone recommends that you use only the necessary protocols, and only the latest versions. For example, implement the latest version of the Transport Layer Security (TLS, currently 1.2) and disable all other cipher suites and obsolete versions of TLS/SSL protocols. This requires configuration of Windows and other system components, and the proper use of digital certificates and keys.



The same recommendation is given for the Management Server. For more information, see Disable non-secure protocols on page 71.

Learn more

The following control(s) provide additional guidance:

- NIST 800-53 AC-17 *Remote Access (Disable Unused Protocols)*
- NIST 800-53 CM-6 *Configuration Settings*
- NIST 800-53 CM-7 *Least Functionality*

Set up users for two-step verification via email

Available functionality depends on the system you are using. See the complete feature list, which is available on the product overview page on the Milestone website (https://www.milestonesys.com/solutions/platform/product-index/).

To impose an additional login step on users of the XProtect Mobile client or XProtect Web Client, set up two-step verification on the Mobile Server. In addition to the standard user name and password, the user must enter a verification code received by email.

Two-step verification increases the protection level of your surveillance system.

Requirements

- You have installed an SMTP server.
- You have added users and groups to your XProtect system in the Management Client on the **Roles** node in the **Site Navigation** pane. On the relevant role, select the **Users and Groups** tab.
- If you upgraded your system from a previous version of XProtect, you must restart the Mobile Server to enable the two-step verification feature.

In the Management Client, perform these steps:

1. Enter information about your SMTP server.
2. Specify the settings for the verification code that will be sent to the client users.
3. Assign login method to users and domain groups.

This topic describes each of these steps.

Enter information about your SMTP server

The provider uses the information about the SMTP server:

1. In the navigation pane, select **Mobile Servers**, and select the relevant Mobile Server.
2. On the **Two-step verification** tab, select the **Enable two-step verification** check box.
3. Below **Provider settings**, on the **Email** tab, enter information about your SMTP server and specify the email that the system will send to client users when they log in and are set up for a secondary login. For details about each parameter, see Two-step verification tab on page 79.

Specify the verification code that will be sent to the users

To specify the complexity of the verification code:

1. On the **Two-step verification** tab, in the **Verification code settings** section, specify the period within which XProtect Mobile client or XProtect Web Client users, do not have to reverify its login in case of, for example, a disconnected network. Default period is 3 minutes.Specify the period within which the user can use the received verification code. After this period, the code is invalid and the user has to request for a new code. Default period is 5 minutes.Specify the maximum number of code entry attempts, before the user will be blocked. Default number is 3.
2. Specify the number of characters for the code. Default length is 6.
3. Specify the complexity of the code that you want the system to compose.

Assign login method to users and Active Directory groups

On the **Two-step verification** tab, in the **User settings** section, the list of users and groups added to your XProtect system appears.

1. In the **Login method** column, select between no login, no two-step verification, or delivery method of codes.
2. In the **Details** field, add the delivery details such as email addresses of individual users. Next time the user logs into the XProtect Mobile client or the XProtect Web Client, he or she is asked for a secondary login.
3. If a group is configured in Active Directory, the Mobile Server uses details, such as email addresses, from Active Directory.

   Windows groups do not support two-step verification.
4. Save your configuration.

You have completed the steps for setting up your users for two-step verification via email.

Two-step verification tab

Available functionality depends on the system you are using. See the complete feature list, which is available on the product overview page on the Milestone website (https://www.milestonesys.com/solutions/platform/product-index/).

Use the **Two-step verification** tab to enable and specify an additional login step on users of:

- XProtect Mobile app on their iOS or Android mobile devices
- XProtect Web Client

The first type of verification is a password. The second type is a verification code, which you can configure to be sent to the user via email.

For more information, see Set up users for two-step verification via email on page 78.

The following tables describe the settings on this tab.

Provider settings > **Email**

Name	Description
SMTP server	Enter the IP address or host name of the simple mail transfer protocol (SMTP) server for two-step verification emails.
SMTP server port	Specify the port of the SMTP server for sending emails. Default port number is 25 without SSL and 465 with SSL.
Use SSL	Select this check box if your SMTP server supports SSL encryption.
User name	Specify the user name for logging in to the SMTP server.
Password	Specify the password for logging in to the SMTP server.
Use Secure Password Authentication (SPA)	Select this check box if your SMTP server supports SPA.
Sender's email address	Specify the email address for sending verification codes.
Email subject	Specify the subject title for the email. Example: Your two-step verification code.
Email text	Enter the message you want to send. Example: Your code is {0}.  If you forget to include the {0} variable, the code is added at the end of the text by default.

Verification code settings

Name	Description
Reconnection timeout (0-30 minutes)	Specify the period within which XProtect Mobile client users do not have to reverify their login in case of, for example, a disconnected network. The default period is three minutes. This setting does not apply to XProtect Web Client.

Name	Description
Code expires after (1-10 minutes)	Specify the period within which the user can use the received verification code. After this period, the code is invalid and the user has to request for a new code. The default period is five minutes.
Code entry attempts (1-10 attempts)	Specify the maximum number of code entry attempts before the the provided code becomes invalid. The default number is three.
Code length (4-6 characters)	Specify the number of characters for the code. The default length is six.
Code composition	Specify the complexity of the code that you want the system to generate. You can select among: • **Latin uppercase (A-Z)** • **Latin lowercase(a-z)** • **Digits (0-9)** • **Special characters (!@#...)**

User settings

Name	Description
Users and groups	Lists the users and groups added to the XProtect system. If a group is configured in Active Directory, the Mobile Server uses details, such as email addresses, from Active Directory. Windows groups do not support two-step verification.
Verification method	Select a verification setting for each user or group. You can select among: • **No login**: the user cannot log in • **No two-step verification**: the user must enter user name and password

Name	Description
	• **Email**: the user must enter a verification code in addition to user name and password
User details	Enter the email address to which each user will receive codes.

Configure the Content Security Policy (CSP)

WebSockets with wildcards should be removed from the CSP headers on the Mobile Server.

Currently the ws://*:* and wss://*:* cannot be removed from the CSP described in Mobile Server configuration due to Safari browser limitations.

To increase the security on your Mobile Server, do the following:

1. Open the VideoOS.MobileServer.Service.exe.config file, which is located in the installation folder of the Mobile Server.
2. Modify the <HttpHeaders> section, where the value of key="Content-Security-Policy" as follows:
   - If Safari browser support is not needed, remove ws://*:* and wss://*:* from the header.
   - If Safari browser support is required, replace ws://*:* and wss://*:* with relevant 'ws://[hostname]:[port] and wss://[hostname]:[port]' values, where hostname and port are the relevant ones used for accessing the Mobile Server.
3. Restart the Mobile Server.

Log Server

Install Log Server on a separate server with SQL Server **82**

Limit the IP access to Log Server **83**

Install Log Server on a separate server with SQL Server

For very large systems with many transactions to and from the log server's SQL database, Milestone recommends that you install the Log Server component on a separate server with its own SQL Server and store logs in an SQL database on that local SQL Server. If the Log Server is affected by performance issues, for example, due to flooding or other reasons, and uses the same SQL Server as the management server, both services can be affected.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 SC-7 *Boundary Protection*
- NIST SP 800-53 CM-9 *Configuration Management Plan*

Limit the IP access to Log Server

Milestone recommends that only VMS components can contact the Log Server. Log Server uses port 22337.

Learn more

The following control(s) provide additional guidance:

- NIST 800-53 CM-6 *Configuration Settings*
- NIST 800-53 CM-7 *Least Functionality*

Client programs

Client programs

This section provides guidance about how to protect the Milestone client programs.

The client programs are:

- XProtect Smart Client
- XProtect Web Client
- XProtect Management Client
- XProtect Mobile client

Basic steps (all client programs)

Use Windows users with AD **84**

Restrict permissions for client users **84**

Always run clients on trusted hardware on trusted networks **86**

Use Windows users with AD

Milestone recommends that, whenever possible, you use Windows users in combination with Active Directory (AD) to log in to the VMS with the client programs. This enables you to enforce a password policy, and apply user settings consistently across the domain and network. It also provides protection against brute force attacks. For more information, see Use Windows users with Active Directory.

Learn more

The following control(s) provide additional guidance:

- NIST 800-53 CM-6 *Configuration Settings*
- NIST 800-53 SA-5 *Information System Documentation*
- NIST 800-53 SA-13 *Trustworthiness*

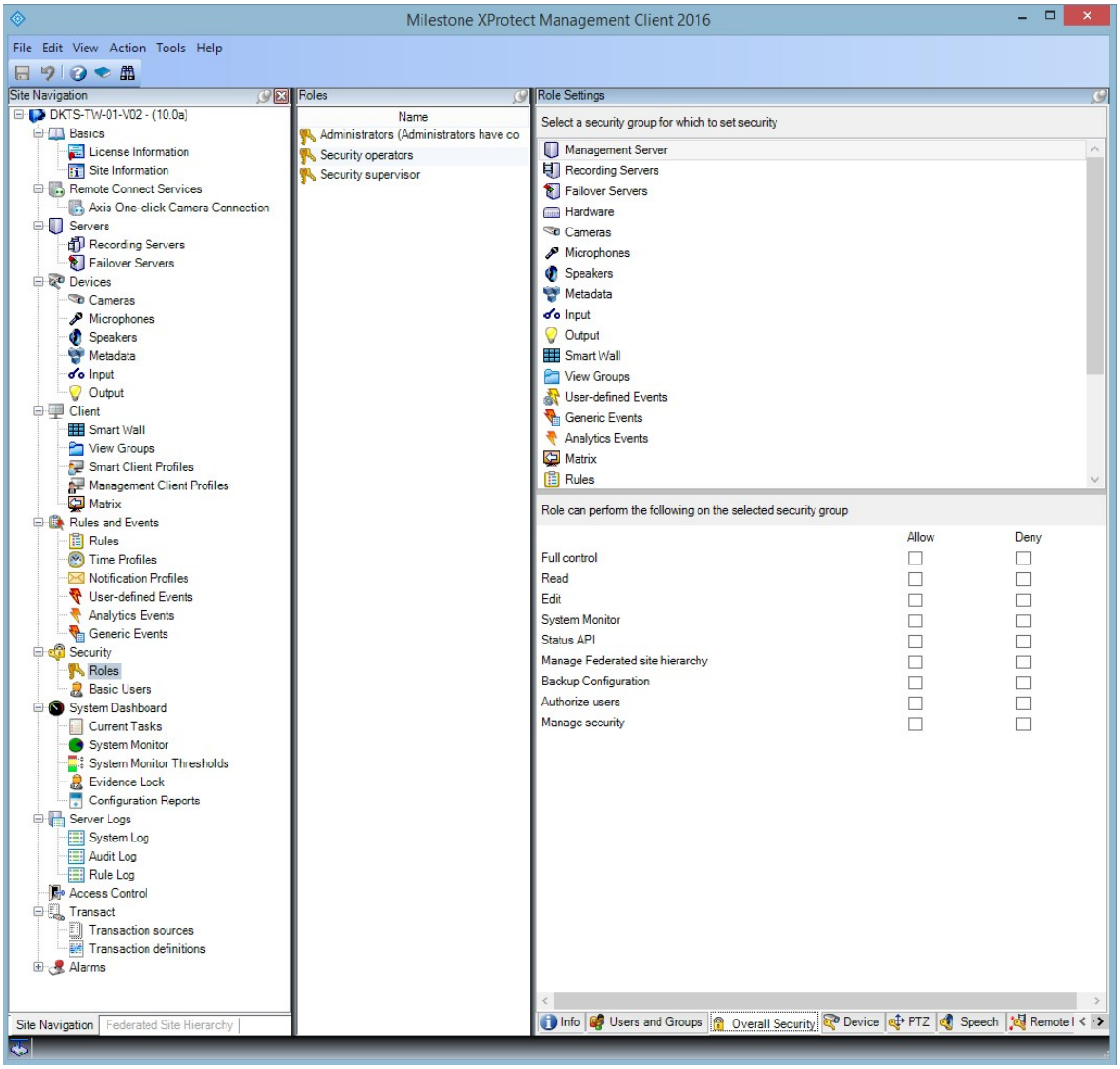
Restrict permissions for client users

Milestone recommends that administrators specify what users can do in Management Client or XProtect Smart Client.

The following instructions describe how to do this. Additional information is available in the Advanced Security Management white paper (https://content.milestonesys.com/media/?mediaId=C5F6BBD5-23E9-4DDD-BE45128071D4F37E).

To restrict client user permissions, follow these steps:

1. Open Management Client.
2. Expand the **Security** node, select **Roles**, and then select the role that the user is associated with.
3. On the tabs at the bottom, you can set permissions and restrictions for the role.



By default, all users associated with the Administrator role have unrestricted access to the system. This includes users who are associated with the Administrator role in AD as well as those with the role of administrator on the management server.

Learn more

The following documents provide additional information:

- NIST 800-53 AC-4 *Least Privilege*
- NIST 800-53 CM-6 *Configuration Settings*
- NIST 800-53 CM-7 *Least Functionality*

Always run clients on trusted hardware on trusted networks

Milestone recommends that you always run XProtect clients on hardware devices with the proper security settings. Specific guidance for mobile devices is available in SP 800-124 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf). These settings are specific to the device.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 SC-7 *Boundary Protection*
- NIST SP800-53 CM-6 *Configuration Settings*

Advanced steps – XProtect Smart Client

Restrict physical access to any computer running XProtect Smart Client **86**

Always use a secure connection by default, particularly over public networks **87**

Activate login authorization **87**

Do not store passwords **90**

Turn on only required client features **91**

Use separate names for user accounts **91**

Prohibit the use of removable media **92**

Restrict physical access to any computer running XProtect Smart Client

Milestone recommends that you restrict physical access to computers running XProtect Smart Client. Allow only authorized personnel to access the computers. For example, keep the door locked, and use access controls and surveillance.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 PE-1 *Physical and Environmental Protection Policy and Procedures*
- NIST SP 800-53 PE-2 *Physical Access Authorizations*
- NIST SP 800-53 PE-3 *Physical Access Control*
- NIST SP 800-53 PE-6 *Monitoring Physical Access*

Always use a secure connection by default, particularly over public networks

If you need to access the VMS with XProtect Smart Client over a public or untrusted network, Milestone recommends that you use a secure connection through VPN. This helps ensure that communication between XProtect Smart Client and the VMS server is protected.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 AC-2 *Account Management*
- NIST SP 800-53 AC-17 *Remote Access*
- NIST SP 800-53 CM-6 *Configuration Settings*

Activate login authorization

Login authorization requires a user to log in on XProtect Smart Client or Management Client, and another user who has an elevated status, such as a supervisor, to provide approval.

You set up login authorization on the roles. Users associated with the role are prompted for a second user (a supervisor) to authorize their access to the system.

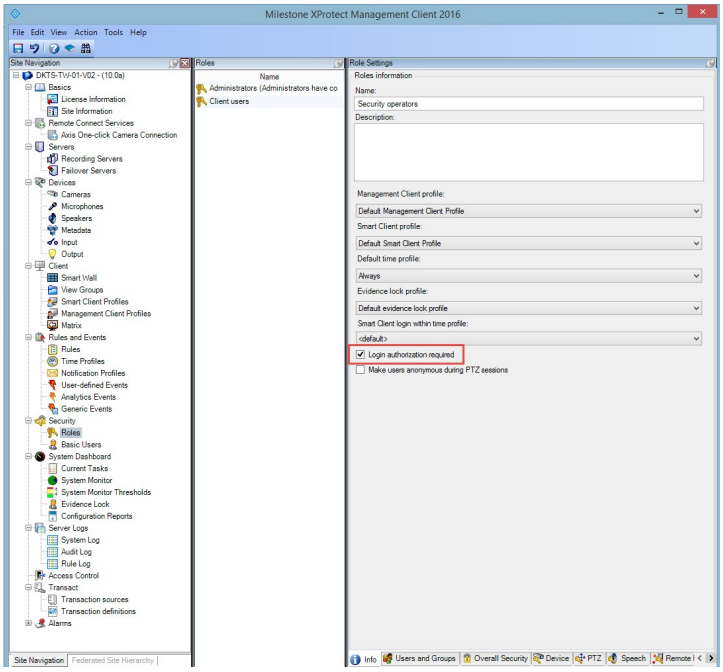


Login authorization is currently not supported by mobile client, and XProtect Web Client, and any Milestone Integration Platform SDK (MIP SDK) integrations.

To turn on login authorization for a role, follow these steps:

1. Open Management Client.
2. Expand the **Security** node, select **Roles**, and then select the relevant role.

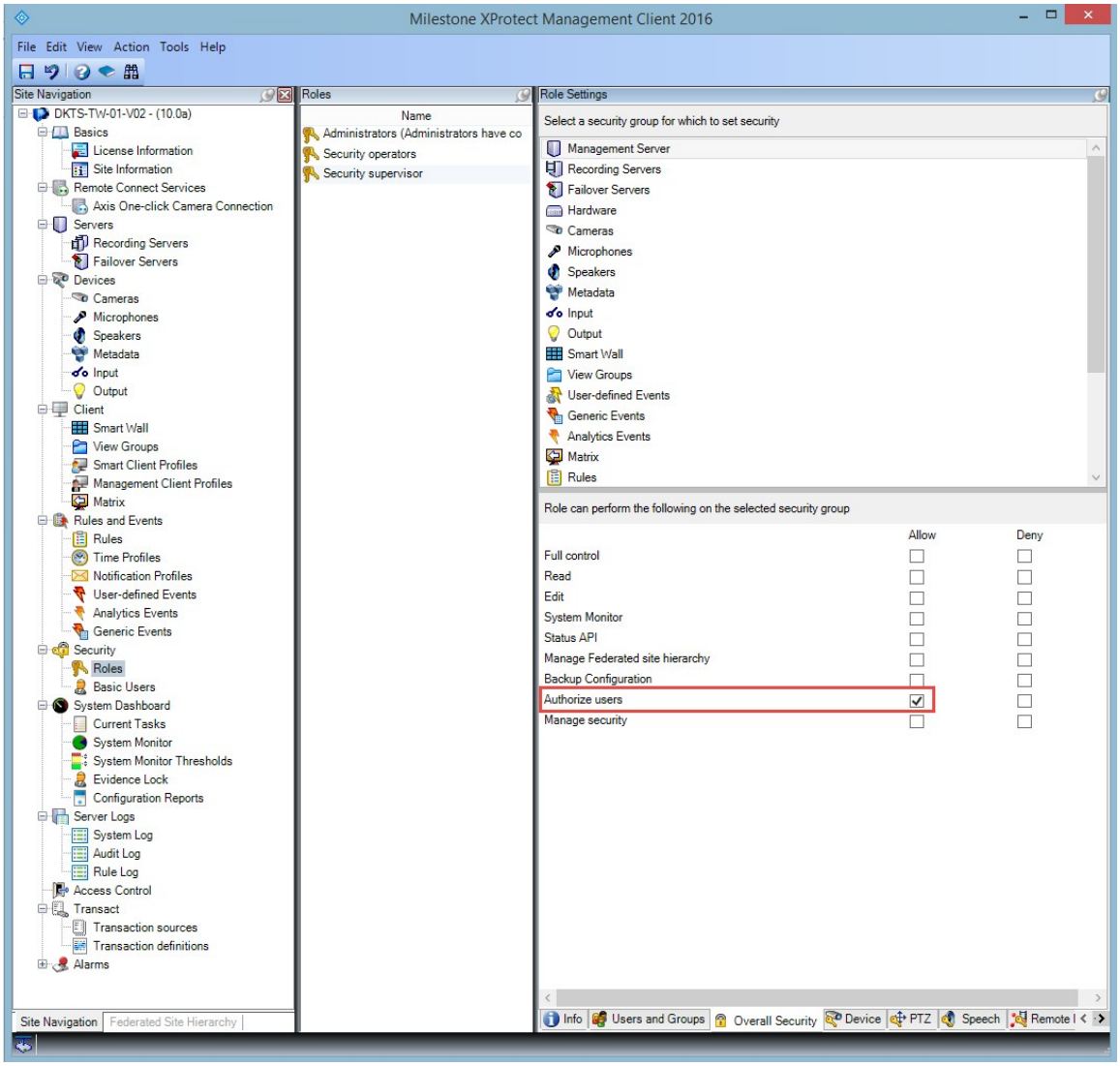
   Select the **Login authorization required** check box.



To configure the roles that authorize and grant access, follow these steps:

1. To create a new role, for example "Security supervisor", expand the **Security** node, right-click **Roles** and create a new role.
2. Click the **Overall Security** tab, and select the **Management Server** node.

   Select the **Allow** check box next to the **Authorize users** check box.



Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 AC-2 *Account Management*
- NIST SP 800-53 AC-6 *Least Privilege*
- NIST SP 800-53 AC-17 *Remote Access*
- NIST SP 800-53 CM-6 *Configuration Settings*

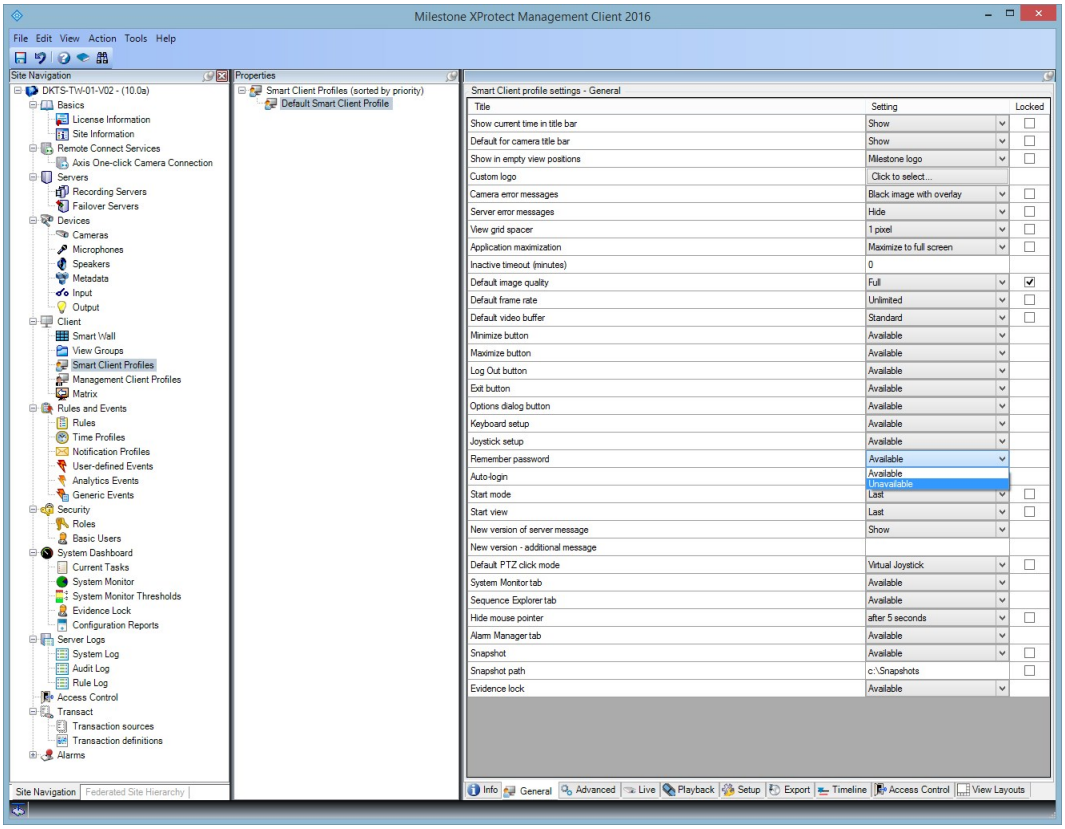
Do not store passwords

XProtect Smart Client provides the option to remember passwords for users. To reduce the risk of unauthorized access, Milestone recommends that you do not use this feature.

To turn off the remember password feature, follow these steps:

1. Open Management Client.
2. Expand the **Client** node, select **Smart Client Profiles**, and then select the relevant Smart Client profile.
3. In the **Remember password** list, select **Unavailable**.

> The **Remember password** option is not available the next time a user with this profile logs into XProtect Smart Client.



Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 AC-2 *Account Management*
- NIST SP 800-53 CM-6 *Configuration Settings*
- NIST SP 800-53 IA-1 *Identification and Authentication Policy and Procedures*

Turn on only required client features

Turn on only required features, and turn off features that a surveillance operator does not need. The point is to limit opportunities for misuse or mistakes.

You can turn on and turn off features in XProtect Smart Client and in XProtect Management Client.

In Management Client, configure Smart Client profiles to specify sets of permissions for users who are assigned to the profile.Smart Client profiles are similar to Management Client profiles, and the same user can be assigned to each type of profile.

To configure a Smart Client profile, follow these steps:

1. Open Management Client.
2. Expand the **Client** node, select **Smart Client Profiles**, and then select the relevant Smart Client profile.
3. Use the tabs to specify settings for features in Smart Client. For example, use the settings on the Playback tab to control features used to investigate recorded video.



Before you assign a user to a Smart Client profile, ensure that the permissions for the user's role are appropriate for the profile. For example, if you want a user to be able to investigate video, make sure that the role allows the user to play back video from cameras, and that Sequence Explorer tab is available on the Smart Client profile.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 AC-2 *Account Management*
- NIST SP 800-53 AC-6 *Least Privilege*
- NIST SP 800-53 CM-6 *Configuration Settings*

Use separate names for user accounts

Milestone recommends that you create a user account for each user, and use a naming convention that makes it easy to identify the user personally, such as their name or initials. This is a best practice for limiting access to only what is necessary, and it also reduces confusion when auditing.

Learn more

The following control(s) provide additional guidance:

- NIST 800-53 AC-4 *Least Privilege*
- NIST 800-53 CM-1 *Configuration Management Policy and Procedures*

- NIST 800-53 CM-2 *Baseline Configuration*
- NIST 800-53 CM-6 *Configuration Settings*
- NIST 800-53 CM-7 *Least Functionality*

Prohibit the use of removable media

For video exports, establish a chain of procedures that are specific to evidence.Milestone recommends that the security policy allows only authorized XProtect Smart Client operators to connect removable storage devices such as USB flash drives, SD cards, and smartphones to the computer where XProtect Smart Client is installed.

Removable media can transfer malware to the network, and subject video to unauthorized distribution.

Alternatively, the security policy can specify that users can export evidence only to a specific location on the network, or to a media burner only. You can control this through the Smart Client profile.

Learn more

The following control(s) provide additional guidance:

- NIST SO 800-53 MP-7 *Media Use*
- NIST SP 800-53 SI-3 *Malicious Code Protection*

Advanced steps – XProtect Mobile client

SP 800-124 revision 1 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf) provides guidance that is specifically for mobile devices. The information it contains applies to all topics in this section.

Always use the XProtect Mobile client on secure devices **92**

Download the XProtect Mobile client from authorized sources **93**

Mobile devices should be secured **93**

Always use the XProtect Mobile client on secure devices

Milestone recommends that you always use the XProtect Mobile client on secure devices that are configured and maintained according to a security policy. For example, ensure that mobile devices do not allow users to install software from unauthorized sources. An enterprise app store is one example of a way to constrain device applications as part of overall mobile device management.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 SC-7 *Boundary Protection*
- NIST SP800-53 CM-6 *Configuration Settings*

Download the XProtect Mobile client from authorized sources

Milestone recommends that you download the XProtect Mobile client from one of these sources:

- Google Play Store
- Apple App Store
- Microsoft Windows Store.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 SC-7 *Boundary Protection*
- NIST SP 800-53 CM-6 *Configuration Settings*

Mobile devices should be secured

If you want to access the VMS with a mobile device over a public or untrusted network, Milestone recommends that you do so with a secure connection, use proper authentication and Transport Layer Security (TLS) (https://datatracker.ietf.org/wg/tls/charter/) (or connect through VPN (https://datatracker.ietf.org/wg/ipsec/documents/)) and HTTPS. This helps protect communications between the mobile device and the VMS.

Milestone recommends that mobile devices use screen-lock. This helps prevent unauthorized access to the VMS, for example, if the smart phone is lost. For maximum security, implement a security policy to prohibit the XProtect Mobile client from remembering the user name and password.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 AC-2 *Account Management*
- NIST SP 800-53 AC-17 *Remote Access*
- NIST SP 800-53 CM-6 *Configuration Settings*

Advanced steps – XProtect Web Client

Always run XProtect Web Client on trusted client computers **93**

Use certificates to confirm the identity of XProtect Mobile server **94**

Use only supported browsers with the latest security updates **94**

Always run XProtect Web Client on trusted client computers

Always securely connect all components of the VMS. Server-to-server and client-to-server connections should use proper authentication and Transport Layer Security (TLS) (https://datatracker.ietf.org/wg/tls/charter/) (or connect through VPN (https://datatracker.ietf.org/wg/ipsec/documents/)) and HTTPS. Always run XProtect Web

Client on trusted computers, for example, do not use a client computer in a public space.Milestone recommends that you educate users about the security measures to remember when using browser-based applications, such as XProtect Web Client. For example, make sure they know to disallow the browser from remembering their password.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 AC-2 *Account Management*
- NIST SP 800-53 CM-6 *Configuration Settings*
- NIST SP 800-53 IA-2 *Identification and Authentication*

Use certificates to confirm the identity of XProtect Mobile server

This document emphasizes the use of the latest TLS. With that comes the need for the proper use of certificates and the implementation of the TLS cipher suite.Milestone recommends that you install a certificate on the XProtect Mobile server to confirm the identity of the server when a user tries to connect through XProtect Web Client.

For more information, see the certificates guide about how to secure your XProtect VMS installations.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 AC-2 *Account Management*
- NIST SP 800-53 CM-6 *Configuration Settings*
- NIST SP 800-53 IA-2 *Identification and Authentication*

Use only supported browsers with the latest security updates

Milestone recommends that you install only one of the following browsers on client computers. Make sure to include the latest security updates.

- Apple Safari
- Google Chrome
- Microsoft Edge
- Mozilla Firefox

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 CM-1 *Configuration Management Policy and Procedures*
- NIST SP 800-53 CM-2 *Baseline Configuration*
- NIST SP 800-53 CM-6 *Configuration Settings*
- NIST SP 800-53 PL-8 *Information Security Architecture*
- NIST SP 800-53 SI-3 *Malicious Code Protection*

Advanced steps – Management Client

Use Management Client profiles to limit what administrators can view **95**

Allow administrators to access relevant parts of the VMS **95**

Run the Management Client on trusted and secure networks **96**

Use Management Client profiles to limit what administrators can view

Milestone recommends that you use Management Client profiles to limit what administrators can view in the Management Client.

Management Client profiles allow system administrators to modify the Management Client user interface. Associate Management Client profiles with roles to limit the user interface to represent the functionality available for each administrator role.

Display only the parts of the VMS that administrators need to perform their duties.

Learn more

The following control(s) provide additional guidance:

- NIST 800-53 AC-4 *Least Privilege*
- NIST 800-53 CM-1 *Configuration Management Policy and Procedures*
- NIST 800-53 CM-2 *Baseline Configuration*
- NIST 800-53 CM-6 *Configuration Settings*
- NIST 800-53 CM-7 *Least Functionality*

Allow administrators to access relevant parts of the VMS

If you have a setup that requires multiple administrators, Milestone recommends that you configure different administrator permissions for administrators who use the Management Client.

To define administrator permissions, follow these steps:

1. In Management Client, expand the **Security** node, select **Roles**, and then select the relevant administrator role.

   You cannot modify the built-in administrator role, so you must create additional administrator roles.
2. On the **Overall Security** tab, specify the actions that the administrator can take for each security group.
3. On the other tabs, specify the security settings for the role in the VMS.

   For more information, see the administrator manual for XProtect VMS.
4. On the **Info** tab, associate the role with a Management Client profile.

> You can turn on or turn off features by using the Management Client profile. Before you assign a user to a Management Client profile, ensure that the permissions for the user's role are appropriate for the profile. For example, if you want a user to be able to manage cameras, make sure that the role allows the user to do this, and that cameras are enabled on the Management Client profile.

Learn more

The following control(s) provide additional guidance:

- NIST 800-53 AC-4 *Least Privilege*
- NIST 800-53 CM-1 *Configuration Management Policy and Procedures*
- NIST 800-53 CM-2 *Baseline Configuration*
- NIST 800-53 CM-6 *Configuration Settings*
- NIST 800-53 CM-7 *Least Functionality*

Run the Management Client on trusted and secure networks

If you access the Management Server with Management Client over HTTP, the plain text communication can contain unencrypted system details.Milestone recommends that you run the Management Client only on trusted and known networks. Use a VPN to provide remote access.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 AC-2 *Account Management*
- NIST SP 800-53 CM-6 *Configuration Settings*
- NIST SP 800-53 IA-2 *Identification and Authentication*

Compliance

FIPS 140-2 compliance

This section discusses FIPS 140-2 and how to configure and use XProtect VMS to operate in FIPS 140-2 compliant mode.

The terms "FIPS 140-2 compliant" and "FIPS 140-2 compliant mode" are not legally binding. The terms are used here for clarity.

FIPS 140-2 compliant means that software uses FIPS 140-2-validated instances of algorithms and hashing functions in all instances in which encrypted or hashed data is imported to or exported from the software. Additionally, this means that software will manage keys in a secure manner, as is required of FIPS 140-2-validated cryptographic modules. The key management process also includes both key generation and key storage.

FIPS 140-2 compliant mode refers to software that contains both FIPS-approved and non-FIPS approved security methods, where the software has at least one "FIPS mode of operation". This mode of operation only allows for the operation of FIPS-approved security methods. This means that when the software is in the "FIPS mode", a non-FIPS approved method is not used in lieu of the FIPS approved method.

The following topics are discussed.

What is FIPS? **97**

What is FIPS 140-2? **98**

Which XProtect VMS applications can operate in a FIPS 140-2 compliant mode? **98**

How to ensure XProtect VMS can operate in FIPS 140-2 compliant mode? **98**

Considerations regarding upgrade **99**

Verify third-party integrations **100**

Connect devices: background **100**

Media database: Considerations regarding backward compatibility **101**

FIPS Group Policy on the Windows operating system **106**

Install XProtect VMS **107**

Encrypt hardware detection passwords **107**

What is FIPS?

Federal Information Processing Standards (FIPS) are a family of standards developed by the following two government bodies:

- The National Institute of Standards and Technology (NIST) in the United States
- The Communications Security Establishment (CSE) in Canada

These standards aim at ensuring computer security and interoperability.

All software solutions deployed in government and highly regulated industries in the United States and Canada are required to comply with FIPS 140-2.

What is FIPS 140-2?

FIPS 140-2, titled "Security Requirements for Cryptographic Modules," specifies which encryption algorithms and which hashing algorithms can be used and how encryption keys are to be generated and managed.

The security requirements specified in this standard are intended to maintain the security provided by a cryptographic module, but conformance to this standard is not sufficient to ensure that a particular module is secure. The operator of a cryptographic module is responsible for ensuring that the security provided by the module is sufficient and acceptable to the owner of the information that is being protected, and that any residual risk is acknowledged and accepted.

Which XProtect VMS applications can operate in a FIPS 140-2 compliant mode?

As of XProtect VMS 2020 R3, all encryption algorithms have been replaced with Microsoft's Cryptography API: Next Generation (CNG), which adheres to the latest security technologies available and is FIPS compliant. That is, all XProtect VMS 2020 R3 applications can operate in FIPS compliant mode.

For the sake of backward compatibility, some non-compliant algorithms and processes persist in XProtect VMS, even after version 2020 R3, but this does not affect the ability to operate the system in FIPS compliant mode.

Is XProtect VMS always FIPS compliant?

No. Some non-compliant algorithms and processes persist in XProtect VMS. But, XProtect VMS can be configured and operate so that it uses only the FIPS 140-2 certified algorithm instances and thereby operate in a FIPS compliant mode.

Should you enable FIPS 140–2 mode?

Before enabling the FIPS 140–2 mode it is necessary to understand whether you need it or not. For instance, if you are working and connected to a US or Canadian government network and infrastructure, then it is mandatory to comply with FIPS 140–2 and enable it on your computer for communication as per the standard. Furthermore, enabling FIPS 140–2 mode on your Windows operating system restricts many programs and services from running, since only FIPS-approved algorithms and services will be supported after that. Therefore, it is advised to check whether there is a necessity or not.

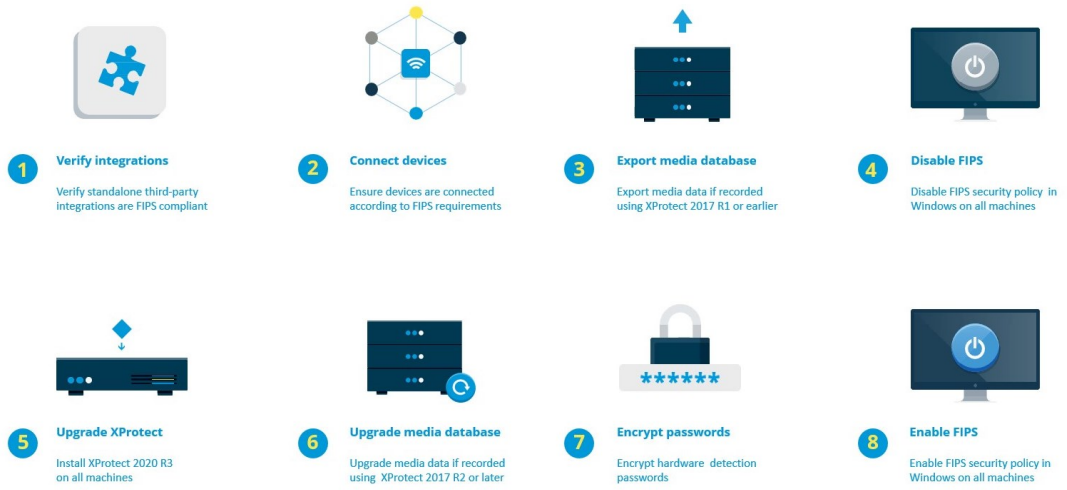
How to ensure XProtect VMS can operate in FIPS 140-2 compliant mode?

In order to operate XProtect VMS in a FIPS 140-2 mode of operation you must:

- Ensure third-party integrations can operate on a FIPS enabled Windows operating system (see Verify third-party integrations on page 100)
- Connect to devices in a way that ensures a FIPS 140-2 compliant mode of operation (see Connect devices: background on page 100)
- Ensure that data in the media database is encrypted with FIPS 140-2 compliant algorithms (see Media database: Considerations regarding backward compatibility on page 101)
- Run Windows operating system in FIPS 140-2 approved mode of operation. See the Microsoft site for information on enabling FIPS.

Considerations regarding upgrade

Upgrading to XProtect VMS 2020 R3 to operate in FIPS compliant mode requires a unique upgrade process. This upgrade process is required only by existing XProtect VMS users who must operate in a FIPS compliant mode.



The upgrade process depends on which version of XProtect VMS you are upgrading from.

Recommended upgrade process for customers running XProtect VMS

1. Start investigation whether third-party integrations are FIPS 140-2 compliant (see Verify third-party integrations on page 100).
2. Prepare device connections to be FIPS 140-2 compliant (see Connect devices: background on page 100).
3. Export recordings made with XProtect VMS versions that are older than 2017 R2 (see Media database: Considerations regarding backward compatibility on page 101).

   This applies to customers who have encrypted or signed recordings at any point in time.
4. Disable FIPS on the Windows operating system (see FIPS Group Policy on the Windows operating system on page 106).

5. Install XProtect VMS (see Install XProtect VMS on page 107).
6. Upgrade the recordings in the media database that are made with XProtect VMS 2019 R3 or earlier (see Media database: Considerations regarding backward compatibility on page 101).
7. Update the encryption of hardware discovery passwords (see Encrypt hardware detection passwords on page 107).
8. Enable FIPS on the Windows operating system and restart all of the computers with XProtect VMS installed.

   > Do not enable FIPS until all of the computers in the XProtect VMS network, including XProtect Smart Client workstations, are prepared for FIPS.

Verify third-party integrations

If an integration is not FIPS 140-2 compliant, it cannot run on a Windows operating system with the FIPS Group Policy flag enabled.

In addition, because of changes made to the MIP SDK in relation to FIPS, integrations that access the feature list in the license must be recompiled.

In order to ensure that the integrations will still work after upgrading to XProtect VMS 2020 R3, you must:

- Make an inventory of all your integrations to XProtect VMS
- Contact the providers of these integrations and ask if the integrations are FIPS 140-2 compliant and whether they foresee that the integrations need to be changed due to the MIP SDK updates
- Deploy the FIPS 140-2 compliant integrations to XProtect VMS after the VMS has been updated

Connect devices: background

If you want to operate XProtect VMS in a FIPS compliant mode, you must make sure that the drivers, and hence the communication to the devices, also adhere to FIPS compliance.

The Milestone XProtect VMS device drivers can be FIPS 140-2 compliant because they can be configured and operate so that they use only FIPS 140-2 compliant algorithm instances. Only specific drivers in a specific configuration are FIPS 140-2 compliant. In this specific FIPS 140-2 configuration the driver will be able to communicate with devices in a compliant way. The devices must fulfill several requirements in order to be able to accept this communication. In addition, the FIPS Group Policy flag must be enabled in Windows on the server where the recording server is installed. When the FIPS Group Policy flag is enabled, the FIPS 140-2 capable drivers will operate in compliant mode and will not use non-approved cryptographic primitives. The drivers will use the algorithms used only for secured channels of communication.

Device connectivity requirements

XProtect VMS is guaranteed and can enforce FIPS 140-2 compliant mode of operation if the following criteria are met:

- Devices use only drivers from the list (Supported drivers on page 108) to connect to XProtect VMS

  This list shows drivers that can assure and enforce compliance.

- Devices use device pack version 11.1 or higher

  Drivers from the legacy driver device packs cannot guarantee a FIPS 140-2 compliant connection.

- Devices are connected over HTTPS and on either Secure Real-Time Transport Protocol (SRTP) or Real Time Streaming Protocol (RTSP) over HTTPS for the video stream

  > Driver modules cannot guarantee FIPS 140-2 compliance of a connection over HTTP. The connection may be compliant, but there is no guarantee that it is in fact compliant.

- The computer that is running the recording server must have the FIPS Group Policy flag enabled in Windows

Effects of operating in FIPS 140-2 compliant mode

When operating in FIPS 140-2 compliant mode, some drivers will be unavailable for use. Drivers which are listed as FIPS 140-2 might not be able to connect to devices that do not fulfill the device requirements.

A driver is FIPS 140-2 compliant and the communication with the device is FIPS 140-2 compliant if the FIPS 140-2 capable driver:

- Operates in an environment with the FIPS Group Policy enabled
- Is connected to a device that fulfills the device requirements (see Device requirements on page 108)
- Is configured properly (see How to configure the device and the driver for FIPS 140-2 on page 109)

If any of the requirements for FIPS 140-2 compliant mode are not fulfilled, then there is no guarantee about the FIPS 140-2 compliancy of the driver or the communication with the device. See Drivers and FIPS 140-2 on page 108 for more information.

Devices running over Milestone Open Network Bridge

When running on a computer that has the FIPS Group Policy flag enabled in Windows, the Milestone Open Network Bridge uses SHA-256 as a hashing algorithm. On a computer that does not have FIPS enabled, then you can select either MD5 or SHA-256 for hashing.

Media database: Considerations regarding backward compatibility

It is possible to have recordings in the same storage from several different versions of XProtect VMS at the same time.

Data that is signed or encrypted must be:

- Exported from the storage if it was recorded with XProtect VMS version 2017 R1 or older

  Data export is done by using the XProtect Smart Client.

- Upgraded, if it was recorded with XProtect VMS version 2017 R2 or newer

  Data upgrade is done in collaboration with Milestone Support, using a media conversion tool provided by Milestone Support.

  > The FIPS Group Policy flag must be disabled on the Windows operating system for the media conversion tool to run.

  > The recording server must also be stopped while the media conversion tool is running, and there are no recordings being made while the tool is running.

Media upgrade depending on XProtect VMS version

- Data recorded with XProtect VMS version 2017 R1 and earlier

  Encrypted media data that was recorded with XProtect VMS 2017 R1 and earlier is not available if enabling FIPS, even if the media conversion tool has been run.

  Export the media data that was recorded with XProtect VMS 2017 R1 and earlier to access it offline.

  See Media database data upgrade: XProtect VMS 2017 R1 and earlier on page 105.

- Data recorded with XProtect VMS version 2017 R2 to 2019 R3

  Media data that was recorded with XProtect VMS versions 2017 R2 to 2019 R3 will not automatically be re-encrypted. Conversion can be time consuming and should be planned in advance.

  To get older data updated to use FIPS compliant algorithms, contact Milestone support to get the media conversion tool.

  See Media database upgrade: XProtect VMS 2017 R2 to XProtect VMS 2019 R3 on page 105.

- Data recorded with XProtect VMS version 2020 R1 or 2020 R2

  Media data that was recorded with XProtect VMS 2020 R1 or 2020 R2 will automatically be re-encrypted with FIPS 140-2 compliant algorithms when the recording server is started after an upgrade. See Media database upgrade: XProtect VMS 2020 R1 or XProtect VMS 2020 R2 on page 106.

Media upgrade details

Re-encrypting the data with a recording server with FIPS compliant algorithms is a central part of the upgrade process. Therefore, the upgrade process varies, based on the version of XProtect VMS used for recording that data.

