MAKE THE
WORLD SEE

Date: 08 October 2025

Manual

XProtect Pro-Watch Integration v3.0

milestone

Table of Content

Target audience for this document

The installation and configuration part of this document is aimed at system administrators of both the Milestone XProtect, Honeywell Pro-Watch Software Suite and Honeywell Pro-Watch API software.

The operation part of this document is aimed at system administrators and system operators with basic knowledge of Milestone XProtect.

As this manual contains specific details about the integration between Milestone XProtect and Honeywell Pro-Watch, it is recommended for system administrators to check the following sources of information:

- Milestone XProtect 2025 R2 (XProtect Management Client and XProtect Smart Client) help which contains detailed information about XProtect Access
- Honeywell Pro-Watch Software Suite Installation Guide v6.5.1 which contains detailed information about installation of Pro-Watch access control system
- Honeywell Pro-Watch User Guide v6.5.1 help which contains detailed information about configuration and use of Pro-Watch access control system
- Honeywell Pro-Watch API Service v6.5.2 contains detailed information about installation, configuration and use of the API

and for the system operators to check at least:

- Milestone XProtect 2025 R2 (XProtect Smart Client) help which contains detailed information about Milestone XProtect Access

Release notes

Build 3.0.51.0

This is the initial release.

Copyright, trademarks & disclaimer

Copyright

Trademarks

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

Microsoft and Windows are registered trademarks of Microsoft Corporation.

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

Disclaimer

This document 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 reserve the right to adjust without prior notification.

All names of people and organizations used in this document's examples 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 surveillance system installation folder.

General description

Introduction

The XProtect Pro-Watch Integration is a Milestone XProtect Access plug-in, which supports a number of features including:

- Events generated by doors/door access points from Honeywell Pro-Watch access control system can be used as sources for Alarms and Rules in Milestone XProtect
- Live monitoring of events in Milestone XProtect based on the association of door access points and cameras
- Control and status monitoring of doors utilizing the Milestone XProtect map feature
- Interactive control from a Smart map view - users can perform actions such as unlocking or locking doors, as well as viewing live camera feeds, all within a single interface.
- Badge Holders from Honeywell Pro-Watch access control system are integrated into Milestone XProtect

Solution overview

The integration consists of a XProtect Event Server plug-in which communicates with Honeywell Pro-Watch API as illustrated here:
<XProtect Event Server> <-> <API> <-> <Pro-Watch access control system> <-> <Panel>

XProtect Event Server plug-in

The machine running the XProtect Event Server must be able to connect to the Pro-Watch API using TCP/IP communication. The configuration of the plug-in is done in the XProtect Management Client where:

- The Pro-Watch system must be added
- Different properties can be set
- It is possible to create Alarms and Rules using the Pro-Watch system supported events as sources

Also, some useful information is logged into the Audit logs of the XProtect Management Client.

XProtect Smart Client plug-in

The integrated features in the XProtect Smart Client include:

- Adding the Pro-Watch system doors/door access points as Access Monitor for live monitoring of the events
- Adding the Pro-Watch system Hardware Actions as Overlay buttons
- Map feature integration used for control, monitoring and visual representation of the Pro-Watch system doors
- Smart map feature integration used for control and visual representation of the Pro-Watch system doors
- Pro-Watch system generated alarms are listed and visualized in the Alarms list
- Acknowledgement of the Pro-Watch system generated alarms
- Centralized overview of Events/Doors/Cardholders in Access Control tab
- Access request notifications

Installation

Prerequisites

The XProtect Pro-Watch Integration is compatible with:

- Milestone XProtect Corporate 2025 R2 or newer
- Honeywell Pro-Watch v6.5.1
- Honeywell Pro-Watch API Service v6.5.2 with Rest API v2

Installer

The XProtect Pro-Watch Integration consists of one installation file supporting Windows 64-bit only:

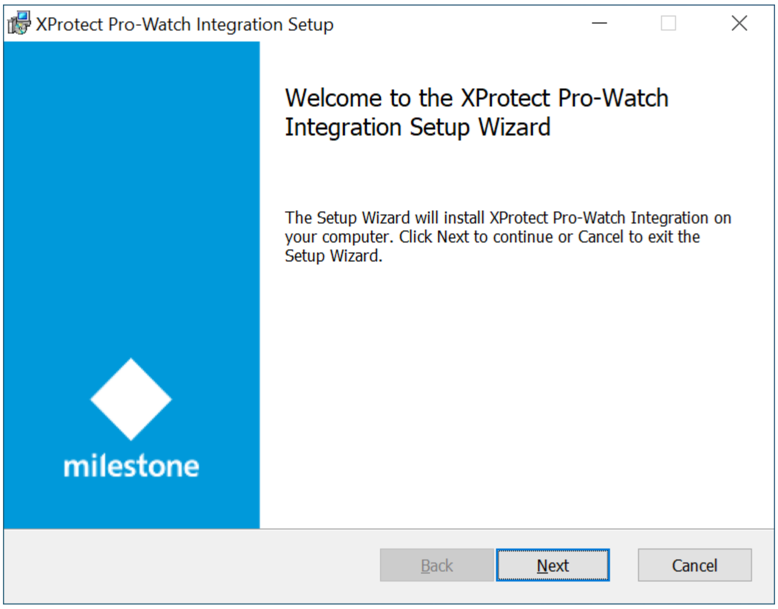
- XProtectProWatchIntegration _3.0.XX.X.msi

The XProtect Pro-Watch Integration must be installed on the following computers:

- On the computer, where the Milestone XProtect Event Server is installed
- On the computers, where the Milestone XProtect Management Client is installed

Installation steps

1. Start the installation by executing *XProtectProWatchIntegration_3.0.XX.X.msi*.
2. Click **Next**.

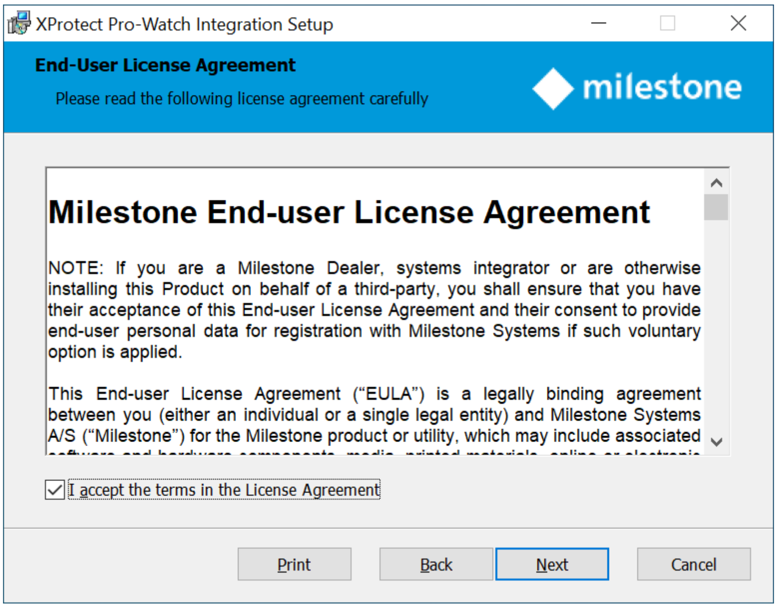


XProtect Pro-Watch Integration Setup

Welcome to the XProtect Pro-Watch Integration Setup Wizard

The Setup Wizard will install XProtect Pro-Watch Integration on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

3. Read the license agreement carefully and select the **I accept the terms in the License Agreement** box. Click **Next**.



XProtect Pro-Watch Integration Setup

End-User License Agreement

Please read the following license agreement carefully

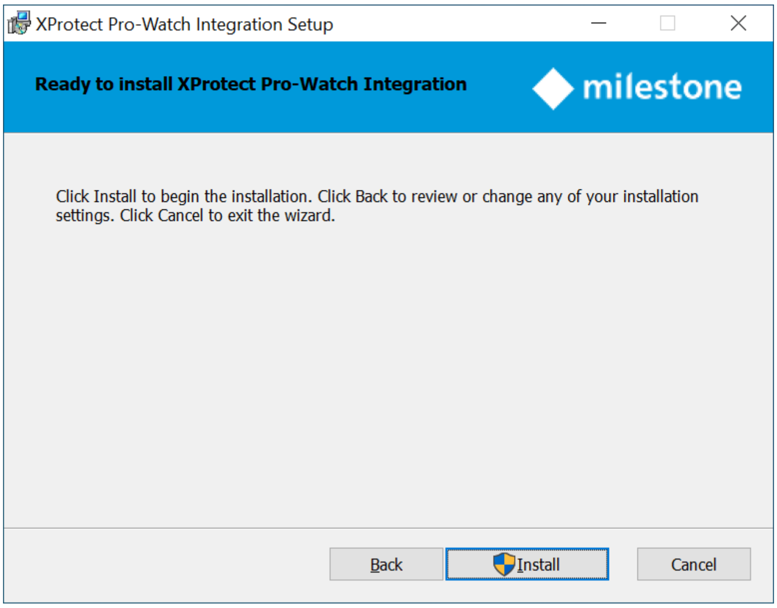
Milestone End-user License Agreement

NOTE: If you are a Milestone Dealer, systems integrator or are otherwise installing this Product on behalf of a third-party, you shall ensure that you have their acceptance of this End-user License Agreement and their consent to provide end-user personal data for registration with Milestone Systems if such voluntary option is applied.

This End-user License Agreement ("EULA") is a legally binding agreement between you (either an individual or a single legal entity) and Milestone Systems A/S ("Milestone") for the Milestone product or utility, which may include associated

☑ I accept the terms in the License Agreement

4. Click **Install**.

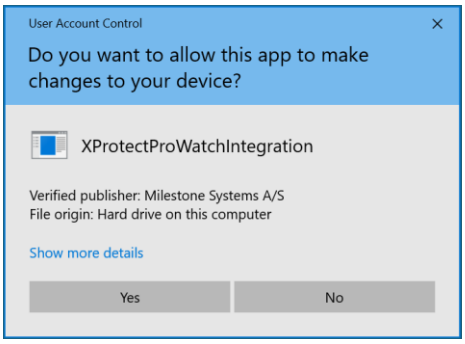


XProtect Pro-Watch Integration Setup

Ready to install XProtect Pro-Watch Integration

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

5. Click **Yes**, in case the following message appears on the screen:



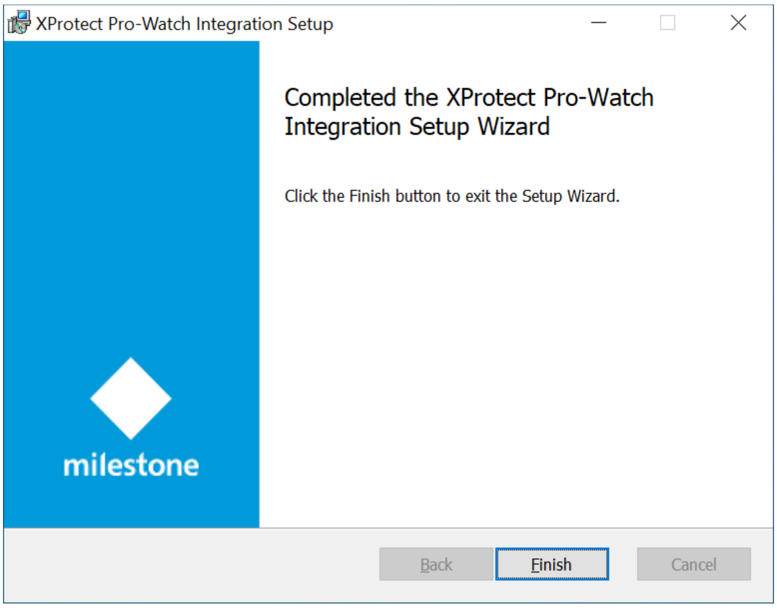
User Account Control

Do you want to allow this app to make changes to your device?

XProtectProWatchIntegration

Verified publisher: Milestone Systems A/S
File origin: Hard drive on this computer

6. The next steps are executed automatically.
7. Click **Finish**.



XProtect Pro-Watch Integration Setup

Completed the XProtect Pro-Watch Integration Setup Wizard

Click the Finish button to exit the Setup Wizard.

8. Restart the XProtect Event Server and the XProtect Management Client.

License

The XProtect Pro-Watch Integration requires the following licenses:

- A **Base** license for Milestone XProtect Access which allows accessing this feature
- An **Access control door** license is needed for each door which needs to be controlled
- **MIP** license for the plug-in

Note: See the Milestone XProtect help for more information about the **Base** and **Access control door** licenses.

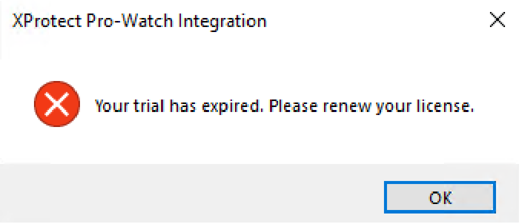
MIP license

This solution does have a build-in **MIP** license check that is locked to the software license code (SLC) of the XProtect installation of which it is a part.

It automatically comes with a 30-day grace period which starts from the date when the plug-in is installed. After the grace period expires, a permanent **MIP** license is needed.

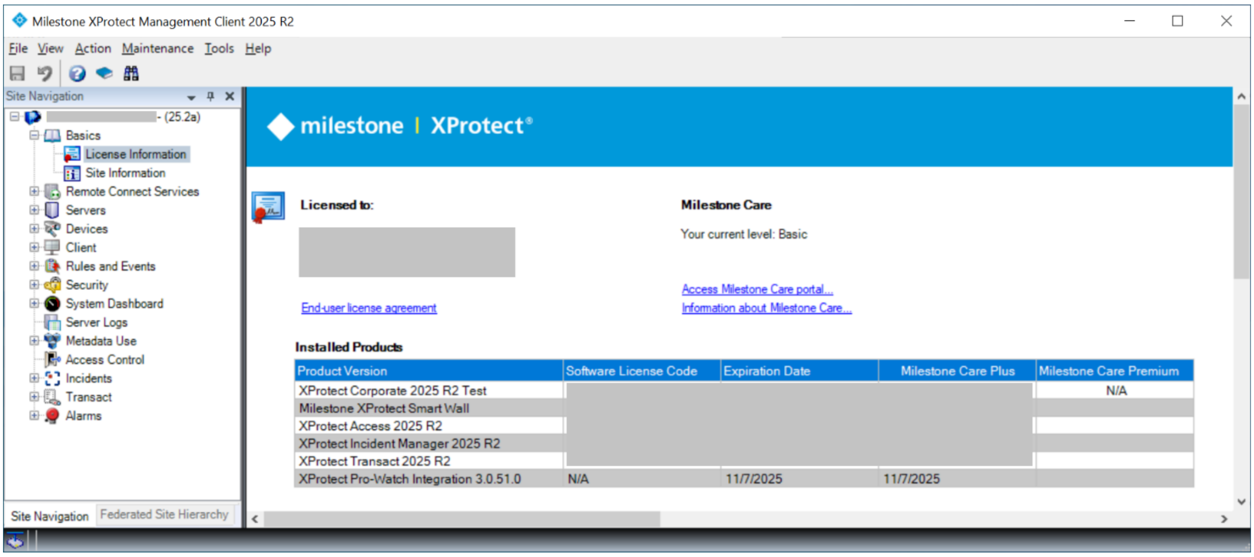
The permanent **MIP** licenses are provided by the distributor. To generate a permanent **MIP** license, the distributor must know the SLC of the XProtect system where the solution has been installed. Collect the SLC and send it to the distributor, preferably via email.