<table>
<tr><th colspan="5">Data recorded with</th></tr>
<tr><th></th><th>2017 R1 and earlier</th><th>2017 R2 - 2019 R3</th><th>2020 R1 - 2020 R2</th><th>2020 R3 and later</th></tr>
<tr><td>Changes</td><td>Data encrypted with DES
Signing using MD5
Passwords:
Cookie in storage CONFIG.XML
Password _a & _b in table CONFIG.XML's
DES encrypted</td><td>Data encrypted with AES
Signing using SHA</td><td>Password list in storage CONFIG.XML
Passwords in password list are DES encrypted</td><td>Passwords in password list are encrypted using AES
A media conversion tool is available for updating table CONFIG.XML's from having password _a & _b, to use updated password list</td></tr>
<tr><td>FIPS disabled</td><td colspan="4">All functionality works as expected</td></tr>
<tr><td>FIPS enabled
Signed data</td><td>Signed data can playback
Verify signing during export fails</td><td colspan="3">Signed data can be played back
Verify signing during export works</td></tr>
<tr><td>FIPS enabled
Encrypted data
Media conversion tool not run</td><td colspan="3">Storage stays offline
(Storage may stay offline if encryption was ever enabled for storage)</td><td>All functionality works as expected</td></tr>
</table>

<table>
<tr><th colspan="5">Data recorded with</th></tr>
<tr><th></th><th>2017 R1 and earlier</th><th>2017 R2 - 2019 R3</th><th>2020 R1 - 2020 R2</th><th>2020 R3 and later</th></tr>
<tr><td>FIPS enabled
No encryption
Media conversion tool not run</td><td colspan="4">All functionality works as expected</td></tr>
<tr><td>Media conversion tool has run</td><td colspan="2">Media conversion tool may require a lot of time to run because it updates table CONFIG.XML's for all encrypted tables</td><td>Media conversion tool runs fast because it only needs to update storage CONFIG.XML</td><td>Media conversion tool runs fast because no update is needed</td></tr>
<tr><td>FIPS enabled
Encrypted data
Media conversion tool has run</td><td>Encrypted data is not available
Connection lost on playback
Archiving with Reduce to key-frames archives entire GoP</td><td colspan="3">Encrypted data can be played back
Archiving with Reduce to key-frames works as expected</td></tr>
<tr><td>FIPS enabled
No encryption
No signing
Media conversion tool has run</td><td colspan="4">All functionality works as expected</td></tr>
</table>

Media database data upgrade: XProtect VMS 2017 R1 and earlier

If you are running XProtect VMS version 2017 R1 or earlier or if you have signed or encrypted data recorded with these versions, the recordings are encrypted with algorithms that are not considered secure by the FIPS 140-2 standard.

It is not possible to access these recordings from a computer where the FIPS Group Policy flag is enabled.

As a consequence, it is required to export the media database to a location where it can still be accessed.

Media database upgrade: XProtect VMS 2017 R2 to XProtect VMS 2019 R3

If you are running a version of XProtect VMS between XProtect VMS 2017 R2 and XProtect VMS 2019 R3 and if at any point in time encryption has been enabled in the media database, in order to access these recordings you must do one of the following options.



Both options require the use of the media conversion tool. The recording server must be stopped while the media conversion tool is running, and there are no recordings being made while the tool is running. See What is the media conversion tool? on page 105 for more information.

- Option 1

  Use this option to be able to operate in a FIPS environment immediately, and if you have a long retention time. The time required to run the media conversion tool could be significant.

  1. Upgrade XProtect VMS to 2020 R3.
  2. With FIPS disabled on the Windows operating system, run the media conversion tool that is provided by Milestone support.
  3. Enable the FIPS Group Policy flag on the Windows operating system.

- Option 2

  Use this option if operating in a FIPS environment can wait, if you have a short retention time, and if you are running the media conversion tool on less data.

  1. Upgrade XProtect VMS to 2020 R3.
  2. Run the XProtect VMS through the retention time without enabling FIPS on the Windows operating system.
  3. Run the media conversion tool to ensure that all the data is converted to be FIPS compliant.
  4. Enable the FIPS Group Policy flag on the Windows operating system.

What is the media conversion tool?

The media conversion tool is a stand-alone PowerShell script, that is delivered in source. It is not part of any installation.

It is to be distributed to customers only through Milestone support.

It can convert all storage in bulk, or it can be run on a specific storage.

Progress indicators show how far the tool has gotten.

If the conversion takes too long, you can cancel the job and continue without FIPS enabled.

The media conversion tool converts encrypted credentials inside existing media table files to the newest format that is FIPS compatible.

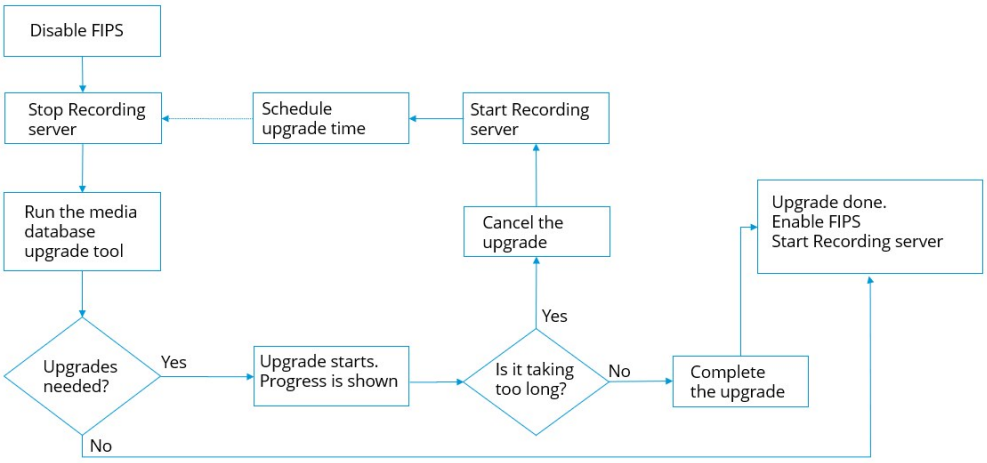
The media conversion tool does not change the encryption of the video data itself. If the video data is encrypted with a non-compliant algorithm (DES), the updated tables will load, but video will be inaccessible in FIPS compliant mode.

The media conversion tool converts and checks if all tables are using FIPS compliant algorithms.

Approved tables will be marked to eliminate them from being checked by media conversion tool again.

After running the media conversion tool, the XProtect VMS 2020 R3 will be able to load tables in FIPS compliant mode.

Media conversion tool workflow



Media database upgrade: XProtect VMS 2020 R1 or XProtect VMS 2020 R2

If you are running XProtect VMS version 2020 R1 or XProtect VMS 2020 R2, media data that is recorded with one of these versions will be automatically re-encrypted with FIPS 140-2 compliant algorithms during the recording server upgrade.

FIPS Group Policy on the Windows operating system

FIPS mode of operation is enabled and disabled with the FIPS Group Policy flag on the Windows operating system. See the Microsoft site for information on enabling and disabling FIPS.

Before you upgrade, you must disable the FIPS Group Policy flag on all the computers that are part of the XProtect VMS, including the computer that hosts the SQL Server and all XProtect Smart Client workstations.

There are two reasons why the FIPS Group Policy flag must be disabled on all computers in the XProtect VMS before you upgrade:

- During the upgrade, data that is encrypted with non-approved FIPS algorithms is re-encrypted with approved algorithms. In order to run the decryption on the Windows operating system, the FIPS Group Policy flag must be disabled.
- If the FIPS Group Policy flag is enabled in Windows, you will not be able to use the XProtect VMS until all components are upgraded. For example, a 2020 R2 XProtect Smart Client will not be able to communicate with a 2020 R3 Management Server if the Management Server is on a computer that has the FIPS Group Policy flag enabled.

FIPS Group Policy and Milestone Federated Architecture

If any site in a Milestone Federated Architecture must operate with the FIPS Group Policy flag enabled in Windows, then all of the sites must also operate with the FIPS Group Policy flag enabled in Windows.

In consequence, the entire Milestone Federated Architecture installation must be upgraded to version 2020 R3.

Install XProtect VMS

When you upgrade, the XProtect VMS installer will check the FIPS security policy and will prevent the upgrade from starting if FIPS is enabled.

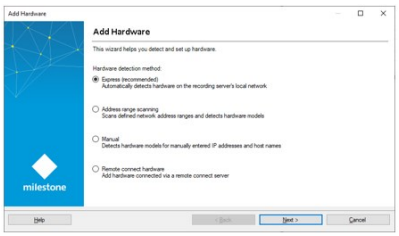
Encrypt hardware detection passwords

The hardware detection passwords must be updated after you upgrade to XProtect VMS 2020 R3.

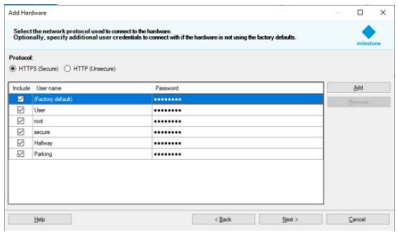
The encryption of the hardware detection passwords is not updated during upgrade from earlier version of XProtect VMS. But, these passwords cannot be read if the FIPS Group Policy flag is enabled in Windows.

You must trigger a conversion of these passwords before you enable FIPS. Do the following:

1. Make sure the FIPS Group Policy flag is disabled in Windows.
2. In XProtect Management Client, open the **Add Hardware** wizard.



3. Select the detection method to open the hardware detection page.



This triggers the re-encryption of the hardware detection passwords with FIPS-compliant algorithms.

The credentials are now encrypted with FIPS-compliant algorithms.

Drivers and FIPS 140-2

This section discusses FIPS 140-2 and how to configure and use the Milestone drivers to operate in FIPS 140-2-compliant mode.

Requirements for FIPS 140-2 compliant mode

The Milestone XProtect VMS device drivers can be FIPS 140-2 compliant because they can be configured and operate so that they use only FIPS 140-2 compliant algorithm instances. Only specific drivers in a specific configuration are FIPS 140-2 compliant. In this specific FIPS 140-2 configuration the driver will be able to communicate with devices in a compliant way. The devices must fulfill several requirements in order to be able to accept this communication. In addition, the FIPS Group Policy flag must be enabled in Windows on the server where the recording server is installed. When the FIPS Group Policy flag is enabled, the FIPS 140-2 capable drivers will operate in compliant mode and will not use non-approved cryptographic primitives. The drivers will use the algorithms used only for secured channels of communication.

Device requirements

For a device to be able to communicate with a driver running in FIPS 140-2 compliant mode it must fulfill all of these:

- The device must support HTTPS communication with at least one FIPS 140-2 compliant cipher suite (for examples see Example of FIPS 140-2 compliant cipher suites on page 114)
- The device must support RTSP over HTTPS (Tunneling RTSP and RTP over HTTP) using HTTP Basic Authentication (RFC2068 Section 11.1) or HTTP Digest Authentication (RFC2069, RFC7616)

  or

  The device must support media streaming using SRTP and RTSPS (RFC3711)

Supported drivers

Currently only a subset of drivers is FIPS 140-2 compliant. These drivers support communication through a secured channel for all available features.

Axis 1 channel	Axis 1 channel PTZ	Axis 2 channel	Axis 3 channel
Axis 4 channel	Axis 8 channel	Axis 11 channel	Axis 12 channel
Axis Audio	Bosch PTZ	Bosch 1 channel	Bosch 2 channel
Bosch 3 channel	Bosch 16 channel	Bosch X20XF	Bosch X40XF
Canon 1 channel	Canon 1 channel PTZ	Canon VBM	Canon VBM 40
Canon VBS	Canon VBS No Ptz	Digital Barriers TVI Decoder	Hanwha Generic
ONVIF	ONVIF16	Universal	Universal 16 channel
Universal 64 channel	VideoPush		

The drivers in the table are capable of running in FIPS 140-2 compliant mode when configured properly. This list is not final and may expand in the future. Some drivers are FIPS 140-2 compliant with limited capabilities. Refer to specific driver sections below for information on how to configure them and any limitations.

FIPS 140-2 compliant mode for drivers is available since Device Pack 11.1.

Effects of running in FIPS 140-2 compliant mode

When operating in FIPS 140-2 compliant mode, some drivers will be unavailable for use. Drivers which are listed as FIPS 140-2 might not be able to connect to devices that do not fulfill the device requirements.

A driver is FIPS 140-2 compliant and the communication with the device is FIPS 140-2 compliant if the FIPS 140-2 capable driver:

- Operates in an environment with the FIPS Group Policy enabled
- Is connected to a device that fulfills the device requirements (see Device requirements on page 108)
- Is configured properly (see How to configure the device and the driver for FIPS 140-2 on page 109)

If any of the requirements for FIPS 140-2 compliant mode are not fulfilled, then there is no guarantee about the FIPS 140-2 compliancy of the driver or the communication with the device.

How to configure the device and the driver for FIPS 140-2

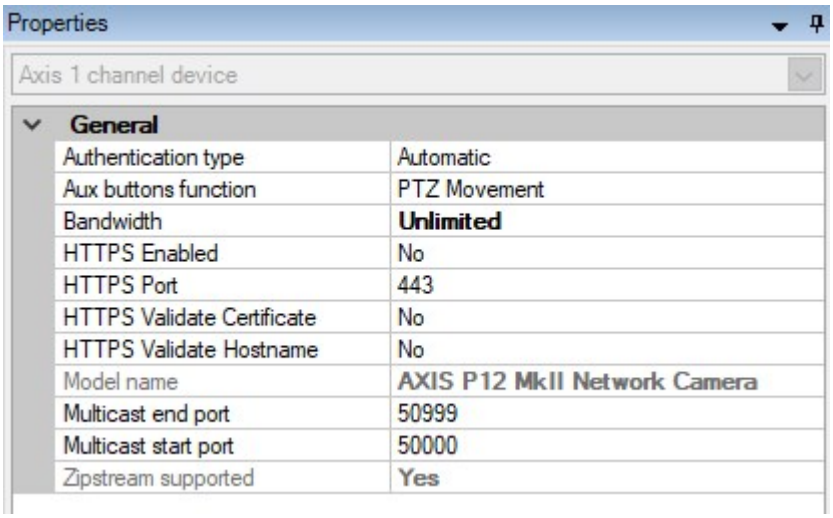
The configuration of the device and driver for FIPS 140-2 compliant mode is device and driver specific. Some general guidelines apply:

- The communication channels between the driver and the device must be secure and encrypted (HTTPS, RTSP over HTTPS, SRTP).
- The device must be configured for operation using secure channels.
- The driver and device must be configured to use secure channels for communication in XProtect VMS.

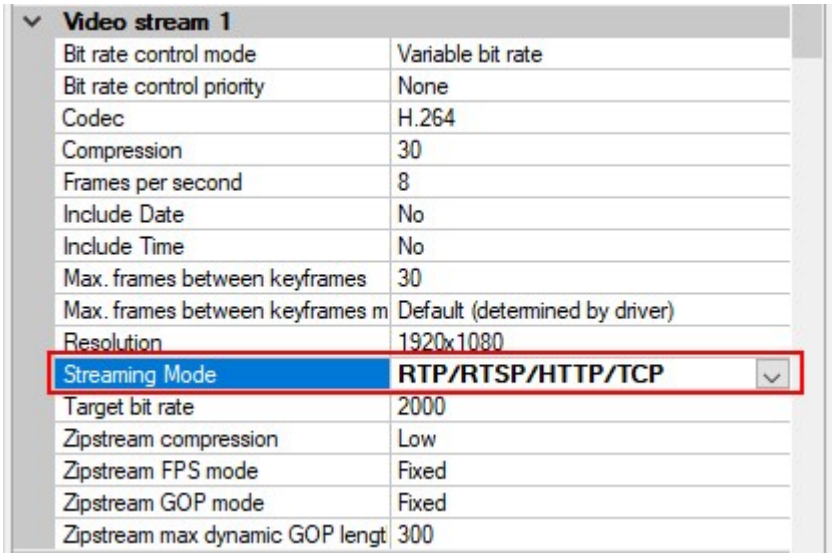
Axis drivers

Do the following:

- Set **HTTPS Enabled** to **Yes**.
- Set **HTTPS Validate Certificate** to **Yes**.
- Set **HTTPS Validate Hostname** to **Yes**.

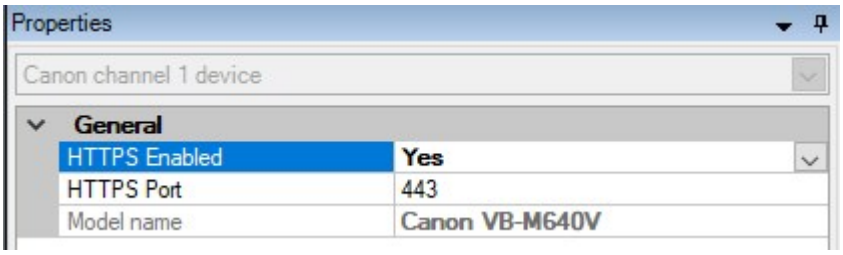


- For every enabled media channel and media stream, set **Streaming Mode** to **RTP/RTSP/HTTP/TCP**.

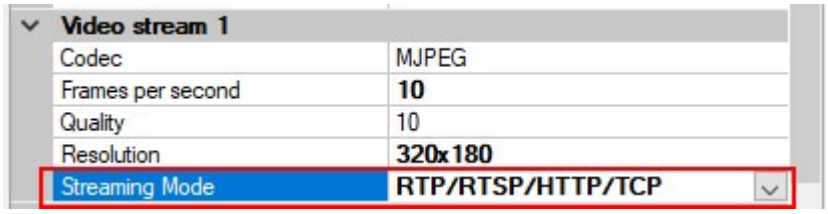


Canon drivers

- Set the **HTTPS Enabled** to **Yes**.



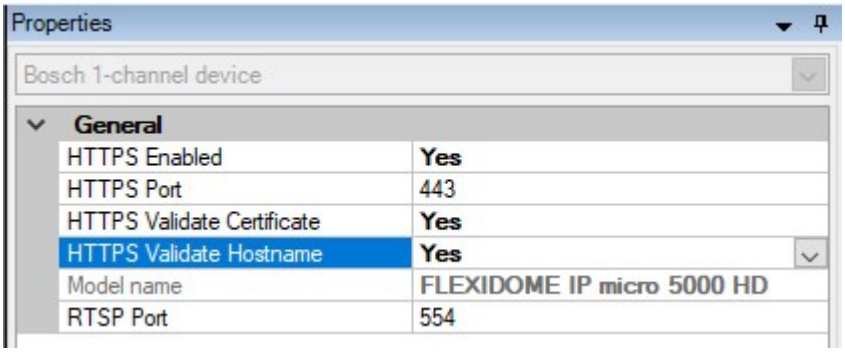
- For every enabled media channel and media stream, set **Streaming Mode** to **RTP/RTSP/HTTP/TCP**.



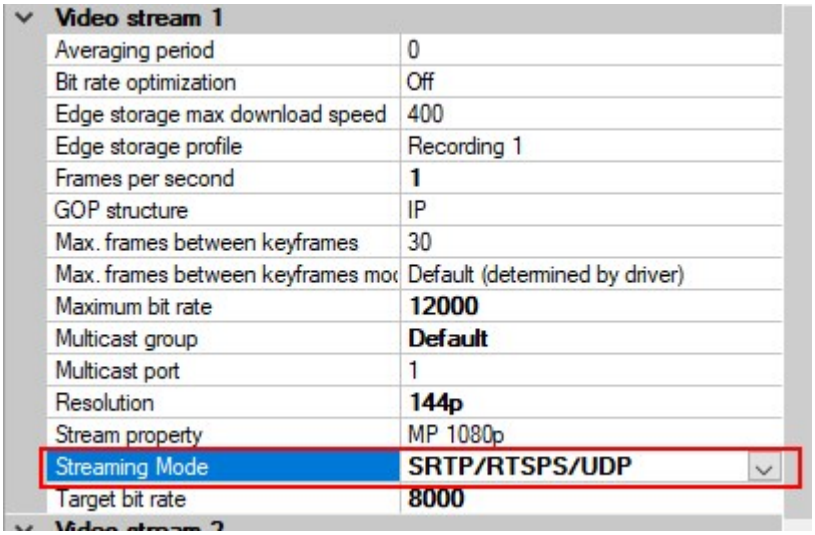
Bosch drivers

Do the following:

- Set **HTTPS Enabled** to **Yes**.
- Set **HTTPS Validate Certificate** to **Yes**.
- Set **HTTPS Validate Hostname** to **Yes**.

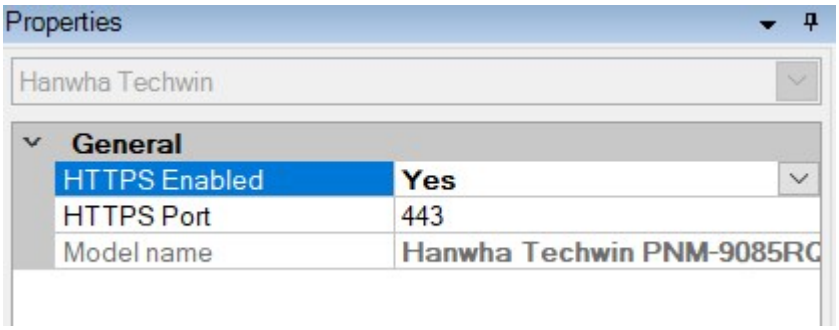


- For every enabled media channel and media stream, set **Streaming Mode** to one of the following:
  - **RTP/RTSP/HTTP/TCP**
  - **SRTP/RTSPS/UDP**
  - **SRT/RTSPS/UDP multicast**

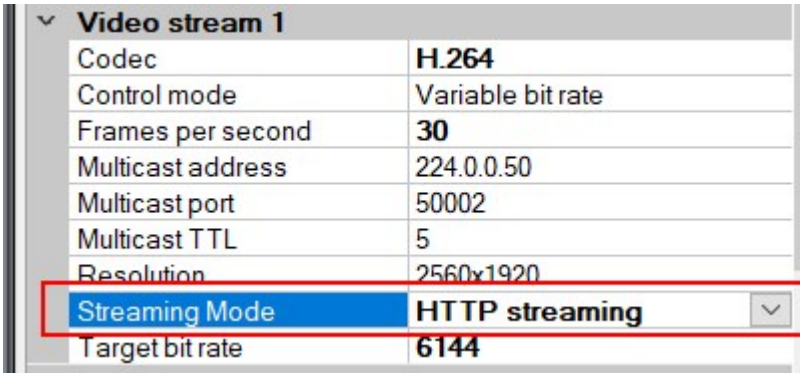


Hanwha drivers

- Set the **HTTPS Enabled** to **Yes**.



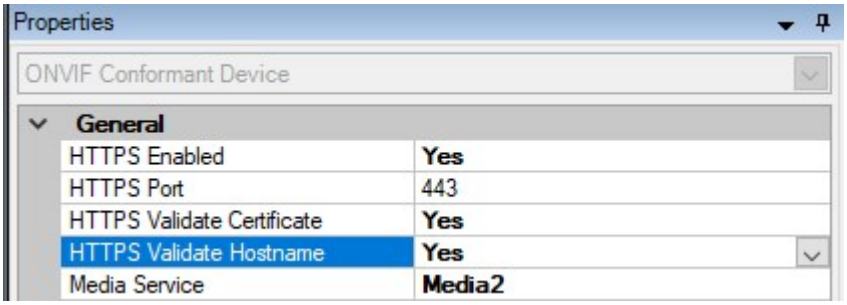
- For every enabled media channel and media stream, set **Streaming Mode** to **HTTP streaming**.



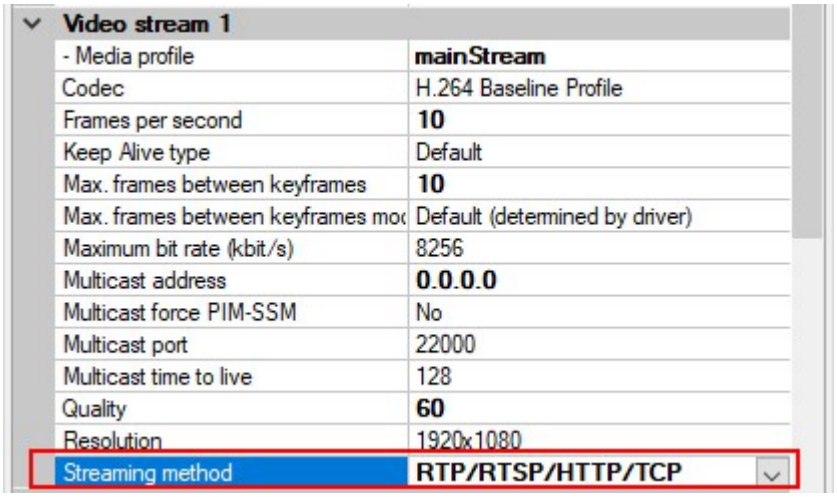
ONVIF drivers

Do the following:

- Set **HTTPS Enabled** to **Yes**.
- Set **HTTPS Validate Certificate** to **Yes**.
- Set **HTTPS Validate Hostname** to **Yes**.



- For every enabled media channel and media stream, set **Streaming method** to **RTP/RTSP/HTTP/TCP**.

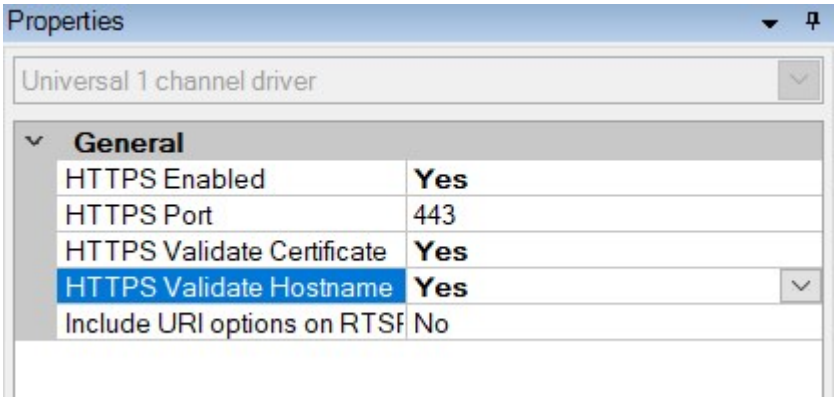


- The Audio backchannel (Audio Out, Device Speaker) must not be used when the driver is running in FIPS 140-2 compliant mode.

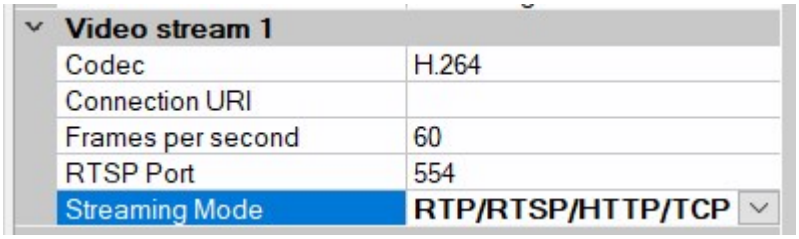
Universal drivers

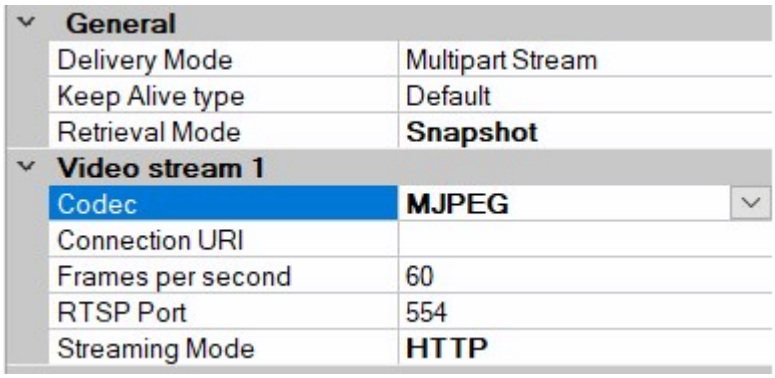
Do the following:

- Set **HTTPS Enabled** to **Yes**.
- Set **HTTPS Validate Certificate** to **Yes**.
- Set **HTTPS Validate Hostname** to **Yes**.



- For every enabled media channel and media stream, set **Streaming Mode** to either **RTP/RTSP/HTTP/TCP** or **HTTP**, depending whether streaming or snapshot retrieval mode is used.





VideoPush driver

No specific configuration is needed. Enabling the FIPS Group Policy will force the driver to communicate with the XProtect Mobile Server in a FIPS 140-2 compliant way.

Example of FIPS 140-2 compliant cipher suites

0x1302	TLS_AES_256_GCM_SHA384

0x1303	TLS_CHACHA20_POLY1305_SHA256
0x1301	TLS_AES_128_GCM_SHA256
0xC02C	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
0xC030	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
0x00A3	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
0x009F	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
0xC02B	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
0xC02F	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
0x00A2	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
0x009E	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
0xC024	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
0xC028	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
0x006B	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
0x006A	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
0xC023	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
0xC027	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
0x0067	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
0x0040	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
0x00AD	TLS_RSA_PSK_WITH_AES_256_GCM_SHA384

0x00AB	TLS_DHE_PSK_WITH_AES_256_GCM_SHA384
0x009D	TLS_RSA_WITH_AES_256_GCM_SHA384
0x00A9	TLS_PSK_WITH_AES_256_GCM_SHA384
0x00AC	TLS_RSA_PSK_WITH_AES_128_GCM_SHA256
0x00AA	TLS_DHE_PSK_WITH_AES_128_GCM_SHA256
0x009C	TLS_RSA_WITH_AES_128_GCM_SHA256
0x00A8	TLS_PSK_WITH_AES_128_GCM_SHA256
0x003D	TLS_RSA_WITH_AES_256_CBC_SHA256
0x003C	TLS_RSA_WITH_AES_128_CBC_SHA256
0x0035	TLS_RSA_WITH_AES_256_CBC_SHA
0x002F	TLS_RSA_WITH_AES_128_CBC_SHA



This list is not exhaustive. There are other cipher suites that are FIPS 140-2 compliant. This list is given only as a sample of cipher suites that are FIPS 140-2 compliant.

FIPS resources

1. FIPS 140-2 Security Requirements for Cryptographic Modules

   https://csrc.nist.gov/publications/detail/fips/140/2/final
2. Annex A: Approved Security Functions for FIPS PUB 140-2

   https://csrc.nist.gov/CSRC/media/Publications/fips/140/2/final/documents/fips1402annexa.pdf
3. Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations

   https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf

4. Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program

   https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/fips140-2/fips1402ig.pdf

5. Microsoft's approach to FIPS 140-2 validation

   https://docs.microsoft.com/en-us/windows/security/threat-protection/fips-140-validation

6. TLS/SSL overview (Schannel SSP)

   https://docs.microsoft.com/en-us/windows-server/security/tls/tls-ssl-schannel-ssp-overview

7. Cipher Suites in TLS/SSL (Schannel SSP)

   https://docs.microsoft.com/en-us/windows/win32/secauthn/cipher-suites-in-schannel

8. TLS Cipher Suites in Windows 10 v1903, v1909, and v2004

   https://docs.microsoft.com/en-us/windows/win32/secauthn/tls-cipher-suites-in-windows-10-v1903

9. TLS Elliptic Curves in Windows 10 version 1607 and later

   https://docs.microsoft.com/en-us/windows/win32/secauthn/tls-elliptic-curves-in-windows-10-1607-and-later

Center for Internet Security (CIS) Benchmarks

CIS Microsoft IIS 10 benchmark

The Center for Internet Security (CIS) is a nonprofit entity with a mission to identify and develop best practice solutions for cyber defense. Cybersecurity and IT professionals from government, business, and academia from around the world follow a consensus decision-making model to develop standards and best practices, including CIS benchmarks, controls, and hardened images.

CIS benchmarks are configuration baselines and best practices for securely configuring a system.

The CIS Microsoft IIS 10 benchmark is a set of best practices that apply to the Microsoft Internet Information Services (IIS) version 10 running on Microsoft Windows Server 2016.

Controls that do not impact XProtect VMS functionality

Milestone has identified that only those controls listed in Controls that impact XProtect VMS functionality on page 118 can impact the VMS functionality. Other controls will not impact the VMS functionality when applied properly.

Controls that impact XProtect VMS functionality

Some of the controls present on the CIS benchmark will affect the functionality of the XProtect VMS.

According to section *4.7 Ensure Unlisted File Extensions are not allowed (Scored)* in the benchmark, it is recommended that all extensions be unallowed at the most global level possible, with only those necessary being allowed.

Following is a list of extensions that the IIS applications use:

- htm
- html
- svc
- png
- css
- js
- gif
- svg
- ttf
- jpg
- xml

- asmx
- exe

  (Only the installation application uses .exe files. It can be disabled for all other applications.)

The benchmark suggests creating an extension whitelist to reduce the attack surface of the web application. Extension filtering can be applied to all applications except the Identity Provider application.

The Identity Provider application follows the OpenID specification and it defines URLs that do not end on any extension. Because of this, if the option **Allow unlisted file name extensions** is not enabled, the application will stop working and reply with the error code 404.7 for any request. The Identity Provider application is a central piece of the VMS services. It cannot be omitted and it must run for the VMS to work.

The installation application uses URLs that do not end with any extension for the purpose of redirection. But, if the option **Allow unlisted file name extensions** is not enabled, the user must enter the entire URL:

- http://localhost/Installation/default-en-US.htm instead of http://localhost/Installation/
- http://localhost/Installation/admin/default-en-US.htm instead of http://localhost/Installation/admin/

Learn more

The following links provide additional guidance:

- CIS Benchmarks FAQ
- CIS Security webpage
- OpenID

Product comparision chart

Product comparison

XProtect VMS includes the following products:

- XProtect Corporate
- XProtect Expert
- XProtect Professional+
- XProtect Express+
- XProtect Essential+

See the complete feature list, which is available on the product overview page on the Milestone website (https://www.milestonesys.com/solutions/platform/product-index/).

Appendix

Appendix 1 - Resources

1. *Axis Communications: Hardening Guide*
2. *Bosch Security Systems: Bosch IP Video and Data Security Guidebook*
3. *British Standard BS EN 62676-1-1: Video surveillance systems for use in security applications, Part 1-1: System requirements – General*

   Describes the minimum requirements for a video surveillance system. See also related standards.
4. *Center for Internet Security: The CIS Critical Security Controls for Effective Cyber Defense*
5. *Cloud Security Alliance (CSA)* and the *Cloud Controls Matrix*
6. *Defense Information Systems Agency (DISA): Security Technical Implementation Guides (STIGs)*
7. *Internet Engineering Task Force (IETF)*, multiple references
8. *ISO/IEC 15048 Information technology - Security techniques - Evaluation criteria for IT security*
9. *ISO/IEC 31000, Risk management – Principles and guidelines*
10. *ISO/IEC 31010, Risk management – Risk assessment techniques*
11. *ISO 27001: A standard and framework for managing threats in an information security management system (ISMS)*
12. *ISO 27002: Information technology — Security techniques — Code of practice for information security controls*
13. *Microsoft Security Update Guide*

    See also *Administer security policy settings*, among others
14. *National Institute of Standards and Technology: Computer Security Division Computer Security Resource Center*
15. *National Institute of Standards and Technology: Cybersecurity Framework*
16. *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
17. *National Institute of Standards and Technology: Managing Information Security Risk*
18. National Institute of Standards and Technology: Security and Privacy Controls for Federal Information Systems and Organizations SP 800-53- Revision 5
19. *NIST SP 800-100 Information Security Handbook: A Guide for Managers*

20. *NIST SP 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise*
21. *SANS Institute* website and the *SANS Critical Security Controls*
22. XProtect® Corporate – Advanced Security Management

Appendix 2 - Acronyms

AD – Active Directory

CSA – Cloud Security Alliance

CVE – Common Vulnerabilities and Exposures

HTTP – Hypertext Transfer Protocol

HTTPS – Hypertext Transfer Protocol Secure

IEC – International Electrotechnical Commission

IETF – Internet Engineering Task Force

IP – Internet Protocol

ISO – International Standards Organization

IT – Information Technology

KB – Knowledge Base

NIST – National Institute of Standards and Technology

RSTP – Rapid Spanning Tree Protocol

SMTP – Simple Mail Transfer Protocol

SSL – Secure Socket Layer

STIG – Security Technical Information Guide

TCP – Transmission Control Protocol

TLS- Transport Layer Security

UDP – User Datagram Protocol

VMS – Video Management Software

VPN – Virtual Private Network

helpfeedback@milestone.dk

About Milestone

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 Systems 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 150,000 sites worldwide. Founded in 1998, Milestone Systems is a stand-alone company in the Canon Group. For more information, visit https://www.milestonesys.com/.

milestone | XProtect® Rapid REVIEW

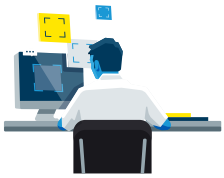
MAKE THE WORLD SEE

FIND WHAT YOU'RE LOOKING FOR, FAST.



Rewind, play. Rewind, play. Rewind, play. And you've still not found what you're looking for. You are not alone. Thousands of terabytes of video footage are recorded daily. Manually going through hours of footage to pinpoint a person or object of interest can take an impossibly long time. Don't you wish there was a way to make video investigations quick, smart and easy? With XProtect Rapid REVIEW there is!

With XProtect Rapid REVIEW powered by BriefCam you get an advanced forensic video analytics add-on solution that enables you to quickly review and analyze video content to find what you are looking for, fast.



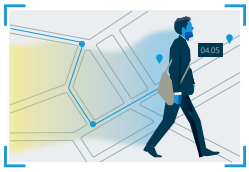
SELECT
Smart case management

Intuitively select video sources through the seamless XProtect Rapid REVIEW integration, instantly create search cases, and organize all investigation video in a single container to efficiently and effectively review video from within the XProtect user interface.



SEARCH
Accelerate investigations

Video footage often captures incidents that need to be investigated. It could be missing persons, vandalism, thefts, assaults, accidents, workplace injuries or harassment claims. Typically, manual forensic review of archived footage is time-consuming – the more the footage, the longer it takes. XProtect Rapid REVIEW enables fast, and intelligent multi-camera searches based on an expanding suite of analytic search filters across multiple cameras so users can quickly find the evidence and information they need.



DISCOVER
Unlock the value of video

Take your installation beyond security and achieve additional value of your video with the ability to analyze object activity, common paths, and dwell times. The results are easily readable visualizations that gives you the power to forensically pinpoint areas with most occupancies for greater scene understanding and insights.
For example, retail store management can identify customer occupancies and traffic direction and understand how customers navigate their stores to ensure better product placement, staffing and a superior customer experience.

milestone | XProtect® Rapid REVIEW

With XProtect Rapid REVIEW you get an advanced forensic analytics add-on solution that enables you to productively and quickly review and analyze forensic video content to find what you are looking for, fast.

Case Management
Instantly organize all video assets of an investigation in a single container, bookmark objects of interest, and summarize case findings (including all relevant exhibits) in an exportable report, while dynamically collaborating on cases with other users.

VIDEO SYNOPSIS
Simultaneously present objects that have appeared at different times within the video. The result is a dramatically shorter video segment that fully preserves the viewer's ability to analyze the scene, enabling the review of hours of video in minutes, and sometimes in mere seconds.

Multi-Camera Search
Advanced multi-camera search powerfully identifies people and vehicles of interest with speed and precision, using face recognition, appearance similarity, apparel, color, size, speed, path, direction, dwell time and illumination change filters.

Face Recognition
Accurate face recognition rapidly pinpoints people of interest using digital images extracted from the video or from external sources.

License Plate Recognition
Differentiated license plate recognition, designed especially for 'in the wild' surveillance scenarios and ease of operation in finding license plates through watch lists, existing video or data uploads.

Appearance Similarity
Instantly locate people, vehicles, and other items of interest by searching for objects that have similar attributes.

Face Mask Detection
Apply Face Mask attribute filter to search and identify face mask usage across video.

Proximity Identification
Search and identify the distance between individuals over time and location for compliance with physical distancing or for contact tracing.

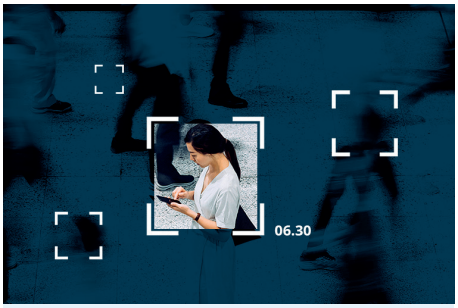
Line Crossing
Detect, filter and count objects that cross a demarcation in a pre-defined direction to drive perimeter protection and directional object count.

Visual Layers
Create heat maps for activity, dwell time, common paths and background changes.

Filter Tolerance
Adjust tolerance levels to refine search results for class, attributes, color, dwell time, direction, area, path, face recognition and appearance similarity.

Density & Speed Control
Increase or decrease the number and speed of events shown at once.

Sort Control
View events by relevance or by order of occurrence and easily zoom in on items of interest.



Changing the way video is reviewed with VIDEO SYNOPSIS®

VIDEO SYNOPSIS is an innovative solution that presents objects that have appeared at different times within the video simultaneously. This information is then presented as a time-compressed video with the ability to link back to the actual video. Despite advancements in technology, the explosive growth in the deployment of cameras worldwide means that viewing and analyzing recorded video footage is still a time-consuming and labor-intensive task. VIDEO SYNOPSIS presents a dramatically shorter video segment that fully preserves the viewer's ability to analyze the scene, enabling the review of hours of video footage in minutes, and sometimes, in just seconds.

System reccomendation
(Small build)

Form factor	Tower
CPU	Intel i5-10500
Memory	64GB RAM
Storage	• 256GB OS SSD • 480GB Mixed-use DB SSD* • 4TB HDD
GPU	1 x NVIDIA Quadro P2200
Throughput	• Up to 10 hours per hour at 1080p, medium activity • 1,5 hours per hour at 4K, medium activity

* Mixed-use SSDs that need a balance of strong Read and Write performance





DNA Fusion/ACM Plugin

Installation Guide



DNA Fusion™ is a trademark of Open Options, LLC.

The DNA Fusion™ Access Control and Security Management System uses equipment that generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this installation manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area may cause harmful interference. In which case the user will be required to correct the interference at the user's expense.

The DNA Fusion™ Access Control and Security Management System shall be installed in accordance with this installation manual and in accordance with the National Electric Code (N.E.C), ANSI and NFPA 70 Regulations and recommendations.

This manual is proprietary information of Open Options, LLC.
Unauthorized reproduction or distribution of this manual is strictly forbidden without the written consent of Open Options, LLC.
The information contained within this manual is for informational purposes only and is subject to change at any time without notice.
Open Options, LLC. assumes no responsibility for incorrect or outdated information that may be contained in this publication.

This manual has been written for DNA Fusion™ version 5.4 or higher

Print Date: August 27, 2014
Manual Number: UM-6.0

©Copyright 2019 Open Options, LLC. All rights reserved.

Warranty

All Open Options products are warranted against defect in materials and workmanship for one year from the date of shipment. Open Options will repair or replace products that prove defective and are returned to Open Options within the warranty period with shipping prepaid. The warranty of Open Options products shall not apply to defects resulting from misuse, accident, alteration, neglect, improper installation, unauthorized repair, or acts of God. Open Options shall have the right of final determination as to the existence and cause of the defect. No other warranty, written or oral is expressed or implied.

Open Options, LLC Software License Agreement and Warranty

THE ENCLOSED SOFTWARE PACKAGE IS LICENSED BY OPEN OPTIONS, LLC TO CUSTOMERS FOR THEIR NON-EXCLUSIVE USE ON A COMPUTER SYSTEM PER THE TERMS SET FORTH BELOW.

DEFINITIONS: Open Options shall mean Open Options, LLC, which has the legal right to license the computer application known as DNA Fusion™ herein known as the Software. Documentation shall mean all printed material included with the Software. Licensee shall mean the end user of this Open Options Software. This Software Package consists of copyrighted computer software and copyrighted user reference manual(s).

LICENSE: Open Options, LLC grants the licensee a limited, non-exclusive license (i) to load a copy of the Software into the memory of a single (one) computer as necessary to use the Program, and (ii) to make one (1) backup or archival copy of the Software for use with the same computer. The archival copy and original copy of the Software are subject to the restrictions in this Agreement and both must be destroyed or returned to Open Options if your continued possession or use of the original copy ceases or this Agreement is terminated.

RESTRICTIONS: Licensee may not sub license, rent, lease, sell, pledge or otherwise transfer or distribute the original copy or archival copy of the Software or the Documentation. Licensee agrees not to translate, modify, disassemble, decompile, reverse engineer, or create derivative works based on the Software or any portion thereof. Licensee also may not copy the Documentation. The license automatically terminates without notice if Licensee breaches any provision of this Agreement.

TRANSFER RIGHTS: Reseller agrees to provide this license and warranty agreement to the end user customer. By installation and acceptance of the software package, the end user customer and reseller agree to be bound by the license agreement and warranty.

LIMITED WARRANTY: Open Options warrants that it has the sole right to license the Software to licensee. Open Options further warrants that the media on which the Software is furnished will be free from defects in materials and workmanship under normal use for a period of ninety (90) days following the delivery of the Software to the licensee. Open Options' entire liability and your exclusive remedy shall be the replacement of the Software if the media on which the Software is furnished proves to be defective. This warranty is void if the media defect has resulted from accident, abuse, or misapplication. Open Options does not warrant that the Software will meet the end user customer requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTIES ARE THE ONLY WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE. NEITHER OPEN OPTIONS, NOR ITS VENDORS SHALL BE LIABLE FOR ANY LOSS OF PROFITS, LOSS OF USE, INTERRUPTION OF BUSINESS, NOR FOR INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND WHETHER UNDER THIS AGREEMENT OR OTHERWISE.

IN NO CASE SHALL OPEN OPTIONS' LIABILITY EXCEED THE PURCHASE PRICE OF THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether you accept the Software.

TERMINATION: Open Options may terminate this license at any time if licensee is in breach of any of its terms or conditions. Upon termination, licensee will immediately destroy the Software or return all copies of the Software to Open Options, along with any copies licensee has made.

APPLICABLE LAWS: This Agreement is governed by the laws of the State of Texas, including patent and copyright laws. This Agreement will govern any upgrades, if any, to the program that the licensee receives and contains the entire understanding between the parties and supersedes any proposal or prior agreement regarding the subject matter hereof.

Table of Contents

Chapter 1: Introduction

DNA Fusion / Milestone ACM Integration Overview 1-3

Chapter 2: Milestone ACM Integration

Install Flex API 2-3
- Flex API Key 2-4
  - Milestone ACM Only 2-4

Installing the Milestone ACM Plug-In 2-5

Configuring the Flex Plug-In 2-7
- DNA Fusion XProtect Management Application Settings 2-9
  - General Settings 2-9
  - Associated Cameras 2-9
  - Access Control Events 2-10
  - Access Control Actions 2-11
- Cardholders 2-13

Chapter 3: SmartClient DNA Fusion Setup

DNA Fusion on the Live tab 3-3
- Add Access Monitors to Views 3-3
- Overlay Buttons 3-4
- Map Integration 3-4

DNA Fusion on the Access Control Tab 3-5
- Events & Doors Status List Tab 3-5
  - Searching the Lists 3-7
  - Filtering the Lists 3-7
  - Export an Access Report 3-8
- About DNA Fusion Request Notifications 3-9
  - Access Request Notification Functionality 3-9
  - Disabling the DNA Access Control Functionality on the Smart Client 3-9

This Page Intentionally Left Blank

Introduction 1

In This Chapter
√ Chapter Overview

This section is designed to introduce you to DNA Fusion™ and the Milestone ACM integration.

How This Section is Organized

This section contains information on the DNA installation and configuration of hardware:

Chapter 1, "Introduction," gives an overview of the integration.

Chapter 2, "Integration and Installation," covers the Milestone installation including both the Milestone and the Open Options pieces as well as the configuration and integration steps.

Chapter 3, "Configuring," provides information on configuring the Milestone ACM. This chapter will provide information on setting up the door and camera view in the Milestone Smart Client

Icons and Conventions Used in This Manual

This manual uses the following icons to help you find useful or important information easily:

	This icon highlights time-saving hints, helpful shortcuts, and advice that you'll find especially helpful.
	This icon marks information that is important enough for you to keep it filed in an easily accessible portion of your gray matter.
	If something you're doing could damage the system, end up costing big bucks, lock you out of the system, or otherwise bring an end to civilization as we know it, you'll find it highlighted with the icon.

In addition to these icons, this manual uses several other conventions that make the instructions easy to understand:

A Special Font: Text that look like this indicates a menu item, toolbar selection, button, or a message from the system.

Boldface: Boldface text, which usually appears in numbered steps, tells you about specific actions that you should take.

DNA Fusion / Milestone ACM Integration Overview

Open Options DNA Fusion™ seamlessly integrates with Milestone Systems' Access Control Module providing operators the ability to view alarms and events from within the XProtect® Smart Client as well as control doors within the system. The integration is supported in XProtect Enterprise and XProtect Corporate video management software.

The Milestone ACM plug-in uses the Open Options Flex API application to deliver access control events into the XProtect Smart Client. This integration provides the following features:

- Ability to view associated cameras with door events
- Report on access events with associated video
- Monitor access events and alarms from the Smart Client
- Integration of mapping
- Cardholder event information as well as photo recall

Once installed and configured, the XProtect Smart Client provides an interface to the DNA Fusion access control system.

This Page Intentionally Left Blank

Milestone ACM Integration 2

In This Manual	
√	Flex API Installation & Milestone ACM API Key
√	Installing and Configuring the Milestone ACM Software
√	Install and Configuring the Milestone Solution

The DNA Fusion integration with the Milestone ACM solution uses the Fusion Flex API. This allows the Milestone ACM plug-in to deliver access control events into the XProtect Smart Client while permitting Smart Client users to easily control access control modules (doors, gates, elevators, etc.).

The Open Options Milestone ACM enables live monitoring of access control events, photo recall of cardholders, ability to view live video linked to events from the DNA Fusion access control system, playback of video associated with access control events and centralized door state overview as well as door control.

Dedicated functions in XProtect Smart Client enables users to effectively monitor access events, manually control doors and conduct investigations on specific access points or cardholders.

The Flex API Milestone Plug-in will need to be installed on the workstation that the XProtect Event Server Service is running.

There are a few configuration items that will need to be setup in order to communicate with the Milestone XProtect application.

This includes the following:

- Install Flex API (Open Options)
  - For more information, see the Flex API manual.
- Acquire the Milestone ACM Flex API Key (Open Options - See page 2-4)
- Install the FlexAPI Milestone Plug-in
  - Requires the correct license (Milestone ACM)
- Configure the Integration

Installation Requirements

- DNA Fusion 6.0 or higher
- Flex API
- Milestone XProtect Professional
- Windows 7 or higher

There are a number of required items that may need to be noted before starting the installation process.

- Flex API Key
- Host Computer URL

This Page Intentionally Left Blank

Install Flex API

The Flex API application will need to be installed on the workstation prior to installing the Milestone ACM plug-in.

The Flex API must be installed on the DNA Fusion server running the DNAdrvr32 service.

1. **Double click** the Flex API Install icon to begin the installation.

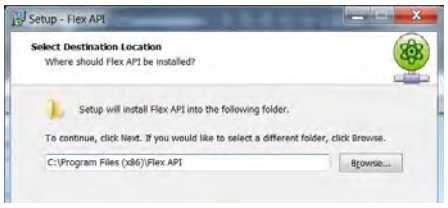
   The Welcome screen will appear.

2. **Click** the Next button to continue.

   The Select Destination window appears.

3. **Click** Next to accept the default Destination Location or **click** the Browse button to **select** a different location.

   The default location for a 32-bit environment is C: Program Files\Flex API and C:\Program Files (x86)\Flex API for 64-bit environments.



   The Startup Credentials screen appears.

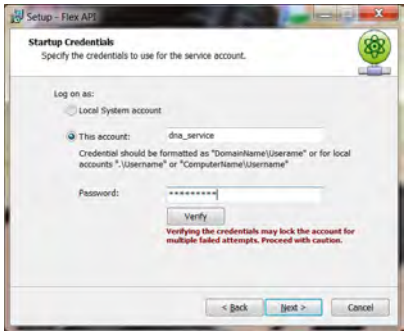
4. If needed, **select** This account, **enter** the Service Account information in the fields and **click** Next.

   Or

   If the DNAdrvr32 service is already running under a named account, the information will be prepopulated.

   The Flex API requires a service account to run the application; this account will need to be a local machine Administrative in order to operate.

   Open Options recommends using the same account the DNA Fusion driver utilizes. The Flex API uses the same COM objects, database connections and file permissions as the DNA Fusion driver (dnadrvr32).



   The Start Menu Folder screen appears.

5. **Click** Next to accept the default Start Menu location or **click** the Browse button to **select** a different folder.

   The installation will attempt to place the Flex API in the same location as the DNA Fusion shortcut.

   The Ready to Install screen appears.

6. **Click** the Install button to start the installation process.

   Installation will begin.

   If the DNAdrvr32 service is running, it will be stopped and a dialog will appear. **Click** the Next button to continue.

7. When installation is complete a dialog box will appear, **press** Finish to complete the set up.

8. The Flex API installation is complete.

Flex API Key

This key will be used during the Milestone ACM Plug-In Configuration.

Milestone ACM Only

For Milestone ACM only integrations, use the following API Key:

RkFQSUtFAAJQAAAAQGVQOeKhSJeWL7Xy35SnPDTXKhaxRGWmRfZhlTsmzNfqSwxyUmkWq6DK90u+IndXBLmtr+RGZd7MdPOE1xE7yn9P3V1NfBHC1eh79sheYqE=

Installing the Milestone ACM Plug-In

The Open Options Milestone ACM Plug-In must be installed on the workstation that is running the XProtect Event Server.

1. **Run** the FlexAPI Milestone Plugin Install page.

   The EasyLobby Welcome screen appears.



2. **Click** the Next button.

   The Ready to Install dialog opens.

3. **Click** the Next button to start the installation.

   The Setup Completed screen appears.



4. **Click** the Finish button.

   The installation is done.

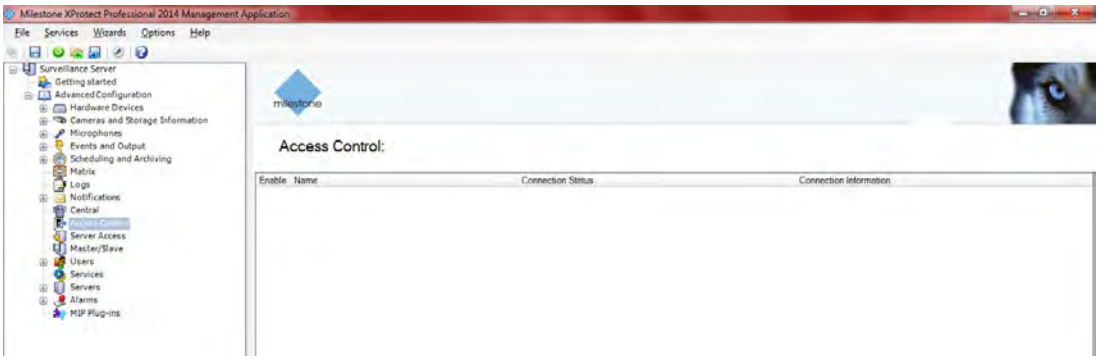
> ***The*** Event Server Service ***must be restarted after the Milestone ACM Plug-In is installed. If the service is not restarted, an error message will appear. The Event Server Service can be restarted from the*** Services ***menu in the XProtect Management Application.***

NOTES:

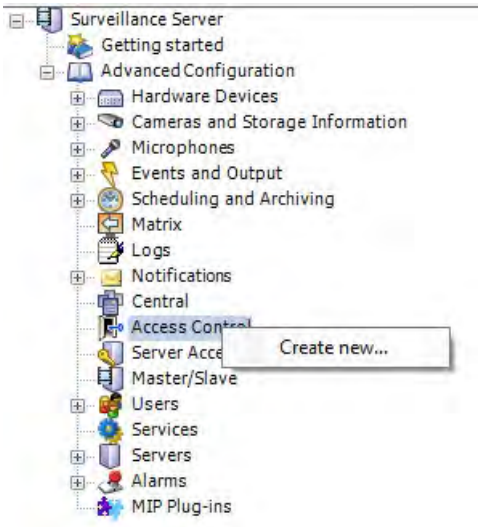
Configuring the Flex Plug-In

Once the FlexAPI Plug-In has been installed and the service restarted, DNA Fusion will need to be configured within the Milestone XProtect Management Application.

1. **Open** the **Milestone Management Application**.

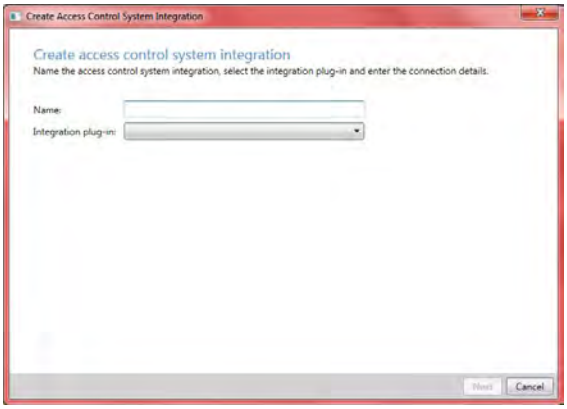


2. **Right click** on the Access Control option in the menu on the left and **select** Create New.



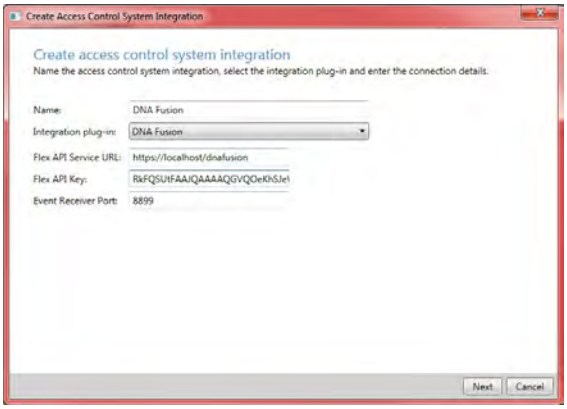
   The Create Access Control System Integration dialog will appear.

   If the Event Server Service was not restarted after the plug-in install, an error message will appear.



3. **Enter** a Name to display in the list.
4. **Select** the DNA Fusion option from the drop down list.

   The dialog will populate with additional fields.



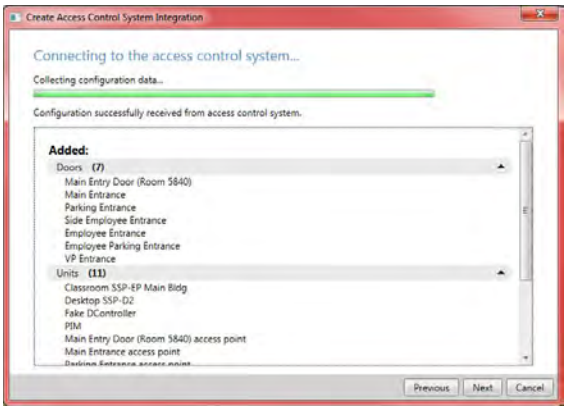
5. **Enter** the Flex API Service URL.

   This field automatically populates with http://localhost however it may need to be modified to match the DNA Fusion server URL address.

6. **Enter** the API Key found on page 2-4 in the API Key field.

7. **Click** the Next button to connect to DNA Fusion and import the various DNA Fusion objects into Milestone.

   The DNA Fusion Doors, Controllers, Sites, Events, Commands and Hardware States will populate the dialog. Review the list to ensure that all items have been integrated before continuing to the next step.

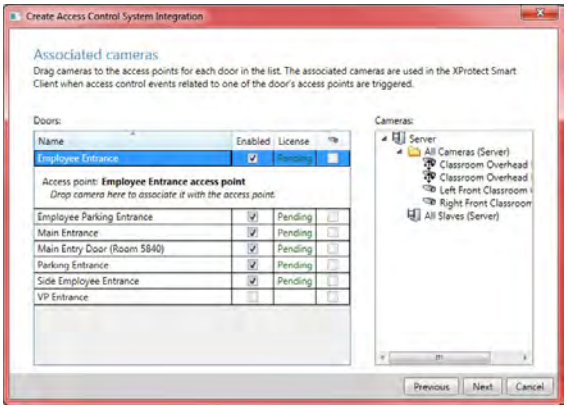


8. **Click** the Next button to proceed with the configuration.

   The Associated Cameras dialog appears.

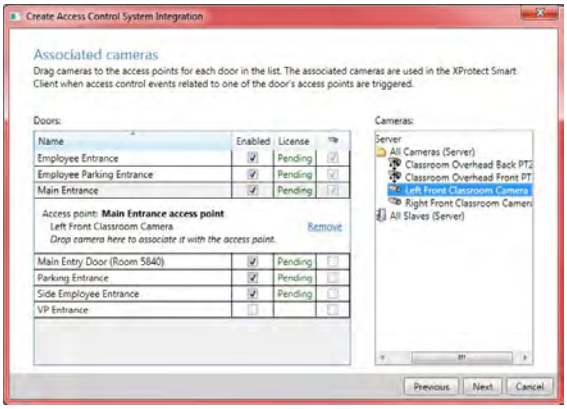
9. **Expand** the Server header in the Cameras pane to reveal the cameras.

   Map access points in the access control system with the cameras in the XProtect system, to show related video for events from the doors.



10. **Drag and drop** the camera to the desired Door.

    The camera is listed under the door; several cameras can be mapped to one access point. The XProtect Smart Client user is then able to view video from all the cameras. The option to Remove the camera becomes available.



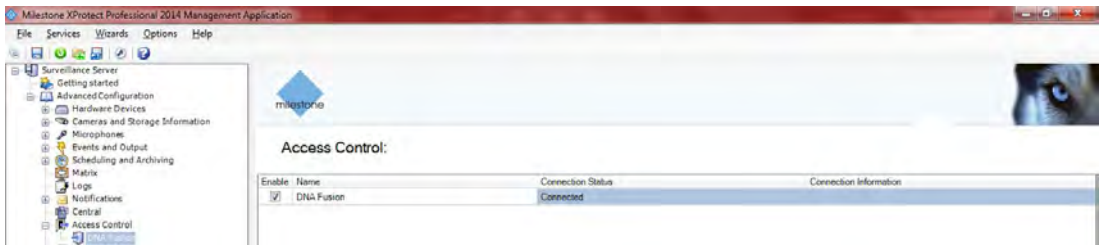
    Licensed doors are by default enabled. **Clear** the check box to disable a door and thereby free a license.

11. **Continue** to associate cameras with doors and **click** the Next button when done.

    The Integration Successful dialog will appear.

12. **Click** the Close button.

    The DNA Fusion Integration will appear under the Access Control header in the XProtect Management Application.

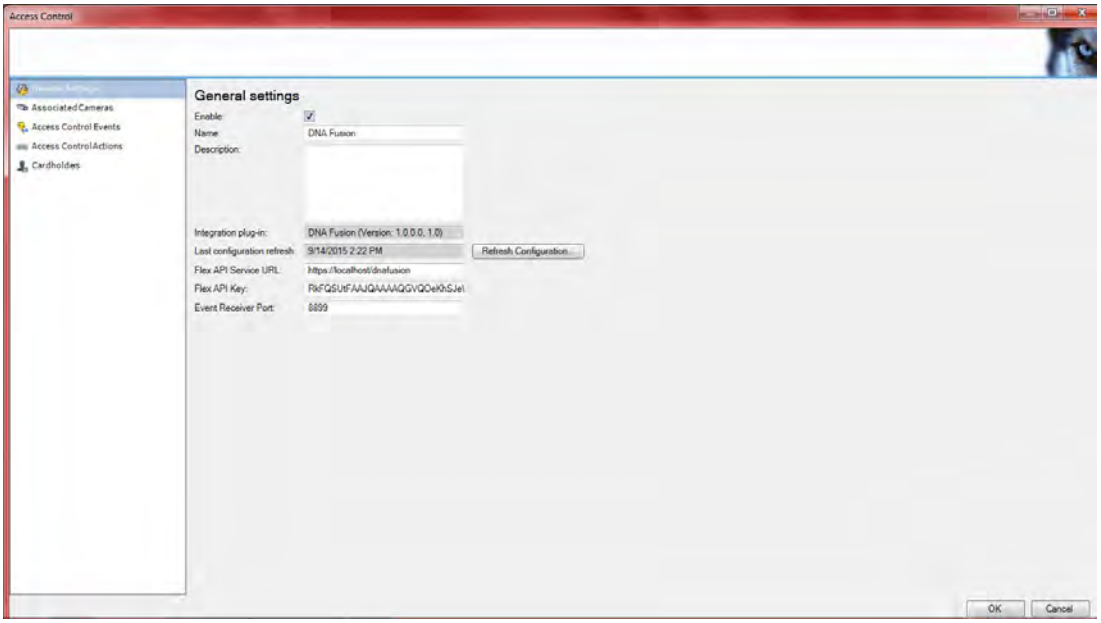


DNA Fusion XProtect Management Application Settings

There are a number of settings that can be configured within the Milestone XProtect Professional Management Application.

From the Access Control header, **expand** the option and **double click** on the Open Options ACM integration.

The Access Control Properties dialog will open.



General Settings

The General Settings page displays the Name and Description along with the Flex API URL and API Key.

Associated Cameras

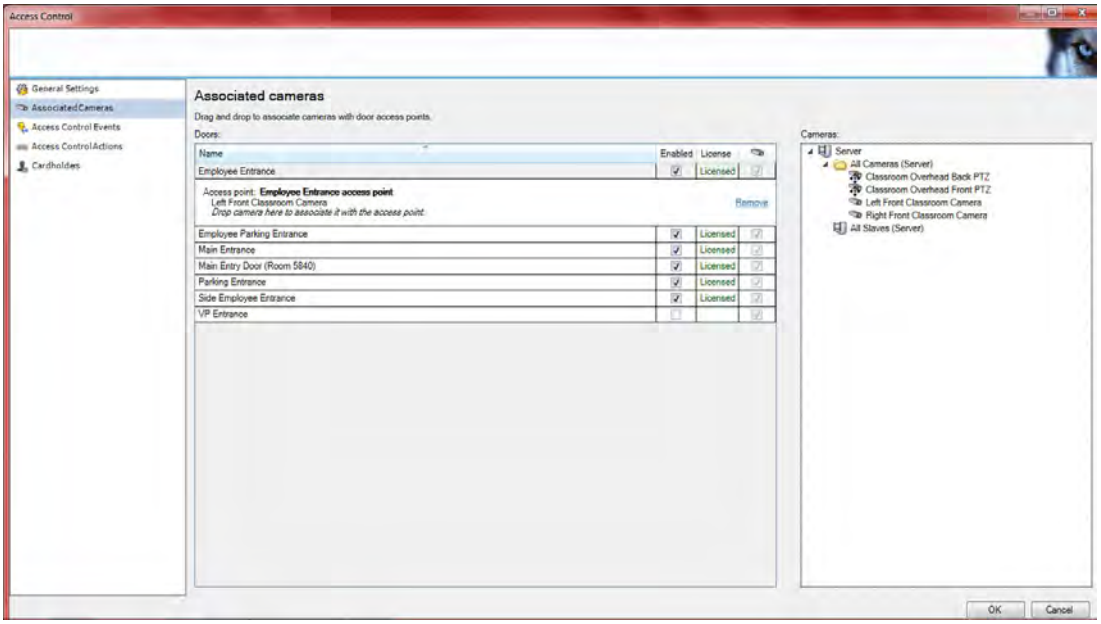
The Associated Cameras dialog lists all the doors that have been imported from DNA Fusion as well as the cameras available through the Milestone server. To associate a camera:

1. **Expand** the list of cameras under the Server header.
2. **Drag and drop** a camera to the desired entry point.

   The camera is assigned to the entry point.

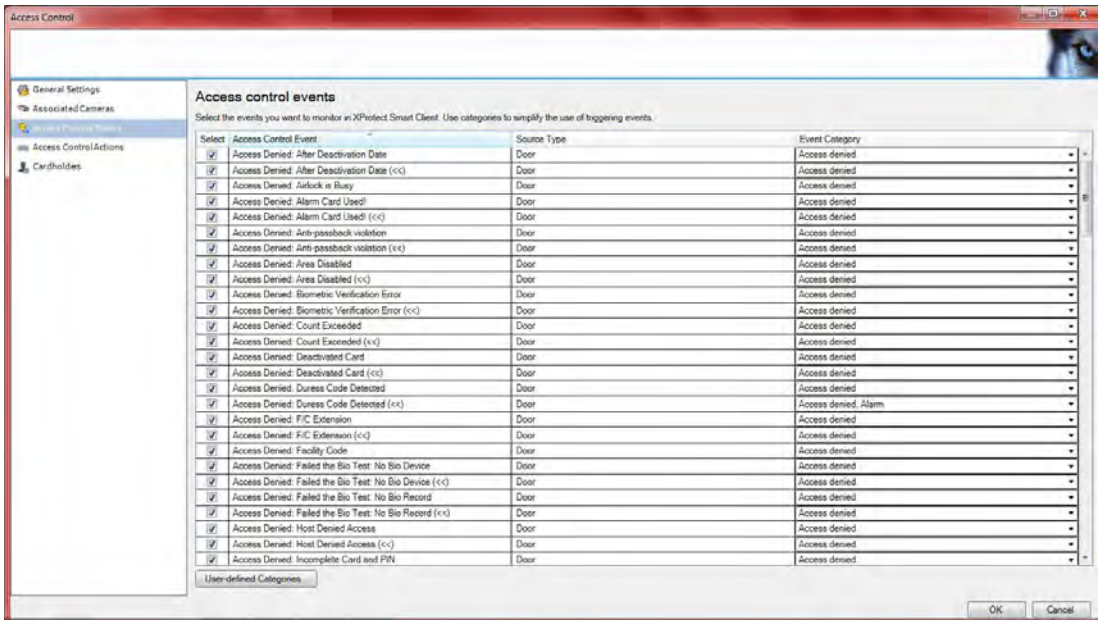
   Click the Remove button to disassociate a camera with an entry point.

   Licensed doors are by default enabled. **Clear** the check box to disable a door and thereby free a license.



Access Control Events

The Access Control Events dialog provides the ability to designate which events will be monitored in the XProtect Smart Client. Categories can be used to simplify the use of triggering events. Custom user defined categories may also be created.



To monitor the event:

1. **Check** the Select box next to the Access Control Event to be monitored.

   When an event is enabled, it is stored in the XProtect event database and is, for example, available for filtering in the XProtect Smart Client.

2. **Select** the Event Category from the drop down list.

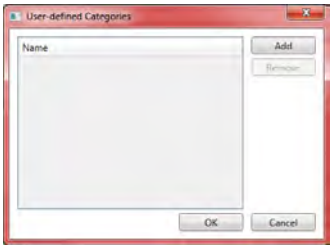
   Assign none, one or more event categories to the access control events. The system automatically maps relevant event categories to the events during integration. This enables a default setup in the XProtect system. Mapping can be changed at any time.

   Built-in event categories are:

   - Access Denied
   - Access Granted
   - Access Request
   - Alarm
   - Error
   - Warning



   If desired, **click** the User-defined Categories button to create new categories.

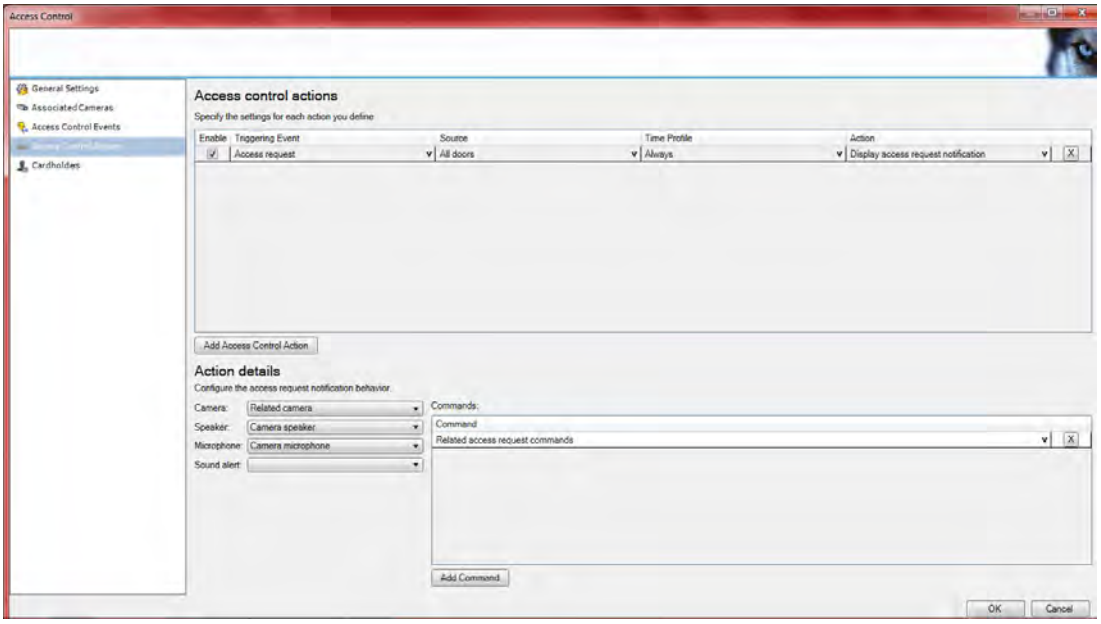


   The categories are global for all integration systems added to the XProtect system. They allow setting up cross-system handling, for example on alarm definitions. If a user-defined event category is deleted, a warning is displayed if it is used by any integration. If you delete it anyway, all configurations made with this category, will not work anymore.

3. **Click** the OK button to save the changes.

Access Control Actions

The Access Control Actions window allows for the definition of actions based on the configuration of the triggering events.

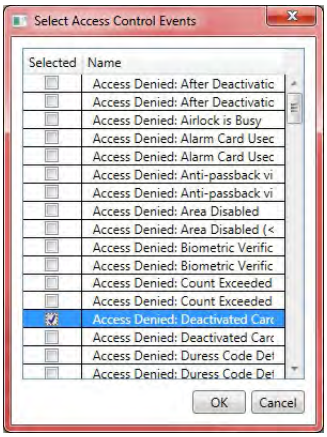


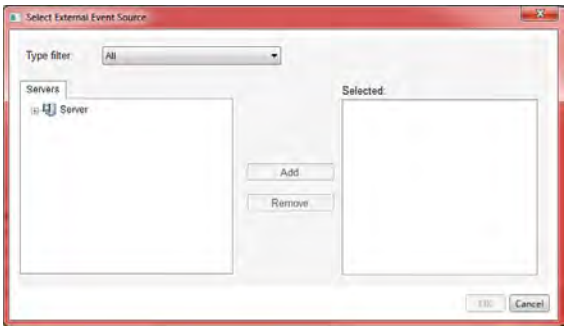
1. **Select** the Triggering Event from the drop down list.

   If needed, configure the triggering event.

   One or more actions related to the following can be specified:

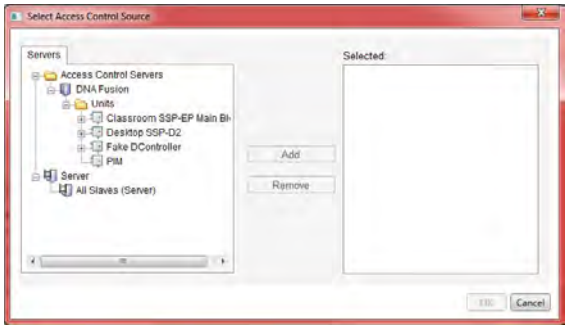
   - Events from the access control system
     - ☐ Check the desired events from DNA Fusion.
   - An event category
   - Events from the XProtect system





2. **Select** the Source from the drop down list.
   - All doors
   - Individual doors
   - Other...

   Click Other to select multiple doors or other units in the DNA Fusion system.



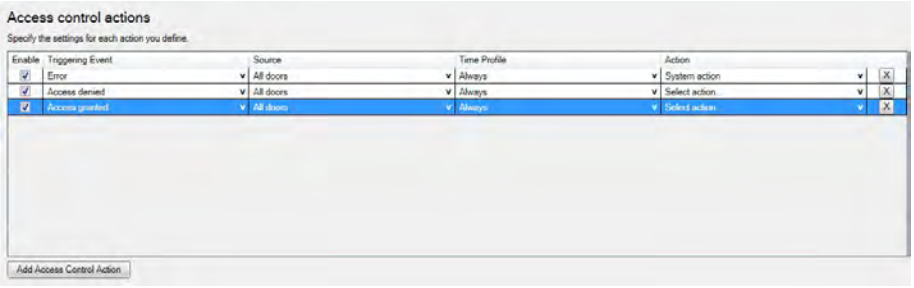
3. **Select** the Time Profile in which you want the action to be performed if triggered.

   Time Profiles are configured as part of Milestone XProtect Professional Advanced Configuration.

4. **Select** the type of action and **specify** the action details

   - Display access request notification
   - Go to PTZ preset
   - Start recording
   - System action

   To set up multiple actions, **click** Add Access Control Action. Example: Different actions triggered by the same event depending on different time schedules.



5. **Configure** the Action.

   - Display access request notification:
     - Specify which cameras, microphones or speakers the XProtect Smart Client user connects to via the notification user interface when a given event occurs. Also specify the sound to alert the user when the notification pops up. To enable more commands in the notification, see Add Command below.
   - Go to PTZ preset:
     - Specify the camera and select from the pre-configured presets a pattern for the camera and the time of return to preset when a given event occurs.
   - Start recording:
     - Specify the cameras that should start recording and the duration when a given event occurs.
   - System action:
     - Specify an action predefined in the XProtect system.

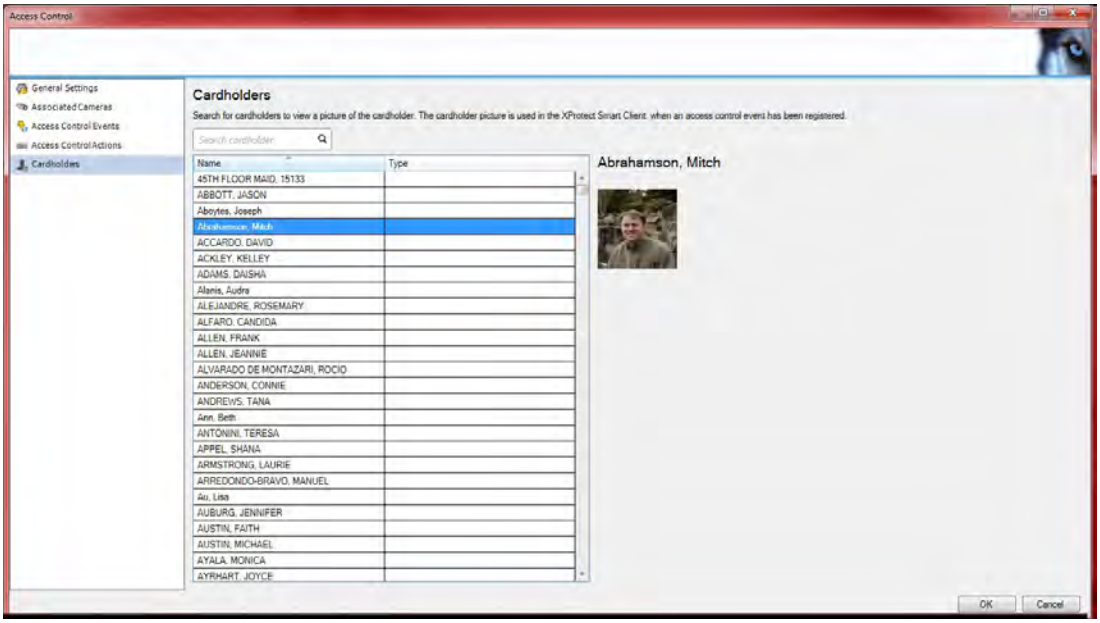
6. If desired, **click** the Add Command button.

   This will provide the ability to select which commands that should be available as buttons in the access request notification dialogs in the XProtect Smart Client.

   - Related access request commands:
     - Enables all commands related to access request operations available on the source unit. For example Open door.
   - All related commands:
     - Enables all commands on the source unit.
   - Access control command:
     - Enables a predefined DNA Fusion access control command in the XProtect system. **Select** the desired command and if needed, **select** the door.
   - System command:
     - Enables a command predefined in the XProtect system.
   - To delete a command, **click** the X on the right side of the command.

Cardholders

The Cardholders tab contains information about cardholders from the DNA Fusion access control system along with their photo.



To search for a cardholder, type the characters of the cardholder name and it will appear in the list, if it exists in the DNA Fusion cardholder database.

This Page Intentionally Left Blank

SmartClient DNA Fusion Setup 3

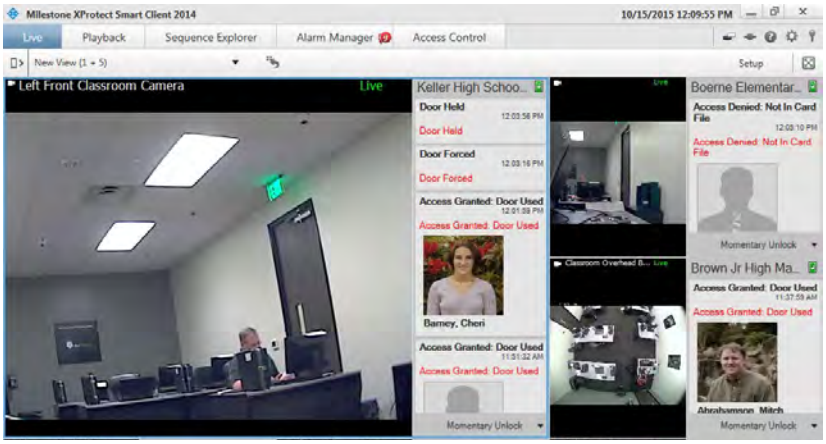
In This Chapter
√ Configuring a SmartClient Access Control View √ Viewing DNA Fusion Events and Controlling Hardware

Access control in the XProtect Smart Client integrates events from the Open Options DNA Fusion access control system with the features of the XProtect video management software. The information from DNA Fusion generates events in the XProtect system.

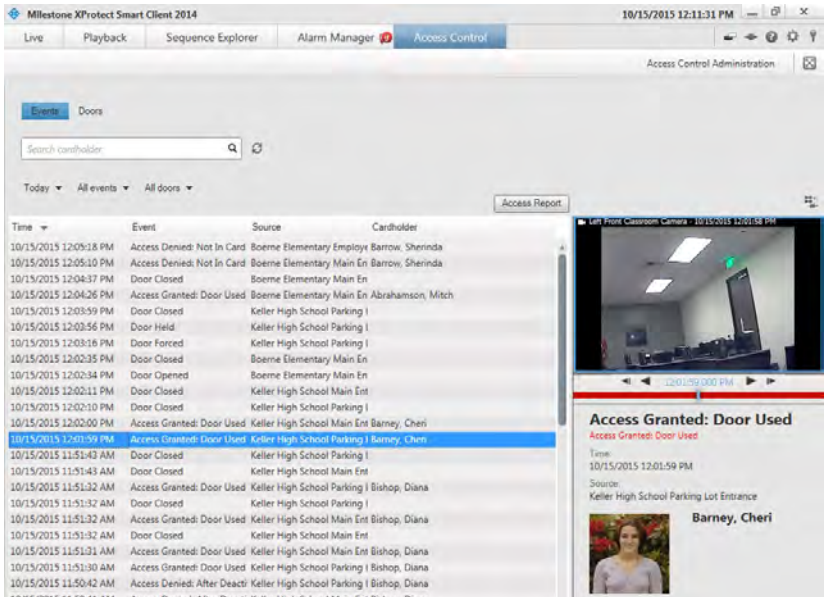
On the Live tab, access control events can be monitored in real time, and on the Access Control tab, particular events and door states can be viewed and investigated as they happen.

The Live tab provides video from the cameras associated with the doors from DNA Fusion. This gives a full overview of the live access control events associated with these cameras.

In setup mode, the view can be customized with overlay buttons and access control commands, such as locking and unlocking of doors as well as direct commands.



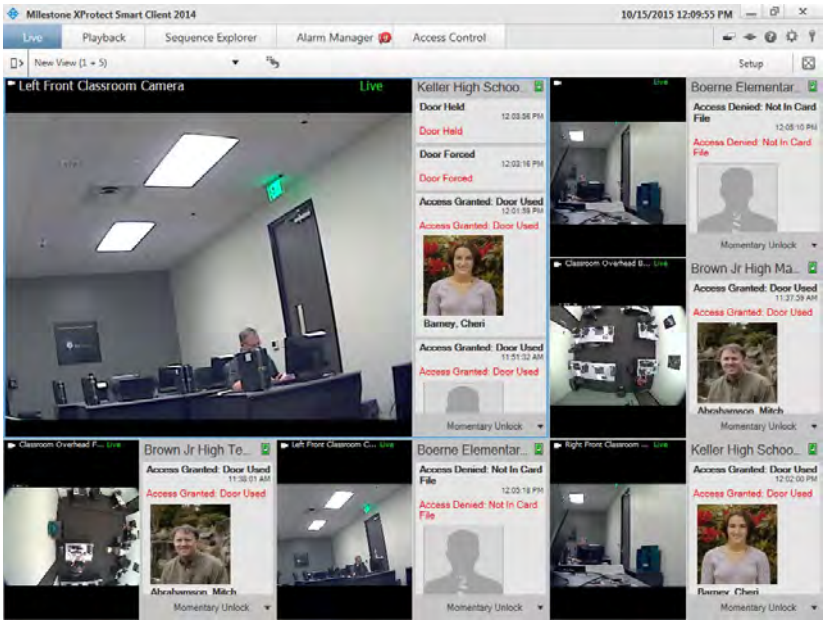
The Access Control tab provides a dedicated view for all the DNA Fusion access control events along with the cardholder information and photo if available. The door view includes a list of the doors and their current state. When an event or door is selected, all the associated cameras show the event or live video on the right-hand side of the screen together with detailed cardholder information.



This Page Intentionally Left Blank

DNA Fusion on the Live tab

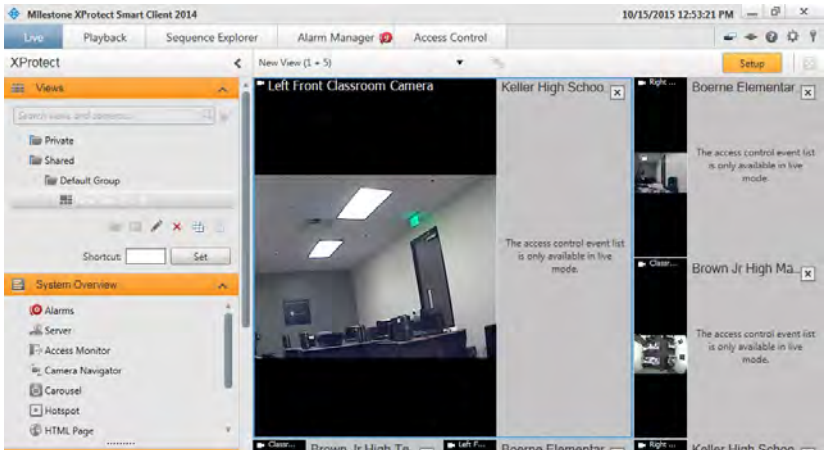
On the Live tab, video from the DNA Fusion events can be viewed from the cameras associated with access control sources. The events and any associated photo are displayed as a list to the right of the video.



When an Event is selected from the list, the live video automatically pauses and changes to independent playback of the event video. To go back to viewing live video, either **click** the event again or **click** the Independent playback icon on the camera toolbar. If the system and the event hold cardholder information, **click** the Search icon next to the cardholder name on a selected event to jump to the Access Control tab and view all events associated with the cardholder.

Add Access Monitors to Views

1. From the Live tab, **click** the Setup button.



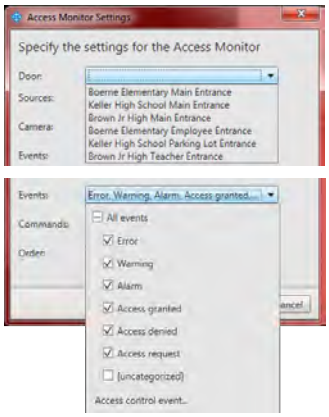
2. **Select** the view you want to associate an Access Control camera with from the Views pane.
3. In the System Overview pane, **click** Access Monitor and **drag** it to the relevant position in the view.

   The Access Monitor Settings dialog will appear.

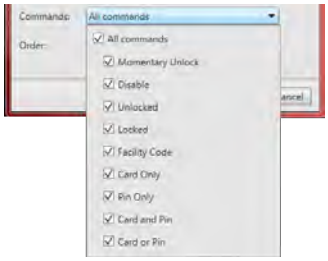


4. In the Access Monitor Settings dialog that appears, **specify** the door and camera, and the appearance of the view item.

   Specify how the access control event will display on the Live tab in the Properties pane.

   - **Select** the door to view along with the associated camera. If a door has multiple access points and associated cameras, a view can be set up for each of the access points.
   - **Specify** which events to view. For example, set up view items for different event types: one for system events and one for access requests.
   - **Select** the commands that will be available to the operator.
   - **Specify** the display order of the event list in the Access Monitor view item.

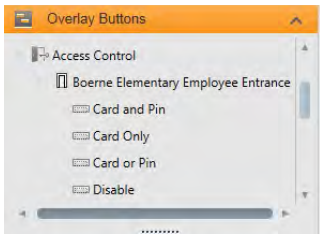
   

5. **Click** the OK button to save the pane.
6. **Repeat** until all the desired DNA Fusion access points are in the view.
7. **Click** the Live button to view the pane.

Overlay Buttons

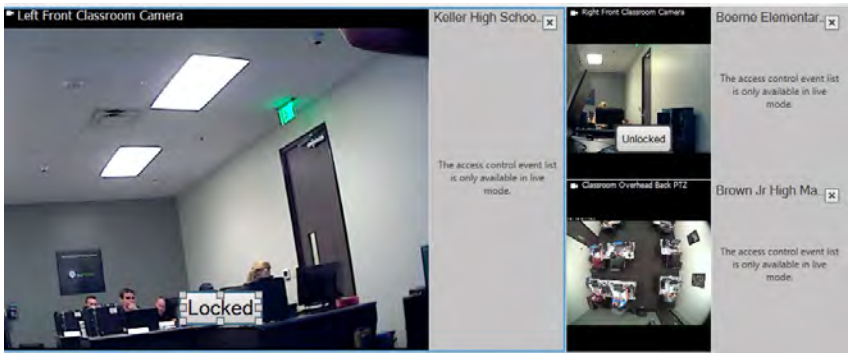
Overlay command buttons tied to DNA Fusion access control commands configured for the doors can be added to a view.

1. From the Live tab, **click** the **Setup** button.
2. **Select** the view you want to associate an Overlay Button with from the Views pane.
3. In the Overlay Button pane, **expand** the Access Control item to locate the desired door.

4. **Expand** the door to reveal the Door Modes and **drag** the Mode to the relevant position in the view.

   The button will appear on the pane view.

5. **Resize** or **edit** the button as needed.