When the permanent **MIP** license is acquired, the XProtect system must be reactivated, either online or offline.
If **MIP** license check fails, the XProtect Management Client plug-in will issue error messages and will have a reduced functionality.



Your trial has expired. Please renew your license.

The license information can also be checked in the XProtect Management Client > **Site Navigation** > **Basics** > **License Information** > **Installed Products** > **XProtect Pro-Watch Integration v3.0.XX.X**.



Licensed to:

[redacted]

Milestone Care

Your current level: Basic

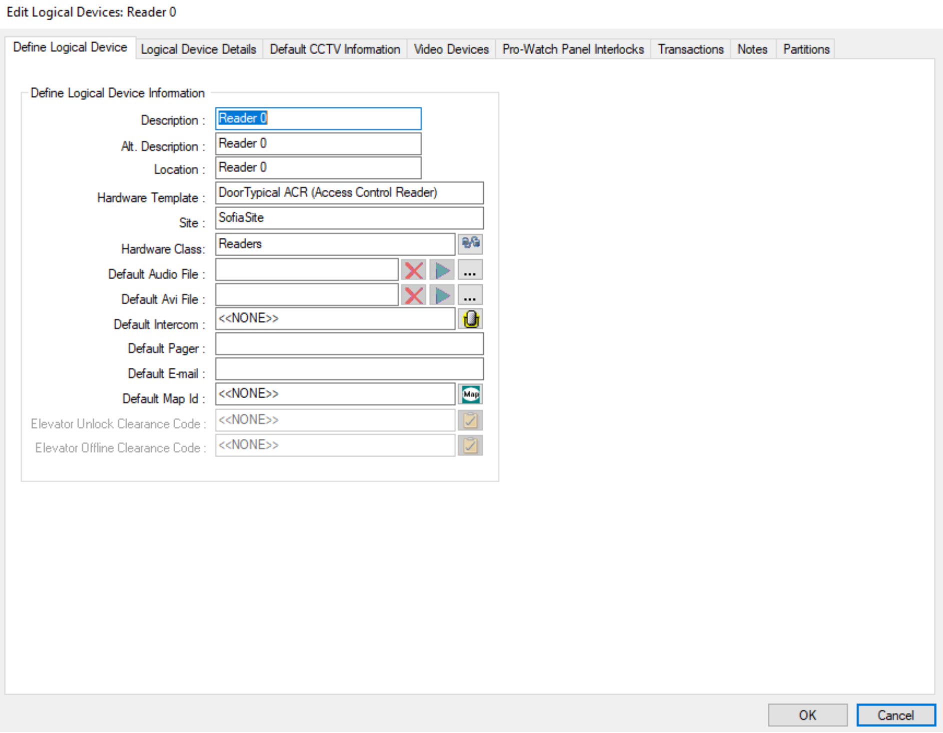
Installed Products

Product Version	Software License Code	Expiration Date	Milestone Care Plus	Milestone Care Premium
XProtect Corporate 2025 R2 Test	[redacted]	[redacted]	[redacted]	N/A
Milestone XProtect Smart Wall	[redacted]	[redacted]	[redacted]	
XProtect Access 2025 R2	[redacted]	[redacted]	[redacted]	
XProtect Incident Manager 2025 R2	[redacted]	[redacted]	[redacted]	
XProtect Transact 2025 R2	[redacted]	[redacted]	[redacted]	
XProtect Pro-Watch Integration 3.0.51.0	N/A	11/7/2025	11/7/2025	

Pro-Watch and XProtect elements mapping

The hierarchy in the Pro-Watch system is usually **Site** > **Channel** > **Panel** > **Logical Devices**. The **Logical Devices** are based on **Hardware Templates** and **Hardware Classes**.

Example:



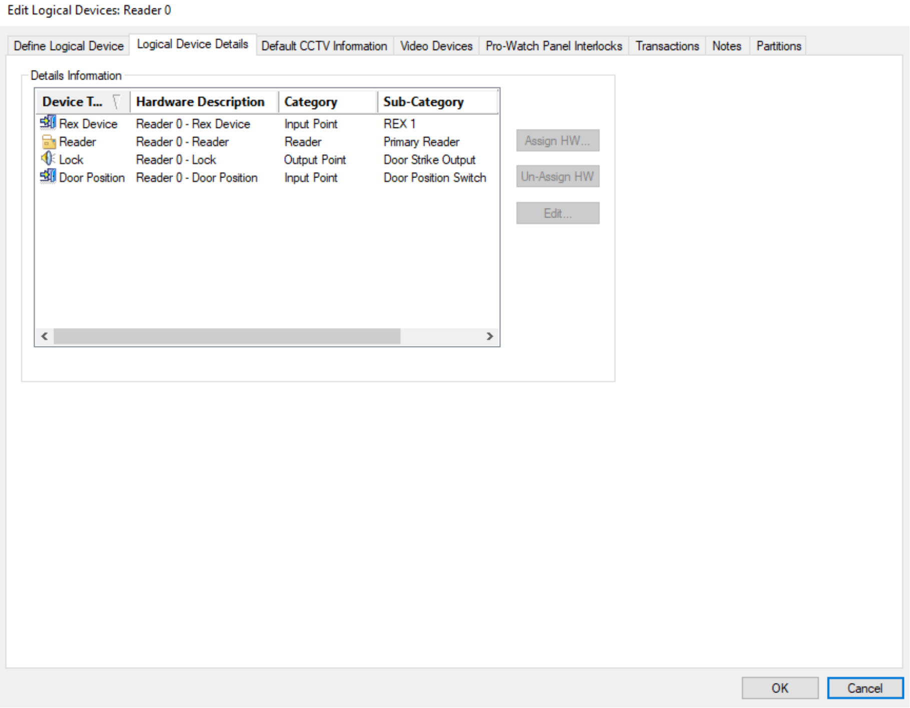
Edit Logical Devices: Reader 0

Define Logical Device Information

Description : Reader 0
Alt. Description : Reader 0
Location : Reader 0
Hardware Template : DoorTypical ACR (Access Control Reader)
Site : SofiaSite
Hardware Class: Readers
Default Audio File :
Default Avi File :
Default Intercom : <<NONE>>
Default Pager :
Default E-mail :
Default Map Id : <<NONE>>
Elevator Unlock Clearance Code : <<NONE>>
Elevator Offline Clearance Code : <<NONE>>

Each of these **Logical Devices** can include several device types of different categories and sub-categories. In the example below, you can see a logical device **Reader 0** based on **Hardware Template**: **DoorTypicalACR (Access Control Reader)** and **Hardware Class**: **Reader**.

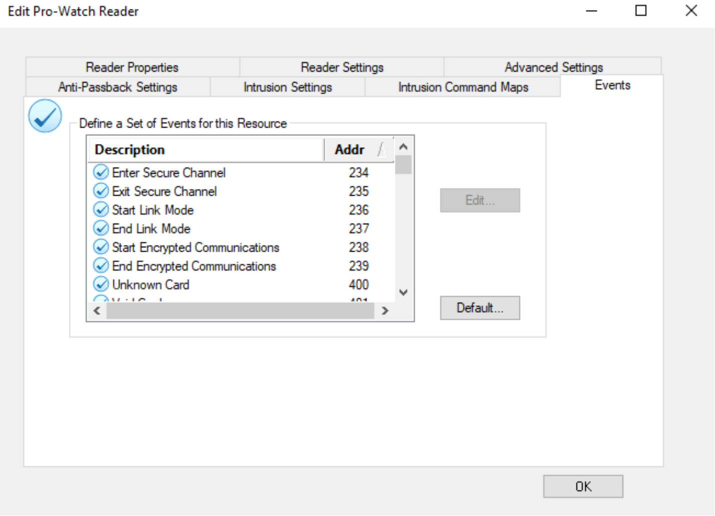
Example:



Device T...	Hardware Description	Category	Sub-Category
Rex Device	Reader 0 - Rex Device	Input Point	REX 1
Reader	Reader 0 - Reader	Reader	Primary Reader
Lock	Reader 0 - Lock	Output Point	Door Strike Output
Door Position	Reader 0 - Door Position	Input Point	Door Position Switch

A set of events is defined for each device type (resource). In the example below you can see the events listed for the **Reader 0 – Reader** resource.

Example:



Description	Addr
Enter Secure Channel	234
Exit Secure Channel	235
Start Link Mode	236
End Link Mode	237
Start Encrypted Communications	238
End Encrypted Communications	239
Unknown Card	400

The XProtect Pro-Watch Integration supports only the logical devices based on **Hardware Template**: **DoorTypicalACR (Access Control Reader)** and **Hardware Class**: **Reader**, their device types (resources) and the defined set of events for these resources. The integration may work with logical devices based on other **Hardware Template** and **Hardware Classes**, but Custom Development does not guarantee that.

The table below contains the mapping between the Pro-Watch system devices and the XProtect Access devices:

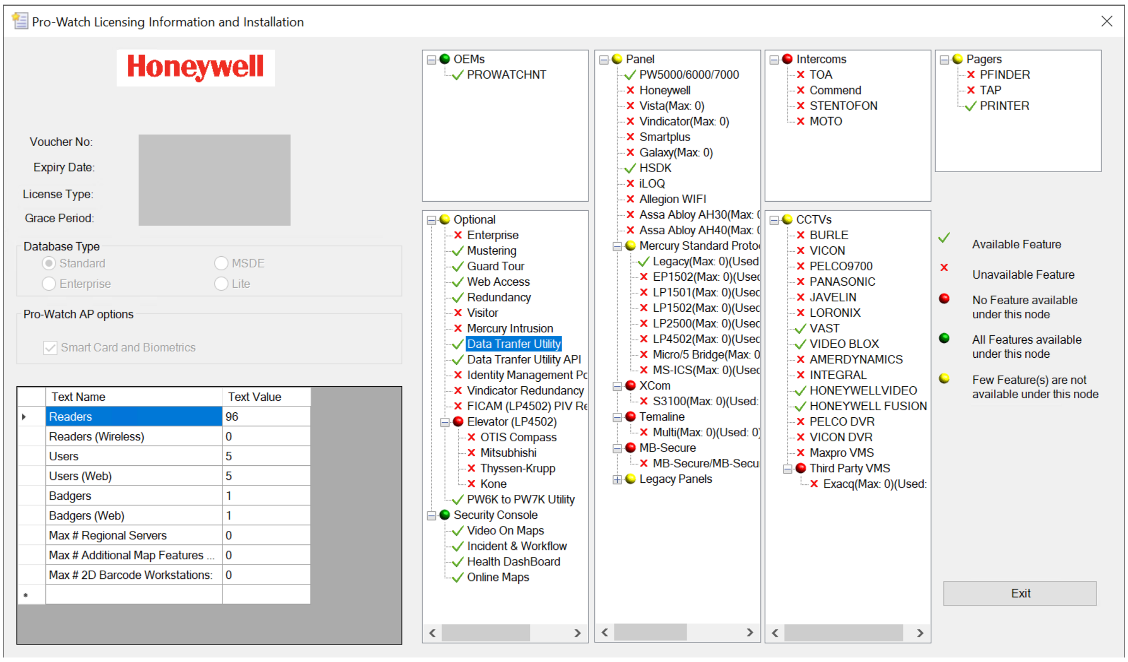
Pro-Watch	**XProtect**	**Notes**
Reader 0 (DoorTypicalACR (Access Control Reader))	Door	• Visible in XProtect Management Client and can be selected as a source of events • Visible in XProtect Smart Client • Takes over the ownership of events generated by the following resources: Rex Device and Door Position in the XProtect system • Hardware Actions from the Pro-Watch system are transferred into actions in the XProtect system
Reader 0 – Rex Device	NA	• Not visible in XProtect Management Client • Not visible in XProtect Smart Client • The parent device (in this case Reader 0) takes over the ownership of the generated events
Reader 0 – Reader	Access Point	• Visible in XProtect Management Client and can be selected as a source of events • Visible in XProtect Smart Client • The generated events are with source Reader 0 – Reader
Reader 0 – Lock	NA	• Not visible in XProtect Management Client • Not visible in XProtect Smart Client • Events generated by this resource are currently not supported in XProtect
Reader 0 – Door Position	NA	• Not visible in XProtect Management Client • Not visible in XProtect Smart Client • The parent device (in this case Reader 0) takes over the ownership of the generated events

Pro-Watch configuration

Note: The configuration steps below represent the minimum required actions to successfully establish XProtect Pro-Watch Integration.

Prerequisites

1. Start Pro-Watch.
2. Open **Pro-Watch Licensing Information and Installation page** and check that **Optional** > **Data Transfer Utility** and **Data Transfer Utility API** are enabled.