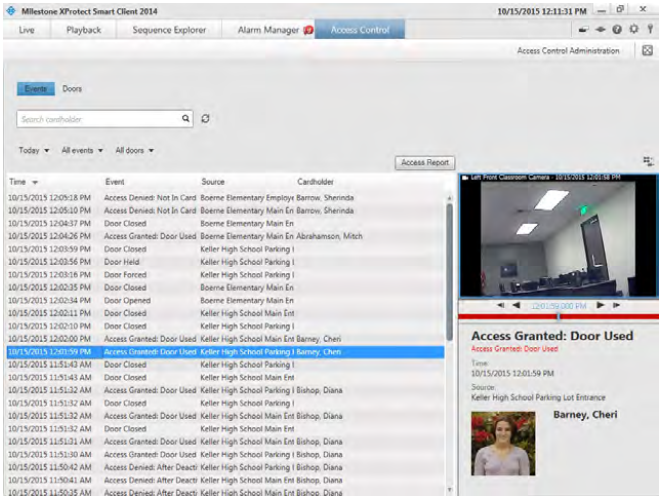
Map Integration

If the map functionality to support will be used to support the surveillance and access control systems, the access control units can be added to a map. From the map toolbox, select access control units, for example a door. Since the state of the access control units are always visible, a map used in this way is a quick way to get a graphical overview of the states of the access control units for the area or building being monitored.

DNA Fusion on the Access Control Tab

DNA Fusion related events and the state of the doors is displayed on the Access Control tab. From this tab, logged events can be investigated, the current door status is visible and certain commands can be initiated.

To allow for optimum performance, the lists only display a maximum of 100 rows at a time. To browse to the previous/next 100 rows, use the arrow buttons in the top right of the list.



The columns can be sorted by clicking on the desired column header; columns may also be dragged to different positions to rearrange the grid.

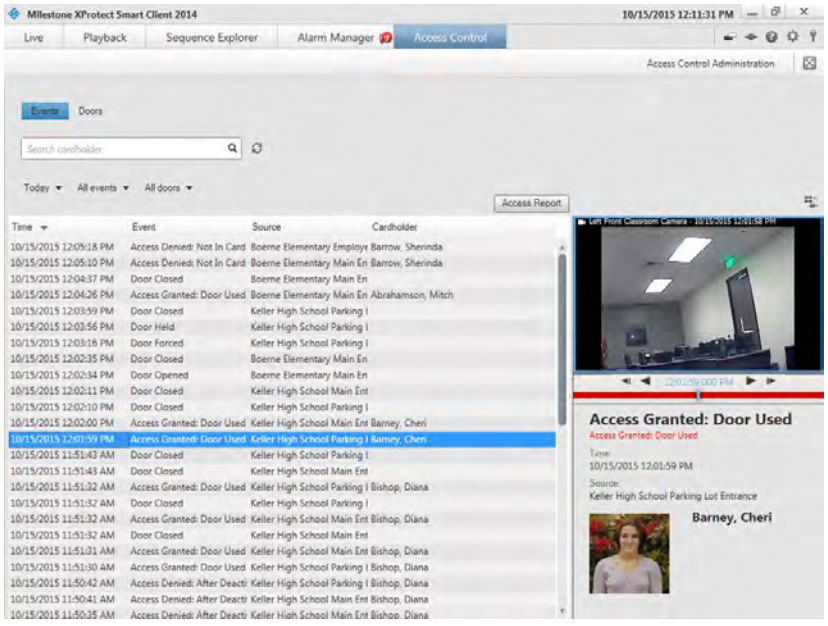
The Access Control tab can be dragged to a separate window, allowing the main window to be open in the background to watch several views simultaneously.

Events & Doors Status List Tab Events Doors

On the Access Control pane, there are 2 status list tabs: Events & Doors. Each tab provides a different view of the DNA Fusion system.

- Events Tab: The Events are logged with a time stamp, event type, the DNA Fusion associated door or access control unit description and cardholder name if available. When an event is selected, the preview on the right displays the related video sequence for the event. The preview camera title bar shows the camera related to the unit that triggered the event.

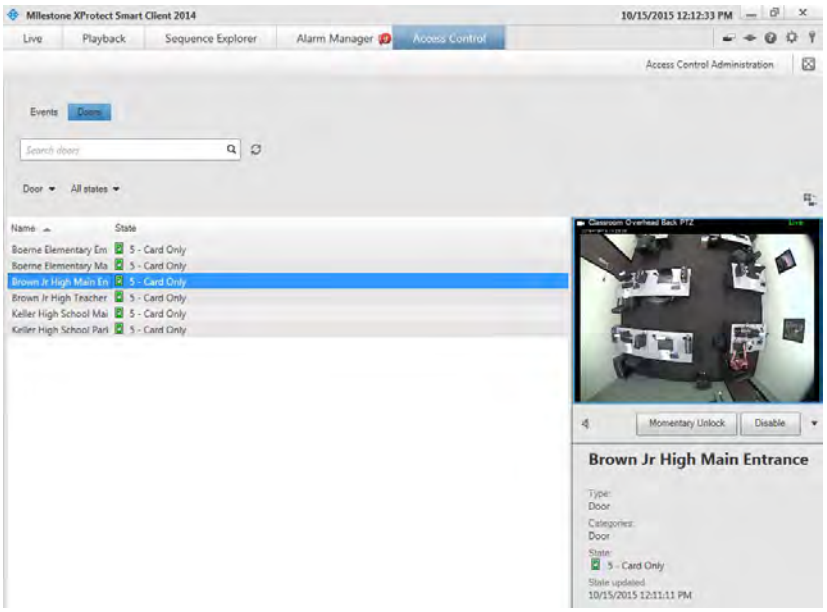
  Related cardholder information, including the cardholders photo, appears below the video preview together with details about the selected event. **Click** to view live video or play back recorded video in a floating window.



Standard playback options are available from the toolbar. If multiple cameras are associated with a door, they all appear in the preview.

- Doors Tab: The Doors lists the doors, access points and other access control units in the DNA Fusion access control system, and their current state. When a door is selected, the associated camera shows live video on the right-hand side of the screen together with detailed information about the doors status.

  Action buttons allow you to perform certain commands related to that door, for example lock or unlock door. Information related to the selected door appears below the live video preview. **Click** to view live video or play back recorded video in a floating window.



Standard playback options are available from the toolbar. If multiple cameras are associated with a door, they all appear in the preview.

Searching the Lists

The Search box can used to search for a particular cardholder in the Event list or for a door or other Fusion component in the Doors list. If the Live Update Time option is not selected in the Time filter, the list only displays data from the time you searched or filtered. To view the latest data, **click** the Refresh button.

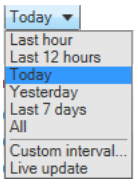
Filtering the Lists

There are several ways to filter the Events or Doors Status List Tabs so they display only the door(s) and/or other desired component(s). **Click** any of the filters at the top of the list to see only data associated with that filter. Any applied filters are immediately reflected in the list.

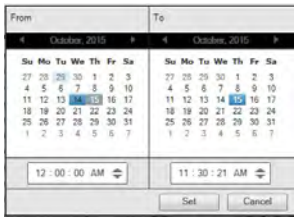
Events List

Time

Select one of the available time periods to see data for that particular period. For example, **click** Today to see only events that took place today or use the Custom interval option to specify a particular time period.



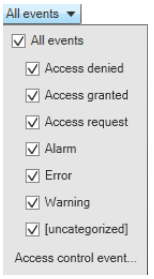
If the Live update option is selected, the list of events is updated instantly when new events occur. The list displays a maximum of 100 events. Cardholders cannot be searched when the Live update option is selected.

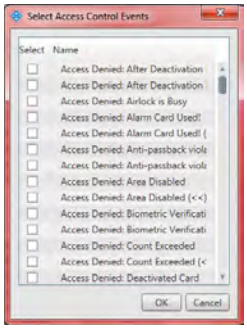




Events

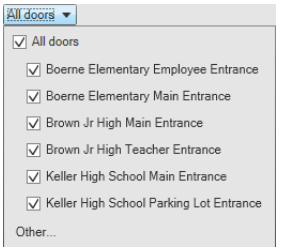
Select one or more of the available event types directly from the list of event categories and uncategorized events or **select** the Access Control Event... item and **check** specific access control events from the resulting dialog.

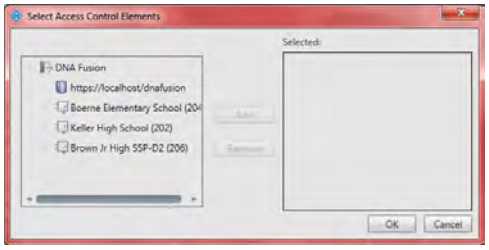




Source (All Doors)

Select one or more of the available DNA Fusion doors directly from the list of doors or select the Other option to choose different sources (for example access points or controllers from DNA Fusion) to view only events for those items.





Cardholder

Enter the cardholder information in the Search dialog. Cardholders cannot be searched when the Live update option is selected.



Right Click Filter

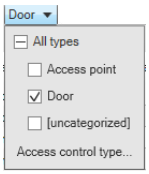
Right clicking on an event will open a filter dialog based on the value in the event. **Selecting** the Filter using this value option will return results related to the selected event.

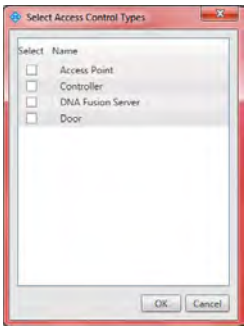


Doors List

Doors

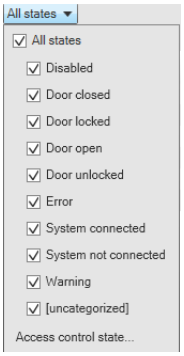
Select one or more of the available doors, access points and uncategorized types or **select** the Access Control Types option and **check** other DNA Fusion components to view.

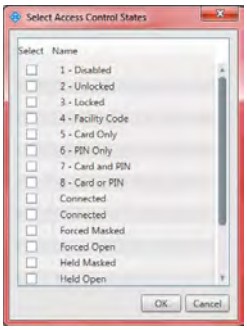




States

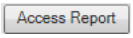
Select one or more of the available states directly from the list of state categories and uncategorized states or select between specific access control states by **selecting** the Access Control State option and **specifying** the desired individual states.



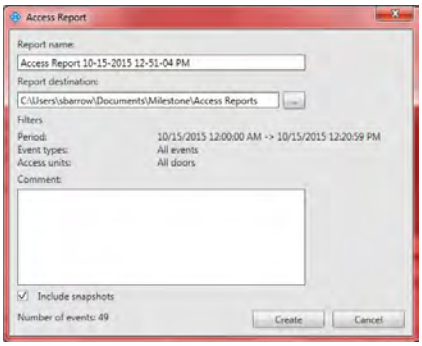


Export an Access Report

The Access Report is available from the Events tab except in Live Update mode. The report can be exported to a PDF file.

1. **Click** the Access Report  button.

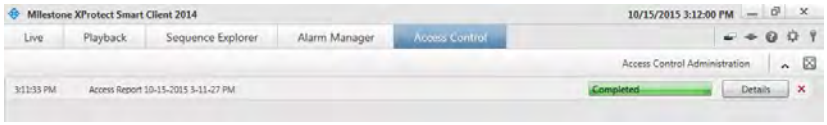
   The Access Report dialog will open.



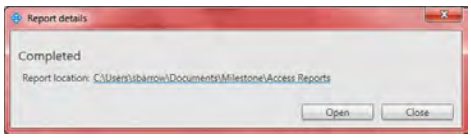
2. **Click** the Create button to generate the report.

   A status bar will appear across the top of the SmartClient.

   Once finished, **click** the Details button to view a summary.



   Click the Open button to open the report in Adobe Reader.



   The report contains:

   - Report name
   - Report destination
   - A list of the applied filters
   - A comment field
   - An option to include snapshots

If the event count is very high, you will receive a recommendation to refine the search and thereby reduce the number of search results.

About DNA Fusion Request Notifications

All conditions that trigger an access request notification have to be specified in the video management system. The notification displays video related to the access request, displaying the person who is requesting access. The name of the door that should open is shown as a headline, indicating, for example, Access Request - Front door. The door state (for example open, closed or forced open) also appears. If you have multiple cameras associated with a door, they appear below each other. Click the Video icon to view video in a floating window.

Access request notifications are temporary. If an access request notification is closed, the access request is no longer present in the system. If XProtect Smart Client is closed while an access request notification is shown, the access request is not restored when the Smart Client is restarted.

Access requests stack up on each other in the access request notification window so that all incoming access request notifications can be handled from the same notification window. The notification window can also be dragged to the other side of the screen. If needed, the access request notification window can be minimized to allow the functionality to continue in the background. The minimized notification window blinks to indicate the presence of new notifications.

Access Request Notification Functionality

Access request notifications allow the operator to speak and listen to the person who wants to enter, if a speaker and/or microphone is attached to the relevant camera that shows the access request notification:

- To listen to what the person requesting access is saying, click the Speaker button.
- To speak to the person requesting access, for example to give instructions on how to proceed or behave in the area, click the Microphone button and hold the button.

To the right of the Microphone and Speaker buttons, are buttons that allow certain actions to be executed. The most typical action is to unlock a door for a person requesting access, but could also be to turn on the lights in the area close to the relevant entry. If available, the cardholder information will be displayed.

Disabling the DNA Access Control Functionality on the Smart Client

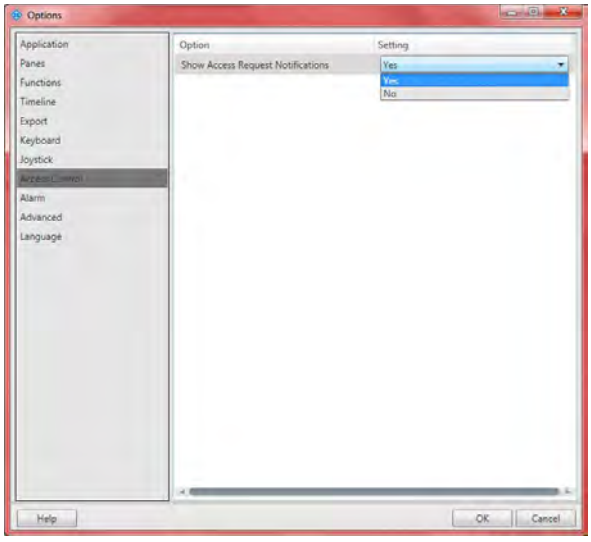
If a client does not need to view the DNA Fusion access control features and functions.

To turn off access request handling

1. **Click** the Options icon .

   The Options dialog will open.

2. **Select** the Access Control item from the menu.



3. From the Show Access Request Notifications drop down, **select** No to turn off access request notifications.

   To handle access requests again, **select** Yes to receive access request notifications from DNA Fusion.

This Page Intentionally Left Blank

Milestone XProtect Access

OnGuard User Manual

Prepared by:

Custom Development Americas

milestone

Table of Content

Copyright, Trademarks & Disclaimers **4**
Copyright 4
Trademarks 4
Disclaimer 4
General Description **5**
What's New in version 4.1? 5
Solution overview 6
Scalability **6**
Planning your Installation **7**
Single System Scenario 7
Multiple Single Systems 8
Milestone XProtect Federation with OnGuard Enterprise 9
Distributed deployment options 10
Single system with Integration Server 11
Milestone XProtect Clustered with Single Clustered OnGuard 11
Version Notes **12**
Version Compatibility **12**
OnGuard Version support 12
Recommended OnGuard Versions 12
XProtect Version Support **13**
Hardware Support **13**
Secure Communication **13**
FIPS-140-2 Compatibility **14**
Prerequisites **14**
Time Synchronization 14
.NET Framework for OnGuard 14
Milestone XProtect License 14
Event Server DNS / Name resolution 15
Smart Client Profiles 15
OnGuard License Options – PLEASE CONSULT CARRIER FOR LICENSING 15
Required OnGuard Services 16
Generate software events 16
Create Single Sign-On (SSO) Directory 16
Create Single Sign-On (SSO) User 18
Installation **20**
Step 1 - OnGuard XProtect Access Service Installation 21
Step 2 – OnGuard XProtect Access MipPlugin Installation 23
MIP Plugin Upgrades 25
Upgrading from DataConduIT 27

milestone

Uninstalling the integration 29
XProtect Management Client Configuration 30
XPA Instance Creation Wizard 30
XPA Instance Status & Properties 33
Personalized Login 36
Commands: 38
Administrative Configuration 42
Door & Camera Association 42
Categorize Events 43
Access Request Notifications 46
Searching for Cardholders 48
Client Profiles & Roles 48
Smart Client Features 49
Access Control Workspace 49
OnGuard Web Admin Link 54
Access Monitor 55
Maps 57
Overlay Buttons & Commands 59
Alarm Acknowledgment 61
Access Control Options 63
Mobile Client 64
Access Control Tab in Milestone Mobile 64
Service Tray Icon 66
Log Viewer 66
Logging 67
Log File Locations 67
Changing logging level 68
Troubleshooting Guide 69
OnGuard loses communication with access control hardware 69
Integration Version Downgrades 69
XProtect 2021 R1 and R2 shows no error if OpenAccess – Password is incorrect. 70
Access Control Rules Stop Working after Upgrade to 4.0 or newer. 72
OnGuard XProtect Access Service: MipPlugin Post-Install Verification 74
Cardholder search data fields are missing 75
Not receiving cardholder or badge changes 78
XPA integration flooding OnGuard user transaction report 78
OnGuard XPA instance not displayed in the XProtect Management Client 78
LS OpenAccess service automatically stops seconds after starting 79
I/Os connected to OSDP readers are no longer detected 79
LS OpenAccess events fail in OnGuard Enterprise systems 79
All other support issues 79
Known issues: 79

Copyright, Trademarks & Disclaimers

Copyright

© 2022 Milestone Systems.

Trademarks

XProtect® is a registered trademark of Milestone Systems.
Microsoft and Windows are registered trademarks of Microsoft Corporation.
All other trademarks mentioned in this document are trademarks of their respective owners.

Disclaimer

This text is intended for general information purposes only, and due care has been taken in its preparation.

Any risk arising from the use of this information rests with the recipient, and nothing herein should be construed as constituting any kind of warranty.

Milestone Systems A/S reserves the right to make adjustments without prior notification.

All names of people and organizations used in the examples in this text are fictitious. Any resemblance to any actual organization or person, living or dead, is purely coincidental and unintended.

This product may make use of third-party software for which specific terms and conditions may apply. When that is the case, you can find more information in the file 3rd_party_software_terms_and_conditions.txt located in your Milestone system installation folder.

General Description

This document describes the XProtect Access (XPA) integration between Milestone XProtect video management system (VMS) and the OnGuard access control (AC) system. This integration supports the following standard XPA features:

- Retrieve and refresh configuration from the OnGuard AC system, e.g. doors and event types.
- Receive AC event streams and hardware status changes from the OnGuard system.
- Display and search cardholder information - both data and images.
- Create alarms in XProtect alarm manager based on AC events.
- Synchronization of alarm status between XProtect and OnGuard.
- Association of access control events to cameras for simultaneous display of events and video.
- Association of access control hardware to cameras for simultaneous display of doors and video.
- Select and categorize events from the OnGuard system to view and work with events in groups.
- Trigger system actions based on AC hardware events. For example: start recording, go to PTZ preset, display access request...etc., triggered by door forced, access granted, access denied...etc.
- Personalized login to support segmented database systems.
- AC hardware status display and command interaction on VMS client map user interface.
- Create customized access reports based on search queries in XProtect Smart Client.
- Smart Client pop-up access request notifications.
- AC hardware interaction via XProtect web and mobile clients.
- Connect to the OnGuard web administration interface from the XProtect Smart Client.

What's New in version 4.1?

The following list contains the most prominent changes to version 4.1 of the OnGuard XProtect Access integration:

Requirements:

- Virtual port 8443 is required as a default port for communication between OnGuard and XProtect. The installation program of the OnGuard XProtect Access Service will configure and open this port on the OnGuard server.
- The installation program for the OnGuard XProtect Access integration has been entirely redesigned. There is now one install file for use on both OnGuard and XProtect systems. This context sensitive installation program will install all needed components, one on OnGuard and one on XProtect. And the ACM wizard program has been removed.

Functionality & User Experience:

- There is a new Access control administration button added to the Access Control workspace in the Smart Client. This launches a web browser that connects to the OnGuard web-based administration interface.
- The location of the log files has been changed and the service tray menu and log viewer for the OnGuard XProtect Access Service has been improved.
- Door opening animations have been added to map icons.
- The ACM acronym and the term Access Control Module, which it stands for have been removed from the integration, the documentation, and the website where the materials are hosted.

Solution overview

The solution provided is split in 2 components:

1. OnGuard XProtect Access Service – Typically installed in the OnGuard environment.
2. OnGuard XProtect Access MipPlugin – Installed in the XProtect environment.

Scalability

This section details the size of the test system at the LenelS2 certification labs and lists the performance that can be expected.

The software interface between the Milestone and OnGuard has been optimized for throughput of events and system status messages. However, server components and computer hardware resources can still limit total throughput.

Type of Device	Count
Panel	1925
Door	1024
Reader	1028
IO Module	14
Input	2074
Output	2055
Card Holders	400,000

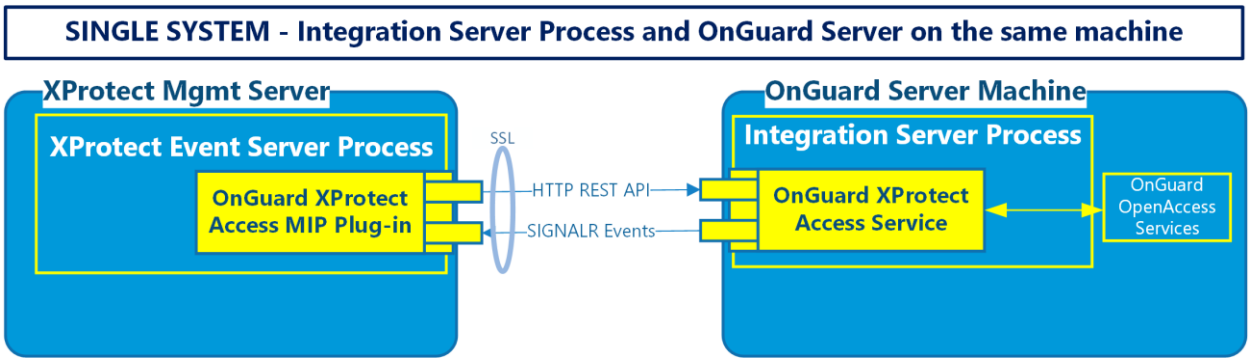
Eventing	Events/sec
OpenAccess	100
OpenAccess – Peak	300+

Planning your Installation

There are many different ways to integrate XProtect with the OnGuard Access Control System. This section is a guide to help you figure out which deployment options you should consider.

Installation Scenario	Use case
Single System	You have a single XProtect system (one event server per system) and a single OnGuard system (one OnGuard database per system).
Multiple Single Systems	You have multiple single XProtect/OnGuard system pairs. The customer just wants each pair to behave independently of each other.
XProtect Federated with OnGuard Enterprise	You have a federated XProtect system and an OnGuard Enterprise system that need pairing. The customer needs centralized configuration and alarms.
Single system – Integration Server and OnGuard Server on separate machines	There is a need to run the required integration software components on a different machine than the OnGuard Server.
XProtect Clustered with OnGuard Clustered	You have a XProtect clustered environment connecting to an OnGuard clustered environment.

Single System Scenario

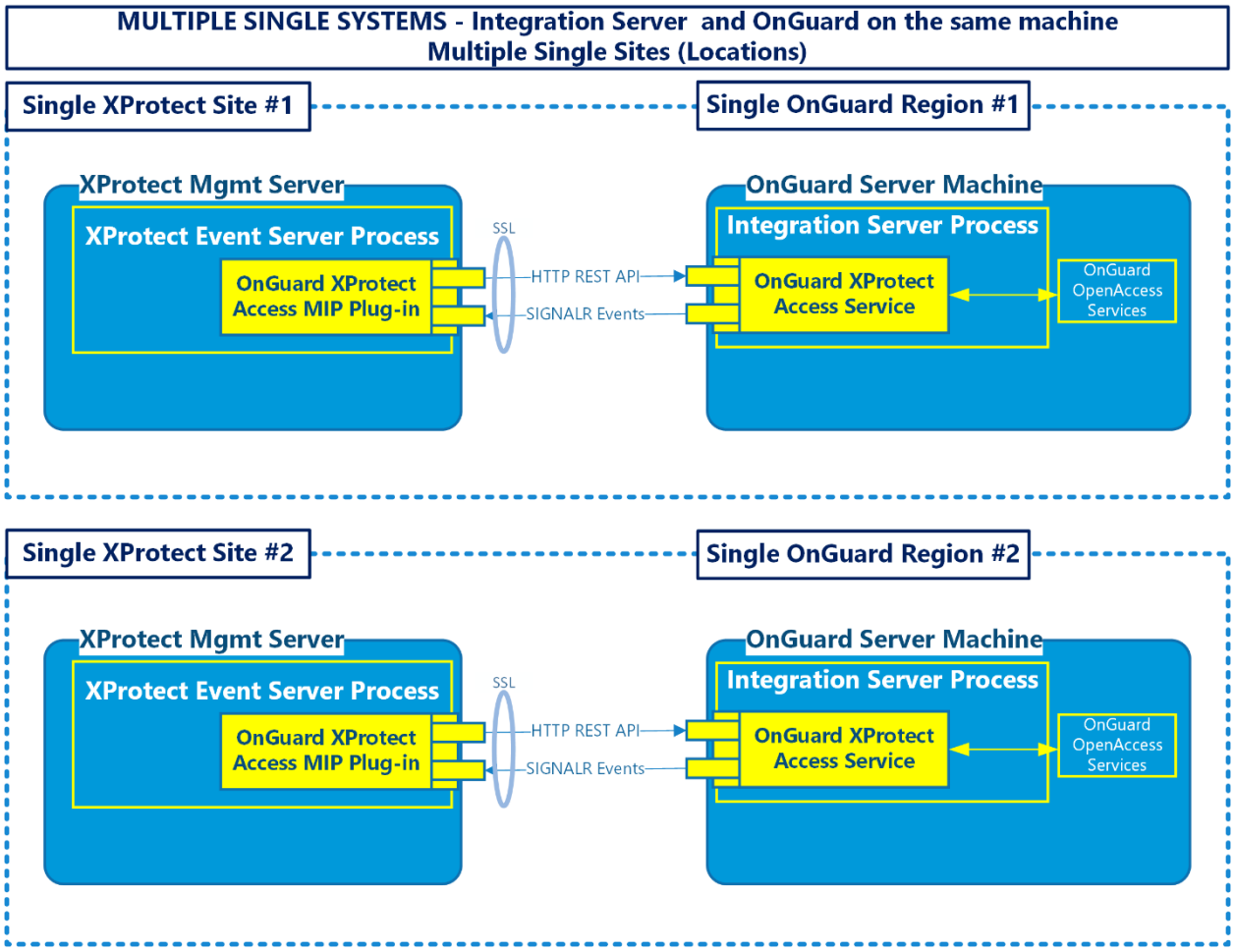


For most systems, this is the recommended installation scenario.

- First – install the OnGuard XProtect Access Service on the OnGuard server.
- Second – install the OnGuard XProtect Access MipPlugin on the XProtect server.

Multiple Single Systems

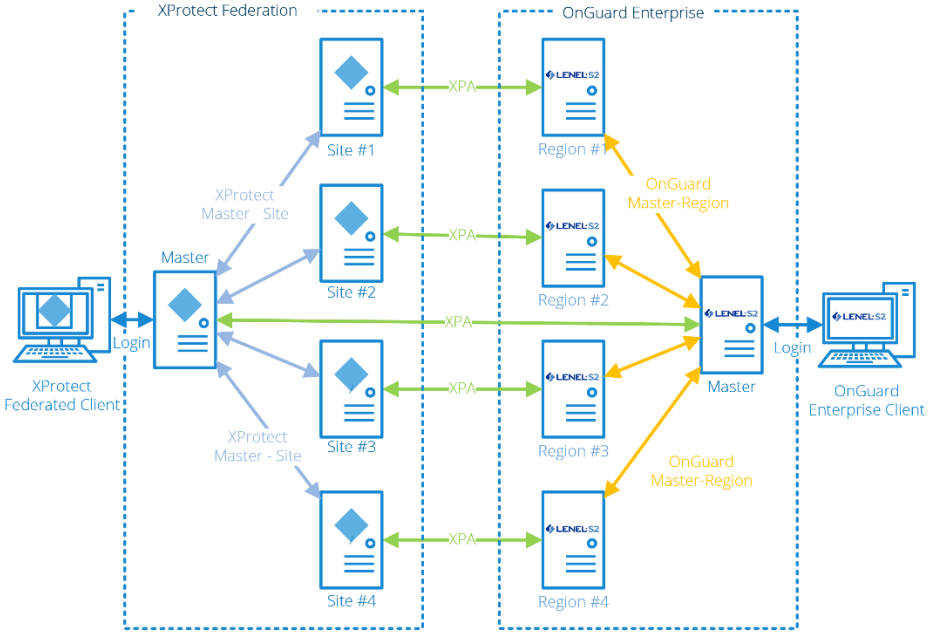
Scaling the default scenario means adding more OnGuard systems and XProtect systems in a 1:1 ratio. The OnGuard and XProtect systems are independent of each other, keeping the OnGuard XProtect Access Service on the OnGuard machine. The customer is NOT interested in centralized configuration or alarms, his multiple XProtect/OnGuard systems are independent of each other.



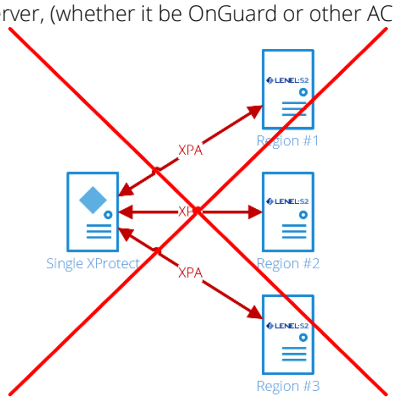
Site #1 and Site #2 are independent of each other and are not communicating with each other, or commonly managed. The same is true for both the XProtect and the OnGuard systems in this scenario.

Milestone XProtect Federation with OnGuard Enterprise

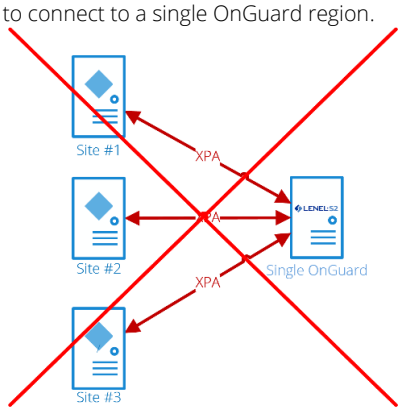
This scenario has multiple uses. It will be common for large scale deployments. This should be the default scenario when the customer already has an Enterprise deployment of OnGuard and wants to integrate XProtect. Also, it should be used when the customer wants centralized alarm and configuration management from the XProtect/OnGuard perspective.



We DO NOT support one single XProtect Site to connect to multiple OnGuard Regions. We do not recommend running more than one XProtect Access integration per event server, (whether it be OnGuard or other AC system) for performance reasons.



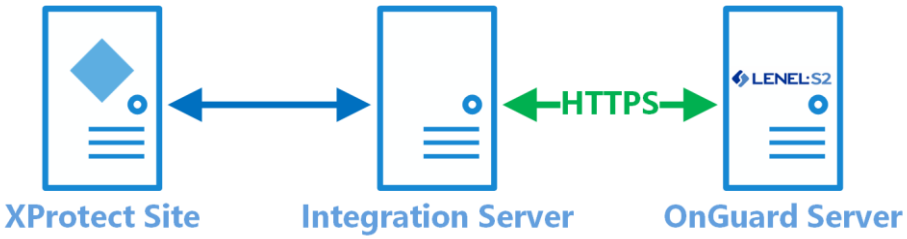
We DO NOT support multiple XProtect Sites to connect to a single OnGuard region.



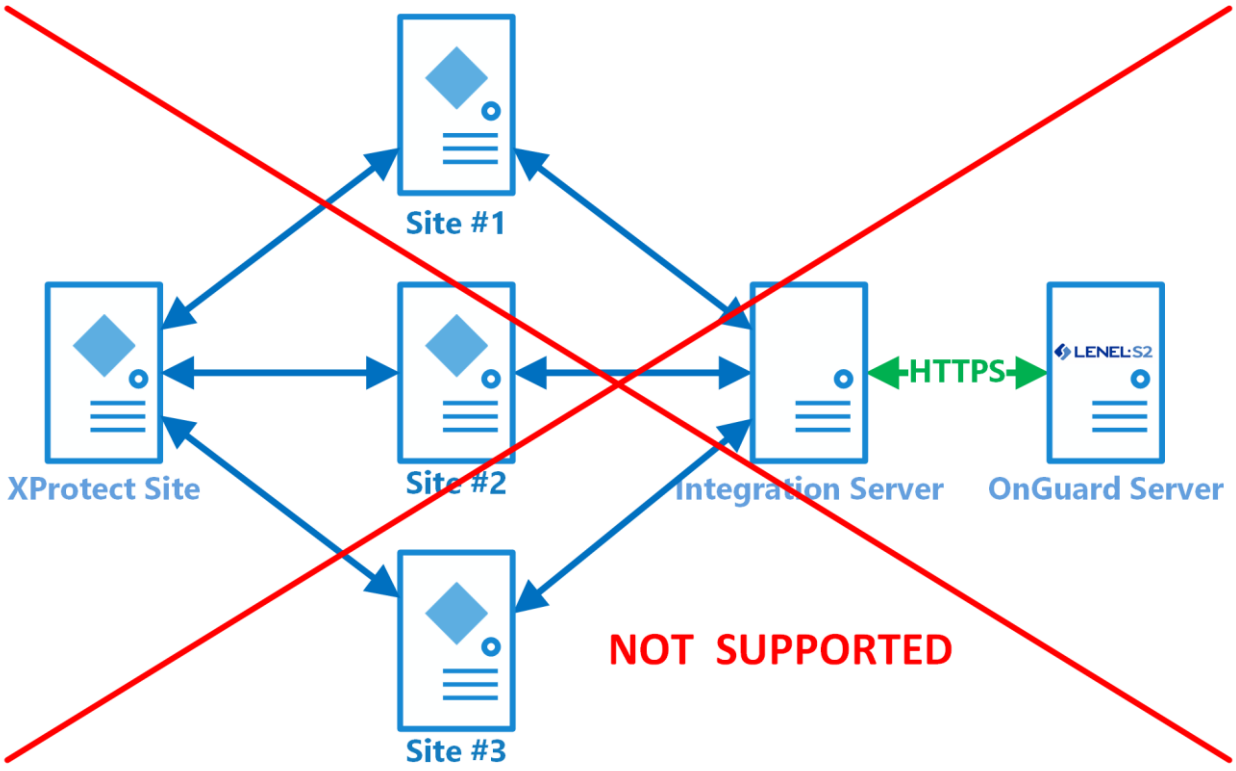
Each green XPA line represents the HTTP/SignalR connection between the Event Server in XProtect and the OnGuard XProtect Access Service on the OnGuard Server. There are some scenarios where the OnGuard XProtect Access Service may not live on the same OnGuard server, see Distributed deployment options for details.

Distributed deployment options

It is possible to have the "integration" server on a different machine than the XProtect server and the OnGuard server. These scenarios allow OnGuard segmentation of hardware and events to multiple XProtect sites and OnGuard clustering support.

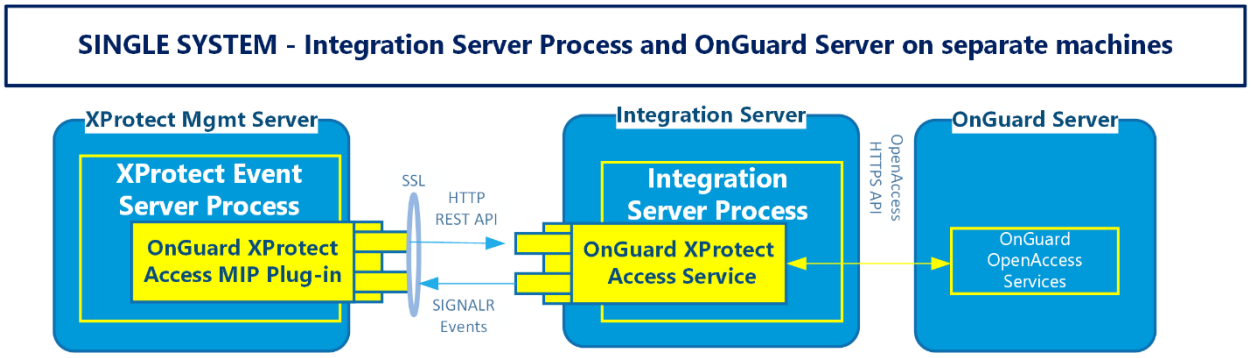


For design, scaling and performance reasons, we do not support connecting multiple XProtect sites to the same Integration Server instance.



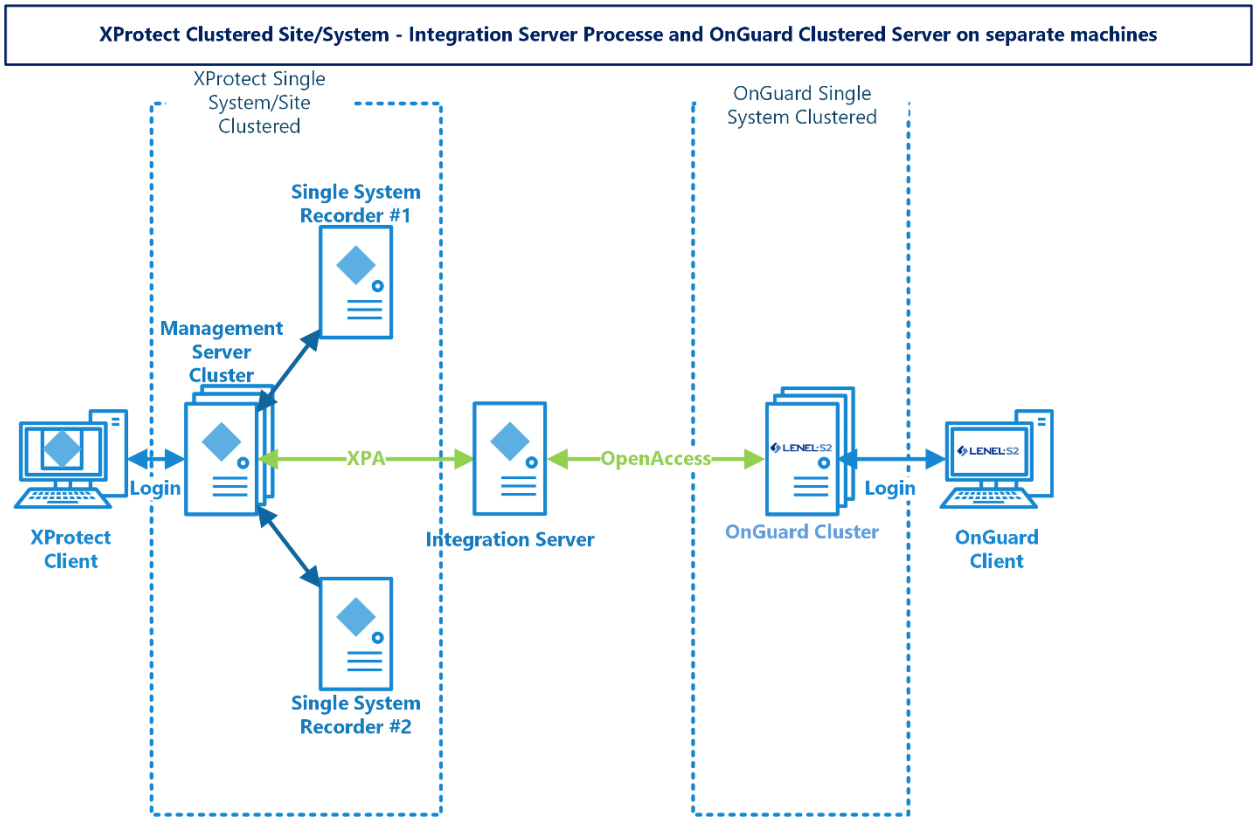
Single system with Integration Server

This scenario is used when it is required to run the Integration Server on a different machine than the OnGuard Server.



Milestone XProtect Clustered with Single Clustered OnGuard

When server clusters are used for redundancy, the OnGuard XProtect Access Service will require a separate Integration Server - distributed from both the XProtect and OnGuard servers. Below is the suggested architecture if both XProtect and OnGuard use server clusters:



Version Notes

Version	Notes
4.1	Current documentation refers to integration versions 4.1 and newer.

For more information on earlier versions, check version specific documents. For version specific change details, check release notes available with each version's documentation.

Version Compatibility

Here is the compatibility matrix between OnGuard and Milestone XProtect.

OnGuard	XP 2019 R1-R3	XP 2020 R1-R3	XP 2021 R1-R2
7.5	T	T	T
7.6	S	T	T
8.0	T	T	T

T: [Tested]	Integration is fully tested and supported on these versions
S: [Supported]	Integration is fully supported on these versions
U: [Unsupported]	Integration may or may not exist but is not supported/maintained on these versions

OnGuard Version support

Version	Minimum update / patch level	Support statement
OnGuard 7.5	7.5.375.0 and up	These versions are fully supported
OnGuard 7.6	7.6.382.0 and up	These versions are fully supported
OnGuard 8.0	8.0.458.0 and up	These versions are fully supported

Recommended OnGuard Versions

The following OnGuard versions have been tested to provide the best performance. These versions contain all documented hotfixes.

Version	Minimum update / patch level	Support statement
OnGuard 7.5	7.5.375.477 and up	Contact Carrier partner support for download
OnGuard 7.6	7.6.382.271 and up	Available through partner center downloads
OnGuard 8.0	8.0.458.29 and up	Available through partner center downloads

XProtect Version Support

Here is the XProtect version compatibility matrix between Milestone Yearly Release Versions and Milestone XProtect VMS Product Versions.

XProtect Version	XProtect Essential+	XProtect Express*	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
XProtect 2019 R1-R3	U	S	S	S	S	S
XProtect 2020 R1-R3	U	S	S	S	S	S
XProtect 2021 R1-R2	U	S	S	S	S	S

S: [Supported]	XProtect is fully tested and supported in these versions
U: [Unsupported]	XProtect is not supported in these versions

*Free XProtect Editions: Go, Essential and Essential+ are NOT supported.

Hardware Support

The following OnGuard panels have been tested and are known to be supported. More hardware models are compatible. Only the specific models listed below are known to be supported by Milestone Technical Support.

Panel Model	Description
LNL-500	Intelligent System Controller
LNL-1100	Input Control Module
LNL-1200	Output Control Module
LNL-1300	Single Reader Interface Module
LNL-1320	Dual Reader Interface Module
LNL-2210	Intelligent Single Door Controller
LNL-2220	Intelligent Dual Reader Controller
LNL-3300	Intelligent System Controller
LNL-4420	Advanced Dual Reader Controller

Secure Communication

End-to-end encryption, also known as secure communication, is compatible with all versions of the OnGuard XProtect Access integration.

You can encrypt two-way connection between the management server and any remote server (i.e., event server, recording server...etc.) in the XProtect System. You can encrypt two-way connection between a

recording server and all clients, servers, and integrations that retrieve data streams from a recording server. You can encrypt two-way connection between mobile servers and all clients, servers and integrations that retrieve data streams. For more information, see the XProtect Certificates Guide.

All versions of the OnGuard XProtect Access integration support XProtect systems configured for secure communication.

FIPS-140-2 Compatibility

Here is the FIPS-140-2 compatibility matrix between OnGuard XProtect Access Integration and Milestone XProtect. This integration is compatible with operating systems that are running in FIPS mode, it is fully tested and supported in these environments. This integration is not officially FIPS-140-2 compliant. However, XProtect and OnGuard are individually both FIPS-140-2 compliant.

OnGuard XProtect Access Integration Version	XP 2019 R1-R3	XP 2020 R1-R2	XP 2020 R3	XP 2021 R1-R2
3.5 and below	U	U	U	U
3.6 and above	U	U	S	S

S: [Supported]	FIPS-140-2 is fully tested and supported on these versions
U: [Unsupported]	FIPS-140-2 is not supported on these versions

Prerequisites

Time Synchronization

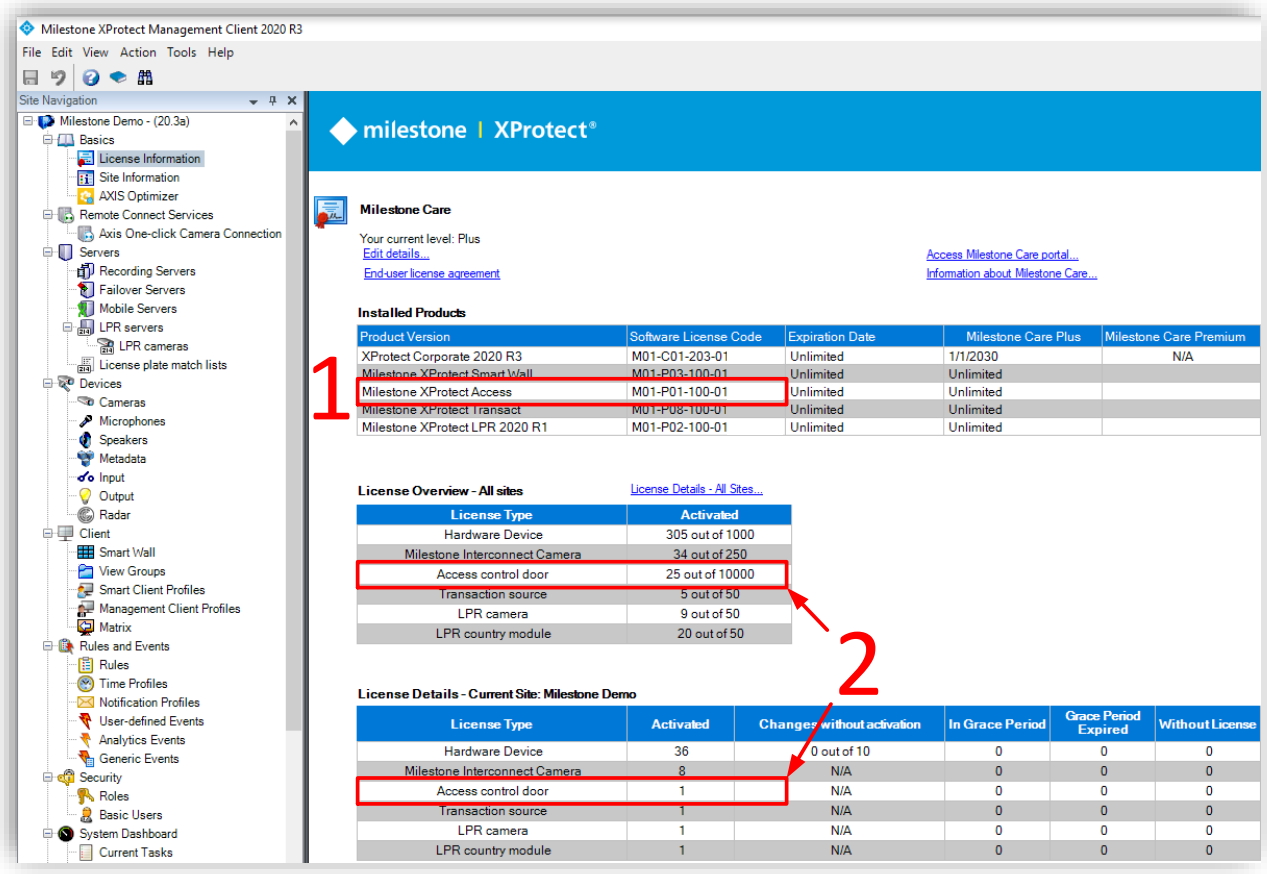
All servers (i.e. the OnGuard and Milestone machines) must be time-synchronized to within a couple of minutes of one another. See Kerberos V5 time skew recommendations here.

.NET Framework for OnGuard

.NET Framework 4.7.2 must be installed on the OnGuard server machine (NDP472-KB4054530-x86-x64-AllOS-ENU.exe). This is mostly for older OS editions; anything above Windows 10 April 2018 Update and Windows Server version 1803 will have it already installed as part of the OS. Milestone recommends that you use Microsoft Windows Server Editions of the OS.

Milestone XProtect License

The customer must have Milestone XProtect Access enabled (1) and the appropriate number of doors (2) in their XProtect SLC. See the management client license screen for more details.



Event Server DNS / Name resolution

The server hosting the Milestone XProtect Event Server must have network name resolution. It must resolve the computer name of the OnGuard Server. The OnGuard Server must also resolve the Milestone Event Server.

Smart Client Profiles

If you customize/add Smart Client Profiles, you need to include Access Control – Show access request notifications = Yes (default setting) if you want your users to see Access Control notifications.

OnGuard License Options – PLEASE CONSULT CARRIER FOR LICENSING

To enable the integration to work the following license options must be enabled in the OnGuard license:

Type of Connection	OnGuard License Options Needed
OpenAccess	OpenAccess Integration (ITM-MLST-001) enabled with an expiration date Partner Integration (IPC-311-MLST01) enabled with an expiration date

For XProtect Access version 3.5 and up, the only supported connection mode is OpenAccess. The OnGuard license must have the OpenAccess license options for the integration to function. If you are upgrading from version 3.4 with a DataConduIT license, please refer to Milestone Knowledge Base article 33277.

Required OnGuard Services

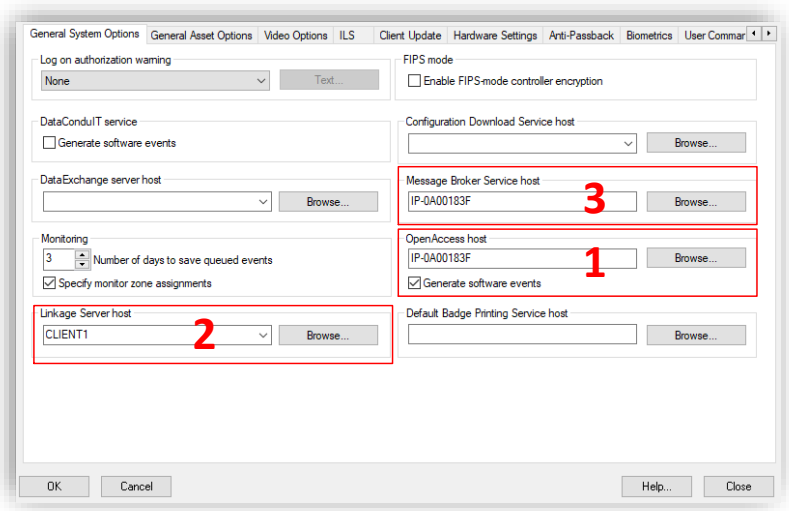
The following Windows services must be running on the OnGuard machine:

OnGuard Windows Service Name	Description
LS Event Context Provider	Required to send events from the OnGuard system
LS Message Broker	Required to receive real-time data from the OnGuard system
LS OpenAccess	Required to interface the OnGuard system web service-based API OpenAccess (REST/JSON web service)
LS Web Event Bridge	Required to receive events from the OnGuard system
LS Web Service	Required to interface the OnGuard system web-service-based events with OpenAccess (SignalR)

Generate software events

Under Administration, System Options:

1. For OnGuard versions greater than or equal to 7.4 using OpenAccess, check the OpenAccess Host and Generate Software Events checkbox.
2. Set the Linkage Server Host to the OnGuard server's machine name.
3. Set the Message Broker Service Host to the OnGuard server's machine name.

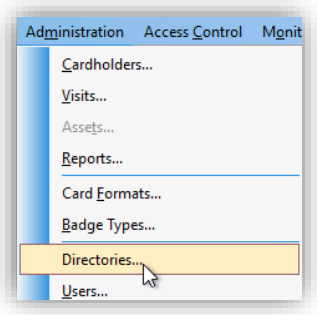


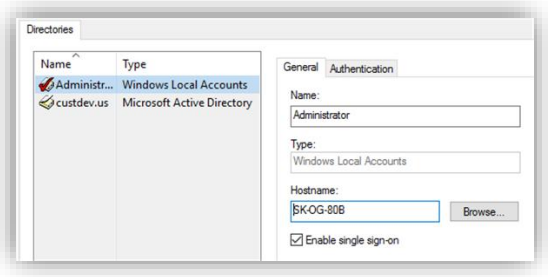
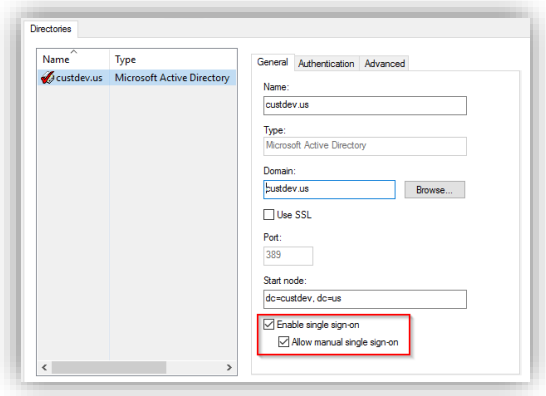
Create Single Sign-On (SSO) Directory

These instructions are not meant to replace the knowledge of a trained OnGuard system administrator. They are here to enable the basic setup of an authentication directory and SSO user, so that the integration can connect to the OnGuard system.

For an OnGuard Enterprise system, you can only create directories on the master. server.

Using the OnGuard System Administration app, go to the Administration menu and select Directories.



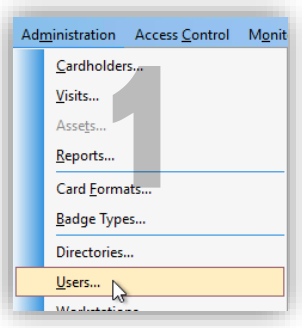
Windows Local Account	Domain User Account
For Windows Local Account support, the single sign-on account MUST be a "Windows Local Account".	For Domain User Account support, the single sign-on account MUST "Allow manual single sign-on" as shown below.
	

If you are creating a Directory of a type other than "Windows Local Accounts" (e.g. LDAP, Active Directory), ensure that the SSO user is a member of the Local Administrators group.

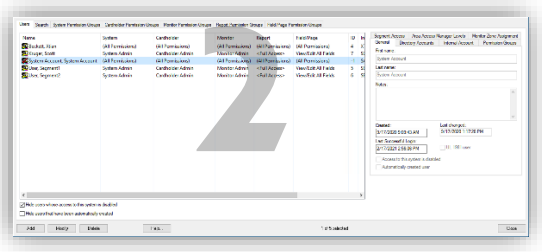
Create Single Sign-On (SSO) User

These instructions are not meant to replace the knowledge of a trained OnGuard system administrator. They are here to enable the basic setup of an authentication directory and SSO user so that the integration can connect to the OnGuard system.

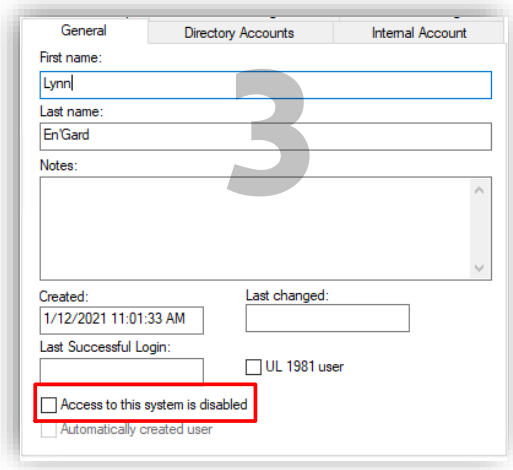
Go to the Administration menu and select Users...



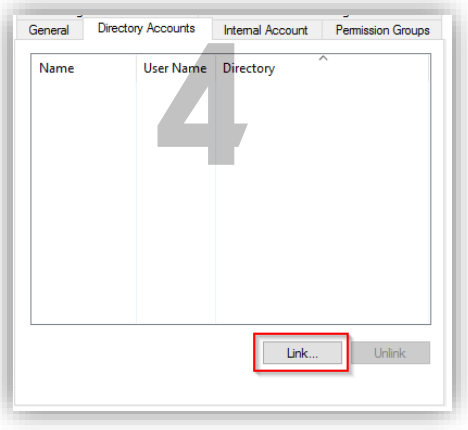
Add a new user, or modify a user from the list of internal system users.



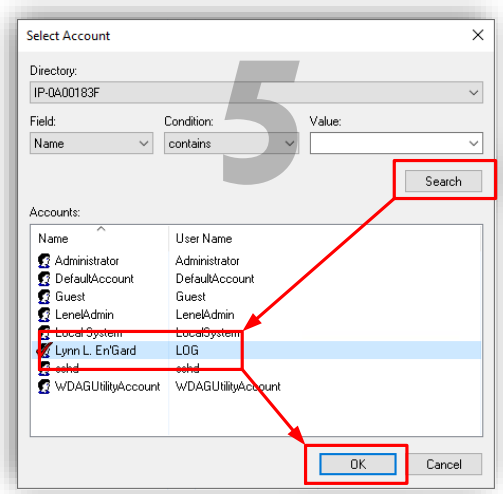
On the General tab "Access to this system is disabled" should NOT be selected.



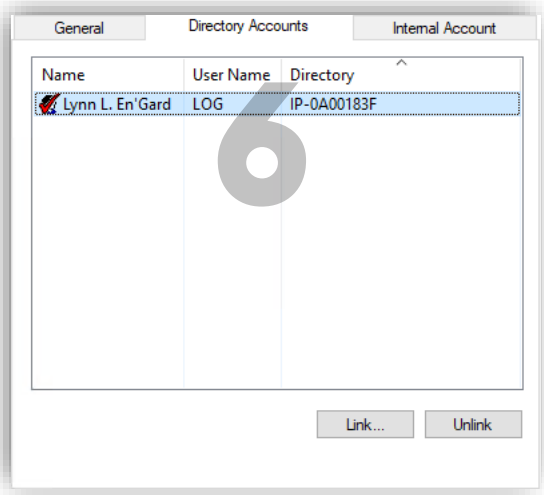
On the Directory Accounts tab click "Link" to associate the user to the directory user (or local account user) from the directory created above.



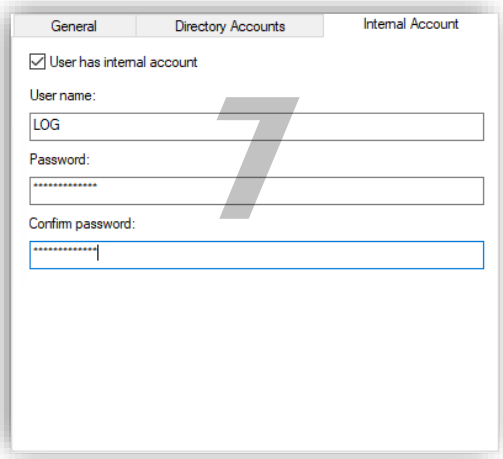
In the Select Account dialog select the directory from the Directory list. Click Search and select a user in Accounts then click OK.



Once selected, the OnGuard user account is linked to the corresponding Directory account.

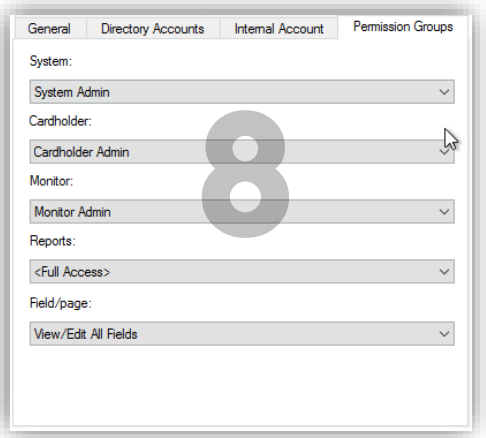


On the Internal Account tab, make sure that the "User has internal account" option is selected. Next, enter the account credentials.



On the Permission Groups tab assign the following permission groups:

- System = System Admin
- Cardholder = Cardholder Admin
- Monitor = Monitor Admin
- Reports = Full Access
- Field/page = View/Edit All Fields



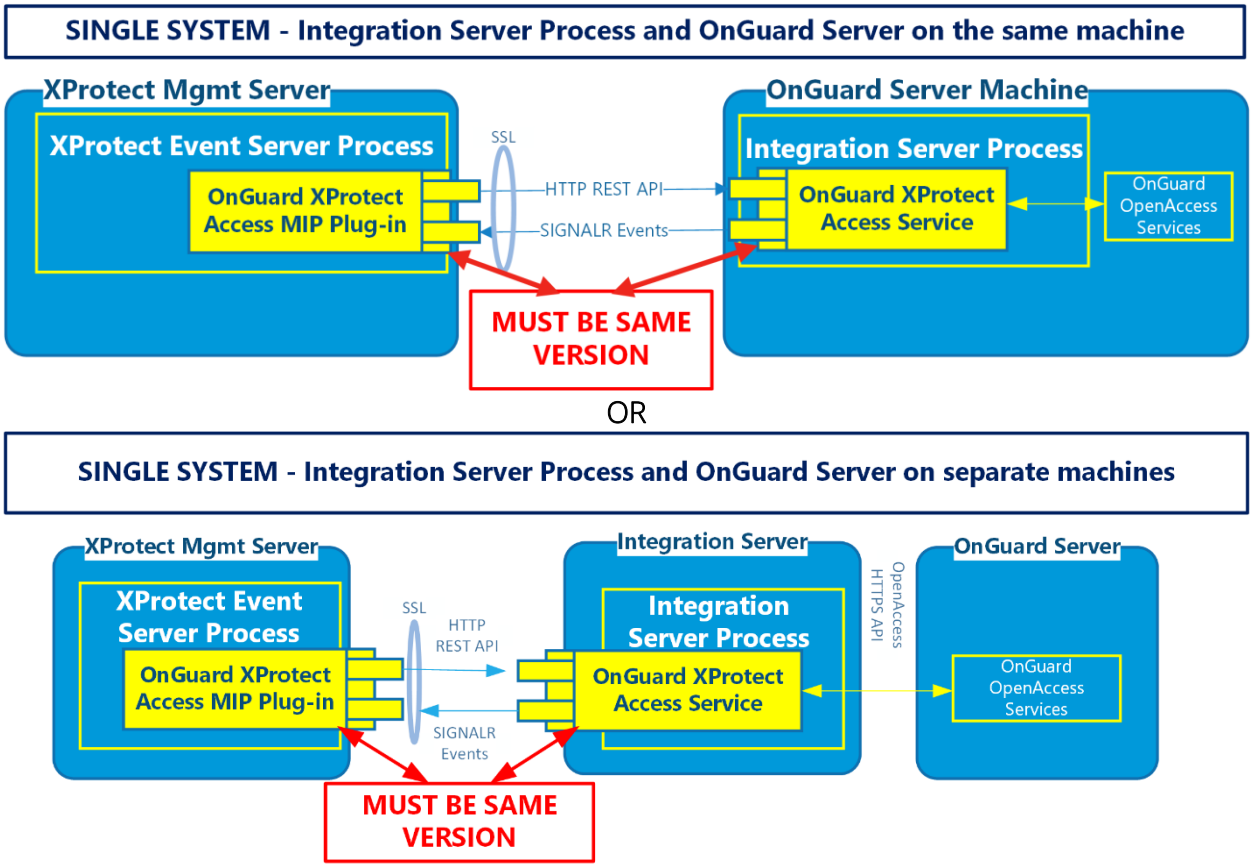
Installation

The installation package consists of one context sensitive installer program:

- XProtectAccess.OnGuard.msi

This program will detect which server it is running on (OnGuard or XProtect): and it will install the following software components:

1. OnGuard XProtect Access Service - OnGuard XProtect Access Service
   – Installed on the OnGuard server machine, or its own integration server.
2. OnGuard XProtect Access MipPlugin - OnGuard Xprotect Access MipPlugin
   – Installed on the XProtect Event Server machine – or on a standalone XProtect Management Server.

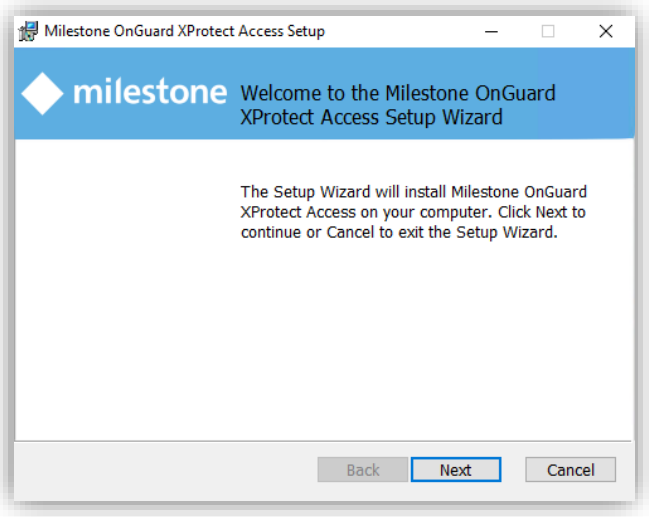


It is required that the exact same versions of the OnGuard XProtect Access Control integration software components are installed on both the XProtect and OnGuard machines.

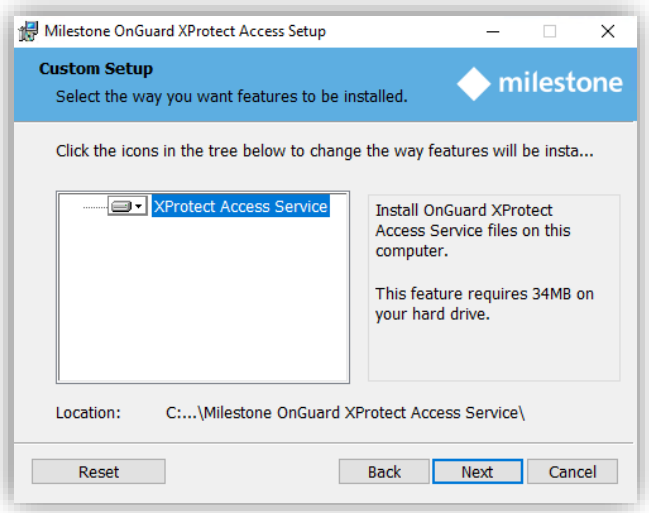
Step 1 - OnGuard XProtect Access Service Installation

Double-click the XprotectAccess.OnGuard.msi file to begin.

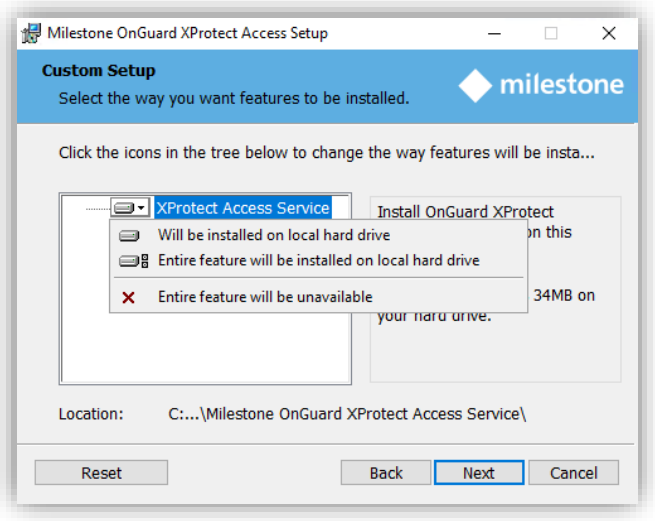
The Installation wizard launches. Click Next to continue.



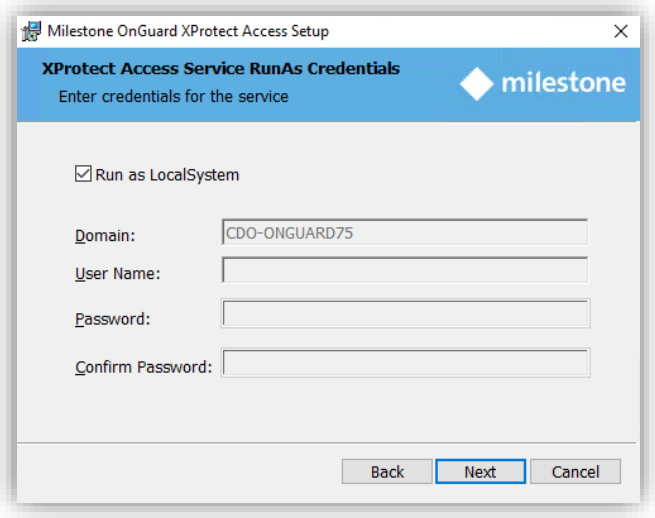
The context sensitive wizard offers to install the required components for the OnGuard XProtect Access Service. Click next to continue.



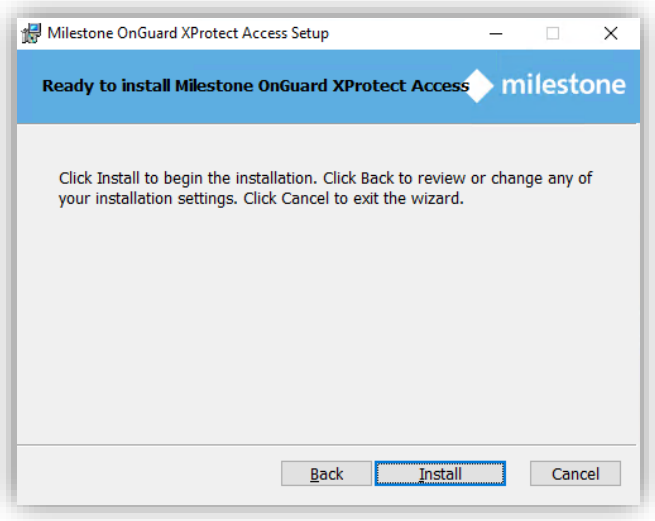
Optionally, expand the server icon menu to view installation options. The Reset button returns the wizard to all default options.



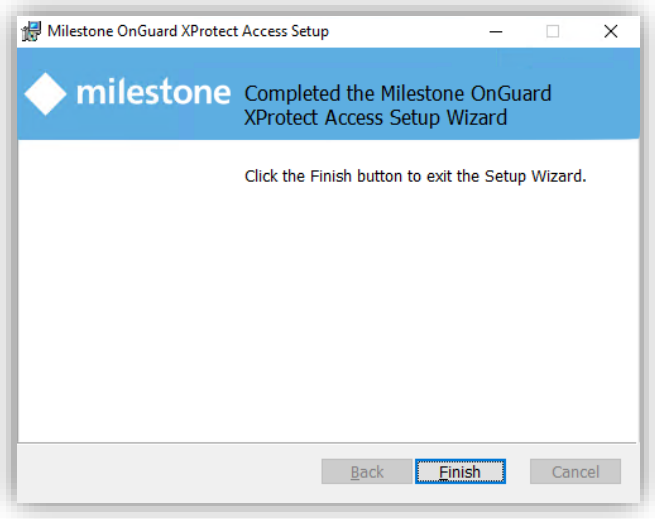
Choose which account is used to run the OnGuard XProtect Access Service. By Default the LocalSystem account should be used. Click Next.



The Ready to Install step confirms that the wizard will begin installation. Click Install.

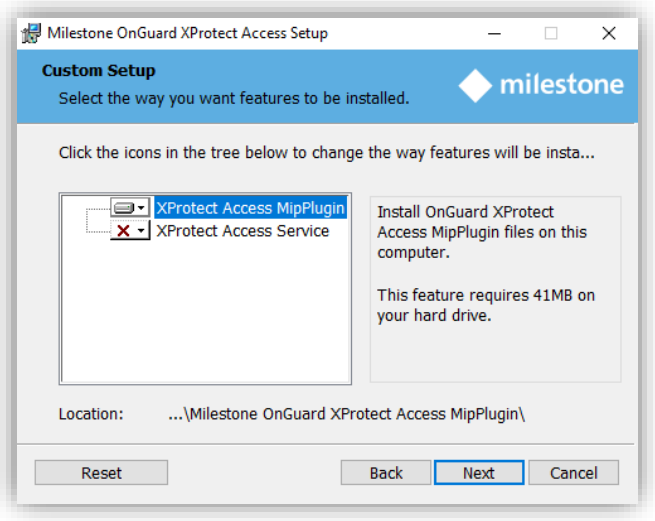


Installation is complete. Click Finish.

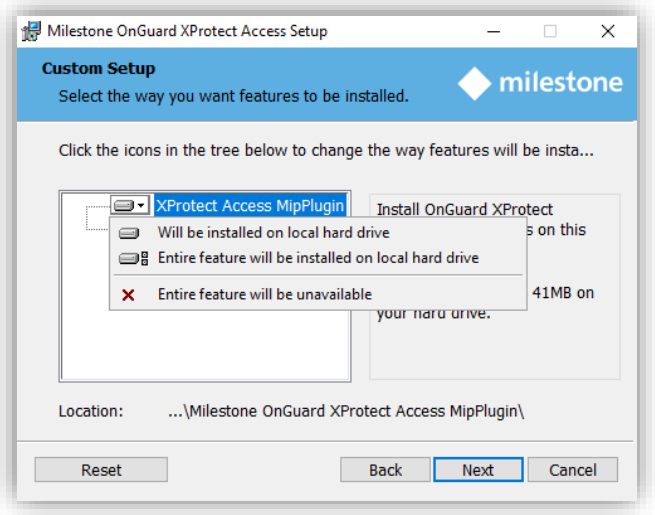


Step 2 – OnGuard XProtect Access MipPlugin Installation

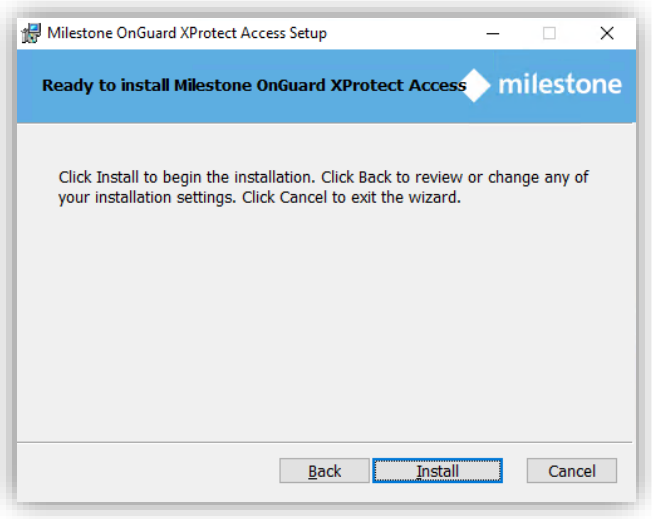
Place the XProtectAccess.OnGuard.msi file on the server where the XProtect Event Server is installed (in a typical deployment, this is the XProtect Management Server), and double-click to begin. After the opening step, the context sensitive installation wizard will offer the option to install the OnGuard XProtect Access MipPlugin. Click Next to continue.



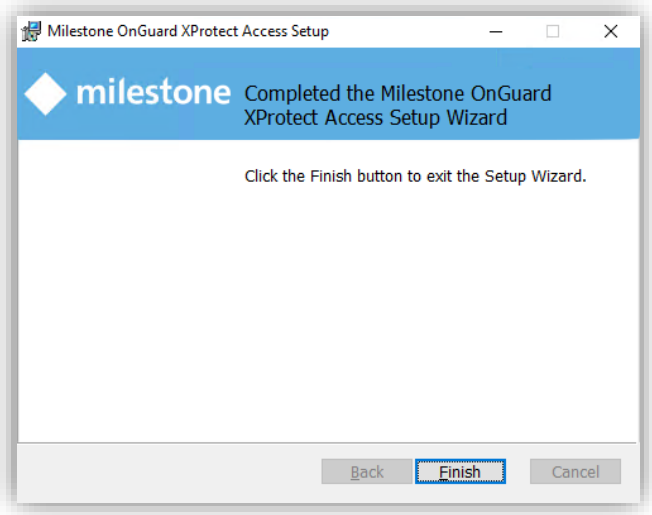
Optionally, expand the server icon menu to view installation options. The Reset button returns the wizard to all default options.



The Ready to Install step confirms that the wizard will begin installation. Click Install.



You have successfully installed the OnGuard Xprotect Access MipPlugin. Click Finish.



MIP Plugin Upgrades

All components are updated with every new OnGuard XProtect Access release. With the 4.1 version of the OnGuard Xprotect Access integration the number of required components has been reduced, and the installation program has been updated to automatically remove and replace the required files and folders during an upgrade from older versions of the integration.

The process for upgrading can be performed in any order. However, the recommended order is as follows:

1. OnGuard Server(s) – All OnGuard machines where the ACM Server is installed.

   a. Run the XProtectAccess.OnGuard.msi installation program. This will perform the following actions:
      i. Uninstall ACM Server OnGuard plugin
      ii. Uninstall ACM Server
      iii. Install the OnGuard XProtect Access Service
2. XProtect Server(s) – XProtect Event Server hosts where the Mip Plugin is installed.
   a. Run the XprotectAccess.OnGuard.msi installation program. This will perform the following actions:
      i. Uninstall the Mip Plugin and ACM Wizard
      ii. Remove the folder created by the ACM Wizard for OnGuard. Default location for this folder is C:\Program Files\Mileston\MipPlugins\OnGuardAcm Server
      iii. Install the OnGuard XProtect Access Mip Plugin and a new folder at the default location C:\Program Files\Milestone\MipPlugins\

Automatic upgrades of configured and installed instances in the Management Client are supported for all versions of the OnGuard XProtect Access integration. Simply run the XprotectAccess.OnGuard.msi installer; it will upgrade any installed components. The system should be up and running, fully functional, after the upgrade.

3. Management Client connection updates
   a. 4.1 adds two additional fields for connection between the OnGuard XProtect Access Mip Plugin and the OnGuard XProtect Access Service.



   b. The upgrade process will fill the Port field with the default value of 8443, however the Host field will remain empty. Before saving any changes in the Management Client this field will need to be filled.
   c. Fill the "XProtect Access Service – Host:" field with the Hostname for the OnGuard server or the Integration Server.
   d. The configuration stored from the previous version (hostname from the connection profile field) will be used in the background, and if that is correct the integration will continue to function. However the UI of the Management Client requires this field to be filled.



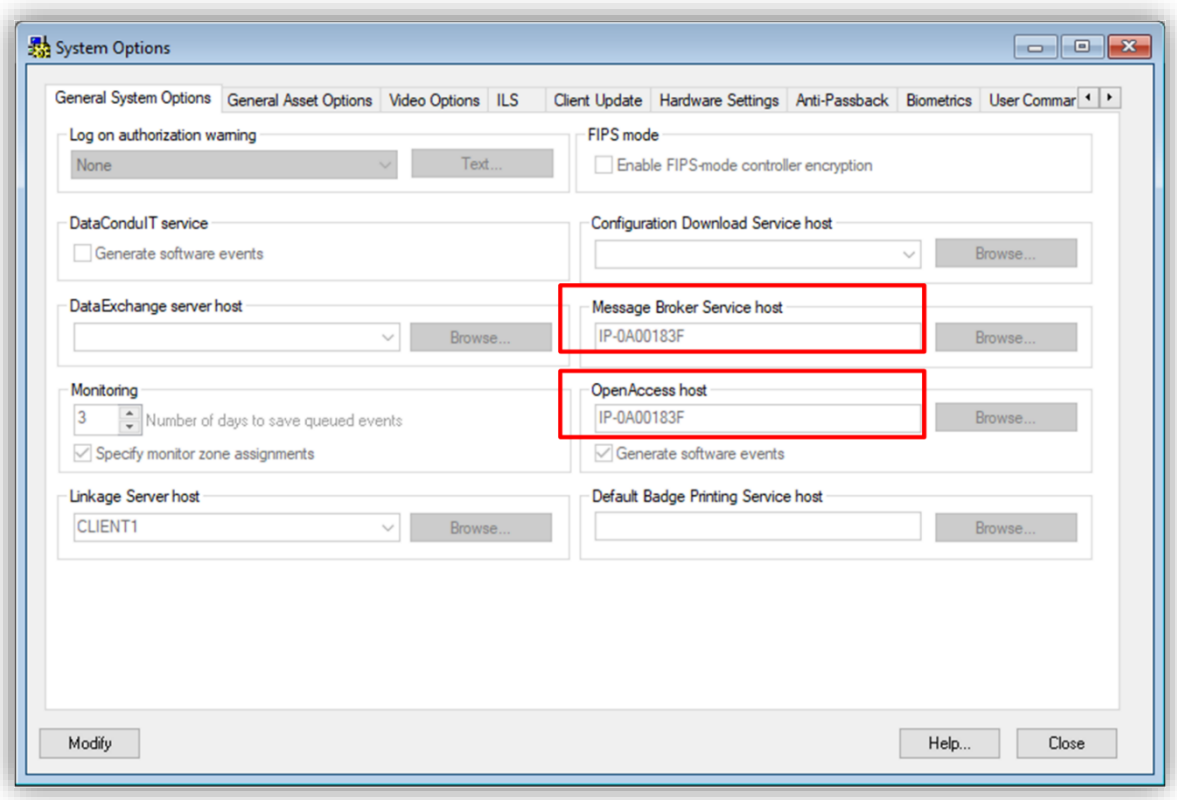
Upgrading to 4.0 or 4.1 from older versions requires reconfiguration of all rules in XProtect triggered by Access Control events or event categories. Door hardware objects are not supported as events sources in 4.0, 4.1 or newer versions, Readers must be used instead. Read the Troubleshooting section for details.

Upgrading from DataConduIT

XProtect Access integrations using versions 3.5, 3.6 or 4.0 with Open Access connection mode, may upgrade directly to 4.1. Any XProtect Access integration currently using the DataConduIT connection mode cannot upgrade directly to version 4.1 or 4.0. DataConduIT is only compatible with XProtect Access version 3.4 or earlier. All systems running XProtect Access versions 3.4 or earlier and DataConduIT need to perform the following procedure to upgrade.

Obtain the OpenAccess License. Contact CARRIER to enable the OpenAccess Integration license (ITM-MLST-001) and the Partner Integration license (IPC-311-MLST01). Once you have the OpenAccess license, go to the License Administration application on the OnGuard server. Go to Start > All Programs > OnGuard (X.X), select License Administration and then login. On the left side of the web interface select "Install new license." Upload the new license file to enable the OpenAccess features.

Verify that OpenAccess is configured in OnGuard. Go to Start > All Programs > OnGuard (X.X), select System Administration. In the System Administration client, go to the Administration menu and select System Options. Identify the host(s) running the Message Broker Service and OpenAccess services:

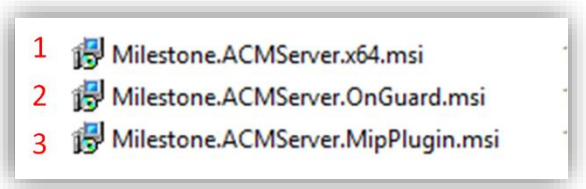


On the host(s) Confirm that the following services are all running:

OnGuard Service Name	Known Good Service Locations
LS Message Broker	On the host identified above
LS OpenAccess	On the host identified above
LS Web Service	By default LS Web Service runs on the same host as the LS OpenAccess service.
LS Event Context Provider	Must run on the same host as the LS OpenAccess service
LS Web Event Bridge	By default LS Web Event Bridge runs on the same host as the LS OpenAccess service.

Verify prerequisites are installed to support the 3.6 version of the OnGuard XProtect Access Plugin. Each downloadable .ZIP file available at download.milestonesys.com/lenels2xpa/ contains a Prerequisites folder containing any required installation programs.

Upgrade your OnGuard XProtect Access Plugin to Version 3.6. Always upgrade the ACM Server and the OnGuard ACM plugin on the OnGuard machine before upgrading the XProtect Event Server ACM MIP plugin. On the OnGuard Server, first install the Milestone ACM Server, second install the Milestone ACM Server: OnGuard Plugin. Lastly, move to the XProtect Event Server and install the XProtect Event Server ACM MIP Plugin. Here is the order of installation for all three software components of the plugin:



Refresh the configuration on the OnGuard XPA instance in the Management Client. Now, the active OnGuard XPA instance is configured to use OpenAccess connection mode, and is running on version 3.6. An upgrade directly to version 4.1 is supported.

Verify prerequisites are installed to support version 4.1. On the OnGuard Server first install the OnGuard XProtect Access Service. Next move to the XProtect Event Server and install the OnGuard XProtect Access MIP Plugin.

Refresh the configuration on the OnGuard XProtect Access instance in the Management Client and reconfigure the connection properties in the General Settings tab as required. In addition, it will be required to reconfigure any rules triggered by Access Control events or event categories which were previously in use.

Uninstalling the integration

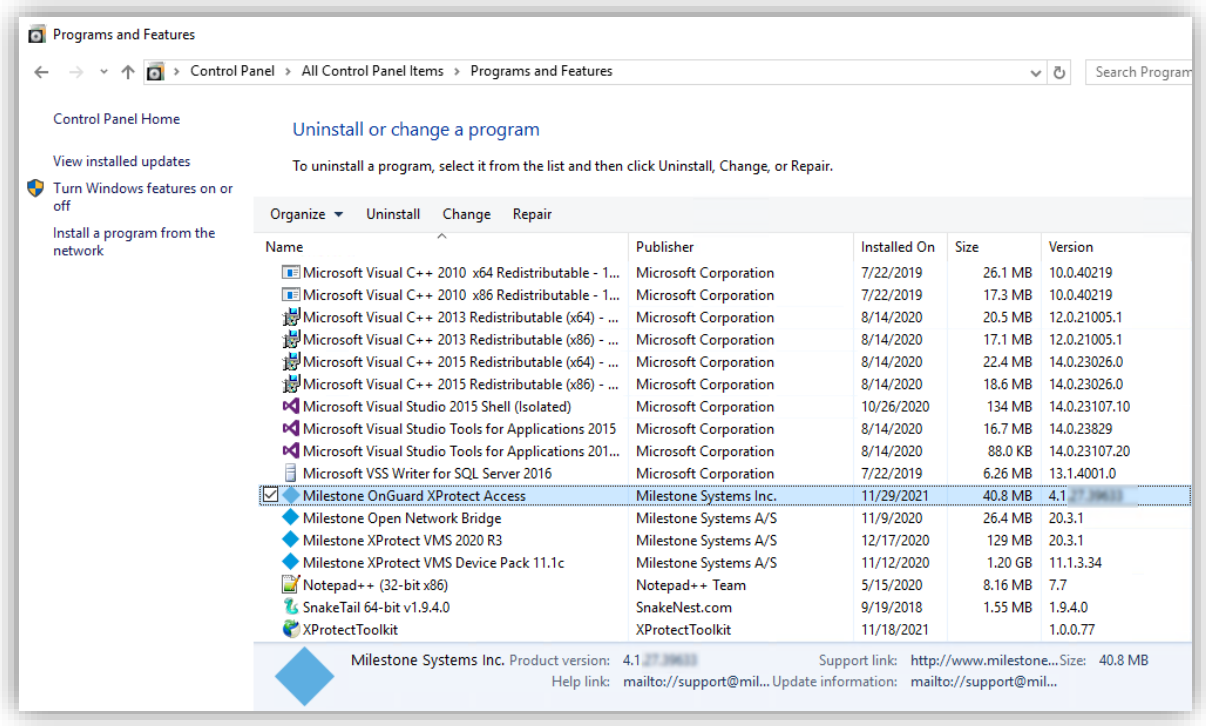
If the integration software is being uninstalled in order to revert to an older version of the integration, please refer to the troubleshooting section of this document.



If it is required to uninstall both the Milestone OnGuard XProtect Access software and the XProtect Event Server on the same server, it is required to first uninstall the Milestone OnGuard XProtect Access components and uninstall the Event Server afterward. If the Event Server is uninstalled first, the integration software will fail to uninstall.

Below is the process required to uninstall the 4.1 version of the plugin.

1. Go to the Programs and Features menu on the Milestone Server.
    a. Uninstall the Milestone OnGuard XProtect Access component.

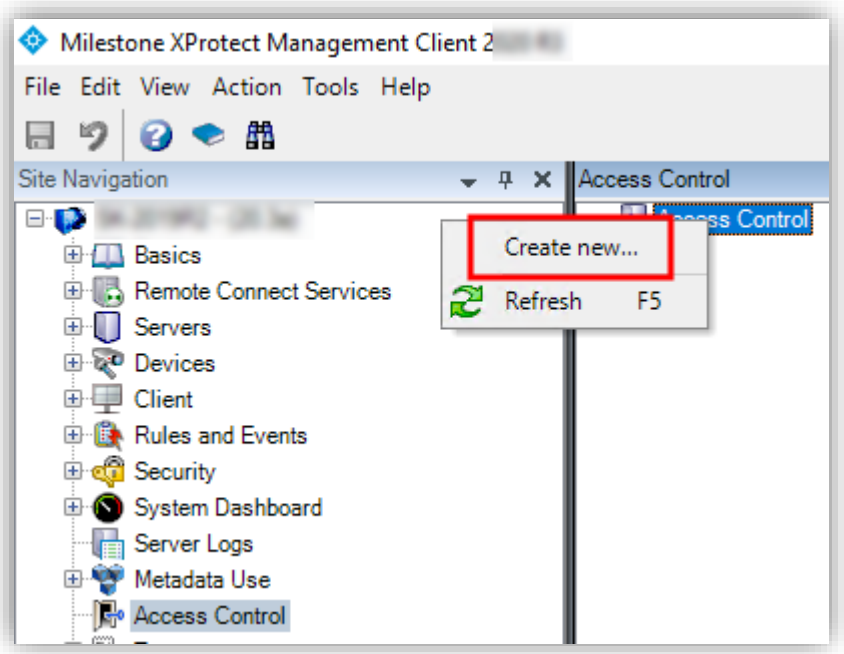


2. Go to the Program and Features menu on the OnGuard Server.
    a. Uninstall the Milestone OnGuard XProtect Access component.