Pro-Watch Licensing Information and Installation

Voucher No:
Expiry Date:
License Type:
Grace Period:

Database Type
◉ Standard ○ MSDE
○ Enterprise ○ Lite

Pro-Watch AP options
☑ Smart Card and Biometrics

Text Name	Text Value
Readers	96
Readers (Wireless)	0
Users	5
Users (Web)	5
Badgers	1
Badgers (Web)	1
Max # Regional Servers	0
Max # Additional Map Features ...	0
Max # 2D Barcode Workstations:	0

● OEMs
- ✓ PROWATCHNT

● Optional
- ✗ Enterprise
- ✓ Mustering
- ✓ Guard Tour
- ✓ Web Access
- ✓ Redundancy
- ✗ Visitor
- ✗ Mercury Intrusion
- ✓ Data Tranfer Utility
- ✓ Data Tranfer Utility API
- ✗ Identity Management Pc
- ✗ Vindicator Redundancy
- ✗ FICAM (LP4502) PIV Re
- ● Elevator (LP4502)
  - ✗ OTIS Compass
  - ✗ Mitsubhishi
  - ✗ Thyssen-Krupp
  - ✗ Kone
- ✓ PW6K to PW7K Utility

● Security Console
- ✓ Video On Maps
- ✓ Incident & Workflow
- ✓ Health DashBoard
- ✓ Online Maps

● Panel
- ✓ PW5000/6000/7000
- ✗ Honeywell
- ✗ Vista(Max: 0)
- ✗ Vindicator(Max: 0)
- ✗ Smartplus
- ✗ Galaxy(Max: 0)
- ✓ HSDK
- ✗ iLOQ
- ✗ Allegion WIFI
- ✗ Assa Abloy AH30(Max: (
- ✗ Assa Abloy AH40(Max: (
- ● Mercury Standard Proto
  - ✓ Legacy(Max: 0)(Used
  - ✗ EP1502(Max: 0)(Usec
  - ✗ LP1501(Max: 0)(Usec
  - ✗ LP1502(Max: 0)(Usec
  - ✗ LP2500(Max: 0)(Usec
  - ✗ LP4502(Max: 0)(Usec
  - ✗ Micro/5 Bridge(Max: 0
  - ✗ MS-ICS(Max: 0)(Usec
- ● XCom
  - ✗ S3100(Max: 0)(Used:
- ● Temaline
  - ✗ Multi(Max: 0)(Used: 0)
- ● MB-Secure
  - ✗ MB-Secure/MB-Secu
- ● Legacy Panels

● Intercoms
- ✗ TOA
- ✗ Commend
- ✗ STENTOFON
- ✗ MOTO

● CCTVs
- ✗ BURLE
- ✗ VICON
- ✗ PELCO9700
- ✗ PANASONIC
- ✗ JAVELIN
- ✗ LORONIX
- ✓ VAST
- ✓ VIDEO BLOX
- ✗ AMERDYNAMICS
- ✗ INTEGRAL
- ✓ HONEYWELLVIDEO
- ✓ HONEYWELL FUSION
- ✗ PELCO DVR
- ✗ VICON DVR
- ✗ Maxpro VMS
- ● Third Party VMS
  - ✗ Exacq(Max: 0)(Used:

● Pagers
- ✗ PFINDER
- ✗ TAP
- ✓ PRINTER

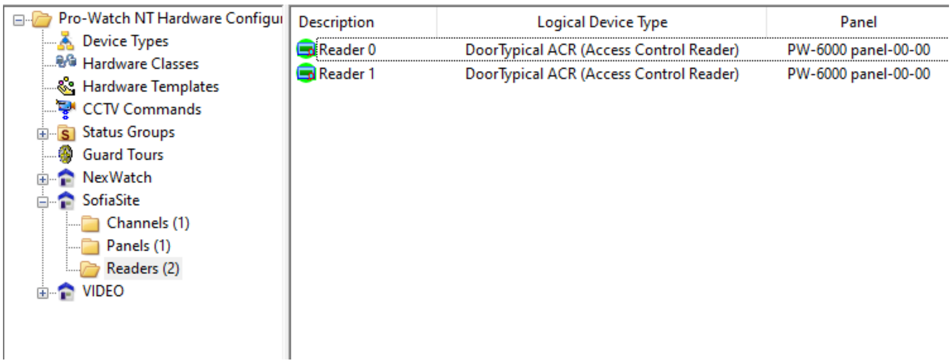
✓	Available Feature
✗	Unavailable Feature
🔴	No Feature available under this node
🟢	All Features available under this node
🟡	Few Feature(s) are not available under this node

Pro-Watch Software Suite & Hardware

1. (Optional) Connect the Pro-Watch panel to the network and turn it on.

   In the example below, a **PW-6000** panel is used.
2. Create a **Site**, a **Channel**, and a **PW-6000** panel.
3. Add at least one **Reader** for the panel.

In the example below, two **Readers** are created.



Description	Logical Device Type	Panel
Reader 0	DoorTypical ACR (Access Control Reader)	PW-6000 panel-00-00
Reader 1	DoorTypical ACR (Access Control Reader)	PW-6000 panel-00-00

4. (Optional) Verify that there is a connection between the **PW-6000** panel and **Pro-Watch Software Suite**.

Pro-Watch API

Configure the Pro-Watch API as per the Honeywell Pro-Watch API Service documentation. Make sure that:

1. The following properties are configured in the API configuration file (**appsettings.json**):

Parameter	Value
StartDataService	1
StartEventService	1
StartRESTService	1
PWRestUrl	http://<Pro-Watch API computer name>:<port01>
PWEventSignalUrl	http://<Pro-Watch API computer name>:<port02>
PWDataSignalUrl	http://<Pro-Watch API computer name>:<port03>
RESTBasePath	/pwapi
UserPWRegistry	0
PWDatabaseServer	<Pro-Watch Software Suite Database computer name>
PWDatabase	<Pro-Watch database name>
PWCommServer	<Pro-Watch Software Suite computer name>
UseIntegratedSecurity	1
TokenExpireMinutes	30

Example:

In the example below the Pro-Watch Software Suite and Pro-Watch API are installed on the same computer.

```
    "StartDataService": "1",
    "StartEventService": "1",
    "StartRESTService": "1",

    "PWRestUrl": "http://PWServer:8734/",
    "PWEventSignalRUrl": "http://PWServer:8735/",
    "PWDataSignalRUrl": "http://PWServer:8736/",
    "RESTBasePath": "/pwapi",

    "UsePWRegistry": "0",
    "PWDatabaseServer": "PWServer",
    "PWDatabase": "PWNT",
    "PWCommServer": "PWServer",
    "UseIntegratedSecurity": "1",
    "TokenExpireMinutes": "30",
```

2. You have (created) a user which is going to be used for the authentication between XProtect and Pro-Watch API.

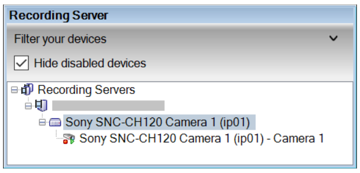
XProtect Management Client configuration

Add camera to a recording server

1. Open XProtect Management Client > **Site Navigation** > **Servers** > **Recording Servers**.
2. Right click on the current recording server and select **Add Hardware…**
3. Follow the wizard to add all available cameras.

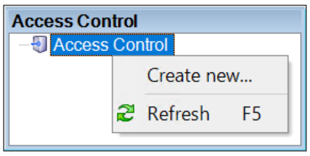
> **Note**: For detailed description on how to add cameras to a recording server, see the Milestone XProtect (XProtect Management Client) help.

Example:



Add Pro-Watch Access Control

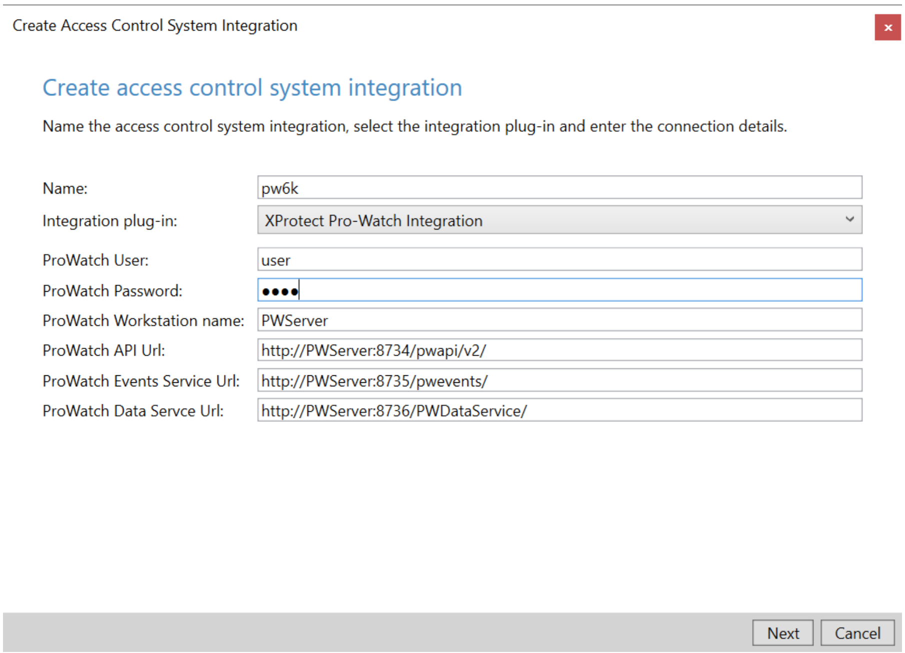
1. Open XProtect Management Client > **Site Navigation** > **Access Control**.
2. Right click on the **Access Control** node and select **Create new…**



3. Enter a proper **Name** and select **XProtect Pro-Watch Integration** from the **Integration plug-in** dropdown. The following connection details appear and need to be specified:

Parameter	Description
Name	Enter a proper **Name**.
Integration plug-in	Select **XProtect Pro-Watch Integration** from the **Integration plug-in** dropdown.
ProWatch User	The user created in chapter Pro-Watch configuration > Pro-Watch API > step 2.
ProWatch Password	The **Web** password of the user.
ProWatch Workstation name	The format is: <computer name> The computer name where the Pro-Watch Software Suite is installed.
ProWatch API Url	The format is: http://<computer name><port>/pwapi/v2/ The computer name and port are the values for the **PWRestUrl** parameter configured in chapter Pro-Watch configuration > Pro-Watch API > step 1.
ProWatch Event Service Url	The format is: http://<computer name><port>/pwevents/ The computer name and port are the values for the **PWEventSignalUrl** parameter configured in chapter Pro-Watch configuration > Pro-Watch API > step 1.
ProWatch Data Service Url	The format is: http://<computer name><port>/PWDataService/ The computer name and port are the values for the **PWDataSignalUrl** parameter configured in chapter Pro-Watch configuration > Pro-Watch API > step 1.

Example:



Create Access Control System Integration

Create access control system integration

Name the access control system integration, select the integration plug-in and enter the connection details.

Name:	pw6k
Integration plug-in:	XProtect Pro-Watch Integration
ProWatch User:	user
ProWatch Password:	••••
ProWatch Workstation name:	PWServer
ProWatch API Url:	http://PWServer:8734/pwapi/v2/
ProWatch Events Service Url:	http://PWServer:8735/pwevents/
ProWatch Data Servce Url:	http://PWServer:8736/PWDataService/

Click **Next**.

4. The configuration data is collected from the access control system. A few items are added based on the configuration data received from the Pro-Watch system:

   Example:
   In the example below, the following items are added:
   Doors (2): The doors which are added in chapter Pro-Watch configuration > Pro-Watch Software Suite & Hardware > step 3:

   Reader 0
   Reader 1

   Units (3): The panel and units (door access points) which are related to the added doors.

   PW-6000 panel 00
   Reader 0 – Reader
   Reader 1 – Reader

   Servers (1): The Pro-Watch system.

   Honeywell ProWatch Server at <Pro-Watch Software Suite computer name>

   Events (444): The list of supported events is dynamically pulled through the Pro-Watch API. It is based on the connected hardware.

   Example:

930: Input Anomaly
924: Input Tampered
923: Input Disarm
922: Input Disable
921: Input Activated
920: Input Failure
911: Monitor Input Alarm
910: Input point disconnected
909: Input point unshunted
908: Input point shunted
907: Input point fault detected
906: Input Point Masked for Exit Delay
905: Input point masked for Entry Delay
904: Input point in trouble
903: Input point held past shunt time
902: Input point is open
901: Input point in short condition
900: Input point in alarm
850: Gateway Open For Exit
849: No Tail escort transit
848: Request To Exit
847: PIN Change Failed
846: PIN Changed
845: PIN Expired
844: Door Restored
843: SAM Authentication Failure
842: Restricted Access
841: Feature Not Authorized
840: Security Block
839: Visitation Required
838: Access Denied
837: Denied Asset Check
836: Denied SAP Check
835: Denied For Number
834: Denied Transit 2
833: Denied For Timeout
832: APB No Block
831: Granted - Range Card
830: Wrong Card Edition
829: Read Unsuccessful
828: Reception Transit
827: Gate Not Shut

342: Reader removed
341: Reader added
331: MAX Module Tamper
330: Illegal MAX Tag
329: Illegal Code Entered
328: MAX Tag Accepted
327: Legal ATM Code Entered
326: Legal Code Entered
325: Invalid Code Entered
324: Wrong Code Alarm Activated
323: RF MVM Memory Failure
322: MAX Door Left open
321: MAX Door Contact Broken
320: MAX Tag Unknown
319: Missing Module Alarm
318: Module NF2AP Fuse Blown
317: Module Battery Fuse Blown
316: Module Low Volts
315: Module Battery Low
309: Module AC Fail Trouble
302: Module Tamper
239: End Encrypted Communications
238: Start Encrypted Communications
237: End Link Mode
236: Start Link Mode
235: Exit Secure Channel
234: Enter Secure Channel
2018: Input Point Omitted
2009: Input Point Activated
1949: User not Activated yet
1947: Invalid User
1945: Authentication
1944: Macro Denied
1943: Macro Granted
1942: Unset Denied
1941: Unset Granted
1940: Part Set Denied
1939: Part Set Granted
1938: Full Set Denied
1937: Full Set Granted
1936: Door Blocked
1935: Partition fullset

826: Too Few Users
825: Path Violation
824: Pass Back Violation
823: Zone Disarmed
822: Zone Armed
821: Automatic Modality
820: Semi Automatic Modality
819: Manual Modality
818: Gate Open
817: Restricted Access
816: Boarding Procedure Not Closed
815: End Boarding
814: Start Boarding
813: Function Not Authorized
812: Security Block
811: Security Inspection
810: Gateway Opened For One Exit Transit
809: Gateway Opened For One Entry Transit
808: Gateway Locked For Exit
807: Gateway Locked For Entry
806: Gateway Open For Entry
805: Gateway Forced Open
804: Transit Not Happened
803: Transit Denied
802: Path Violation Alarm
801: Incorrect Card Reading
661: Double Card
660: Escape and Return
659: IPB Pressed Multiple Times
658: Piggyback at door
657: Loitering at Portal/Door
656: Banned person detected
655: pivCLASS Reader Message
651: Interior Pushbutton Pressed
650: Deadbolt thrown
642: Intrusion Input Zone Proc disable
642: Intrusion ACR Zone Proc Disable
641: Intrusion Input Zone Proc Activate
641: Intrusion ACR Zone Proc Activate
640: Intrusion Input Zone Proc Bypass
640: Intrusion ACR Zone Proc Bypass
639: Intrusion Input Zone Keypad disable
639: Intrusion ACR Zone Keypad Disable

1934: Input TimeOut
1933: Different User
1932: Mode Disabled
1931: Wrong Token
1930: No Door Code
1929: No Macro
1928: No Ready State
1927: MPA Error
1926: No Schedule Active
1925: No Partition
1924: No Access Point
1923: Group Disabled
1922: No Group
1921: MPA Access Granted
1920: Unknown
1919: Valid User
1918: User Location
1917: Reader MPATimeout
1916: Reader FailAttemptAlarm
1915: Reader LockoutOn
1734: Door Mode Unknown
1638: Door Locked
1637: Door UnLocked
1636: Door Disabled
1635: Door Forced Open Masked
1634: Door Open Time Exceeded Masked
1633: Door Contact Fault Masked
1632: Control Unit Tamper Masked
1631: Bolt Unlocked Masked
1630: Holdup Alarm Masked - Ambush
1629: Control Unit Not Connected Masked
1628: Sabotage Alarm
1627: Lock Not Bolted
1626: Holdup - Ambush
1625: Reader Security Breach
1624: Holdup-PIN-Code Used
1623: S3100 - Input Masked
1622: Input Tamper
1620: Masking Reset
1486: Lock Out Of Sync
1485: DSR Offline
1484: Integrity Check Failed
1483: Missed Callbacks From Dsr

638: Intrusion Input Zone Keypad Activate	1482: Audit Log
638: Intrusion ACR Zone Keypad Activate	1481: Lock Tampered
637: Intrusion Input Zone Keypad Bypass	1480: Firmware Tampered
637: Intrusion ACR Zone Keypad Bypass	1479: Log Retrieved
636: Intrusion Input Zone Host disable	1478: Internal Error
636: Intrusion ACR Zone Host Disable	1477: Accesspoint Request Clock Reset
635: Intrusion Input Zone Host Activate	1476: Accesspoint Offline
635: Intrusion ACR Zone Host Activate	1475: Accesspoint Online
634: Intrusion Input Zone Host Bypass	1474: Accesspoint Unconfirmed
634: Intrusion ACR Zone Host Bypass	1473: Accesspoint Confirmed
633: Intrusion Zone is detached	1472: Accesspoint Replaced
632: Intrusion Zone in Entry Delay	1471: Accesspoint Created
631: Intrusion Zone Local Mask	1470: Accesspoint Deleted
630: Intrusion Zone Bypassed	1469: Accesspoint Rxheld
629: Intrusion Zone Offline	1468: Rxoverrun
628: Intrusion Zone Supervisory Fault	1467: Remote Authorization Request
627: Intrusion Zone Non-settling Error	1466: Reset Performed
626: Intrusion Zone Foreign Voltage	1465: Communication End
625: Intrusion Zone Open Circuit	1464: Communication Start
624: Intrusion Zone Short Circuit	1463: Communication Hw Disabled
623: Intrusion Zone in Ground Fault	1462: Communication Timeout
622: Intrusion Zone is Inactive	1461: Communication Error
621: Intrusion Zone is Active	1460: Hw Dpac Error
620: Door Open too long	1459: Hw Power Error
619: Door Forced Open	1458: Hw Mortise Error
618: Door Closed	1457: Nvram Checksum
617: Guard Is Now Late	1456: Nvram Layut Changed
616: Guard Never Arrived	1455: Nvram Clear User
615: Guard Arrived Late	1454: Nvram Ok
614: Guard Arrived Early	1453: Nvram Clear
613: Host Rex, Door used	1452: Clock Reset
612: Host Rex, Door not used	1451: Clock Error
611: Host Rex, Non-verified	1450: Clock Dstback
610: Rex Pressed, Door used	1449: Clock Dstforward
609: Rex Pressed, Door not used	1448: Clock Datetimeset
608: Rex Pressed, Non-verified	1447: Db Userdb Reset User
607: Reader in Card OR PIN mode	1446: Db Userdb Reset
606: Reader Card+PIN mode	1445: Firmware Update Fail
605: Reader in PIN only mode	1444: Firmware Update Success
604: Reader in card only mode	1443: Firmware Update Timeout
603: Reader in facility code mode only	1442: Firmware Update Error
602: Reader has been locked	1441: Firmware Update Abort
601: Reader has been unlocked	1440: Log Logwrapped

601: Control Unit Not Locked
600: Reader has been disabled
588: Kiosk Offline
587: Access Denied - Authentication Failed
586: Authentication Failed - Timeout
577: Access Lockout
534: Access Denied
519: Pre-Grant: Host Grant in Progress
518: Pre-Grant: Local Grant in Progress
517: Host Grant (Verification Viewer)
516: Cypher Mode Enabled
515: Local Grant - Door not used
514: Local Grant - Duress - Used
513: Local Grant - APB Error - Used
512: Local Grant - APB Error - Not Used
509: Local Grant - Duress - Not Used
508: Opened Unlocked Door
507: Timed override expired
506: Timed override disabled by host
505: Timed override enabled by host
504: Timed override disabled
503: Timed override enabled
502: Executive Privilege
501: Host Grant
500: Local Grant
479: Battery Critical
467: Tamper Rdr No Signal
466: Tamper Rdr Fault
465: Tamper Rdr Lock Jammed
464: Tamper Rdr Offline
463: Tamper Rdr R/F Jammed
462: Incomplete Card/PIN Sequence
461: Wireless Reader Key Override
460: Tamper - Wireless Rdr Motor
459: Tamper - Wireless Rdr R/F Loss
458: Tamper - Wireless Rdr Low Batt
457: Wireless Rdr Tamper Inactive
456: Wireless Rdr Tamper Active
455: Auto-Disabled Card
454: Biometric Verification Failed: No Device
453: Biometric Verification Failed: No Record
452: Biometric Verification Failed
451: Host denied access (Verification Viewer)

1439: Log Logcleared
1438: Authorization Fail Master
1437: Authorization Success Master
1436: Authorization Deny Commuser
1435: Authorization Success Commuser
1434: Access Keyoverride
1433: Access Granted Deadbolt Override
1432: Access Granted Notify
1431: Access Granted One Time User
1430: Access Granted Remoteunlock
1429: Access Denied Passage
1428: Access Denied Panic
1427: Access Denied Busy
1426: Access Denied Bolted
1425: Access Denied Lockout
1424: Access Denied
1423: User Ok
1422: User Invalid
1421: User Badtime
1420: User Add
1419: User Revoke
1418: User Modify
1417: Mode Panic End
1416: Mode Secured
1415: Mode Locked User
1414: Mode Locked Timed
1413: Mode Locked
1412: Mode Passage User
1411: Mode Passage Timed
1410: Mode Passage
1409: Mode Normal
1408: Mode Reset
1407: Mode Panic
1406: Mode Emergency
1405: Mode Relock
1404: Mode Lockout User
1403: Mode Lockout Timed
1402: Mode Lockout
1401: Mode Programming
1400: Proprietary
1256: Battery Check Error
1255: Battery Warn
1254: Battery Critical

450: Keypad Failure
449: Reader/Device Tamper
449: Control Unit Sabotage
448: Reader/Device Comm Fail
447: Building Close Fail- User
446: MSM Failure
445: VIP Tamper
444: VIP Tamper unshunt
443: VIP Tamper Shunt
442: Denied - ABA card expired
441: Denied - ABA Site Code
440: Sensor shunted
439: Coax shunted
438: Auto locked
437: Auto unlocked
436: Exit Denied
435: Exit Granted
434: Coax Failure
433: Sensor Fail
432: Building Close Fail- Key
431: Denied - Building not open
430: Invalid Card - Before Activation
429: Access denied - Use limit reached
428: Access denied - Area disabled
427: Access denied - Occupancy limit reached
426: Second not presented
425: Duress Detected - Access Denied
423: Attempt to open Locked Door
422: Invalid Reverse Card Read
421: Invalid Forward Card Read
420: Pincode Retry Exceeded
419: Antipassback error
418: Invalid threat level
417: Invalid IN-X-IT status
416: Invalid Timed override
415: Valid card with an incorrect issue level
414: Invalid Facility Code
413: Invalid PIN code has been entered
412: Invalid Reader Time Zone
411: Invalid Card Time Zone
410: Terminated Card Attempt
409: Deactivated Card Attempt
408: Unaccounted for Card Attempt

1253: Battery Replaced
1252: Battery Depleted
1251: Door Boltretracted
1250: Door Boltthrown
1244: Entry Out Of Seq
1243: Exit Out Of Seq
1242: Skip Step
1241: Full Comm Fail
1240: Partial Comm Fail
1239: Overall Route Early Alarm
1238: Trouble
1237: Overall Route Late Alarm
1236: Entry Late
1235: Exit Late
1234: Occupation Late
1233: Sequence Alarm
1232: Alarm
1231: Tour Step Early Alarm
1230: Tour Step Late Alarm
1229: Tamper
1228: Override Late
1227: Tour Step Reset
1226: Next
1225: Comm. Restore
1224: Reported
1223: Test Fail
1222: Test Pass
1221: Sensor Active
1220: Sensor Restore
1219: Secure
1218: Start Entry
1217: Start Exit
1216: Access
1215: Confirm Entry
1214: Confirm Exit
1213: Dismiss
1212: Competed
1211: Local Secure
1210: Route Reset
1209: Local Access
1208: Started
1207: Acknowledge
1206: Group Access

407: Stolen Card Attempt	1205: Group Secure
406: Lost Card Attempt	1204: Auto Secure
405: Valid card at an unauthorized reader	1203: Tag
404: Host denied access	1202: Trouble No More
403: Card Trace	1201: Command Fail
402: Expired Card Attempt	1200: Update
401: Void Card	Server connected
400: Unknown Card	Server connection lost

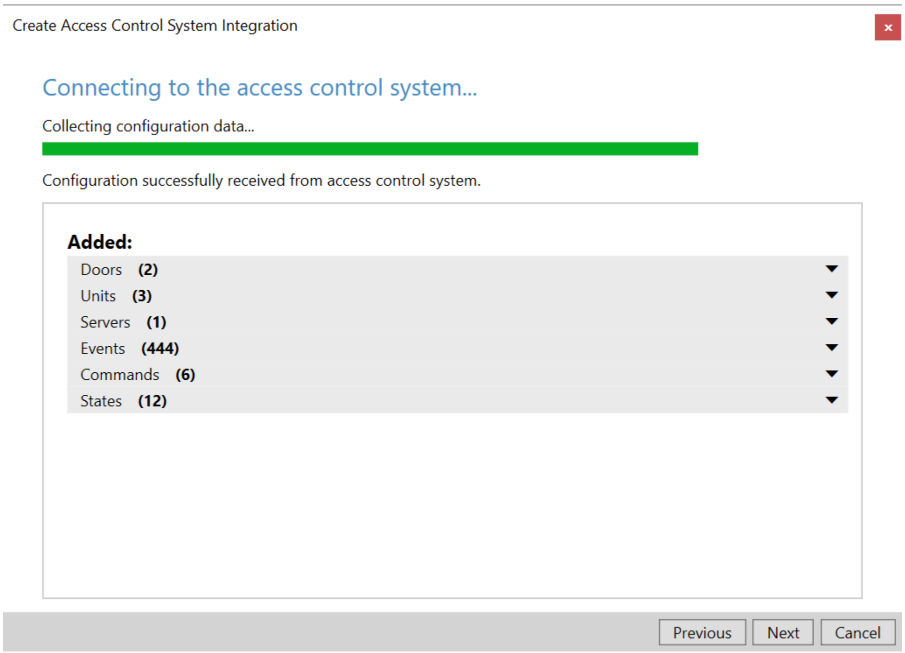
Commands (6): A list of supported actions (commands) for the doors added:

Lock
Unlock
Momentary Unlock
Mask
Unmask
TimeOverride

States (9): A list of supported states for the added doors and server:

Disconnected	Card Only
Connected	Pin Only
Unknown	Card and Pin
Locked	Card or Pin
Unlocked	Open
Facility Code Only	Closed

Example:



Create Access Control System Integration

Connecting to the access control system...

Collecting configuration data...

Configuration successfully received from access control system.

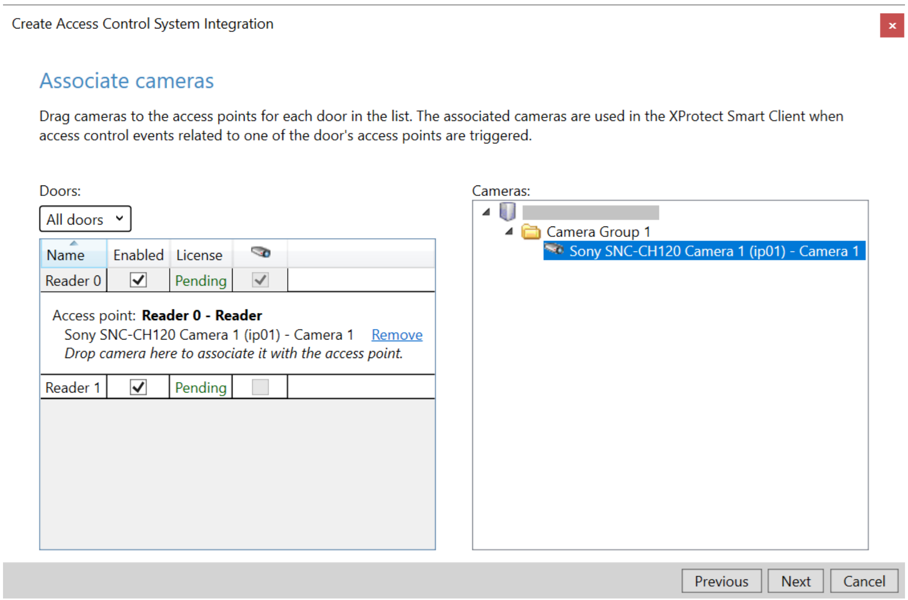
Added:

Doors **(2)**
Units **(3)**
Servers **(1)**
Events **(444)**
Commands **(6)**
States **(12)**

Click **Next**.

5. (Optional) Drag and drop cameras to the door access points for each door in the list. The associated cameras are used in XProtect Smart Client when access control events related to each door are triggered.

   In this example, **Sony SNC-CH120 Camera 1 (ip01) – Camera 1** is associated to **Reader 0 – Reader**.



Create Access Control System Integration

Associate cameras

Drag cameras to the access points for each door in the list. The associated cameras are used in the XProtect Smart Client when access control events related to one of the door's access points are triggered.