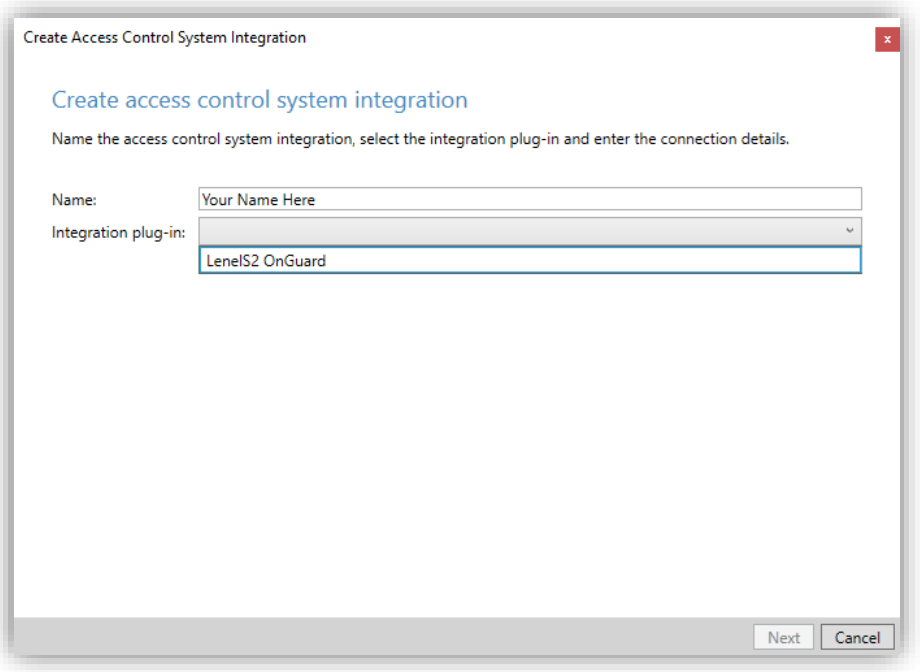
XProtect Management Client Configuration

XPA Instance Creation Wizard

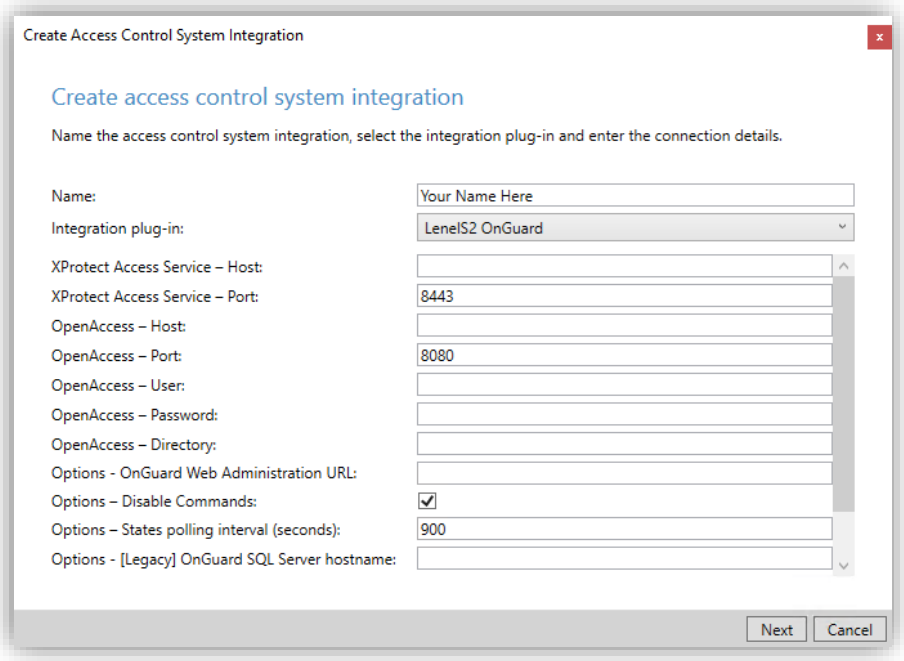
After the OnGuard XProtect Access Mip Plugin is installed and configured on the XProtect Event Server, the Access Control instance can be created in the XProtect Management Client. Right-click on the Access Control Root Node and select Create new... to begin the wizard.



Enter a name for the instance and select the Integration plug-in. Note that you will find a plugin named LenelS2 OnGuard.



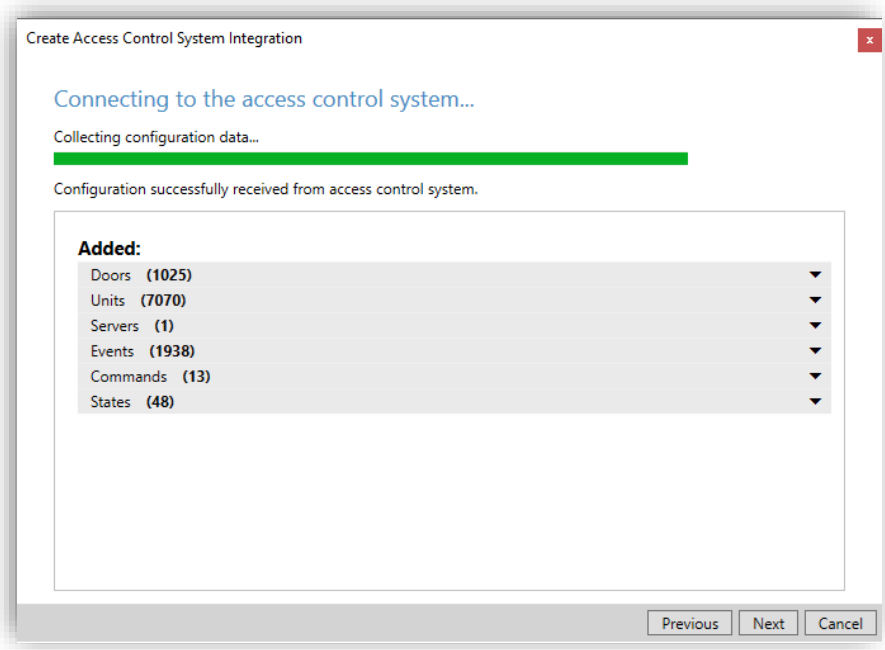
After naming and selecting the plugin there are a set of required credentials, parameters, and options to complete. These are required to define the connection to the OnGuard server. All the properties used for all versions of OnGuard are shown in the Management Client wizard.



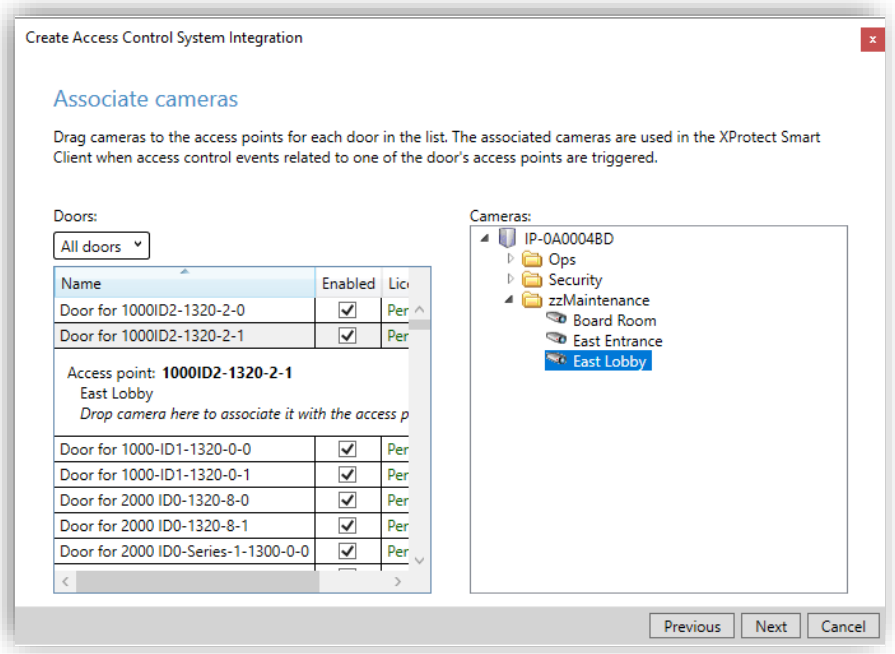
Fields required to establish the connection are listed below. It is possible to populate any field available at this step in the process, the fields listed are the minimum required and will allow successful connection.

Empty Field Names	Required Values
XProtect Access Service – Host:	Hostname for the OnGuard server or the Integration Server.
XProtect Access Service – Port:	Default port is 8443.
OpenAccess – Host:	IP address for the OnGuard server.
OpenAccess – Port:	Default port is 8080.
OpenAccess – User:	SSO user defined in OnGuard
OpenAccess – Password:	Password for SSO user.
OpenAccess – Directory:	Directory for SSO user.

After the connection is created, the wizard will import data from the OnGuard server. This includes Doors, Units, Servers, Events, Commands, and States. Click Next.

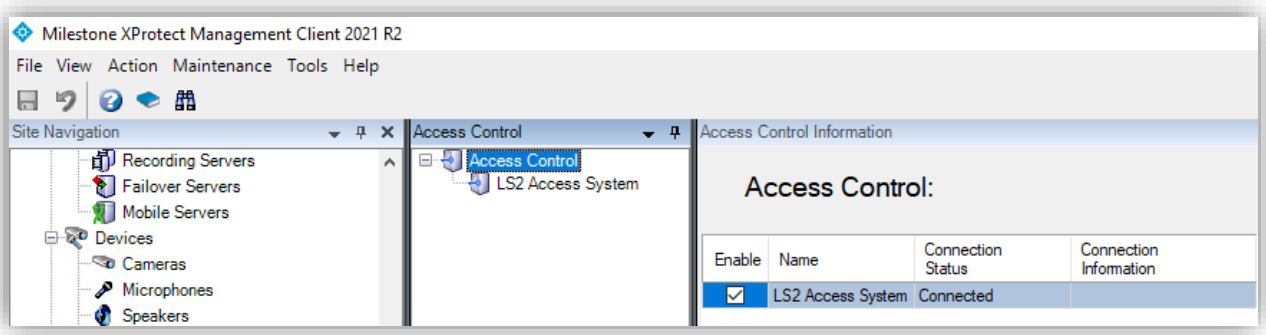


On the following page you can associate doors with cameras. This is done by selecting a camera and dragging it to one of the imported doors. Click Next after association of doors and cameras. The configuration will be saved, and the wizard is complete.

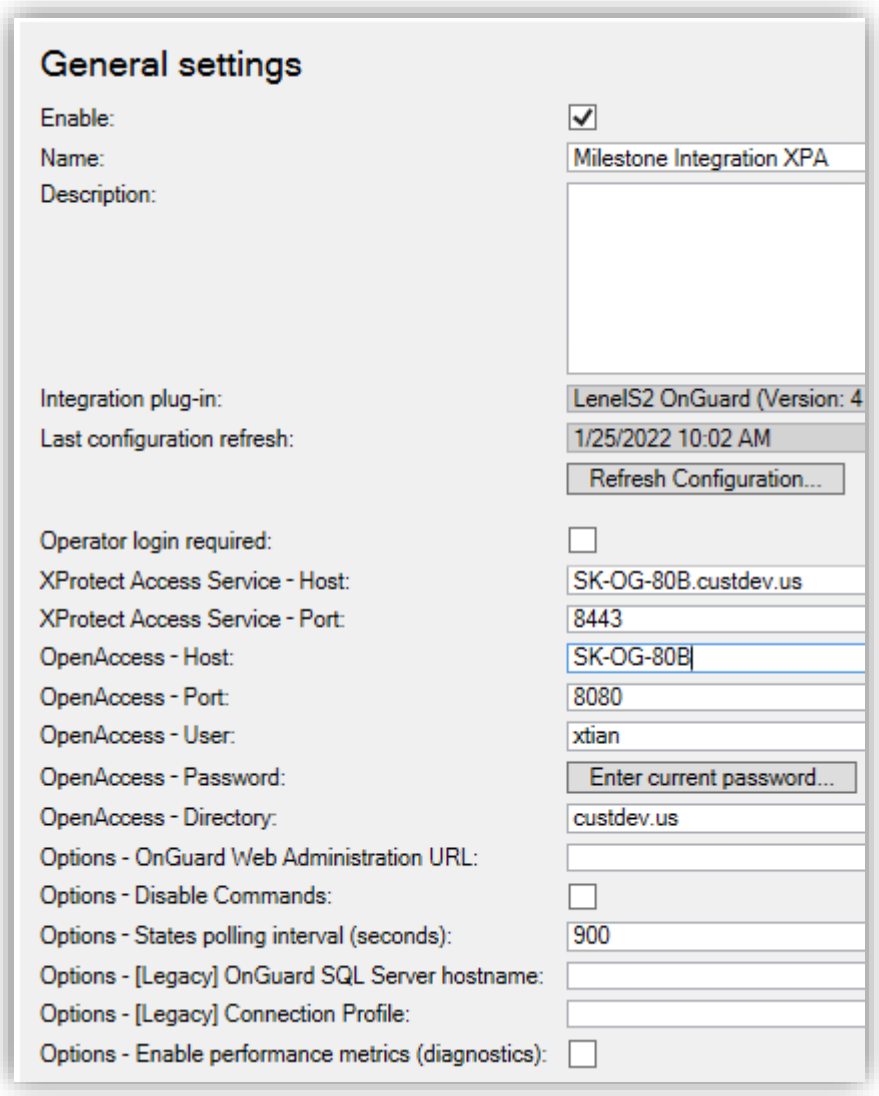


XPA Instance Status & Properties

Go to the Access Control menu in the directory tree of the XProtect Management Client. You can check the status of all instances by selecting the root of the Access control directory.

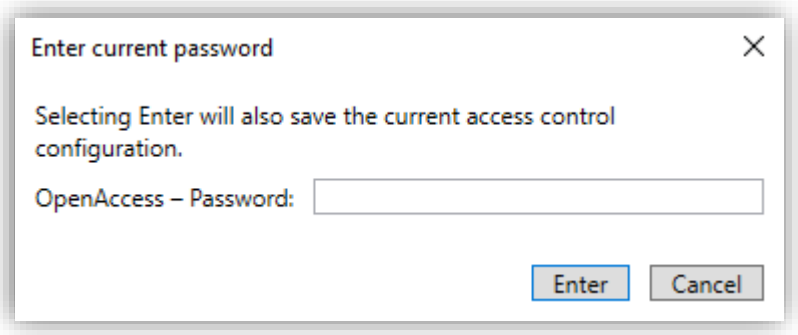


Click on your OnGuard XPA Instance to view or modify the properties of the connection.



Below, the properties are listed.

Property Name	Description - Purpose
Enable:	Selected by default. Remain selected to keep connection properties active.
Name:	Custom name field.
Description:	Reference information field.
Integration plug-in:	Displays the current version of the OnGuard XProtect Access Mip Plugin.
Last configuration refresh:	Displays the date and time the last system configuration refresh was performed.
Operator login required:	Not selected by default. This option should be selected to enable the personalized login feature.
XProtect Access Service – Host:	Host name of the OnGuard server or the Integration Server where the OnGuard XProtect Access Service is installed.

XProtect Access Service – Port:	8443 is the default port.
OpenAccess – Host	IP address of the machine hosting the OnGuard OpenAccess service.
OpenAccess – Port:	The port the OnGuard OpenAccess service is listening on. 8080 is the default port.
OpenAccess – User:	An OnGuard administrative user to log into the OnGuard OpenAccess web service. This user should have access to all hardware, cardholders, etc in the system. Windows user account if using Directory users, OnGuard internal user account if using internal directory.
OpenAccess – Password:	The password of an OnGuard user which is used to log into the OnGuard OpenAccess web service. In XProtect versions 2021 R1 forward, after the password is entered correctly in the XPA instance creation wizard, this field is replaced by the "Enter current password..." button in the General Settings tab. If the SSO user account is changed to modify the integrated hardware device set, or the current user's password needs to be updated - click the button to open a dialog box which allows the password to be changed. 
OpenAccess – Directory:	The name of the OnGuard directory to be used when logging into the OnGuard OpenAccess web service. If left blank, the OnGuard internal directory will be used.
Options – OnGuard Web Administration URL:	A URL that opens the OnGuard web-based administration portal can be added. This will provide a link to the portal from the Smart Client Access Control Workspace. By default the location for this URL is: https://HostName:8080/#/Login - Where HostName is replaced with the hostname of the OnGuard server.
Options – Disable Commands:	Selected by default. This option controls all Command interaction between XProtect and OnGuard access control hardware devices.
Options – States polling interval (seconds):	Default value is 900 seconds. Frequency of status updates retrieved for AC hardware devices. Increase this value to provide more consistent event processing throughput.
Options – [Legacy] OnGuard SQL Server hostname:	The SQL server hostname in systems upgraded from 3.X versions to the current 4.X version which does not require a SQL server hostname to establish the connection.

Options – [Legacy] Connection Profile:	This value will be automatically filled for systems upgrading to 4.1 or newer versions of the integration from a 4.0 or older version. It is not required.
Options – Enable performance metrics (diagnostics):	Not selected by default. Select this option to include performance statistic logging on event metadata.

You can verify that the integration module is now connected by looking at the Access control tree.

Personalized Login

Personalized login is an optional feature of XProtect Access. Personalized login takes advantage of OnGuard segments to divide system users, access control hardware, events and alarms into groups, or "segments."

When a user logs into Smart Client, the personalized login feature presents a second login procedure that authenticates with the integrated OnGuard system. When the user presents valid OnGuard credentials, the Smart Client's XPA features will be dedicated to access control hardware, events and alarms within that user's OnGuard segment.

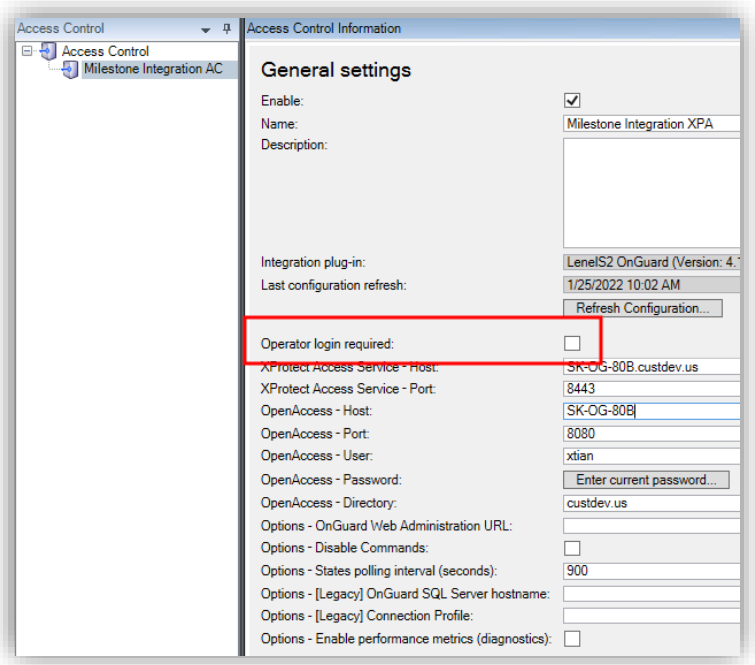
Personalized login manages two configurations. First, is the global configuration used by the Management Client. Second, is the personalized configuration used in the Smart Client. Personalized configurations are subsets of the global configuration. This helps ensure accurate event handling, command execution...etc.

Personalized login has specific requirements:

- OnGuard 7.4 or higher
- XPA 3.5 or higher

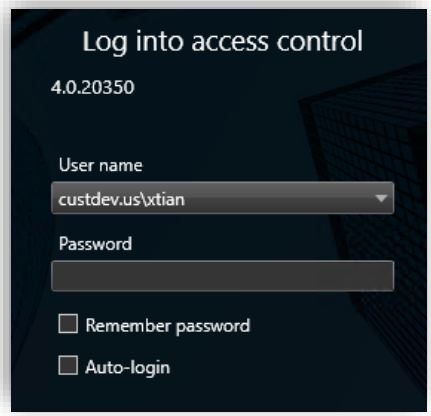
Enable/Disable Personalized Login

Enabling/disabling personalized login for a specific access control plugin is done in the Management Client. The option is located in the General setting menu and is titled "Operator login required:"



Smart Client Personalized Login

A second Log into access control dialog is required. It occurs immediately after the standard Smart Client login dialog.



OnGuard requires three pieces of data:

1. directory
2. user name
3. password

The XProtect Smart Client dialog only has boxes for user name and password. Enter the directory with the user name in this format:

- DirectoryName\UserName

If no directory is provided, the OnGuard "internal" directory is used. OnGuard allows special non-alphanumeric characters, control characters, and spaces in directory names. Use of these characters is NOT COMPATIBLE with XProtect. If these types of characters are included in the OnGuard directory, authentication will fail.

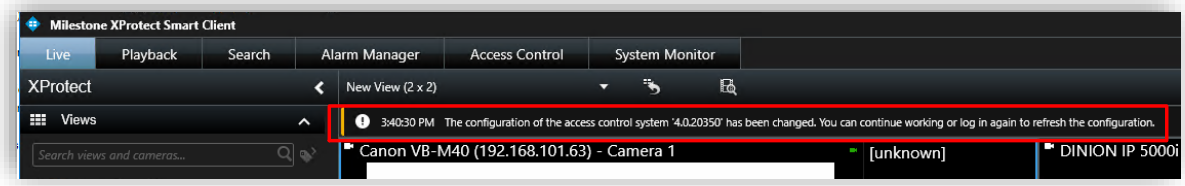
After entering the directory\username and password, the XProtect Smart Client validates the credentials. If you click Skip this step, the Smart Client is opened without using personalized login, and no XPA features are available in the Smart Client. After authentication with OnGuard, Smart Client loads a personalized configuration. The Smart Client will only display access control information from the same segment of the user account that logged in during the personalized configuration login dialog. This includes:

- Alarms related to hardware in their segment.
- Events related to hardware in their segment.
- Devices in the map element selector that are in their segment.

Refreshing Personalized Configurations

The XProtect Event Server stores personalized configurations for XProtect Smart Client users. Stored personalized configurations are cleared when the Event Server restarts. When the global configuration of the XPA instance is refreshed, the Event Server updates all stored personalized configurations.

After the global configuration is updated, all open Smart Clients using a personalized configuration will have the following info message displayed.



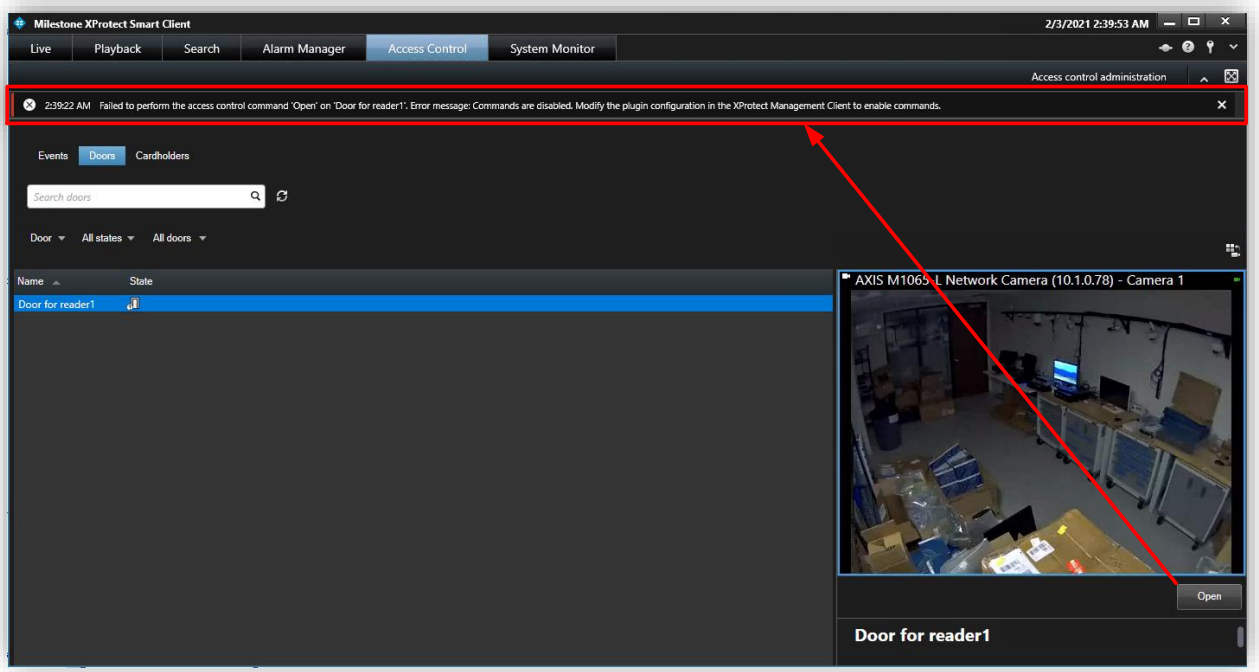
Log out of the Smart Client and log back in using the personalized configuration to load the updated configuration.

Commands:

Commands are used in the XProtect Access OnGuard integration to interact with access control devices. By default, commands are disabled in the plugin configuration. This can be changed in the XProtect Management Client by clearing the "Options - Disable Commands" check box.

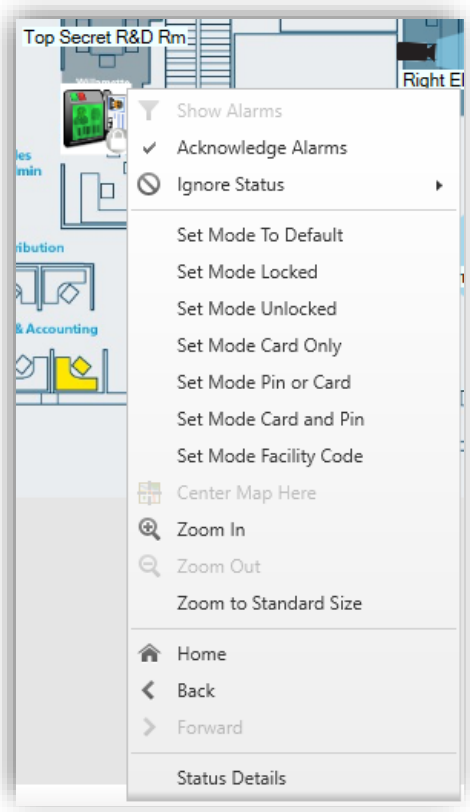
If Commands are disabled, none of the functionality will work, however it is still possible to view Command buttons in the Smart Client and create rules in XProtect which use Commands. These rules will validate, and the buttons can be clicked, but nothing will happen. In the Smart Client users will receive the following error message:

*"HH:MM:SS AM/PM Failed to perform the access control command '**COMAND**' on '**DEVICE**'. Error Message: Commands are disabled. Modify the plugin configuration in the XProtect Management Client to enable commands."*

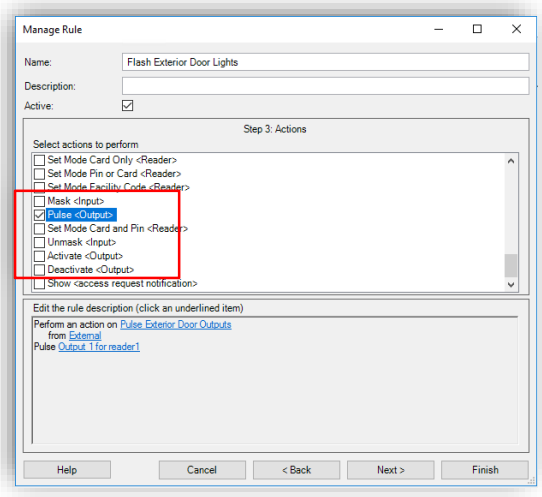


Commands trigger state changes in the access control hardware devices. Commands can be triggered in four ways with the XProtect Access OnGuard integration. The XProtect Rules system can be used to trigger Commands. Access Request Notifications can include commands. Any location in the Smart Client where doors are visualized, such as the Access Monitor or the Access Control workspace, can contain Command buttons. And lastly, the Map interface within the XProtect Smart Client can include Access Control device icons which can be used to trigger commands.

The following are the devices and their supported commands.

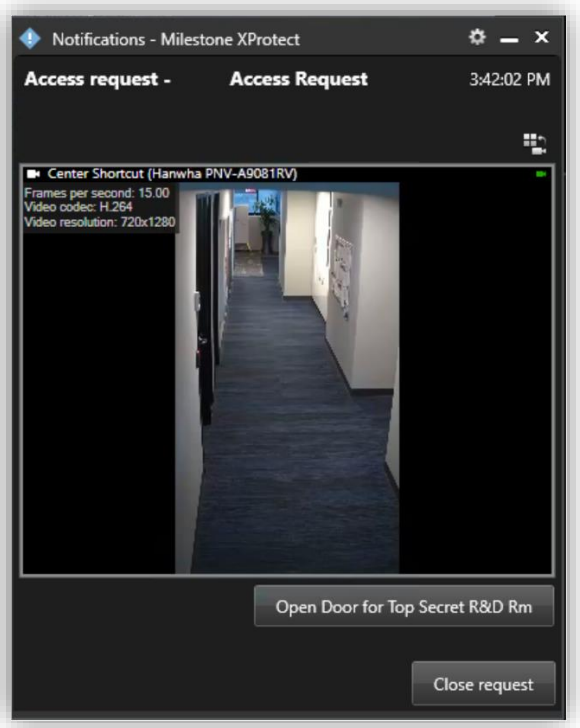
Readers:	• Set Mode To Default • Set Mode Locked • Set Mode Unlocked • Set Mode Card Only • Set Mode Pin or Card • Set Mode Card and Pin • Set mode Facility Code	

Set Mode Commands for readers will change the type of authentication mode the reader can respond to. For example: a rule could be used to switch readers into unlocked mode during business hours.

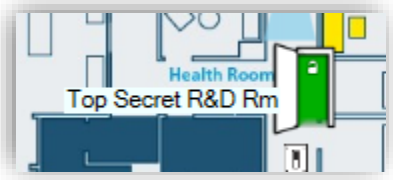
Reader Inputs:	• Mask • Unmask	
Reader Outputs:	• Activate • Deactivate • Pulse	

Reader inputs can be masked or unmasked. When an input is masked, status of that input is not reported or saved in the OnGuard system. When it is masked, the reader input has a "mask" icon attached

to it on the Smart Client Map. Unmask removes the mask on the icon and allows the status of that input to be reported and saved within OnGuard. Reader outputs can be activated, de-activated and pulsed using the respective commands. The Pulse Command will activate the output temporarily, then deactivate it. An activated output will have a red circle icon attached to it when viewed on the Smart Client Map.

Doors:	• Open	

Doors can be opened via the Command. When the door is opened, the door icon animation displays this status on the Smart Client Map.



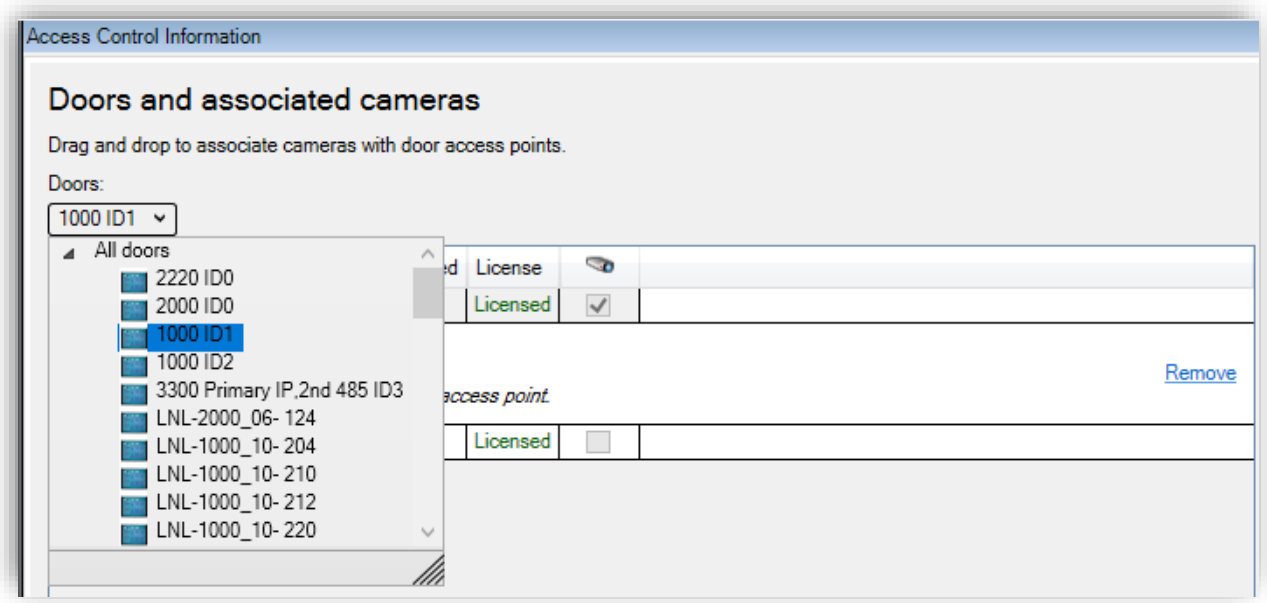
Administrative Configuration

Door & Camera Association

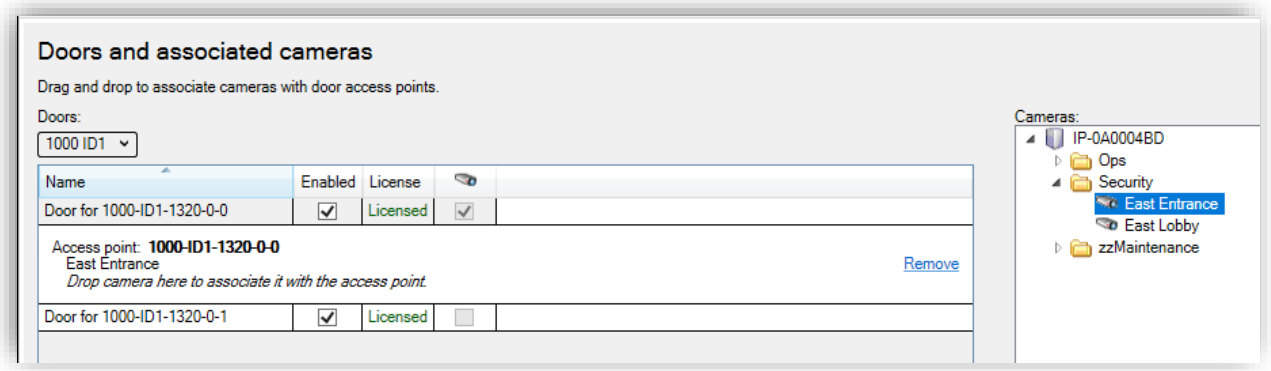
In the Doors and Associated Cameras menu of the XPA Instance it is possible to verify the status of all connected doors, and create, reassign, and remove the association between cameras and doors.

Doors require associated cameras to view live and recorded video - and listen to or play audio through any XProtect client application that supports visualization of doors.

Open the doors list and select a panel to view all doors connected to that panel.



Click on a door. Under it all associated cameras are listed. Select a camera from the Cameras list on the right and drag the selected camera into the list of cameras associated to the chosen door. Click the Remove link to end the association between the camera and the door.



Categorize Events

Large scale access control systems, such as those managed by OnGuard, need to functionally integrate with XProtect without programming large numbers of individual alarms and rules. Categorizing access control events greatly minimizes the number of individual alarms and rules that need to be programmed.

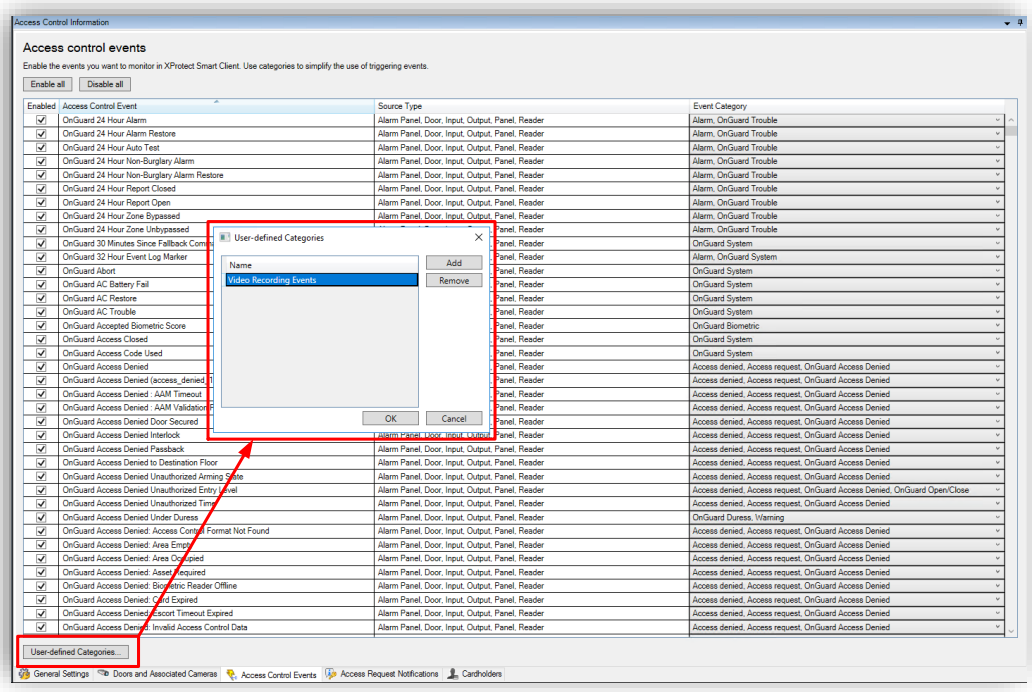
To generate XProtect alarms or rule-based actions triggered by any one of a group of individual OnGuard events, the events must be categorized. For example, the integration can be configured to start recording video from associated cameras based on any number of unique OnGuard hardware events: "Door Forced," "Denied, Badge Not in Panel," and "Access Denied Unauthorized Entry Level." Chosen events are placed in the same category, and then a rule is created to start recording based on the receipt within XPA of any event in that category.

The categories are:

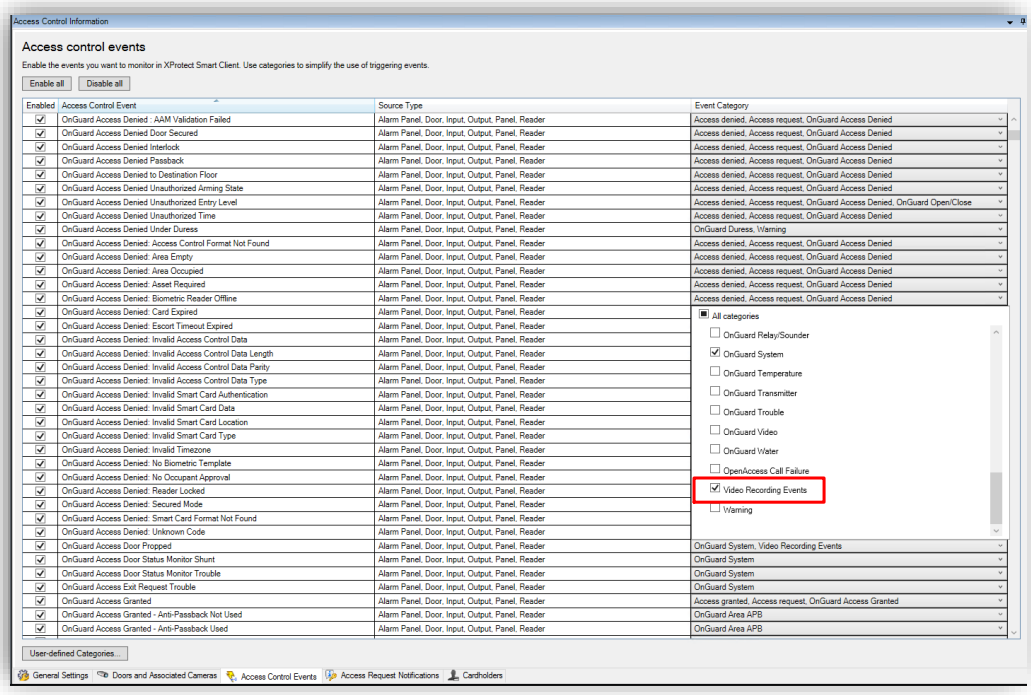
Default XPA Events	OnGuard Events	Custom Events
• Access Granted • Access Request • Access Denied • Alarm • Error • Warning	• OnGuard Access Denied • OnGuard Access Granted • OnGuard Area APB • OnGuard Asset • OnGuard Biometric • OnGuard Burglary • OnGuard C900 • OnGuard Digitize • OnGuard Duress	• User Defined Category...

	• OnGuard Fire 7 • OnGuard Fire 8 • OnGuard Fire 9 • OnGuard Gas • OnGuard Generic • OnGuard Host Messages • OnGuard Intercom • OnGuard Medical • OnGuard Muster • OnGuard Open/Close • OnGuard Point of Sale • OnGuard Portable Programmer • OnGuard Relay/Sounder • OnGuard System • OnGuard Temperature • OnGuard Transmitter • OnGuard Trouble • OnGuard Video • OnGuard Water • OpenAccess Call Failure	

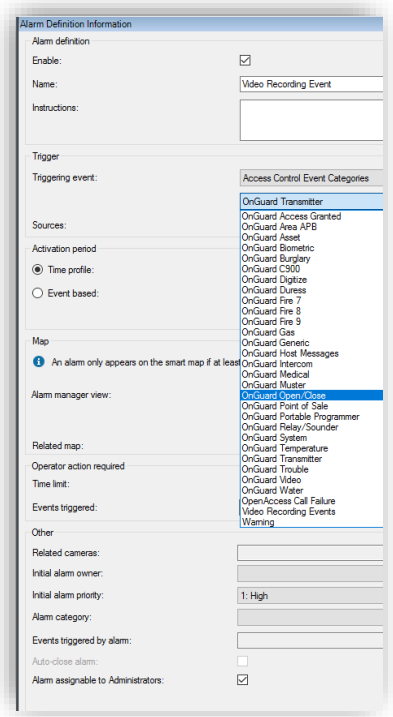
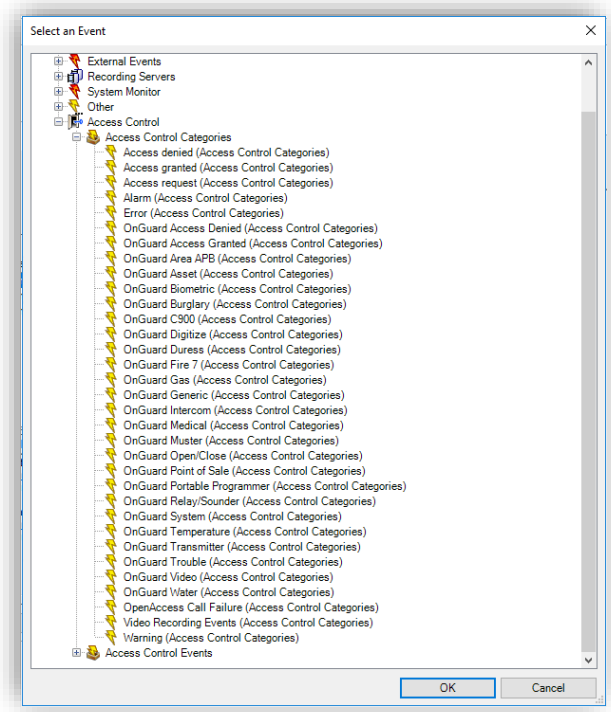
To create a User-defined Category, there is a User-defined Categories button on the bottom left corner of the Access control events menu. Click the User-defined Categories button to create your own custom event category.



Click Add, name the category, and press OK. The User-defined Category appears as an option in the Event Category list.



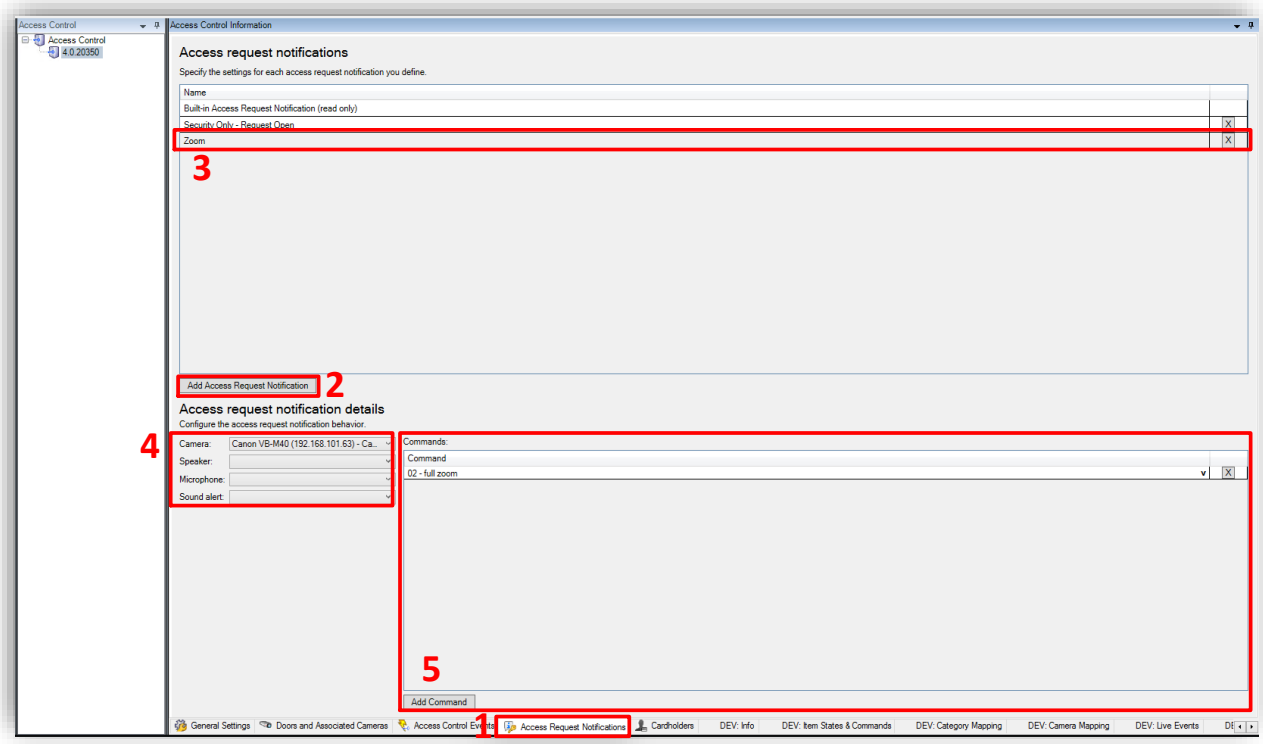
Alarms and Rules in XProtect are triggered using any category of event.