Doors: All doors

Name	Enabled	License	
Reader 0	☑	Pending	☑
Reader 1	☑	Pending	□

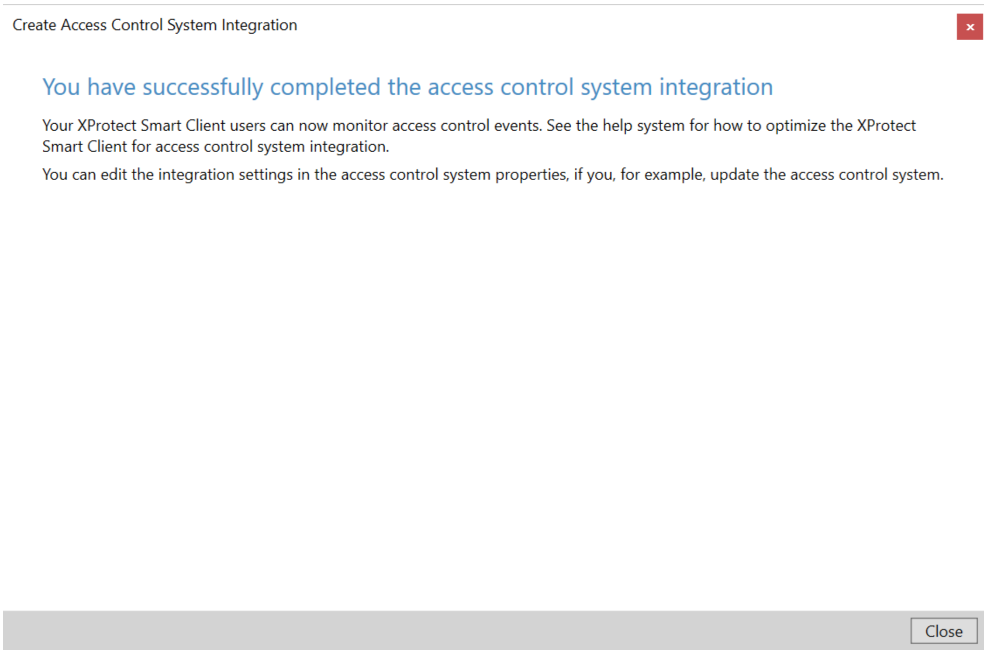
Access point: **Reader 0 - Reader**
Sony SNC-CH120 Camera 1 (ip01) - Camera 1 Remove
Drop camera here to associate it with the access point.

Cameras:
Camera Group 1
Sony SNC-CH120 Camera 1 (ip01) - Camera 1

Click **Next**.

6. The configuration of the access control system integration is saved successfully to the server. Click **Close**.

   Example:



Create Access Control System Integration

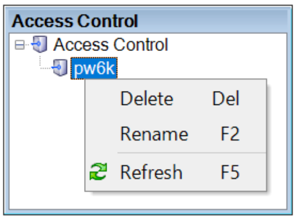
You have successfully completed the access control system integration

Your XProtect Smart Client users can now monitor access control events. See the help system for how to optimize the XProtect Smart Client for access control system integration.

You can edit the integration settings in the access control system properties, if you, for example, update the access control system.

Remove ProWatch Access Control

1. Open XProtect Management Client > **Site Navigation** > **Access Control**.
2. Right click on the access control and select **Delete** or press the **Del** button on the keyboard.

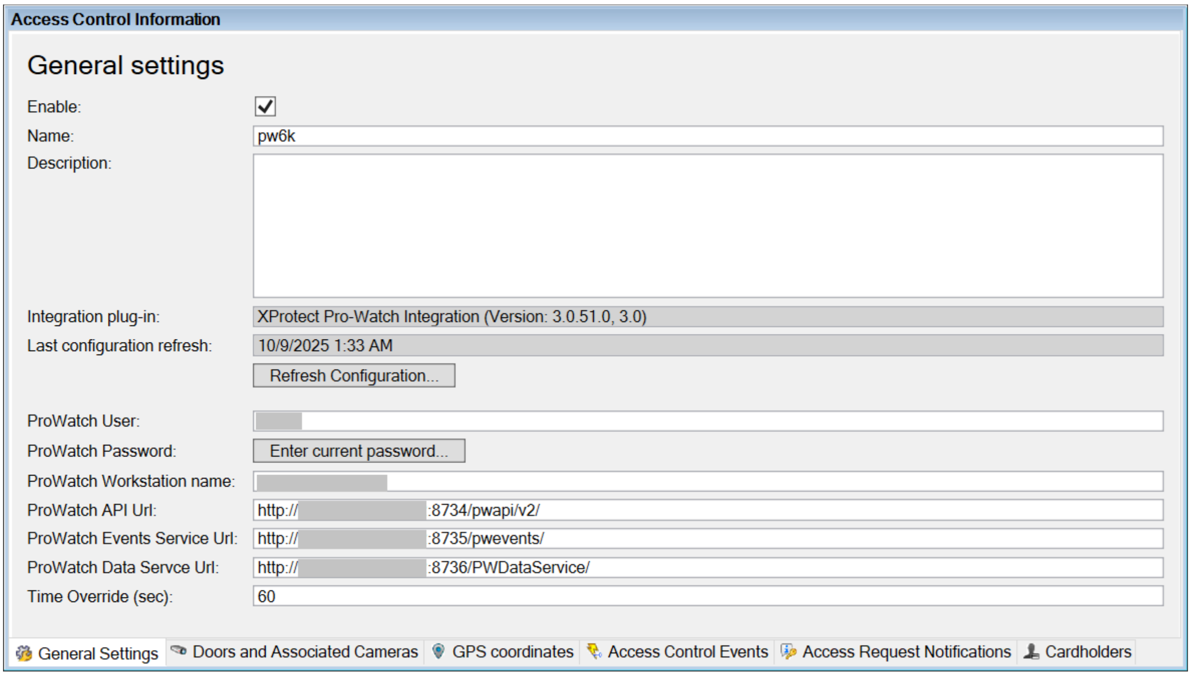


ProWatch Access Control Properties

Note: See Milestone XProtect (XProtect Management Client) help for detailed **Access Control** properties.

General Settings

Example:



Access Control Information

General settings

Enable: ☑

Name: pw6k

Description:

Integration plug-in: XProtect Pro-Watch Integration (Version: 3.0.51.0, 3.0)

Last configuration refresh: 10/9/2025 1:33 AM

ProWatch User: [redacted]

ProWatch Password:

ProWatch Workstation name: [redacted]

ProWatch API Url: http://[redacted]:8734/pwapi/v2/

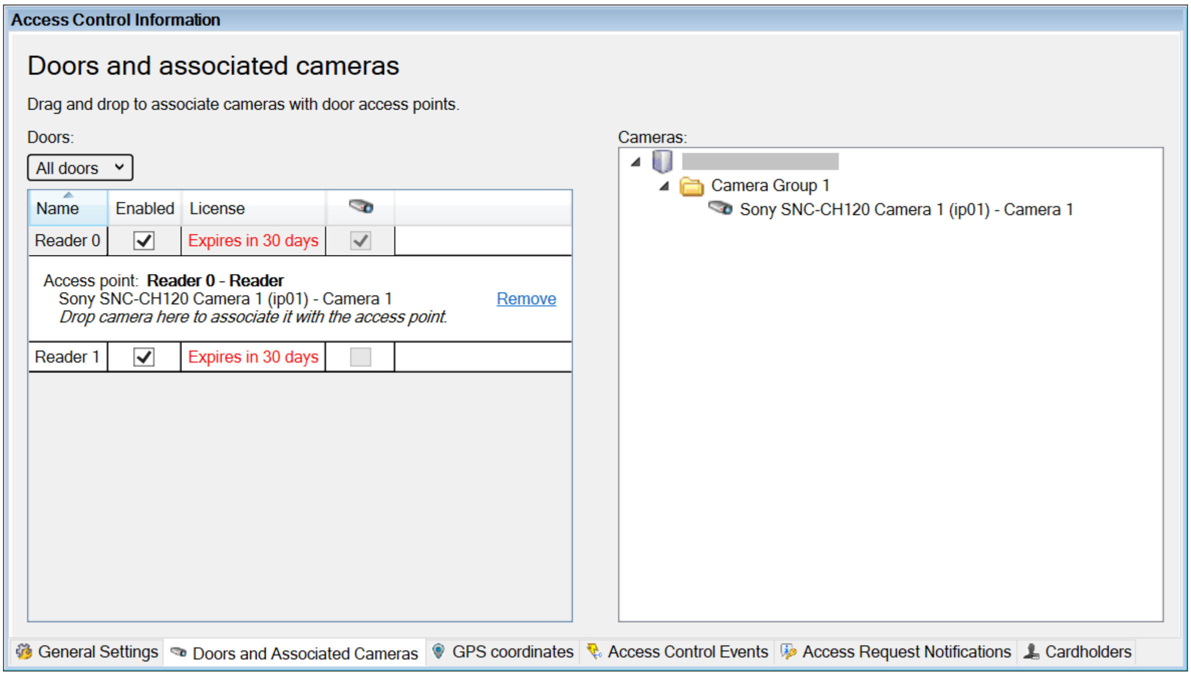
ProWatch Events Service Url: http://[redacted]:8735/pwevents/

ProWatch Data Serve Url: http://[redacted]:8736/PWDataService/

Time Override (sec): 60

Doors and Associated Cameras

Example:



Access Control Information

Doors and associated cameras

Drag and drop to associate cameras with door access points.

Doors: All doors

Name	Enabled	License	
Reader 0	☑	Expires in 30 days	☑
Reader 1	☑	Expires in 30 days	□

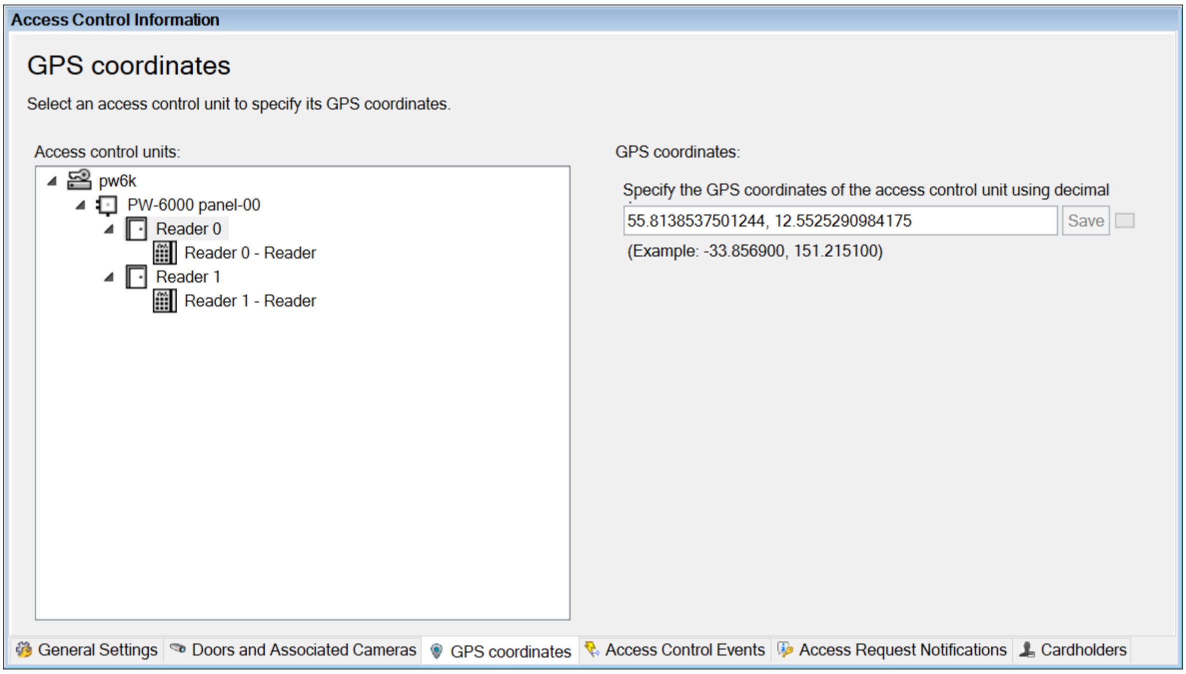
Access point: **Reader 0 - Reader**
Sony SNC-CH120 Camera 1 (ip01) - Camera 1 Remove
Drop camera here to associate it with the access point.

Cameras:
[redacted]
Camera Group 1
Sony SNC-CH120 Camera 1 (ip01) - Camera 1

GPS coordinates

Note: The coordinates must be entered manually (as they are not automatically updated from the API) and will be working only on the Smart Map feature in XProtect Smart Client.

Example:



Access Control Information

GPS coordinates

Select an access control unit to specify its GPS coordinates.

Access control units:

- pw6k
  - PW-6000 panel-00
    - Reader 0
      - Reader 0 - Reader
    - Reader 1
      - Reader 1 - Reader

GPS coordinates:

Specify the GPS coordinates of the access control unit using decimal

55.8138537501244, 12.5525290984175

(Example: -33.856900, 151.215100)

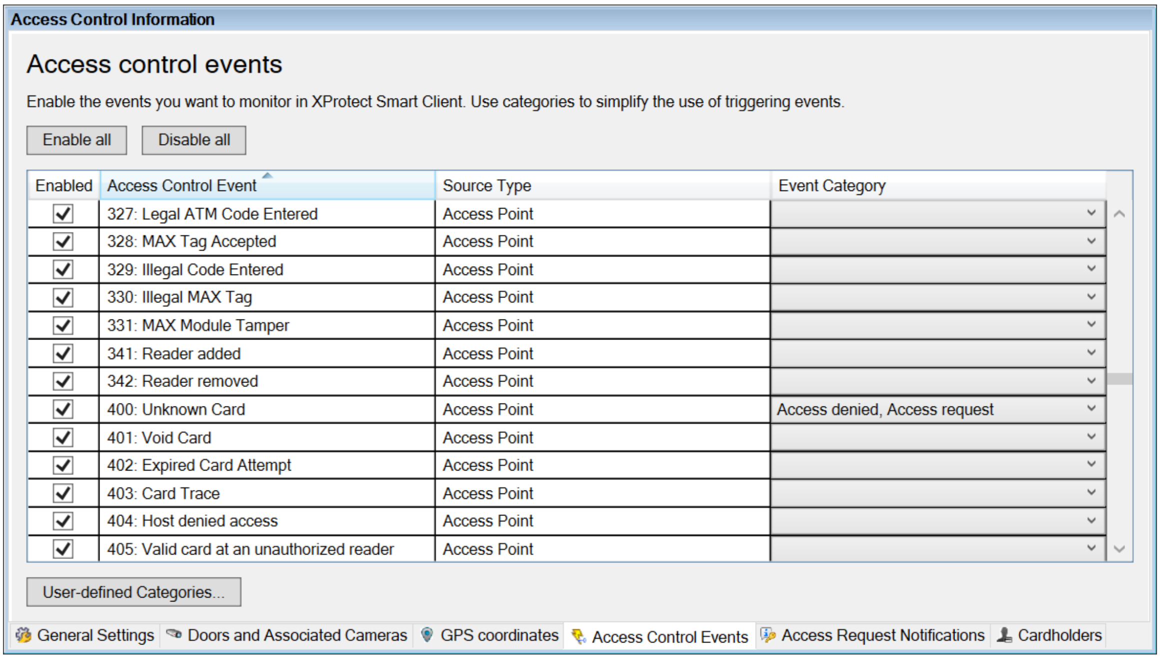
Access Control Events

All listed events are enabled, but currently only one is assigned to an **Event Category** by default:

Access Control Event	Source Type	Event Category
Server connection lost	ProWatch Server	Error

Access denied and **Access request** are assigned to **400: Unknown Card** in this example as this access control event will be used in chapters Alarms based on Pro-Watch Access Control events and Access request notifications.

Example:



Access Control Information

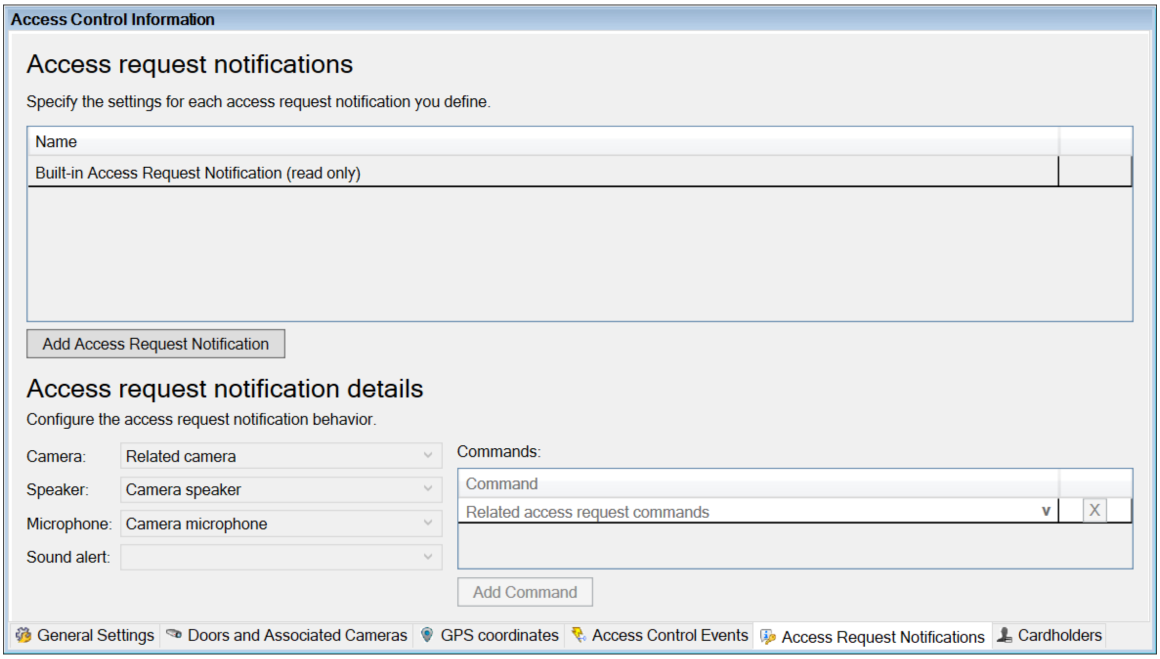
Access control events

Enable the events you want to monitor in XProtect Smart Client. Use categories to simplify the use of triggering events.

Enabled	Access Control Event	Source Type	Event Category
☑	327: Legal ATM Code Entered	Access Point	
☑	328: MAX Tag Accepted	Access Point	
☑	329: Illegal Code Entered	Access Point	
☑	330: Illegal MAX Tag	Access Point	
☑	331: MAX Module Tamper	Access Point	
☑	341: Reader added	Access Point	
☑	342: Reader removed	Access Point	
☑	400: Unknown Card	Access Point	Access denied, Access request
☑	401: Void Card	Access Point	
☑	402: Expired Card Attempt	Access Point	
☑	403: Card Trace	Access Point	
☑	404: Host denied access	Access Point	
☑	405: Valid card at an unauthorized reader	Access Point	

Access Request Notifications

Example:



Access Control Information

Access request notifications

Specify the settings for each access request notification you define.

Name
Built-in Access Request Notification (read only)

Access request notification details

Configure the access request notification behavior.

Camera: Related camera

Speaker: Camera speaker

Microphone: Camera microphone

Sound alert:

Commands:

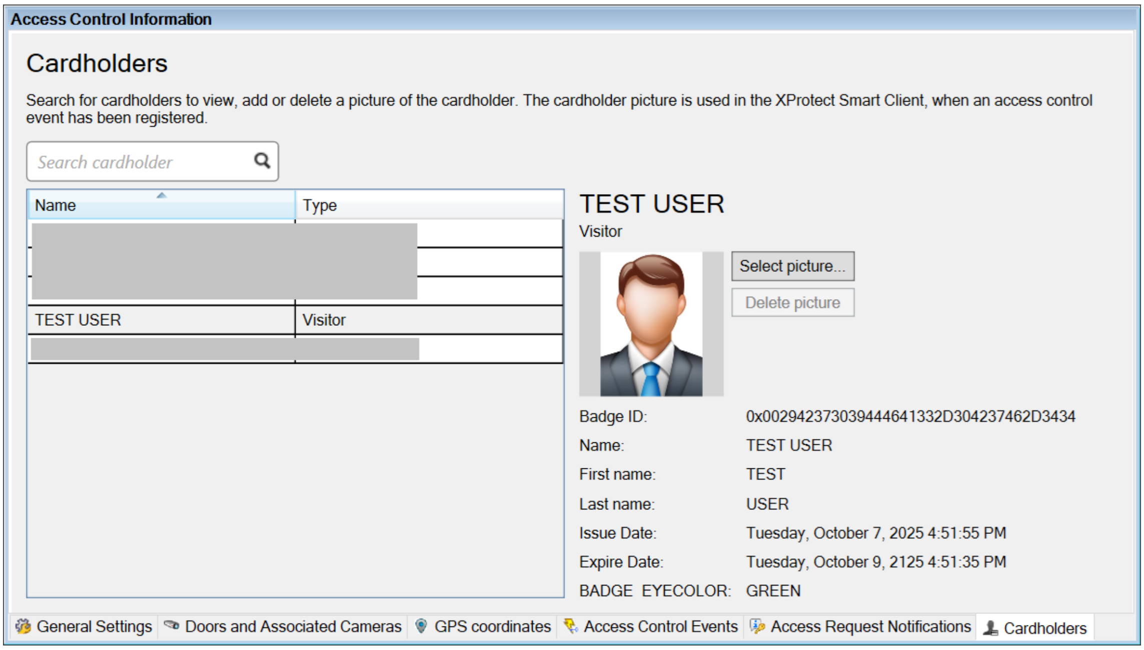
Command
Related access request commands

Add Access Request Notification
Add Command
General Settings
Doors and Associated Cameras
GPS coordinates
Access Control Events
Access Request Notifications
Cardholders

Cardholders

Badge Holders from the ProWatch system are transferred into the XProtect system, including some basic information and the picture.

The information for the **Test User** is shown in the example below.



Access Control Information

Cardholders

Search for cardholders to view, add or delete a picture of the cardholder. The cardholder picture is used in the XProtect Smart Client, when an access control event has been registered.

Search cardholder

Name	Type
[redacted]	[redacted]
[redacted]	[redacted]
TEST USER	Visitor
[redacted]	[redacted]

TEST USER
Visitor

Select picture...
Delete picture

Badge ID:	0x002942373039444641332D304237462D3434
Name:	TEST USER
First name:	TEST
Last name:	USER
Issue Date:	Tuesday, October 7, 2025 4:51:55 PM
Expire Date:	Tuesday, October 9, 2125 4:51:35 PM
BADGE EYECOLOR:	GREEN

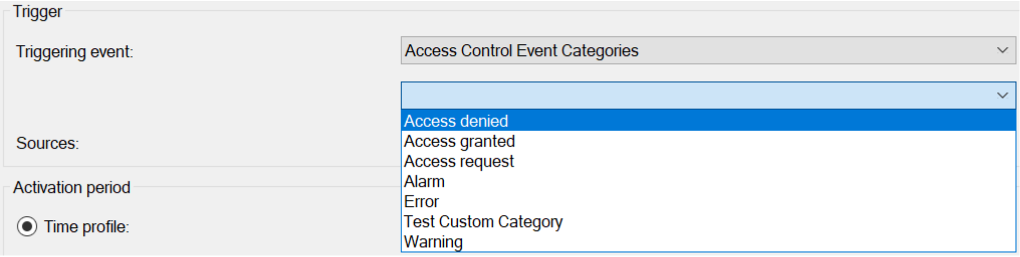
Alarms based on Pro-Watch Access Control events

1. Open XProtect Management Client > **Site Navigation** > **Alarms** > **Alarm Definitions**.
2. In the **Alarm Definitions** panel right click the **Alarm Definitions** node and select **Add New...**.

> **Note**: For detailed descriptions on how to configure **Alarm Definitions**, see the Milestone XProtect (XProtect Management Client) help.

3. On the **Alarm Definition Information** page, locate the group of settings called **Trigger**.
4. Specify the **Triggering event** by selecting from the top dropdown list the **Access Control Event Categories** event group, and from the next dropdown list, select the appropriate **Event Category**. The default **Event Categories** as well as the **User-defined Categories** are listed here.

Example:



Trigger

Triggering event: Access Control Event Categories

Sources:

Activation period

● Time profile:

Access denied
Access granted
Access request
Alarm
Error
Test Custom Category
Warning

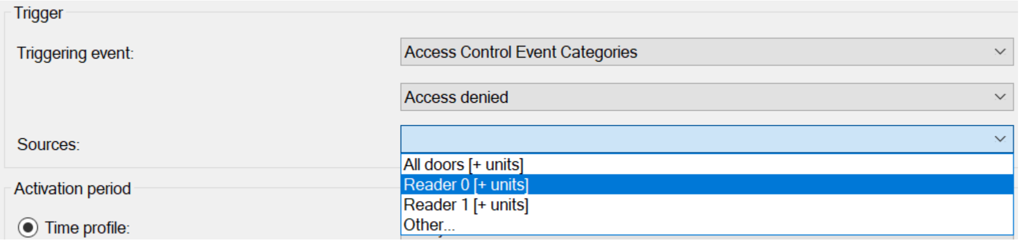
In the example below, **Access denied** is selected.

5. From the **Sources** dropdown list, select a proper source depending on the required configuration. The default options are:

Option	**Description**
All doors [+ units]	This option selects all added doors as a source for triggering the alarm.
Reader 0 [+ units]	This option selects only **Reader 0** as a source.
Reader 1 [+ units]	This option selects only **Reader 1** as a source.
Other…	This option opens the **Select Sources** dialog. The following three options are available: • **Access Control Servers** - This option lists all added access control systems and related access control units. • **All Access Control Servers** - This option selects all added access control servers as sources. • **All Access Control Units** - This option selects all added access control units as sources. • **Current XProtect server** - This option is currently not supported.

Select a proper source(s). Click **OK** when the selection is done.

Example:



Trigger

Triggering event: Access Control Event Categories

Access denied

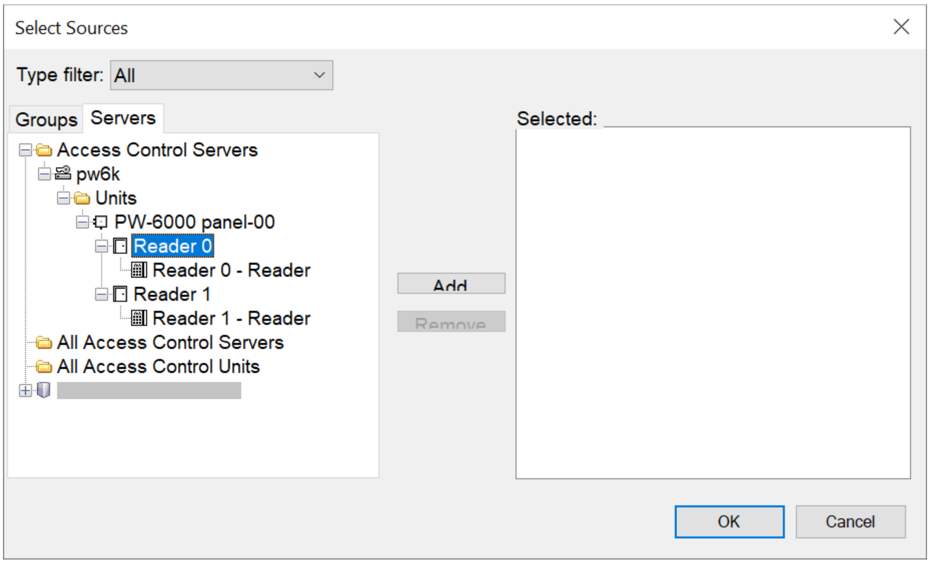
Sources:

All doors [+ units]
Reader 0 [+ units]
Reader 1 [+ units]
Other...