Alarm Access Control Categories Event list	Rule Access Control Categories Event list
	

Access Request Notifications

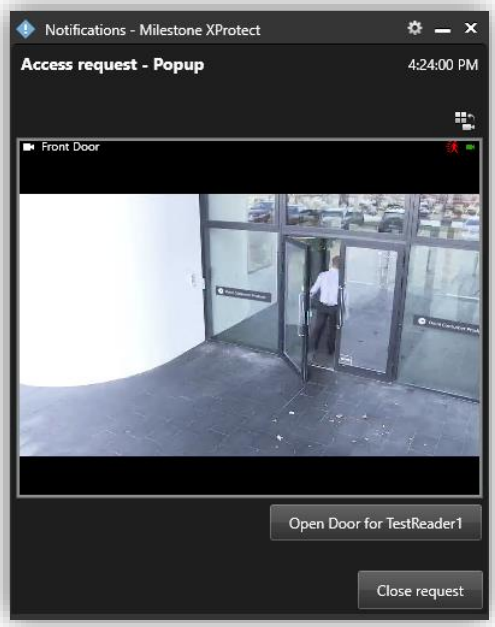
Access Request Notifications are pop-up notifications which appear in front of all other desktop applications for all users logged into the Smart Client with access to view XPA features and devices. These notifications can be customized in the Access Request Notifications menu. The XPA integration includes a Built-in Access Request Notification.

1. Go to the Access Request Notification menu.
2. Click the Add Access Request Notification button.
3. Name the new notification.
4. Associate cameras, speakers, microphones, and sounds.
5. Click the Add Command button and open the Command list to select which Commands appear on the Notification.



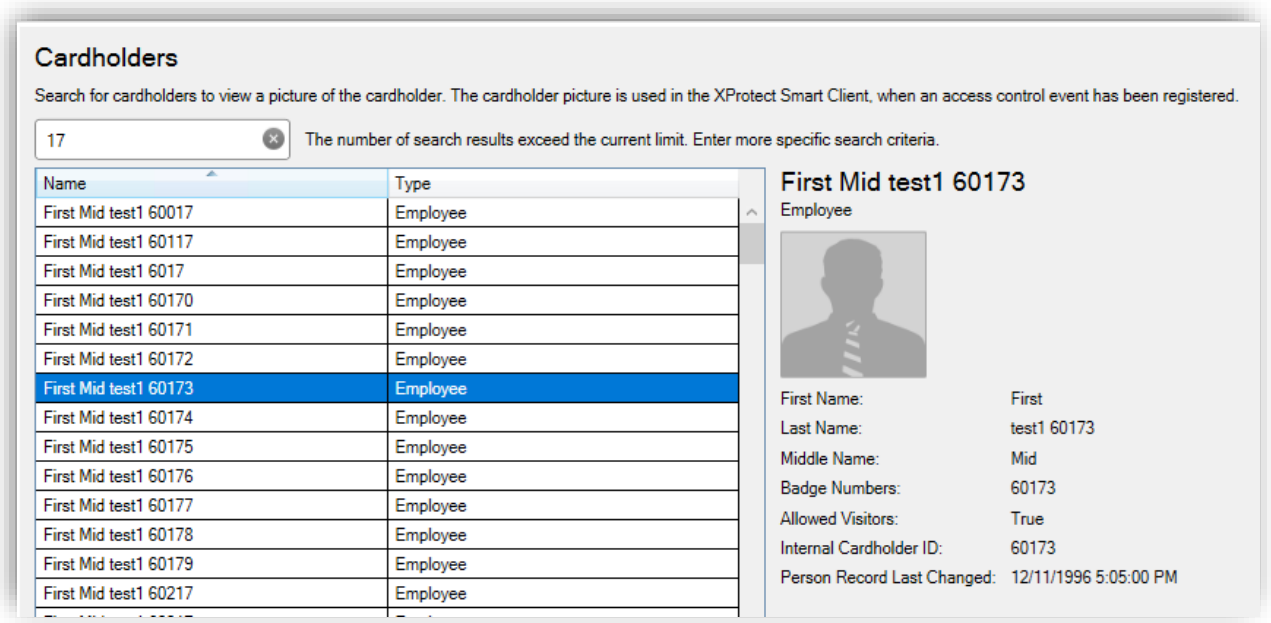
When the notification pops up on the desktop a sound will play if you choose to include a Sound alert. The Built-in Access Request Notification does not include a Sound alert.

Access Request Notifications can be used to trigger pop up notifications from within the XProtect rules system, and the notifications do not need to be connected to access control hardware devices.



Searching for Cardholders

All "active" cardholders in the OnGuard system are imported from the connected OnGuard server. "Active" cardholders have one or more badge(s) with a status of "active." Search for cardholders in the Cardholders menu of the XPA instance. First Name, Last Name, Badge Numbers, and Cardholder ID are all included in the search. As characters are typed in the box, searching begins:



Visibility of Cardholder information, such as name, Badge numbers...etc., are controlled within the OnGuard database.

Client Profiles & Roles

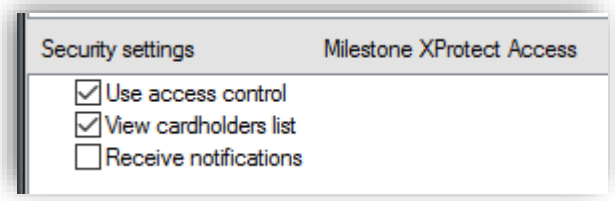
Smart Client Profiles and User Roles in XProtect allow administrators to control the features available in the XProtect Smart Client.

Smart Client Profiles allow control over the visibility of access request notifications. Roles allow control over access control globally, visibility of the cardholder list, and access request notifications. For example, if a user cannot receive access request notifications it could be disabled in both the Smart Client Profile that user is assigned, or in their Role.

To manage Smart Client Profiles – open the Management Client, expand Client and select Smart Client Profiles. The Access Control menu contains the setting for notifications.



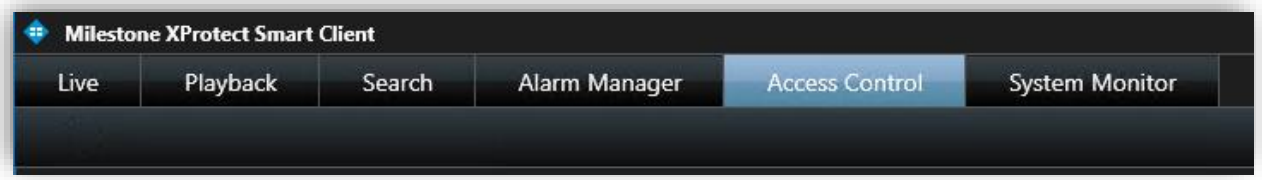
To manage Roles – open the Management Client, expand Security and select Roles. Select the role to manage and click on the Access Control menu to adjust the available settings.



Smart Client Features

Access Control Workspace

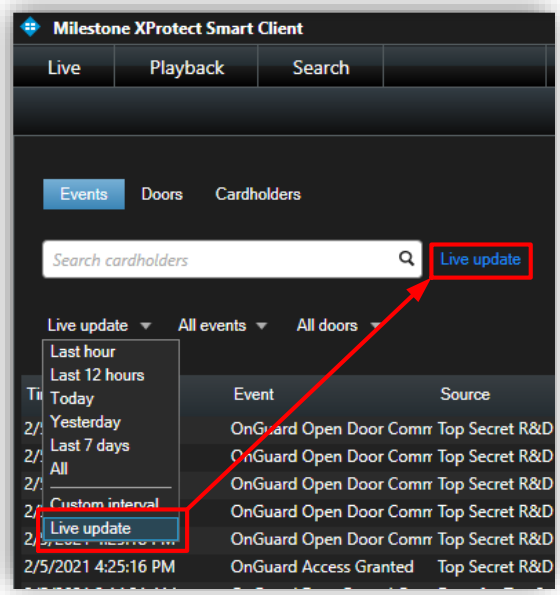
The XPA OnGuard integration adds a new workspace, or tab, into the XProtect Smart Client. The Access Control workspace should appear in the Smart Client.



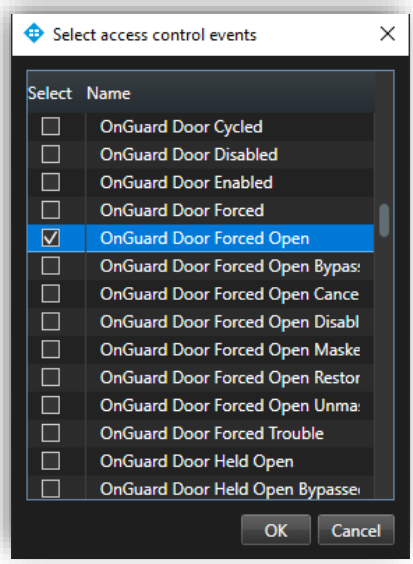
This workspace is used to search and filter Events, Doors and Cardholders.

Events:

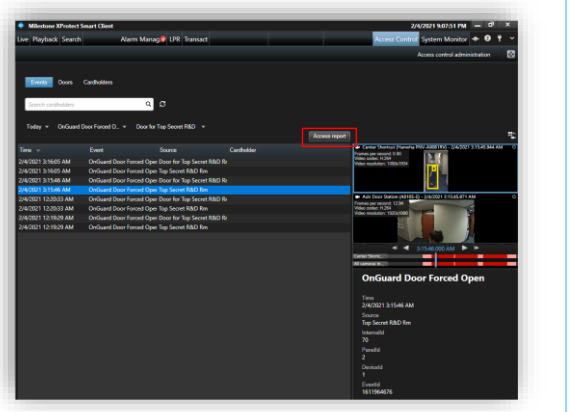
Choose a time range, including a custom time range, or live update. Choose the Live update time range to view a real-time display of access control events.

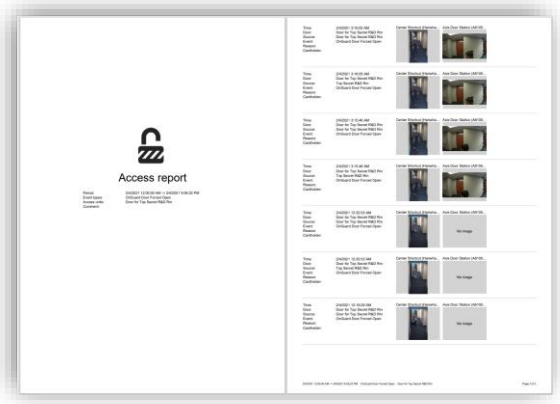


Filter for specific events including custom events and all integrated OnGuard events. Open the All events list and select the "Access control event..." option to open the Select access control events window. Choose a specific OnGuard event from this list.



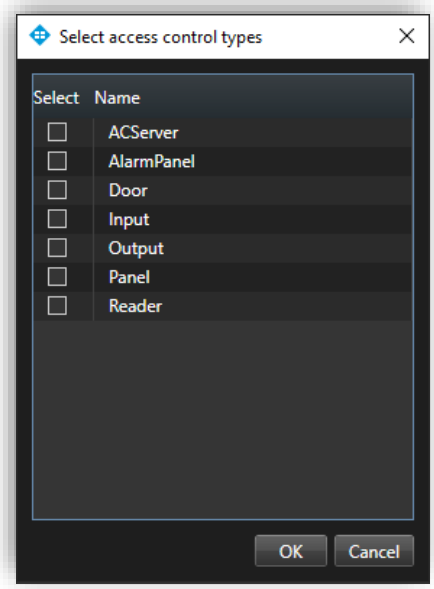
Filter for specific hardware devices. Click the Access report button to create a PDF file of the events in the current list. In the Access report window: name the report, choose a destination to save the report, include comments, and select the option to include snapshots.



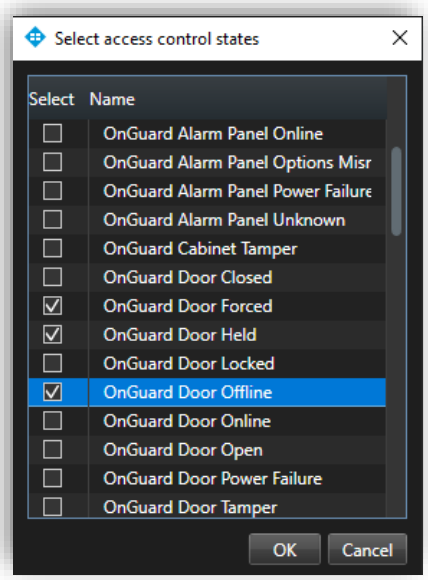


Doors:

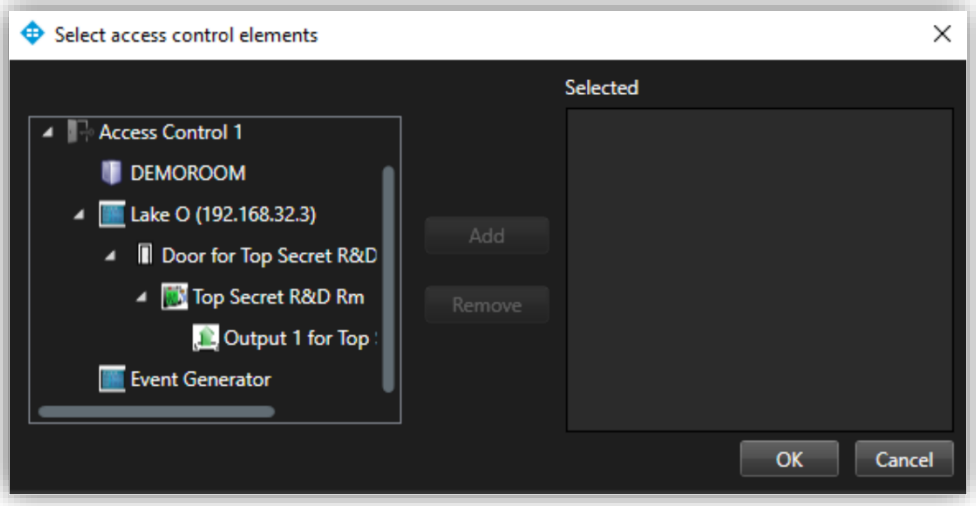
Open the Door list and select the type of access control hardware to display. Choose the “Access control type...,” option to open the “Select access control types” window. “Door” is the default option for this list, however, servers, panels, and any type of access control hardware in the system can be selected.



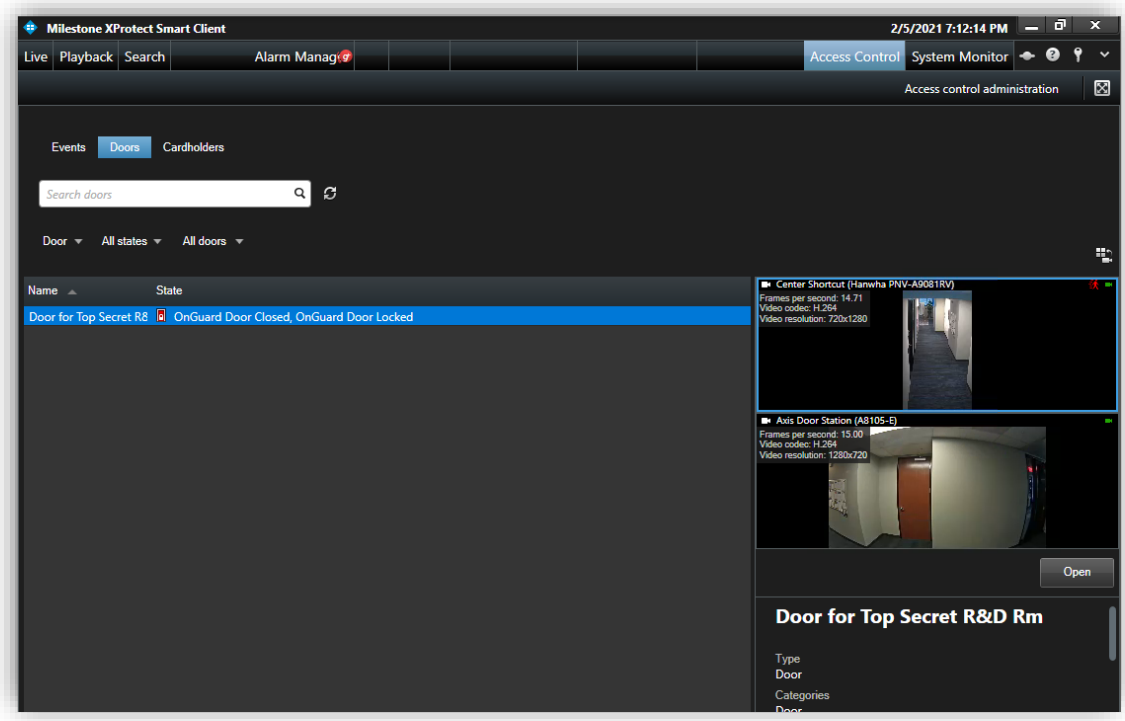
Open the All states list to filter hardware by status. Choose the “Access control state...,” option to open the Select access control states window and select from the list of all available OnGuard hardware states.



Open the "All doors" list and select the "Other…," option to open the Select access control elements window. This window provides a directory of all the OnGuard hardware in the system. Expand the directory, find the hardware device(s), and add them to the selected list.

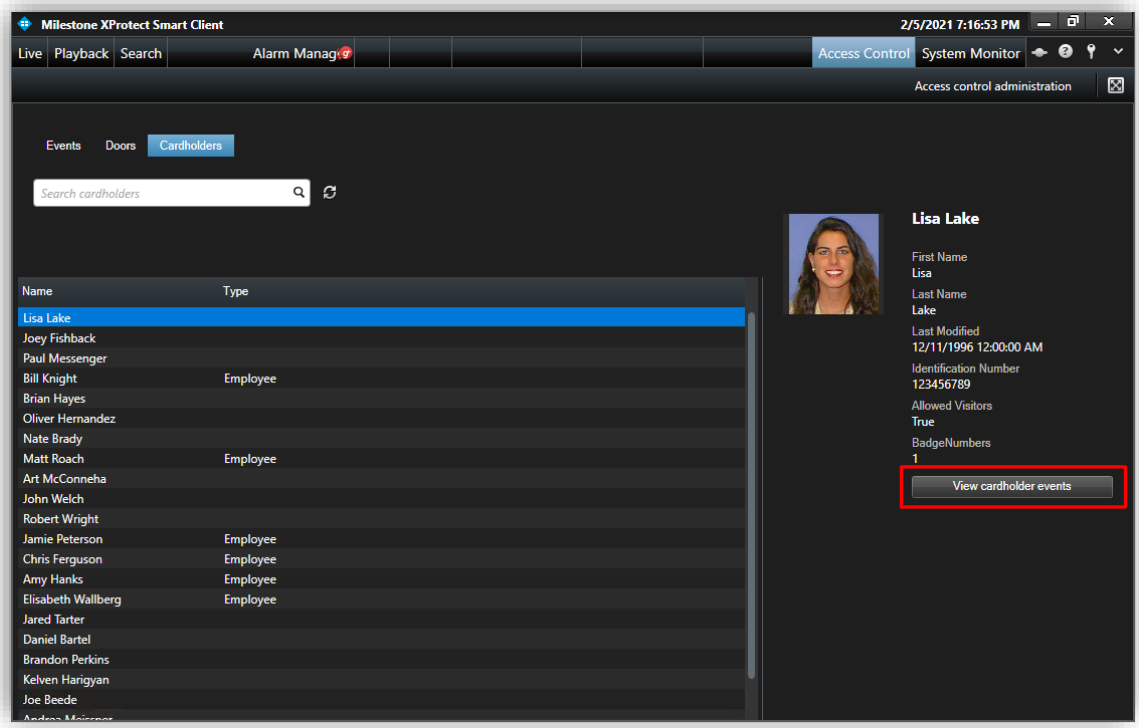


Select a Door in the list to see video from associated cameras, view door status information, and Command buttons available for that door.



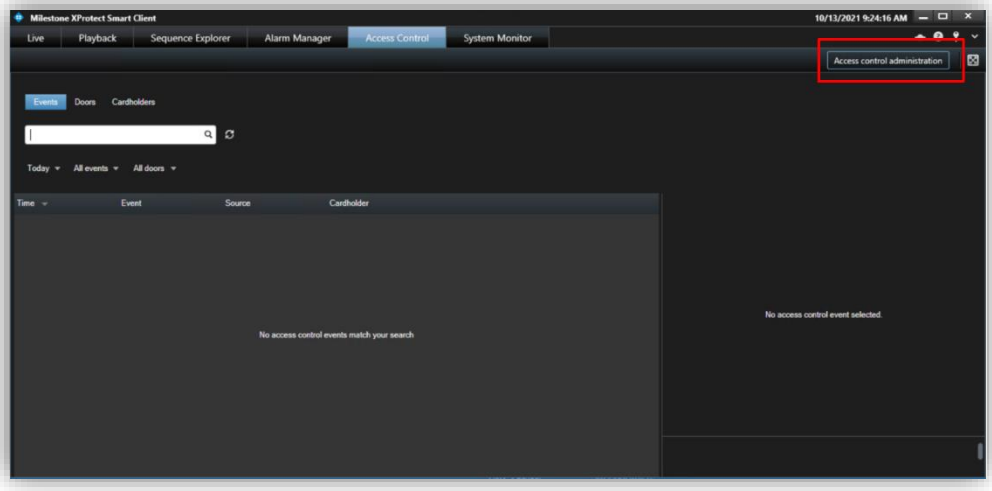
Cardholders:

By default, all cardholders in the system are displayed in the list. Filter for specific cardholders by typing into the search field. Select a cardholder to view their data. Click the View cardholder events button to switch to the Events list automatically filtered to display events only from the chosen cardholder.



OnGuard Web Admin Link

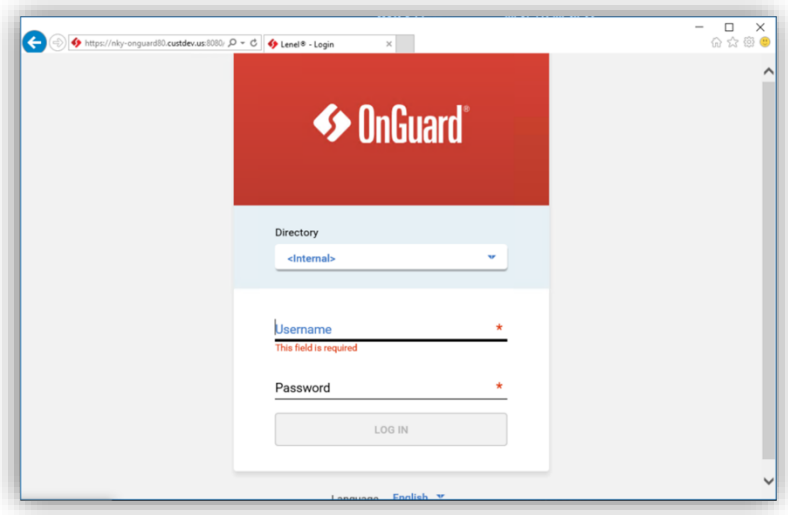
If a link has been configured in the General settings of the XPA OnGuard integration within I the XProtect Management Client, then the "Access control administration" link in the Access Control Workspace of the XProtect Smart Client will be active.



Click on the "Access control administration" Link to open the "OnGuard Admin" button.

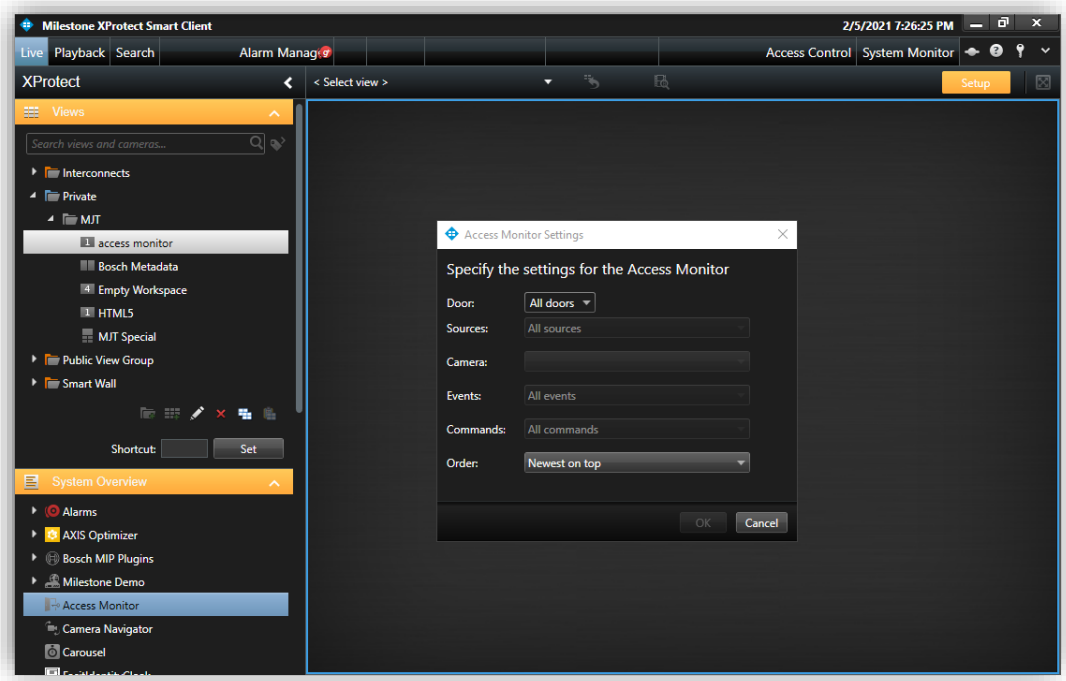


Select the "OnGuard Admin" button to launch the OnGuard web administration portal. It should be noted, that if multiple XProtect Access systems are integrated with the same XProtect VMS it would be possible to have more than one button appear in the Smart Client at this step.

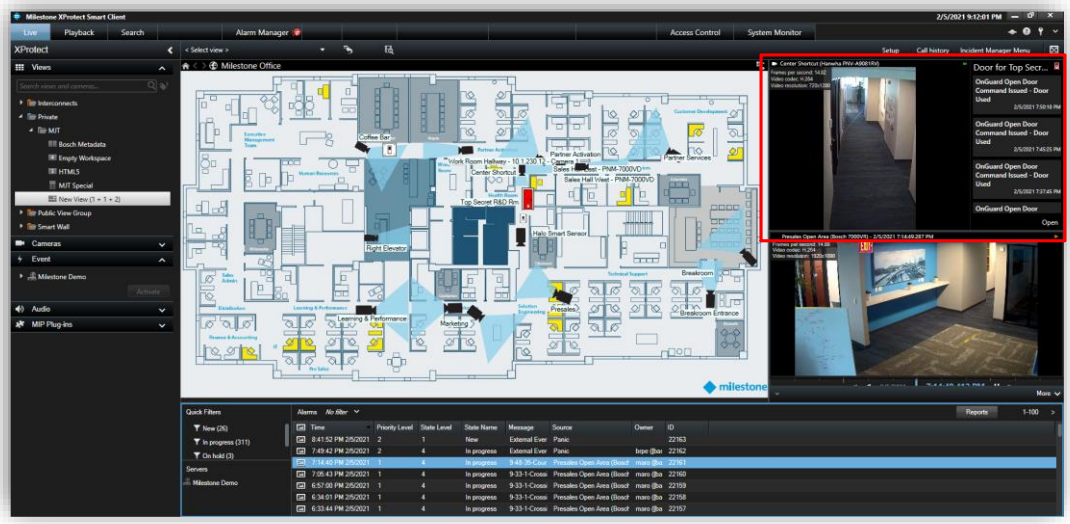


Access Monitor

The Access Monitor view item displays live status from doors and video from associated cameras in a single view pane in the Smart Client. Click Setup in the Smart Client and expand the System Overview panel menu. Select the Access Monitor view item and drag it into any available view pane:



In the access monitor settings window open the lists to select the door, sources, cameras, events, commands, and the order in which new events appear in the access monitor. Once the door is selected, many of the other options will change, based upon the available cameras, events, and commands. The access monitor view item can be added to any available view pane and works in a view alongside all available view items.

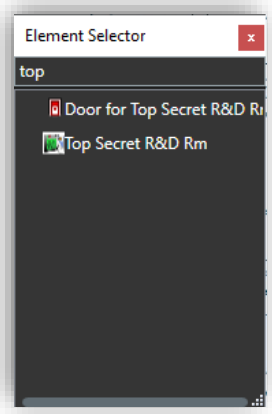


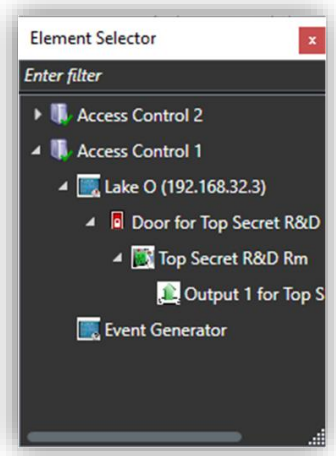
Maps

It is possible to place doors, readers, inputs, outputs, panels and OnGuard server(s) on an existing Smart Client Map. The map icons display hardware status as well as execute commands. With the Smart Client in setup mode a Tools window will appear in the view pane. From this window, select the Add access control icon:



The Element selector window will appear. Type the name of a hardware device into the filter to quickly find a device or expand the servers and panels to find all available hardware icons in the system.

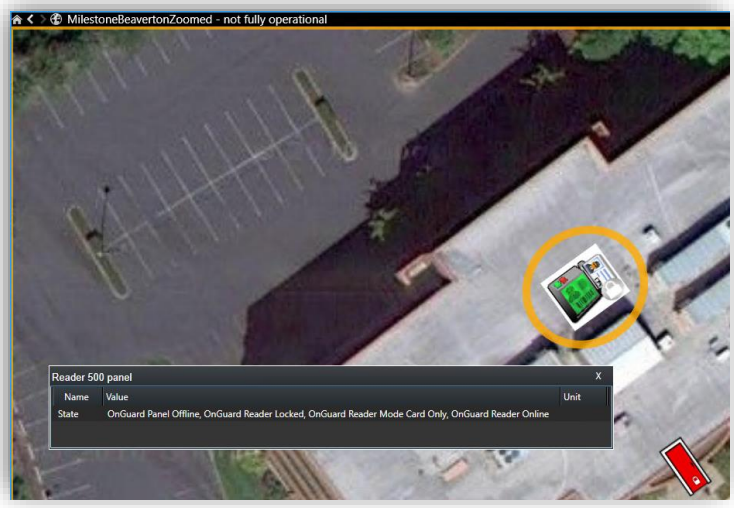




Drag the chosen icon onto the map. During normal operations, it is possible to right-click on any of these icons to execute the commands from the shortcut menu.

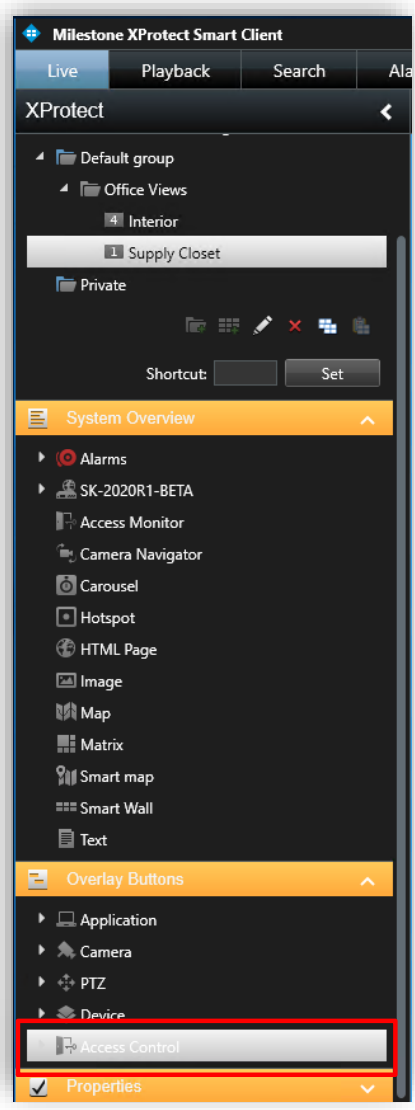


Right click the device icon and select Status Details from the shortcut menu to view more information.

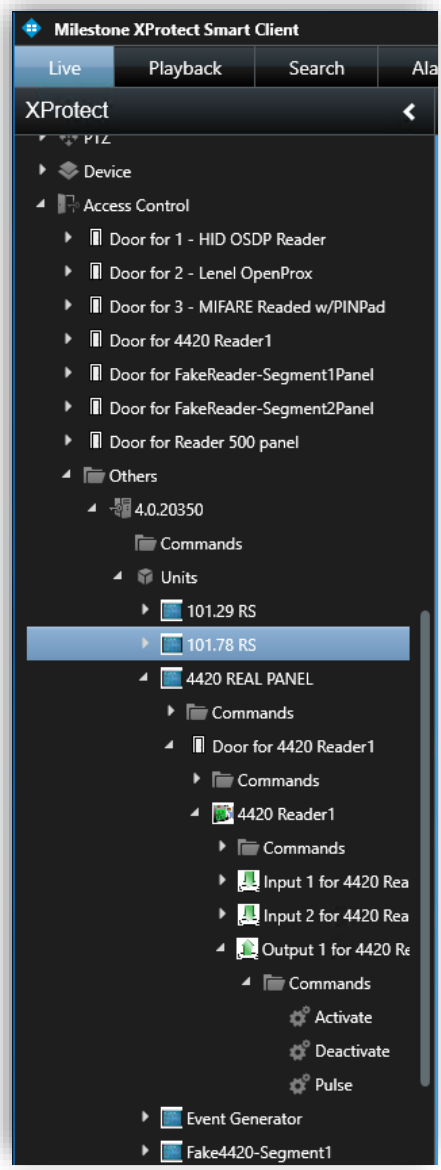


Overlay Buttons & Commands

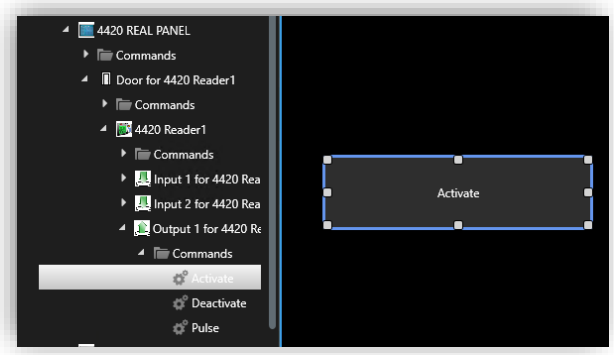
Overlay buttons are used to add manual buttons to video panes. Anything that can be triggered by a command can be added with an overlay button in the Smart Client. When the Smart Client is in setup mode, there is an Overlay Buttons panel on the left side of the client, select the Access Control icon.



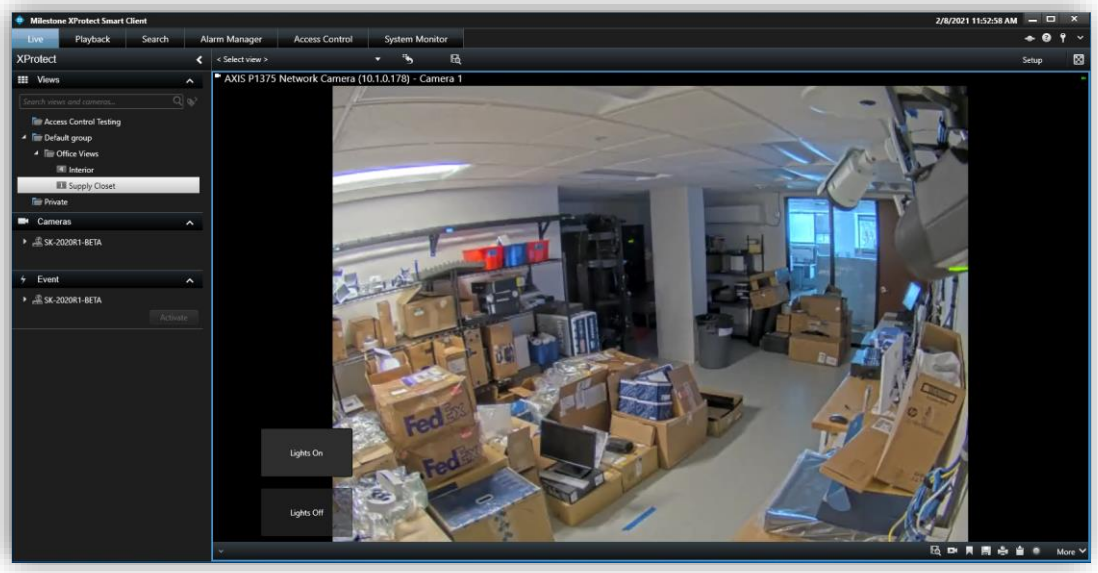
Expand the Access Control icon to find all the doors and readers, panels, and the connected inputs and outputs in the system.



Select a Command from the list and drag it onto the view pane.



The output commands include activate and deactivate. Once the commands are visible on a camera view pane they can be resized, moved around, and - with a right click - the name of the command can be edited.



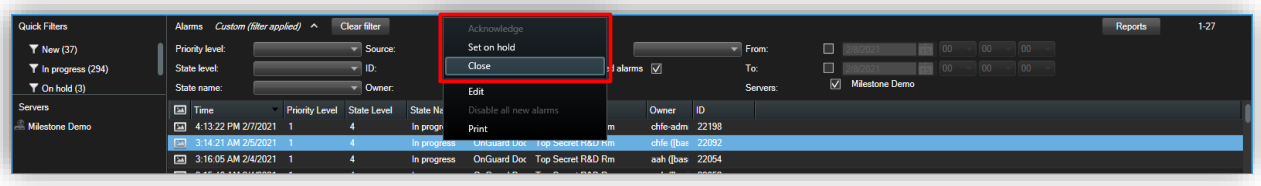
Alarm Acknowledgment

Alarm status between XProtect and OnGuard is shared. When alarms are closed in XProtect that state is shared with OnGuard. In the OnGuard system the same alarm will be acknowledged/closed. Alarm status is shared in the opposite direction as well – from OnGuard to XProtect.

Possible alarm states in XProtect and OnGuard are not identical. In XProtect alarms can be new, acknowledged, set on hold, or closed. In OnGuard alarms are either active or acknowledged. For the XPA OnGuard integration, acknowledged alarms in OnGuard are the same as closed alarms in XProtect. All other alarm states in XProtect are equivalent to active alarms in OnGuard.

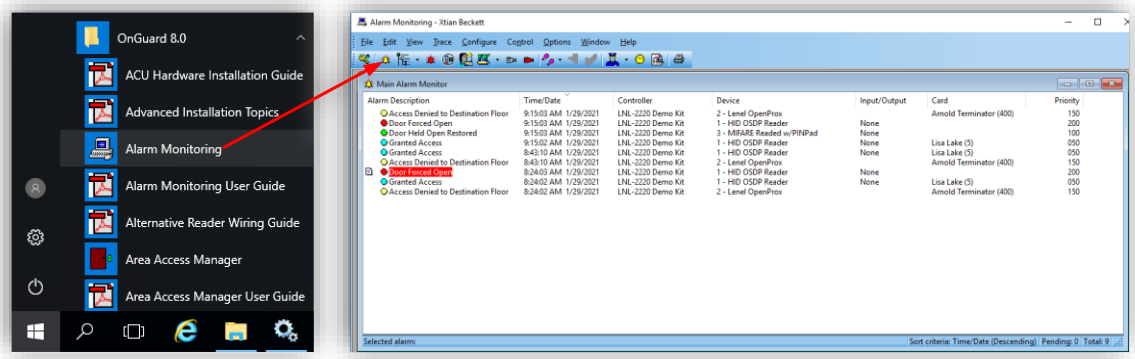
OnGuard Alarm Status	XProtect Alarm Status
• ACTIVE	• NEW • ACKNOWLEDGED > IN PROGRESS • ON HOLD
• ACKNOWLEDGED	• CLOSED

Alarm acknowledgment and other alarm status change operations are performed manually in the XProtect Smart Client. In the Alarm Manager, or any alarm list view item, right-click an alarm, and choose a new status from the shortcut menu. Close will close the event in XProtect and in OnGuard.

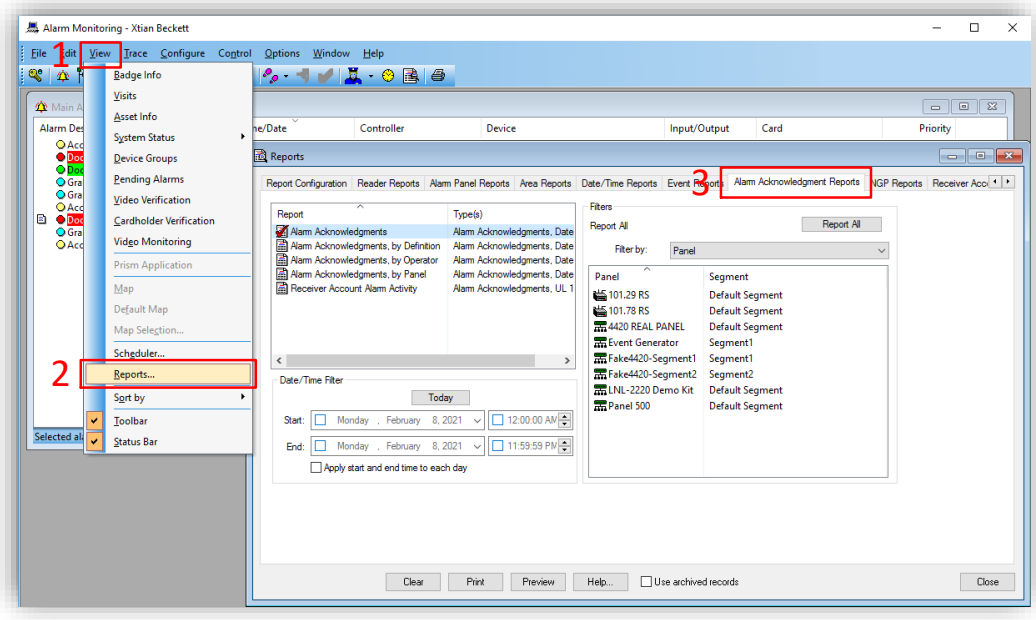


When alarms are acknowledged in OnGuard, the alarm is closed, and the associated alarm is also closed in XProtect. If the alarm is acknowledged within XProtect it will not change status in OnGuard. The status of the alarm in OnGuard will only change when the alarm is closed in XProtect.

Verify state changes of alarms in the OnGuard system in real time by opening the Alarm Monitoring application from the Start menu. If it is not automatically opened, click the View Alarms icon to open the Main Alarm Monitor window. Status of OnGuard alarms is displayed in this window in real time. Right click an alarm in this window to acknowledge the alarm.



Verify closed alarms from the View > Reports window and the Alarm Acknowledgement Reports menu. Choose a time range and export a report of all acknowledged alarms in the OnGuard system.

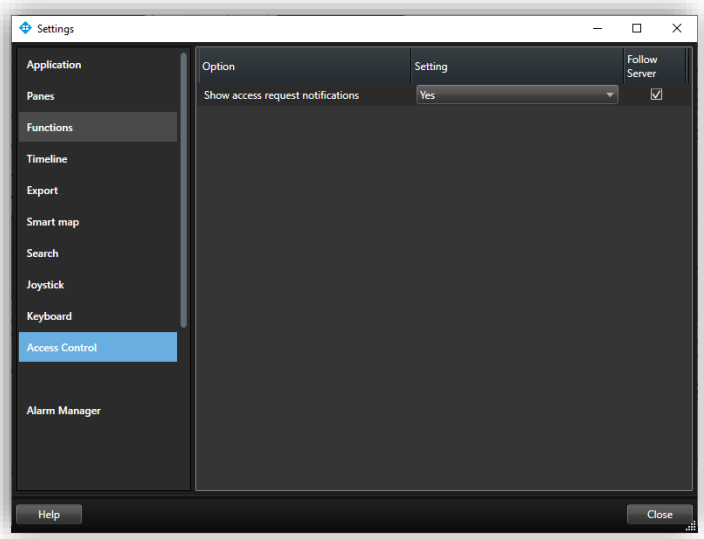


Access Control Options

In the upper right corner of the Smart Client application is a down arrow icon.



Click on this icon and choose the settings option to enter the Smart Client settings window. Select the Access control menu in the Settings window. Choose to show or block access request notifications in the Smart Client.