Activation period

● Time profile:

The **Other...** option



Select Sources

Type filter: All

Groups | Servers

- Access Control Servers
  - pw6k
    - Units
      - PW-6000 panel-00
        - Reader 0
          - Reader 0 - Reader
        - Reader 1
          - Reader 1 - Reader
  - All Access Control Servers
  - All Access Control Units

Selected:

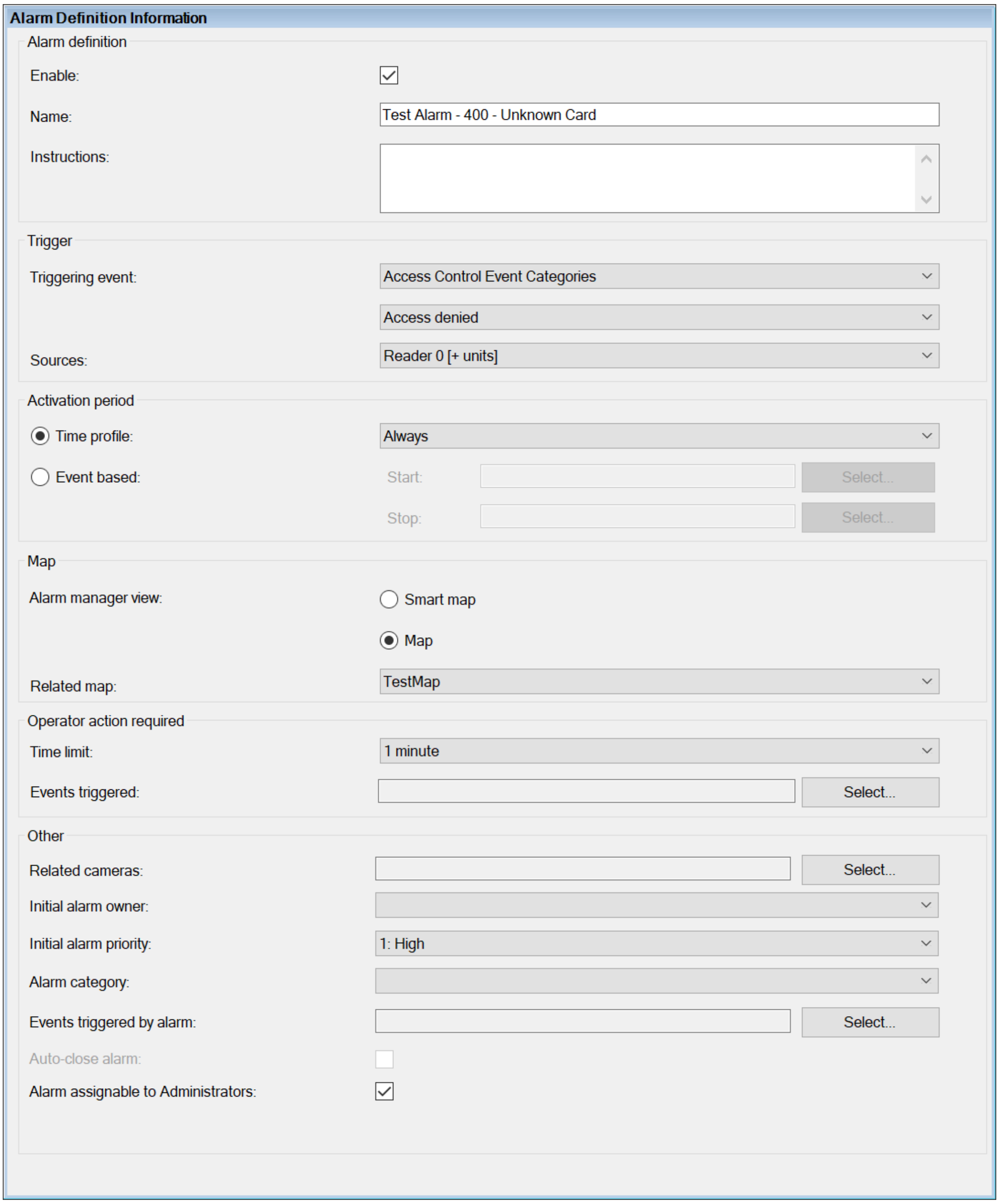
Reader 0 [+ units] from the initial listings is selected in the example above. Click **OK**.

6. (Optional) Specify a map by selecting it from the **Map** group of settings > **Alarm manager view** > **Map**.

Note: In order a map to be available for selection, it needs to be loaded in XProtect Smart Client as explained in XProtect Smart Client configuration > Add Pro-Watch system units on the map.

7. Click **Save** in the toolbar to save the alarm.

Example:



Alarm Definition Information

Alarm definition

Enable: ☑

Name: Test Alarm - 400 - Unknown Card

Instructions:

Trigger

Triggering event: Access Control Event Categories

Access denied

Sources: Reader 0 [+ units]

Activation period

● Time profile: Always

○ Event based: Start: Select... Stop: Select...

Map

Alarm manager view: ○ Smart map ● Map

Related map: TestMap

Operator action required

Time limit: 1 minute

Events triggered: Select...

Other

Related cameras: Select...

Initial alarm owner:

Initial alarm priority: 1: High

Alarm category:

Events triggered by alarm: Select...

Auto-close alarm: □

Alarm assignable to Administrators: ☑

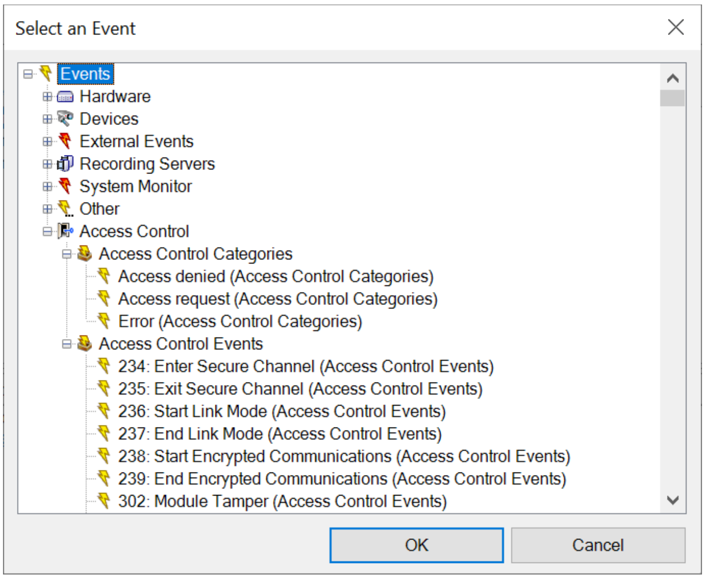
Rules based on ProWatch Access Control events

1. Open XProtect Management Client > **Site Navigation** > **Rules and Events** > **Rules**.
2. In the **Rules** panel, right click on the **Rules** node and select **Add Rule...**.

> **Note**: For detailed description on how to configure **Rules**, see the Milestone XProtect (XProtect Management Client) help.

3. In **Step 1: Type of rule section**, select **Perform an action on <event>**.
4. In the **Edit the rule description section (click an underlined item)**, click **event**.
5. In the **Select an Event** dialog box, expand **Access Control**. The following options are available - **Access Control Categories** and **Access Control Events**:

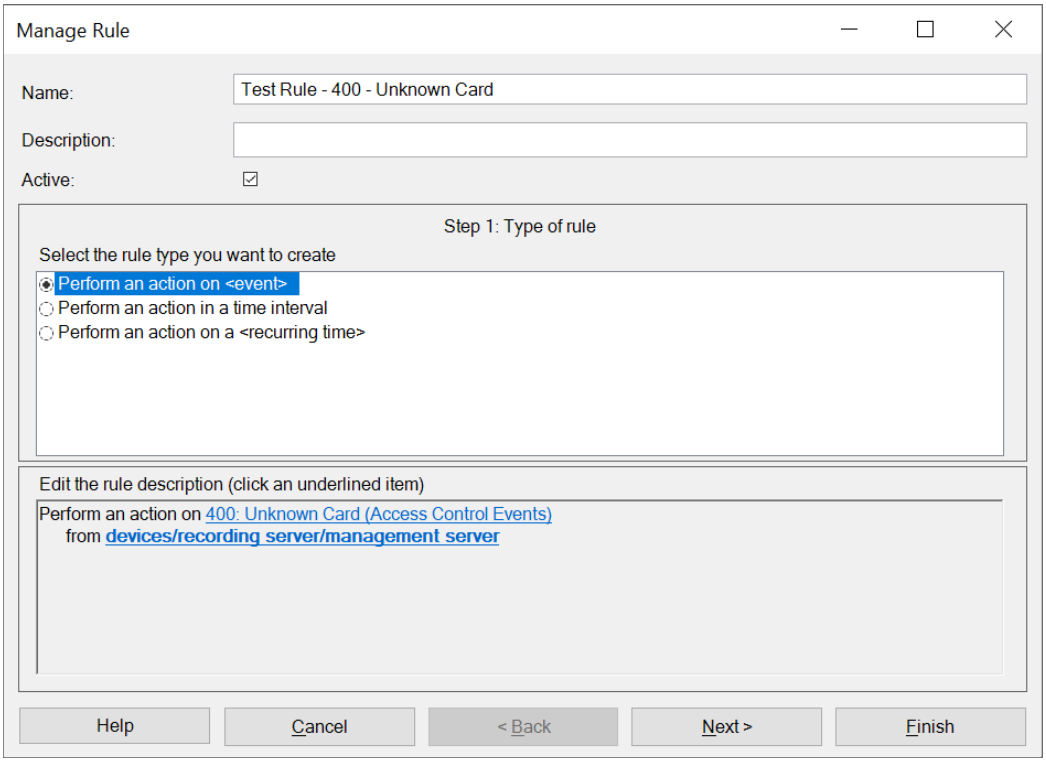
Example:



Select an Event

- Events
  - Hardware
  - Devices
  - External Events
  - Recording Servers
  - System Monitor
  - Other
  - Access Control
    - Access Control Categories
      - Access denied (Access Control Categories)
      - Access request (Access Control Categories)
      - Error (Access Control Categories)
    - Access Control Events
      - 234: Enter Secure Channel (Access Control Events)
      - 235: Exit Secure Channel (Access Control Events)
      - 236: Start Link Mode (Access Control Events)
      - 237: End Link Mode (Access Control Events)
      - 238: Start Encrypted Communications (Access Control Events)
      - 239: End Encrypted Communications (Access Control Events)
      - 302: Module Tamper (Access Control Events)

400: Unknown Card (Access Control Events) is selected in the example above. Click **OK**.



Manage Rule

Name: Test Rule - 400 - Unknown Card

Description:

Active: ☑

Step 1: Type of rule

Select the rule type you want to create

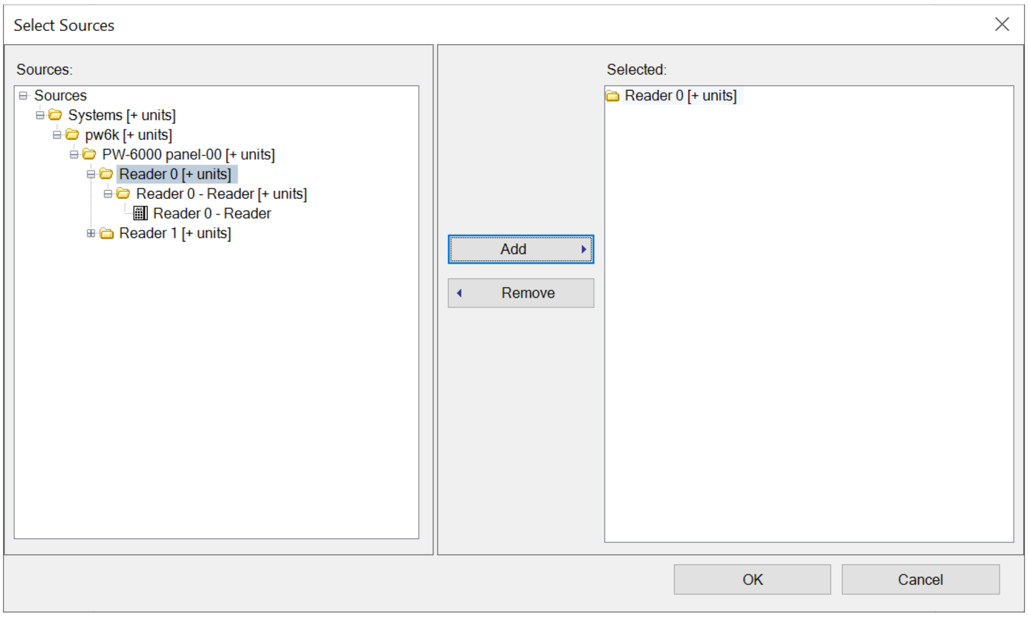
● Perform an action on <event>
○ Perform an action in a time interval
○ Perform an action on a <recurring time>

Edit the rule description (click an underlined item)

Perform an action on 400: Unknown Card (Access Control Events)
from **devices/recording server/management server**

6. In the **Edit the rule description section (click an underlined item)**, click **devices/recording server/management server**.
7. In the **Select Sources** dialog box, select **Systems [+ units]** or expand it, and select devices as per your requirements. Click **OK**.

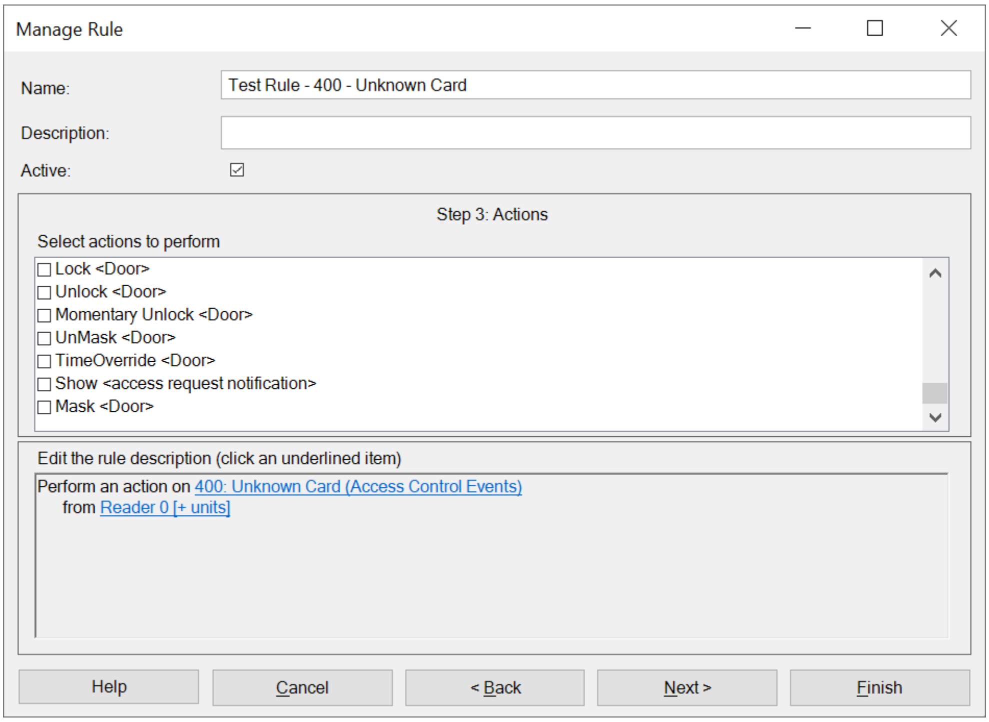
   Reader 0 [+ units] is selected in the example below. Click **OK**.