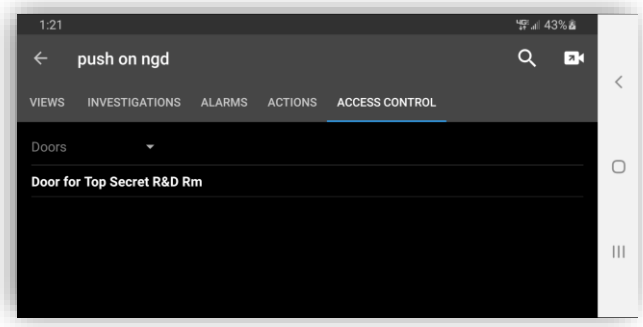


Mobile Client

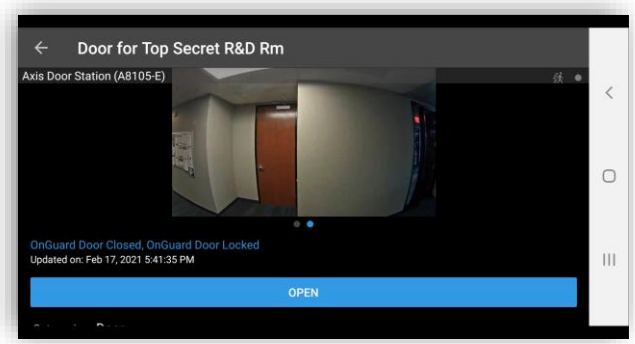
Milestone Mobile is a smartphone app that connects to your VMS system. The XProtect Access OnGuard Integration adds functionality to Milestone Mobile. Using Milestone Mobile it is possible to receive a push notification from the access control system, view live video related to the notification, and open the door – all remotely from a smartphone.

Access Control Tab in Milestone Mobile

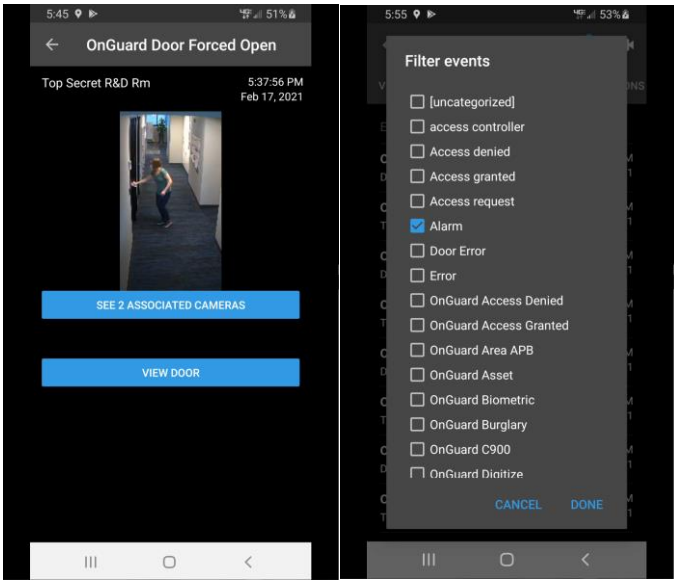
After logging into the VMS with Milestone Mobile the Views tab is presented by default. From this tab it is possible to select the Access Control tab. The Access Control tab shows the list of doors available.



Filter for specific doors or select a door to view cameras associated to that door or interact with commands available for the selected door. Swipe to switch between cameras when multiple cameras are associated to a door.



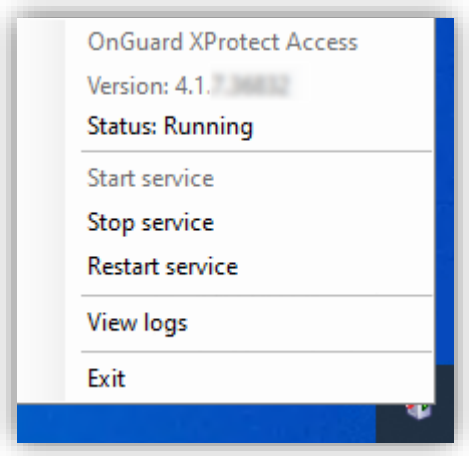
Switch between Doors, Events, and Access Requests. Select an event from the event list to view still images associated to the event and playback video related to the event. Filter the event list.



Access requests are only visible if the Smart Client profile assigned to the role of the current user has the ability to view access requests.

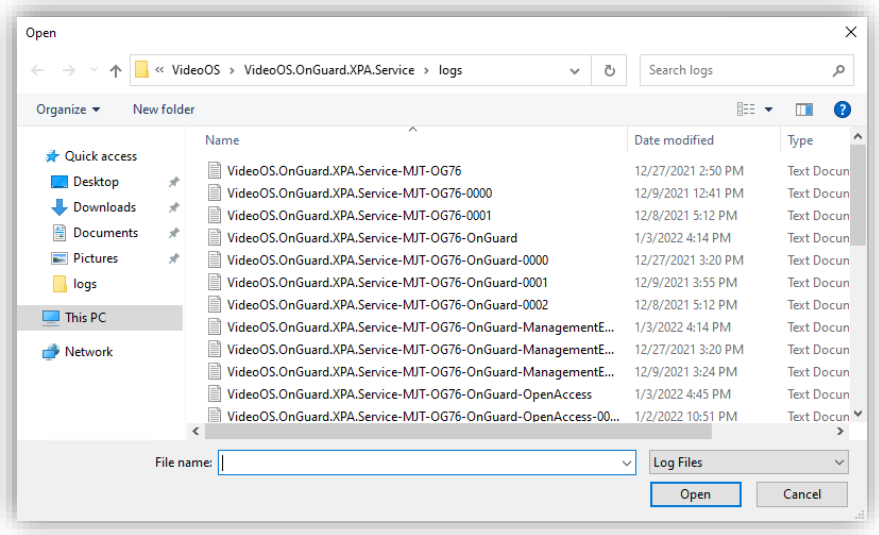
Service Tray Icon

The OnGuard XProtect Access Service, that runs on the OnGuard server has a service tray icon with a shortcut menu used for viewing status of the service, viewing logs, and starting and stopping the service. Right click on the OnGuard XProtect Access Service service tray icon to view the shortcut menu.

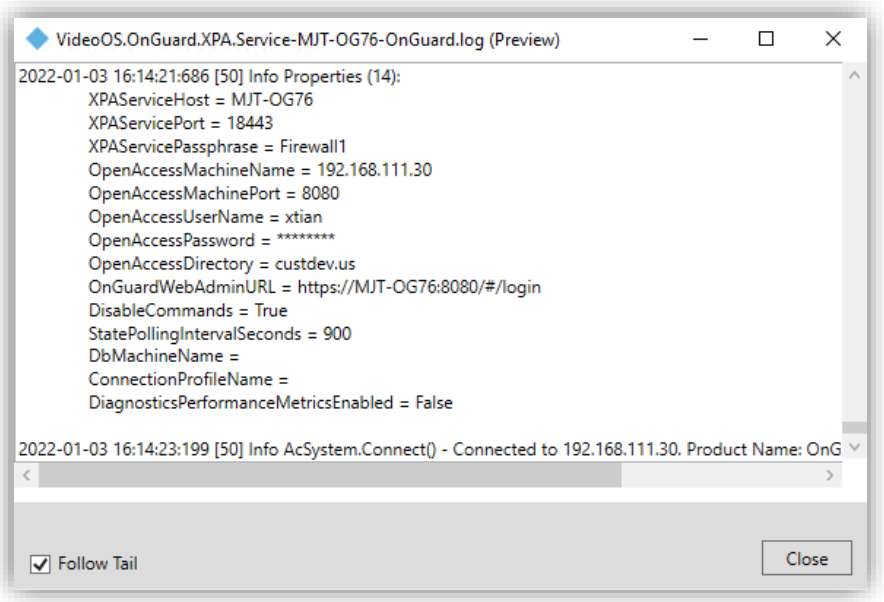


Log Viewer

Choose the "View logs" option from the shortcut menu of the service tray icon to launch a file explorer window of the location containing the OnGuard XProtect Access Service log files.



Select a log file to open the Log Viewer application and browse the log messages.



Logging

Debug logs are enabled on the OnGuard XProtect Access Mip Plugin and the OnGuard XProtect Access Service. The default log level is info, which is the least detailed level. The level of detail can be increased.

Log File Locations

Milestone

1) Go to the Milestone Event Server.
2) Open File Explorer. Select the View menu and enable Hidden items.
3) Log files in these locations are relevant:
   a) C:\ProgramData\VideoOS\VideoOS.Event.Server\logs
   b) C:\ProgramData\Milestone\XProtect Event Server\logs

OnGuard

1) Go to the OnGuard server.
2) Open File Explorer. Select the View menu and enable Hidden items.
3) Log files in these locations are relevant:
   a) C:\ProgramData\VideoOS\VideoOS.OnGuard.XPA.Service\logs

Changing logging level

The log's level of detail can be changed by setting the logging level. The logging level can be set at any of the following values:

- Off
- Fatal
- Error
- Warn
- Info
- Debug
- Trace

"Off" writes no information to the file and "Trace" writes as much information as possible to file. The default setting is "Info."

New log files are created each day or whenever a log file reaches 1 MB in size. After 10 total log files of the same type have been created, the oldest file is automatically deleted when the next one is created. If more than 10 MB of data is needed in the log files, please contact Milestone Technical Support.

Here is the procedure to change the log levels:

Milestone

1. Go to the Milestone Event Server.
2. Open File Explorer. Select the View menu and enable Hidden items.
3. Open the following folder:
    a. C:\ProgramData\VideoOS\VideoOS.Event.Server
4. Find the file: VideoOS.Event.ServerNLog.xml and open it with notepad.
    a. The second to last line in the file is like this "<logger name="*" minlevel="Info" writeTo="mainlog" />"
    b. Change the "Info" to "Debug" or "Trace," or any other log level and save the file.
    c. Depending on the OS you are running you may have to save the file to the desktop and copy it back to that folder because windows permissions will not let you save a file there directly.

OnGuard

1. Go to the OnGuard server.
2. Open File Explorer. Select the View menu and enable Hidden items.
3. Open the following folder:
    a. C:\ProgramData\VideoOS\VideoOS.OnGuard.XPA.Service
    b. Find the file: "VideoOS.OnGuard.XPA.ServiceNLog.xml" and open it with notepad.
    c. Near the bottom of the file, find the lines that begin with:
        i. <logger name="VideoOS.OnGuard.XPA.Translator.Managers.EventManager.ManagementEvents"
        ii. <logger name="VideoOS.OnGuard.XPA.Translator.Managers.EventManager"
        iii. <logger name="VideoOS.OnGuard.XPA.Translator.Managers.StateManager"

iv. <logger name="VideoOS.OnGuard.XPA.Translator.BackwardCompatibility.BackwardCompatibilityManager"
v. <logger name="VideoOS.OnGuard.XPA.Translator.*"
vi. <logger name="VideoOS.OnGuard.Client.*”

d. Change the “minlevel” attribute values in those lines from their current values to “Debug” or “Trace,” or any other log level.
e. Near the bottom, find this line in the file:
    i. <logger name="*" minlevel="Info" writeTo="mainlog" />
f. Change the “minlevel” attribute values in that line from the current value to “Debug” or “Trace,” or any other log level and save the file.
g. Depending on the OS you are running you may have to save the file to the desktop and copy it back to that folder because windows permissions will not let you save a file there directly.

Troubleshooting Guide

OnGuard loses communication with access control hardware

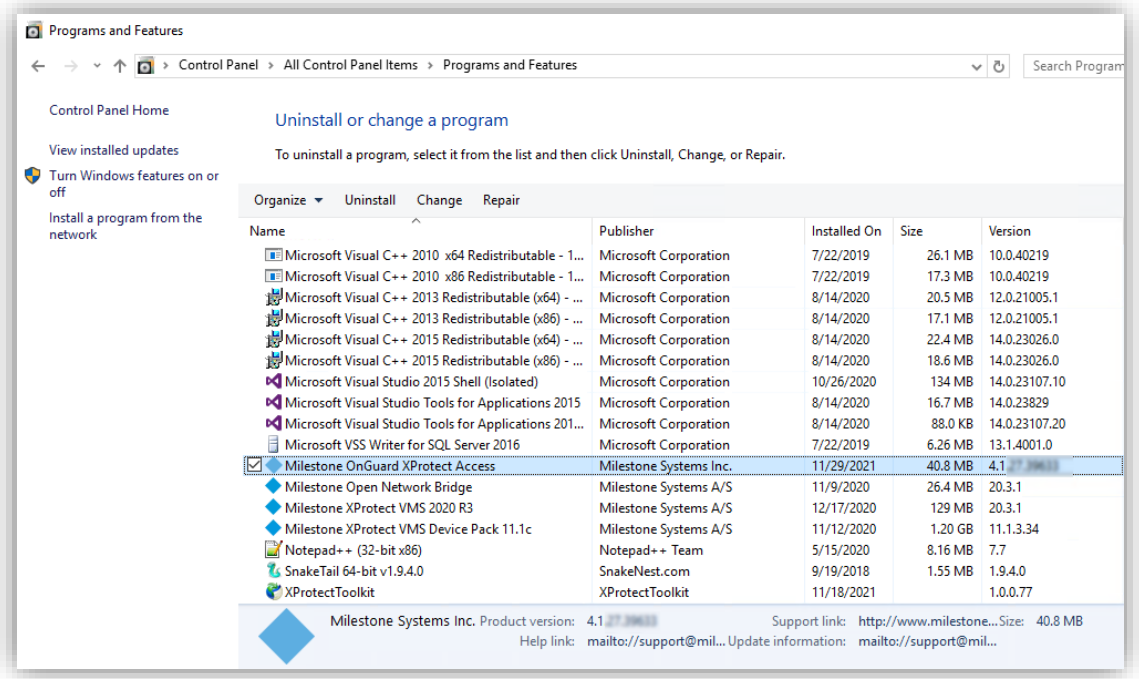
Communication can be lost for the following reasons:

1) Firewall blocking traffic
2) The OnGuard LS Communication Server service is not running or needs to be restarted.
3) The OnGuard LS Web Service service is not running or needs to be restarted.

Integration Version Downgrades

Here is the process required to uninstall the 4.1 version of the plugin.

3. Go to the Programs and Features menu on the Milestone Server.
    a. Uninstall the Milestone OnGuard XProtect Access component.



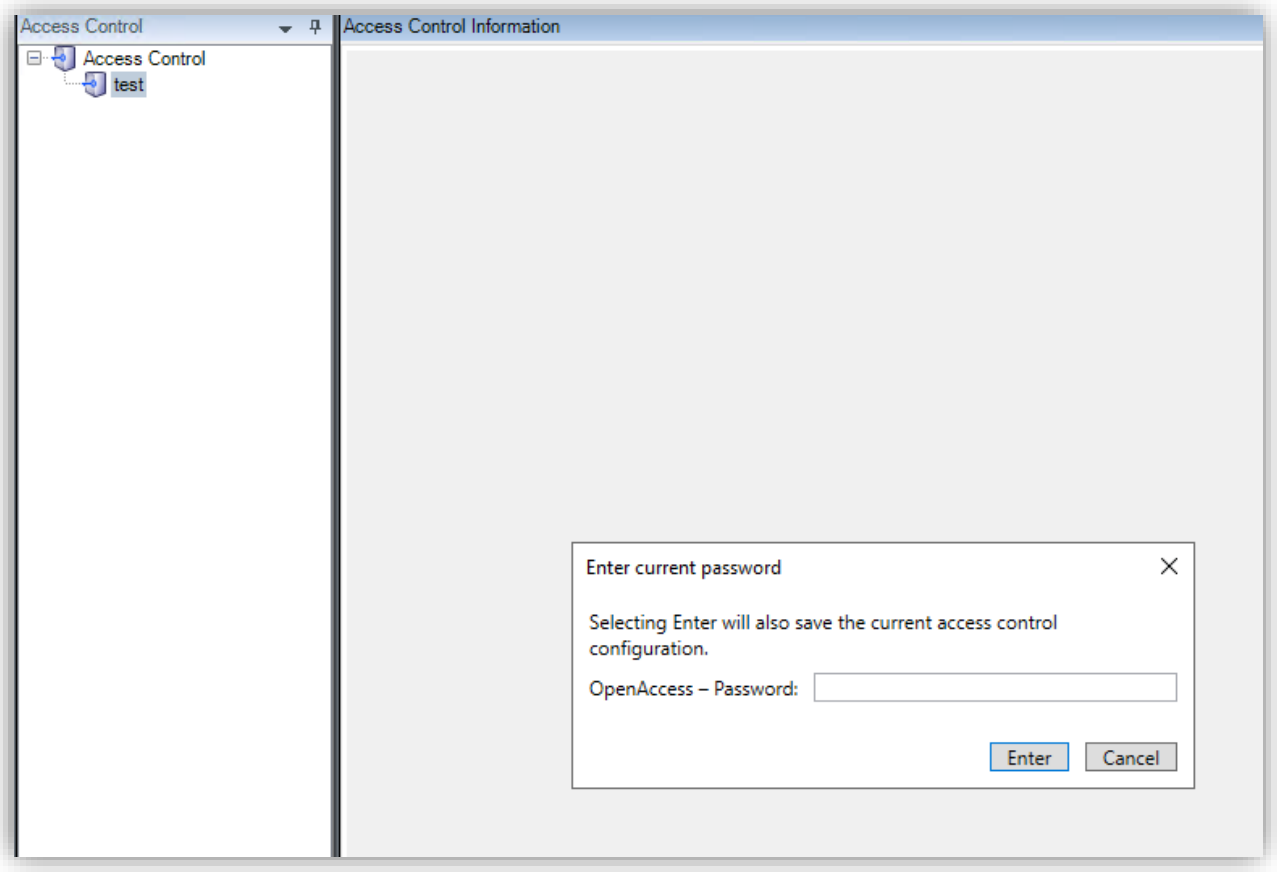
4. Go to the Program and Features menu on the OnGuard Server.
    a. Uninstall the Milestone OnGuard XProtect Access component.
5. Obtain the previous version of the integration from download.milestonesys.com/lenelacm
6. On the OnGuard Server.
    a. Re-install the Milestone.ACMServer.x64.msi
    b. Re-install the Milestone.ACMServer.OnGuard.msi
7. On the Milestone Server.
    a. Re-install the Milestone.ACMServer.MipPlugin.msi
    b. Run the ACM Server wizard to add the XProtect Access instance.
8. In the XProtect Management Client.
    a. Reconfigure any connection properties in the General Settings tab of the XPA instance as needed. Save the settings.
    b. Refresh the configuration of the XProtect Access instance.

XProtect 2021 R1 and R2 shows no error if OpenAccess – Password is incorrect.

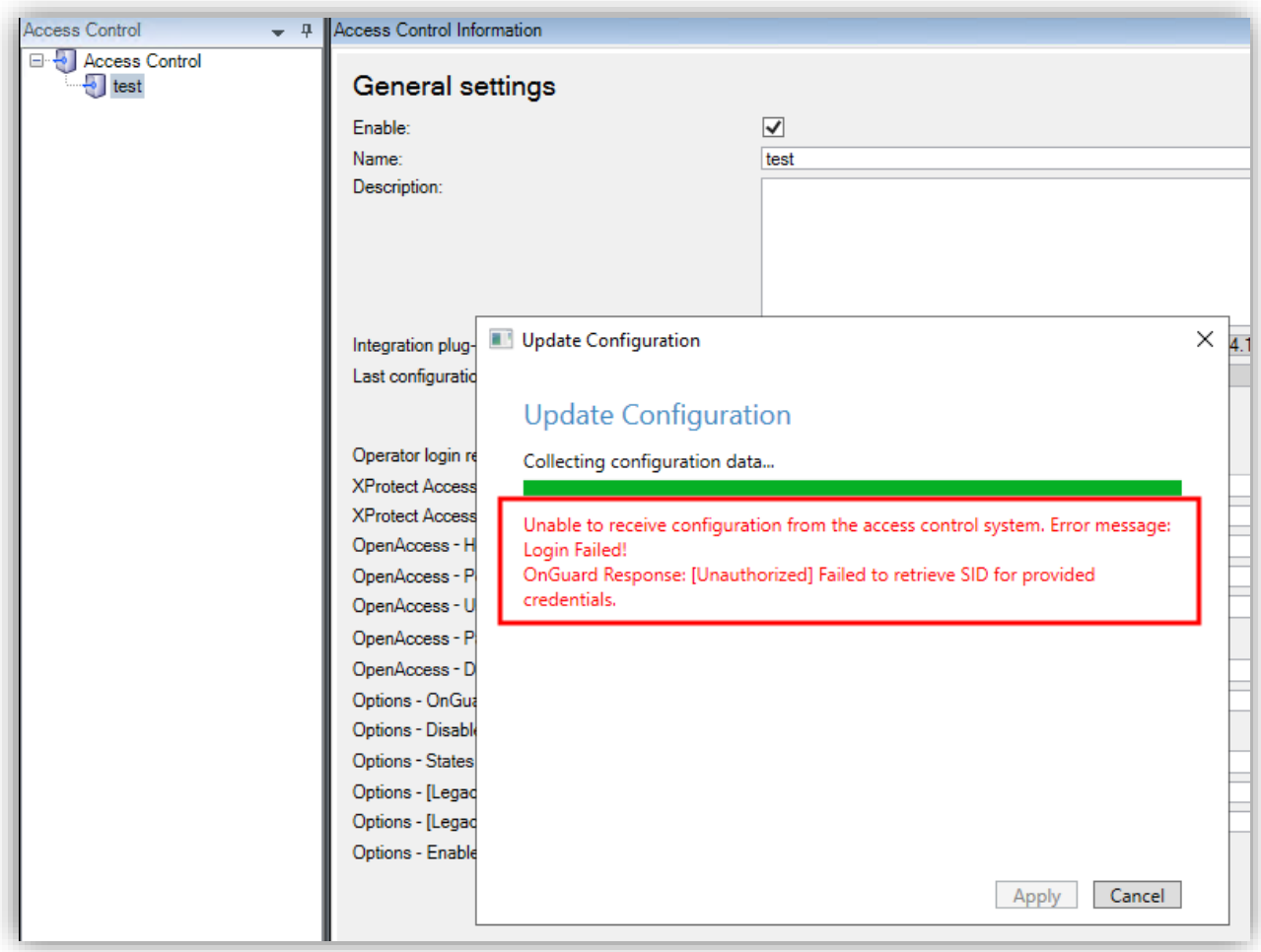
When running XProtect VMS 2021 R1 or 2021 R2, if a change to the configuration on any XProtect Access integration in the General Settings tab is saved, the system will prompt for a password. This is the password for the account that authenticates between XProtect and the integrated Access Control system. If the wrong password is provided, there will be no error or warning displayed and the integration will be broken, without any warning, until the password is changed again to the correct one.

This issue can occur every time the XProtect Management Client is opened and the XProtect Access

system configuration is changed. When any information or setting controlled within the XProtect Access integration section of the Management Client is changed and saved, the system will ask for a password.



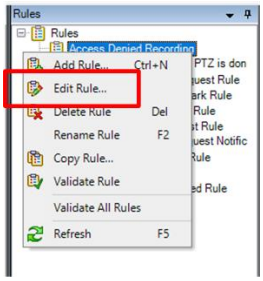
To verify the correct settings are in place for the password and all other parameters controlling the connection between integrated Access Control systems and the XProtect Event Server, it is recommended to "Refresh Configuration" each time the password is entered, and each time any of the settings on the General Settings page are changed and saved. If the connection is broken, because the password was entered with a typo, then the Refresh Configuration process will produce an error.



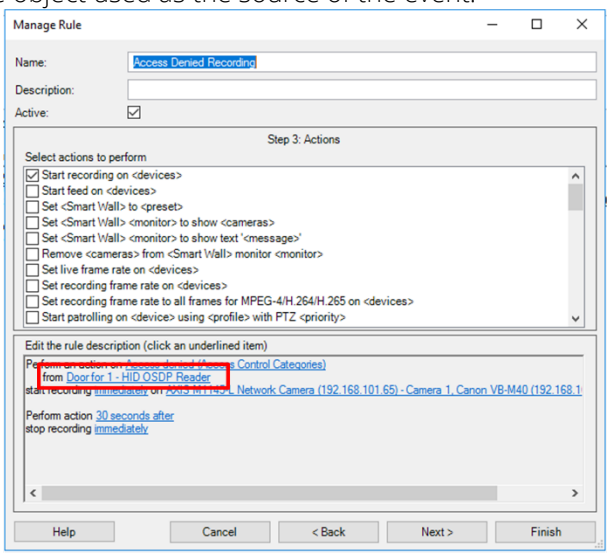
Access Control Rules Stop Working after Upgrade to 4.0 or newer.

In versions 4.0 and newer of the XProtect Access LenelS2 OnGuard integration Doors cannot be used as a source for Access Control events or event categories in the XProtect VMS rule system. For existing rules to continue to function, and for all new rules, readers must be used as the source for all events. In order to fix broken rules which stopped functioning after a system upgrade, the door hardware objects which were used as the event source can be replaced by the associated reader hardware objects. Edit the existing rules, remove the doors as the source and replace them with the associated readers. Below is the process to execute this change.

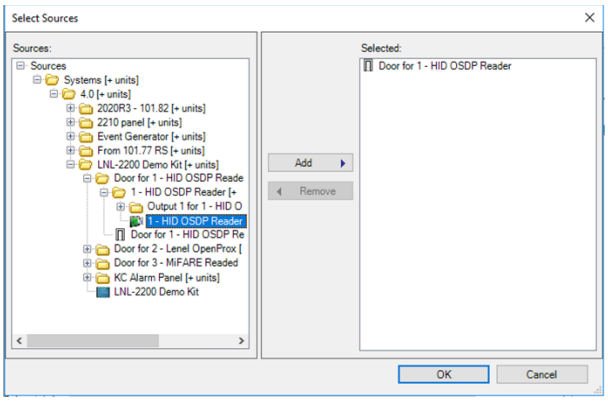
Find all Access Control related rules in the XProtect Rules menu. Right click on each individual rule, and select "Edit Rule..." from the shortcut menu.



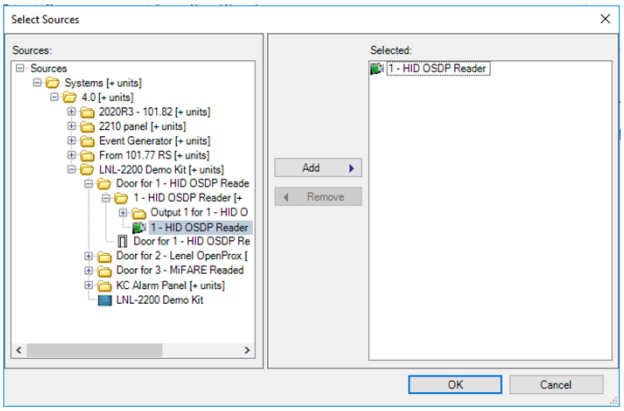
Click on the door hardware object used as the source of the event.



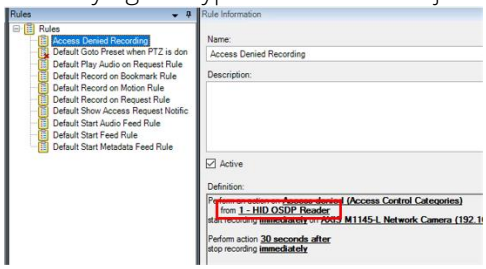
The Select Sources window opens. Expand the source directory to identify the door hardware object(s) that match the "Selected" hardware objects. Associated to that door hardware object are one or more reader hardware objects. Choose the correct reader associated to the door for this rule.



Select the reader hardware object from the directory and click the Add button. Select the door hardware object from the "Selected" list, and click the Remove button.

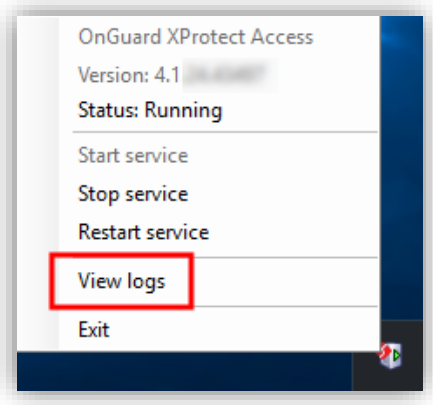


Finish editing the rule. Perform this same process for all access control related rules in the XProtect VMS. Check by selecting a rule and verifying the type of hardware object used as the source.



OnGuard XProtect Access Service: MipPlugin Post-Install Verification

Verify the MipPlugin (located on the Milestone Event Server server) successfully installed by checking in the logs below. The fastest way to find the log files is to right click on the OnGuard XProtect Access Service tray icon, and select "View Logs" from the shortcut menu.

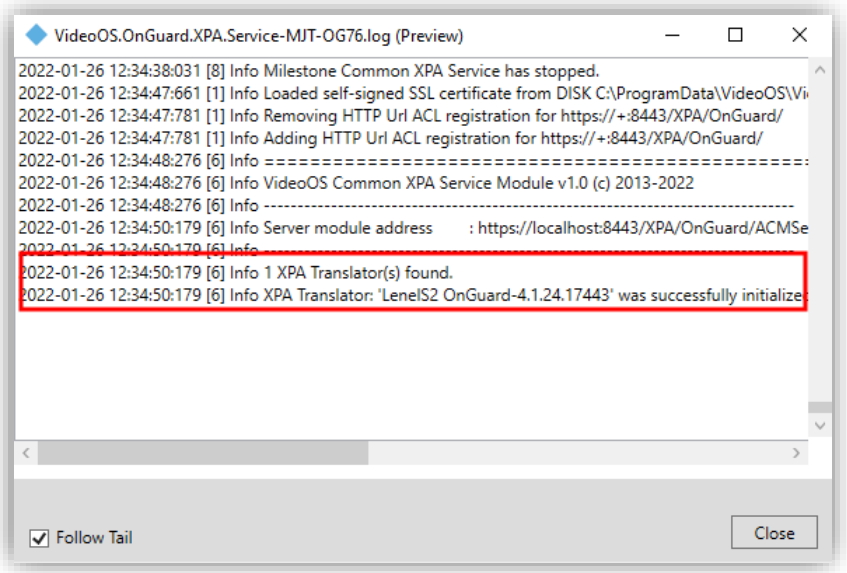


This will open the file explorer at the following location:

C:\ProgramData\VideoOS\VideoOS.OnGuard.XPA.Service\logs

Open the VideoOS.ServiceHost-LocalhostPCName.log file – the LocalhostPCName section of the file name is the PC name of the OnGuard Server. Double-Click the file to open it in the log viewer application. Verify that the following entries are in the Log file:

Info 1 XPA Translator(s) found.
Info XPA Translator: 'LenelS2 OnGuard-4.1.xx.xxxxx' was successfully initialized.



Cardholder search data fields are missing

The OnGuard XPA Integration uses a default list of cardholder data fields when searching for cardholders. A .json file is created automatically when the first search is performed. This file is named "PluginSettings.json" and it is located on the OnGuard server or the host of the OnGuard XProtect Access Service. The file location should be:

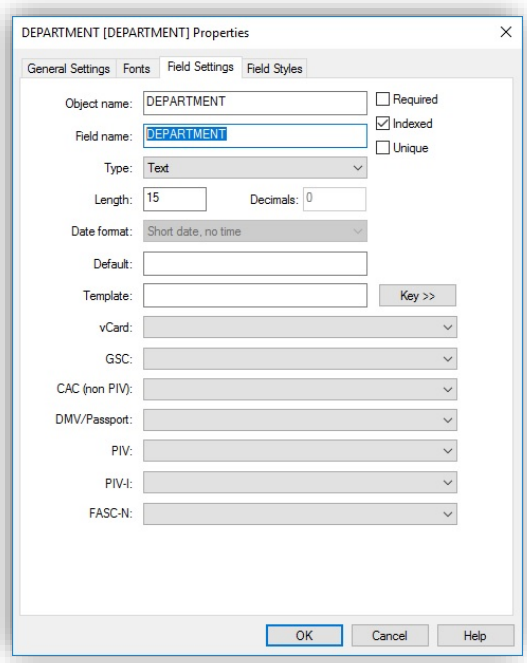
- C:\ProgramData\VideoOS\VideoOS.OnGuard.XPA.Service\Translators\OnGuard\PluginSettings.json

The default list of cardholder data fields contains the following data types:

JSON file data field text	Description
LASTNAME	Cardholders last name
FIRSTNAME	Cardholders first name
MIDNAME	Cardholders middle name
ADDR1	Street address on file for cardholder

CITY	City on file for cardholder
ZIP	Zip code or postal code on file for cardholder
PHONE	Phone number on file for cardholder
OPHONE	Additional phone number on file for cardholder

The list in this .json file can be modified to add new data fields or to remove existing data fields. If the list, in the .json file is left empty, then the complete range of searchable fields available with OnGuard will be used. To edit the list of data fields the name of the fields must match the "field name" values as displayed in the OnGuard FormsDesigner application:



The default .json file should look like this:

```
{
  "Version": "1.0",
  "CredentialHolderSettings": {
    /*The Onguard Cardholder fields used when searching for Credential Holders in XProtect. Leave empty to use all available searchable string fields in OnGuard.*/
    "CardholderSearchFields": {
```

```
      "LASTNAME",
      "FIRSTNAME",
      "MIDNAME",
      "ADDR1",
      "CITY",
      "ZIP",
      "PHONE",
      "OPHONE"
    }
  }
}
```

An empty .JSON file will look like this:

```
{
  "Version": "1.0",
  "CredentialHolderSettings": {
    /*The Onguard Cardholder fields used when searching for Credential Holders in XProtect. Leave empty to use all available searchable string fields in OnGuard.*/
    "CardholderSearchFields": {}
  }
}
```

After editing and saving the .json file, changes will take effect after the next restart of the OnGuard XProtect Access Service. Follow this process to use a non-default or full list of searchable fields:

1. Complete the first cardholder search.
2. .json file is created with default list.
3. Edit the .json file to meet the new requirements.
4. Restart the OnGuard XProtect Access Service application.

NOTE: If the .json file is deleted, it will be recreated with the default search fields the next time the OnGuard XProtect Access Service is restarted and a new search is performed. It is recommended to edit the file instead of deleting it, if the full list of searchable fields is required.

Not receiving cardholder or badge changes

If cardholder or badge changes are not reflected in either the Milestone Management or Smart Clients, ensure that software events are enabled in OnGuard.

XPA integration flooding OnGuard user transaction report

Milestone's XProtect system regularly requests status of OnGuard hardware. To get the current state of a hardware device, the integration must update the hardware status on the parent panel, then query for the device state. A transaction for each hardware status update/query is entered into OnGuard for the single sign-on (SSO) user.

Customers making use of OnGuard's built-in "User Transaction" report from OnGuard's Sys Admin + Reports will see these many transactions from the OnGuard XProtect Access integration under the SSO user in the report. It is not possible to filter the User Transaction report to omit the SSO user.

Possible workarounds include:

- Install a compatible version of Crystal Reports and customize the report. However, OnGuard Technical Support, OAAP, etc., will not support custom reports.
- Contact the OnGuard Custom Solutions group and have them create/customize the reports.

OnGuard XPA instance not displayed in the XProtect Management Client

If XProtect is unable to communicate with the OnGuard XPA instance, the instance will not appear in the Access Control section of the Management Client. This process should restore visibility:

On the Milestone Server:

1. Close the Management Client and Smart Client
2. Stop the Milestone Event Server

On the OnGuard Server:

3. Stop the OnGuard XProtect Access Service
4. Ensure required OnGuard services are running.
    a. LS Event Context Provider
    b. LS Message Broker
    c. LS OpenAccess
    d. LS Web Event Bridge
    e. LS Web Service.
5. Start the OnGuard XProtect Access Service

On the Milestone Server:

6. Start the Milestone Event Server and wait for it to begin running.

7. Start the Management Client

If the instance still is not in the Management Client, investigate the logs and contact Milestone Technical Support.

LS OpenAccess service automatically stops seconds after starting

There is a known issue with OnGuard caused by an Active Directory account logging into the OpenAccess service shortly after it starts, which can cause OpenAccess to crash. The OnGuard XProtect Access Service will attempt to log into OpenAccess when both services are running. This can trigger the crash. The recommended workaround is to switch the Single Sign-On user to a local Windows account and adjust the services to use this same local Windows account.

For questions and information concerning a fix for this issue, please contact support for information regarding this bug at oaaptechnical@carrier.com. Reference LenelS2 Bug DE40122.

I/Os connected to OSDP readers are no longer detected

This is a known issue with OnGuard 7.4 Update 1 (7.4.457.69) where I/Os connected to OSDP readers are not detected in the OnGuard XProtect Access integration.

For questions and information concerning a fix for this issue, please contact support for information regarding this bug oaaptechnical@carrier.com. Reference LenelS2 Bug DE40122.

LS OpenAccess events fail in OnGuard Enterprise systems

This is a known issue with OnGuard 7.4 Update 1 (7.4.457.69) running in an Enterprise configuration. Devices do not send events through OpenAccess to the OnGuard XProtect Access integration.

For questions and information concerning a fix for this issue, please contact support for information regarding this bug at oaaptechnical@carrier.com. Reference LenelS2 Bug DE40122.

All other support issues

For issues not covered in this guide, please contact Milestone Support at support@milestone.us, or by phone at 503-350-1100.

Known issues:

- This XProtect Access (XPA) integration has only been tested when running the OnGuard and Milestone systems on Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019.

- OnGuard doesn't model doors; they work only with readers. But XProtect Access requires doors to be modelled. Therefore, the OnGuard plugin creates virtual doors based on reader properties (i.e. panel id, panel address, reader number, etc). Currently, the virtual door names are based on the first reader that has a non-empty display name. So if that reader is named "reader 1", that's what the door will be named. This may not be intuitive when viewed in the XProtect Management or Smart Client applications' hardware hierarchy.
- When creating a new XPA instance on the Access Control tab in the XProtect Management Client, especially when creating the first instance, it may take 1 or 2 clicks of the Next button in the wizard before configuration is successfully fetched from the OnGuard system.
- The XPA Instance (MIPPlugin) in the Management Client can fail to load after the Event Server starts or is restarted if the XProtect Access Service on the OnGuard Server is not started or not yet ready. Symptoms of this issue include:
    - Existing XPA Instance disappears from Management Client.
    - Creation of new XPA Instance is not allowed.
    - NullReferenceException log entries appear in the Event Server log file.



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 150,000 sites worldwide. Founded in 1998, Milestone is a stand-alone company in the Canon Group.

milestone



the system recorded, which will help the district to combat vandalism and theft," said Jason Beardsley, vice president of the Security Division of HCI Systems, an Ontario, California-based systems integrator that installed the security system.

Lacking a centralized security system for prevention and protection

The Anaheim Union High School District is a public school district serving portions of the Orange County cities of Anaheim, Buena Park, Cypress, La Palma, and Stanton. The district office oversees 21 schools spanning 46 square miles across 20 campuses, including eight junior high schools, 10 high schools, two alternative education schools, and one virtual school. Responsible for the safety of 29,000 students and 3,000 employees, the district is among the top 10 largest employers in the city of Anaheim.

Located south of Los Angeles, the suburban school district had one school shooting in 1989 at Loara High School in Anaheim where one student was injured. Since then, the district has mainly had issues with theft and vandalism, including graffiti and destruction of property.

Despite its student population size and geographic expanse, AUHSD only had a few surveillance cameras set up with DVR-based systems at a handful of campuses. Starting in 2014, the AUHSD community actively began the process of hardening their security infrastructure to better prevent and protect against future school attacks.

"Some of our schools have an open layout where the campus is fairly open to the public. This led us to explore ways to make our campuses safer," said Erik Greenwood, chief technology officer at AUHSD. "In addition to a centralized security system, we also put fencing at all of our schools."

To keep schools safe, AUHSD has focused on a number of measures, including deploying the video surveillance system, establishing lock-down procedures, and providing safety training guidelines for a potential active shooter incident. The district does not use metal detectors or employ school resource officers (SROs), but they plan on integrating their existing ID badge and gate access control system into the VMS in future security installation phases.

"As we were installing cameras, the schools were getting images of vandalism and even images of golf carts being stolen. It was phenomenal to see how many issues the system recorded, which will help the district to combat vandalism and theft."

Jason Beardsley,
Vice President of the
Security Division,
HCI Systems

Strengthening the district's security infrastructure

Funding for AUHSD's $2 million security system came from the voter-approved Measure H bond passed in 2014, which provided $249 million for facility improvements on school campuses. The installation, which began in 2019, was completed in 2020 just as the COVID-19 pandemic hit the United States and temporarily closed school campuses in California through mid-2021.

Working with HCI Systems, AUHSD installed Milestone XProtect Enterprise to provide a consolidated video management system at the district office's IT department. Velesea, a server distributor based in Irvine, California, installed a 1.4 petabyte DDN storage solution with 12 pre-racked and pre-loaded servers. The VMS retains video content for a 30-day period. In addition, approximately 1,450 Hanwha Techwin America QNV-7080R 4MP Network IR Vandal Resistant Cameras were installed.

The video surveillance system was installed ahead of time and on budget, even after a few design iterations to expand camera coverage to eliminate blind spots. More importantly, as the system was being installed, it immediately began capturing incidents at the 20 campuses. One area of continued unwelcomed activity was occurring at the recently installed pool at Anaheim High School.

"Once this brand new, beautiful pool was put in, we had alerts that people were jumping the fence to go swimming," said Greenwood. Now school authorities are



able to respond quickly if anyone has gained access to the pool after hours. In addition, based on concerns from the school community, fencing was added to all campuses with strategically placed perimeter sensors, including a boundary sensor at the new pool.

For future expansions, AUHSD will continue to identify blind spots and high traffic areas that require more camera coverage, as well as perimeter sensors for assets such as the maintenance yard.

Improved vandalism and theft prevention

The district initially installed 1,250 Hanwha Wisenet Q series cameras throughout the school campuses in entrances, exits, exterior restroom doors, staff work areas, and in general meeting areas. As schools began using the VMS system, AUHSD added an additional 200 cameras to expand coverage and avoid blind spots in campus surveillance. The cameras are able to capture sharp images in dimly lit areas, improving campus security at night. With its vandal resistant features, the camera domes can easily be cleaned or swapped without replacing the camera.

The VMS's consolidated view of all the cameras across the district helps improve response time to threats and incidents because administrators can precisely locate trouble spots and security breaches on campuses. Interactive, multilayered maps provide a comprehensive overview of cameras and layouts of the entire

One area of continued unwelcomed activity was occurring at the recently installed pool at Anaheim High School.

Fencing was added to all campuses with strategically placed perimeter sensors, including a boundary sensor at the new pool.

Now school authorities are able to respond quickly if anyone has gained access to the pool after hours.





surveillance installation, allowing quick detection of trouble areas. The camera navigator increases visual verification — whenever a school administrator views a camera feed, nearby cameras are automatically displayed on screen, making it easy to switch between cameras to follow a moving object in different directions, helping to authenticate evidence of vandalism, theft, or other potential incidents of violence on campus.

"The features are robust, so it's fairly easy to go in to review footage, to playback, and to export," said Greenwood. "It's a straightforward, reliable system."

School administrators can quickly review footage of incidents by using the VMS's instant playback to view recorded video for one or more cameras. With smart search, an image can be searched for motion by time, creating thumbnail images for fast delivery of evidence to authorities.

"The VMS also gives us the ability to better manage the cameras in terms of giving the appropriate people the appropriate permissions to only the cameras they need to see," said Greenwood. The VMS uses Active Directory, making it simple to manage user rights for many aspects of the system, including control of privileges and camera actions, which helps protect students' privacy.

In addition, Greenwood found that Milestone licensing was favorable compared to other companies with its automatic online activation of system and camera licenses. The VMS gathers all camera information and automatically requests the corresponding licenses online, enabling faster deployment as newly added cameras are fully functional during a 30-day grace period.

"It's definitely an additional tool in our belt to be able to potentially resolve issues where we have video footage if there's some type of vandalism going on," said Greenwood.

Protecting lives during emergencies

In terms of active shooter response, the hybrid on-premise VMS uses a cloud mobile server so that Orange County Public Safety and the police departments that serve the five cities located in the district boundaries can access the system during an emergency situation. With video sharing, law enforcement can view live feeds. Getting critical data to first responders is important when it comes to preventing or protecting lives during campus incidents.

"We worked with the resource officers for each one of those departments to keep them involved. Giving them the knowledge of the cameras' strategic locations will

"For me, the big takeaway is the human element. We installed the new system, and now we have the partnership going forward to help us continue using this system successfully."

Erik Greenwood,
Chief Technology Officer,
Anaheim Union High
School District



ultimately make their job safer and also give them more investigation ability," said HCI's Beardsley.

In an effort to help first responders during a potential active shooter incident, AUHSD also uses The Sobel Group's TSG 360° at Anaheim High School, Katella High School, and the North Orange Continuing Education Campus. This legacy digital-campus mapping system stiches up to 16,000 individual images into high resolution 360-degree images, giving the Anaheim Police Department digital eyes on campus.

Training existing staff to monitor campus activity

"Our goal was to make the district as effective and self-supportive as possible, right from the beginning," said Greenwood. "On the plus side, the district has not needed to hire additional staff to manage the VMS."

An important component of the video management system involved Milestone's ability to provide on-site user training. Milestone certified instructors provided detailed training and instruction for about 100 school administrators, security professionals, and IT personnel.

On school campuses, site administration, including principals and assistant principals, are the primary VMS users. At the district office, business directors have camera access to view facility operations. For example, the transportation director has a view into the bus yard. The purchasing director manages the warehouse with a view into the warehouse dock and the surrounding area. Using the VMS, the food service director oversees delivery vehicles. The maintenance and operations director has camera access to all campuses to manage the repair of buildings and landscapes.

Finally, the collaborative partnership that AUHSD has built with Milestone, Hanwha, and HCI has played a critical role in the school's security system success.

"For me, the big takeaway is the human element," said Greenwood. "We installed the new system, and now we have the partnership going forward to help us continue using this system successfully."

"We worked with the resource officers for each one of those [police] departments to keep them involved. Giving them the knowledge of the cameras' strategic locations will ultimately make their job safer and also give them more investigation ability."

Jason Beardsley,
Vice President of the Security Division,
HCI Systems

About Milestone Systems

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 installations worldwide. Founded in 1998, Milestone is a stand-alone company in the Canon Group. For more information visit: www.milestonesys.com.

MAKE THE WORLD SEE