8. In **Step 2: Conditions**, select conditions if those are required and click **Next**.
9. In **Step 3: Actions**, following actions are added based on the integration (These actions were added when Pro-Watch Access Control is added to XProtect):

   Lock <Door>
   Unlock <Door>
   Momentary Unlock <Door>
   Unmask <Door>
   TimeOveride <Door>
   Mask <Door>

Example:



Name: Test Rule - 400 - Unknown Card

Description:

Active: ☑

Step 3: Actions

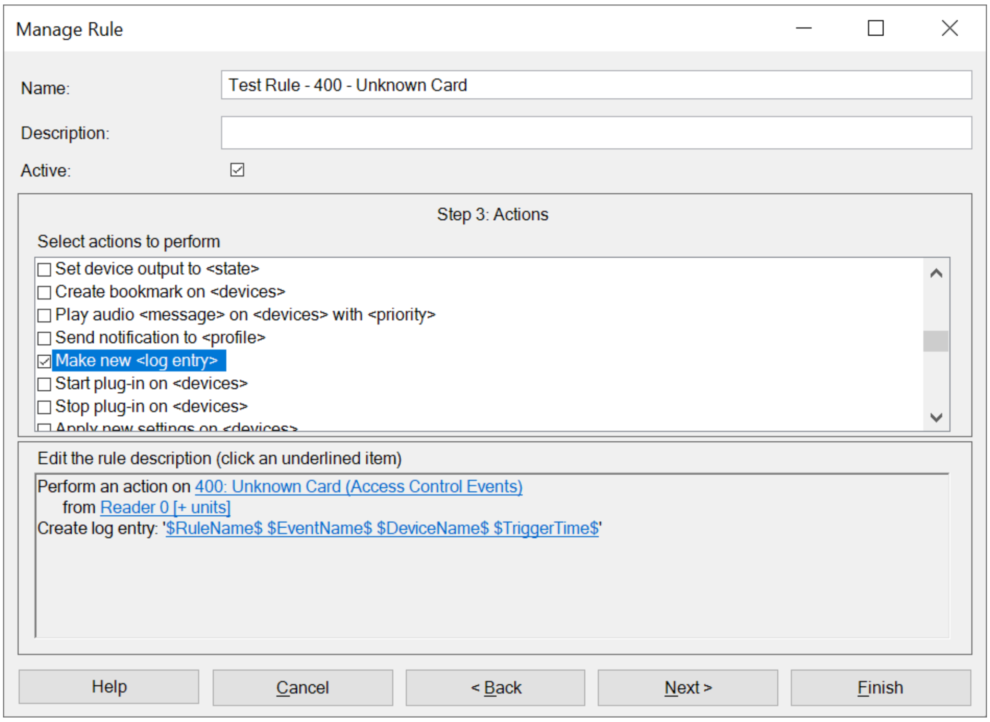
Select actions to perform

- □ Lock <Door>
- □ Unlock <Door>
- □ Momentary Unlock <Door>
- □ UnMask <Door>
- □ TimeOverride <Door>
- □ Show <access request notification>
- □ Mask <Door>

Edit the rule description (click an underlined item)

Perform an action on 400: Unknown Card (Access Control Events)
from Reader 0 [+ units]

In the example below one of the default XProtect actions is selected – **Make new <log entry>** with variables **$RuleName$ $EventName$ $DeviceName $TriggerTime$**. In this way, a new log entry is created in the **Rule-triggered logs** when the event is triggered.



Name: Test Rule - 400 - Unknown Card

Description:

Active: ☑

Step 3: Actions

Select actions to perform

- □ Set device output to <state>
- □ Create bookmark on <devices>
- □ Play audio <message> on <devices> with <priority>
- □ Send notification to <profile>
- ☑ Make new <log entry>
- □ Start plug-in on <devices>
- □ Stop plug-in on <devices>
- □ Apply new settings on <devices>

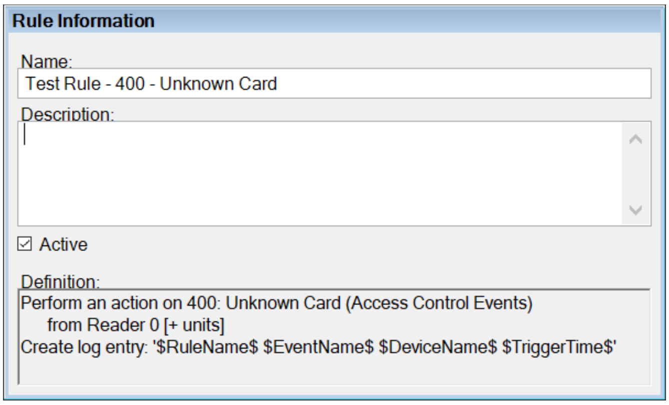
Edit the rule description (click an underlined item)

Perform an action on 400: Unknown Card (Access Control Events)
from Reader 0 [+ units]
Create log entry: '$RuleName$ $EventName$ $DeviceName$ $TriggerTime$'

10. In **Step 4:** Select **Stop criteria**, if needed, and click **Next**.
    Stop criteria is not selected in the example.

11. Click **Finish**.

    Example:



Rule Information

Name:
Test Rule - 400 - Unknown Card

Description:

☑ Active

Definition:
Perform an action on 400: Unknown Card (Access Control Events)
from Reader 0 [+ units]
Create log entry: '$RuleName$ $EventName$ $DeviceName$ $TriggerTime$'

Access rights for Pro-Watch Access Control based on Roles

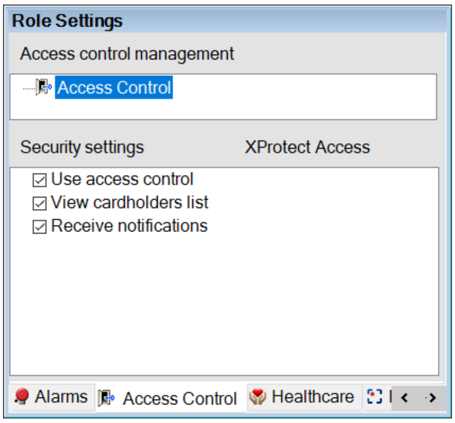
1. Open XProtect Management Client > **Site Navigation** > **Security** > **Roles**.
2. Click on a specific role and navigate to **Role Settings** > **Access Control** tab.

> **Note**: For detailed description on how to configure **Roles**, see the Milestone XProtect (XProtect Smart Client) help.

3. Select the **Access Control** from the **Access control management** section and mark any option in the **Security settings** section based on the requirements:

Security setting	Description
Use access control	The role (and its users) is allowed to use the Pro-Watch Access Control.
View cardholders list	The role (and its users) is allowed to see the Pro-Watch Access Control cardholders.
Receive notifications	The role (and its users) is allowed to receive Pro-Watch Access Control notifications in the XProtect Smart Client.

Example:



Role Settings

Access control management

Access Control

Security settings XProtect Access

☑ Use access control
☑ View cardholders list
☑ Receive notifications

XProtect Smart Client configuration

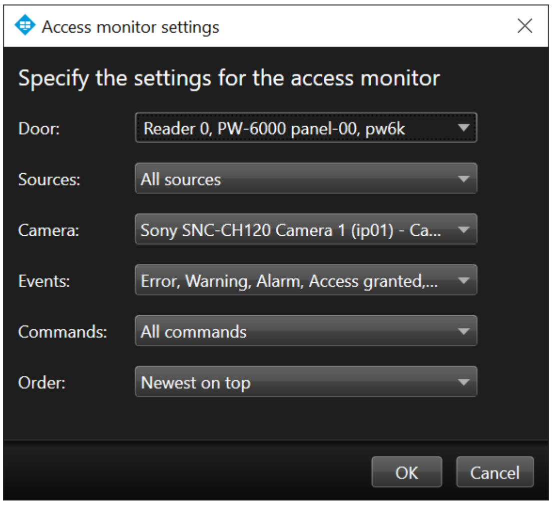
Add Pro-Watch Access monitor

1. Open XProtect Smart Client > **Live** tab.
2. In the upper-right corner, click **Setup**.
3. Add a **Group** and a **View**.

> **Note**: For detailed description on how to configure **Access monitor**, see the Milestone XProtect (XProtect Smart Client) help.

4. In the **System overview** pane, click **Access monitor** and drag it to the view.
5. In the **Access monitor settings** dialog box, specify the settings based on the requirements.

   In the example below, **Reader 0** is selected and all other settings are set by default. Click **OK**.



Access monitor settings

Specify the settings for the access monitor

Door: Reader 0, PW-6000 panel-00, pw6k

Sources: All sources

Camera: Sony SNC-CH120 Camera 1 (ip01) - Ca...

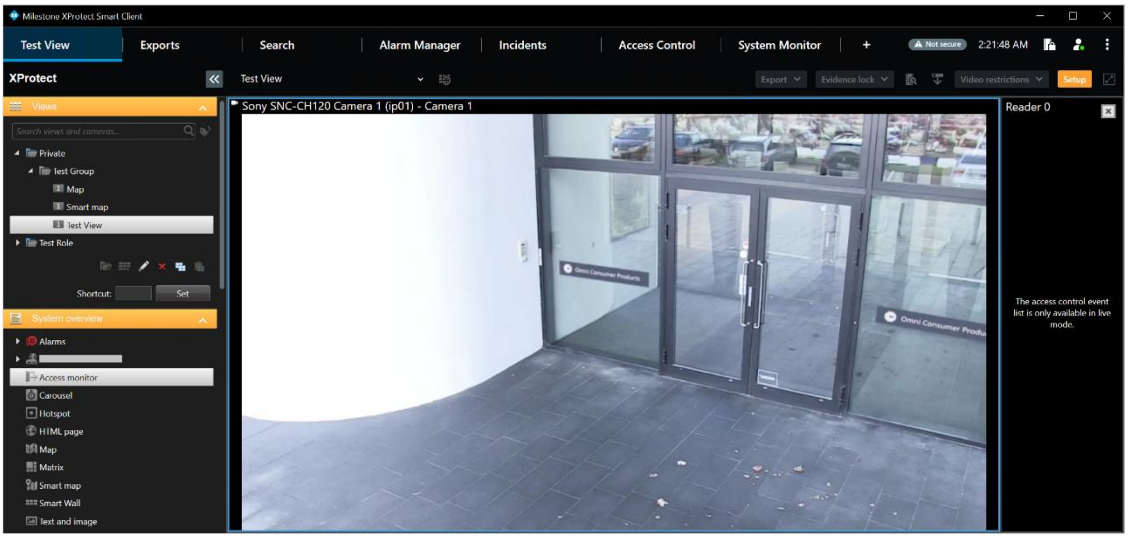
Events: Error, Warning, Alarm, Access granted,...

Commands: All commands

Order: Newest on top

6. The **Access monitor** with the given configuration will be added to the view. If an access control event is triggered, it appears on the right side of the view. Check subchapter [XProtect Smart Client operation > Live]() to see how it looks when an event is triggered.

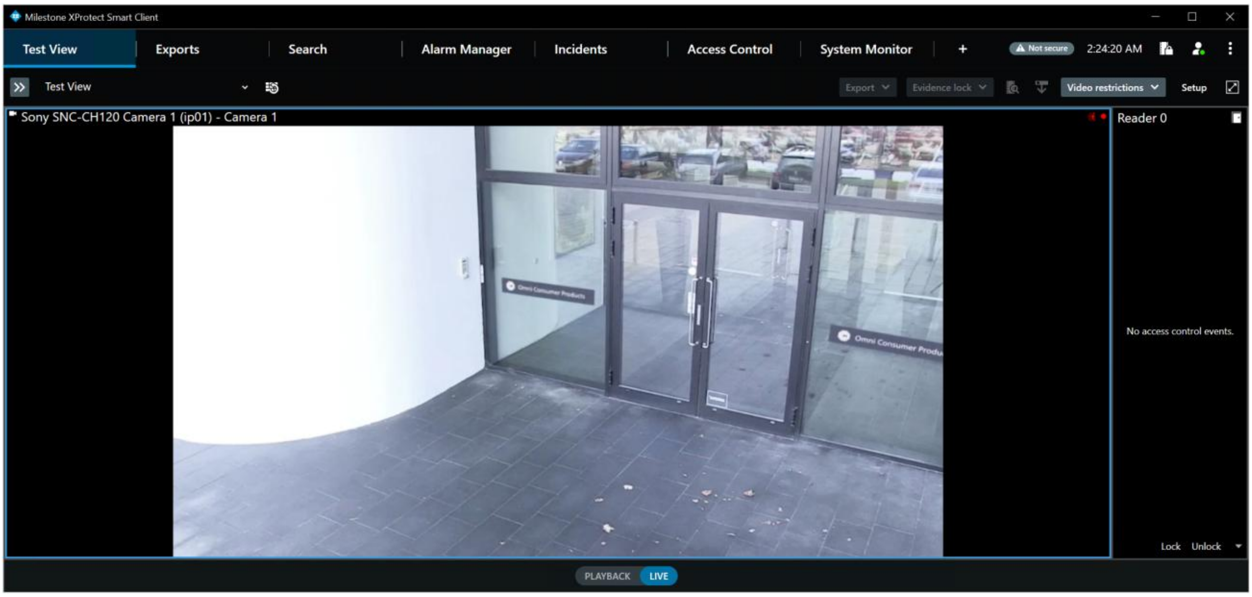
   Example:



The access control event list is only available in live mode.

7. Click **Setup** to complete the configuration.

Example:



No access control events.

Add Pro-Watch Overlay buttons

1. Open XProtect Smart Client > **Live** tab.
2. Click **Setup** in the upper-right corner.

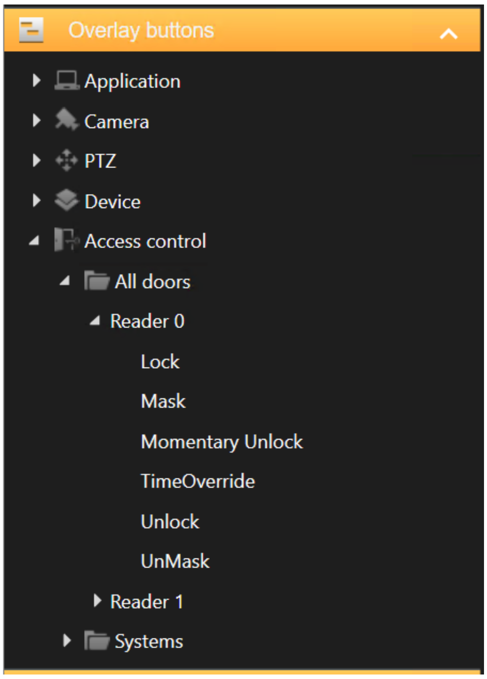
3. Add a **Group** and a **View**.
4. Add a **Camera** or **Access monitor**.

Note: For detailed description on how to configure **Overlay buttons**, see the Milestone XProtect (XProtect Smart Client) help.

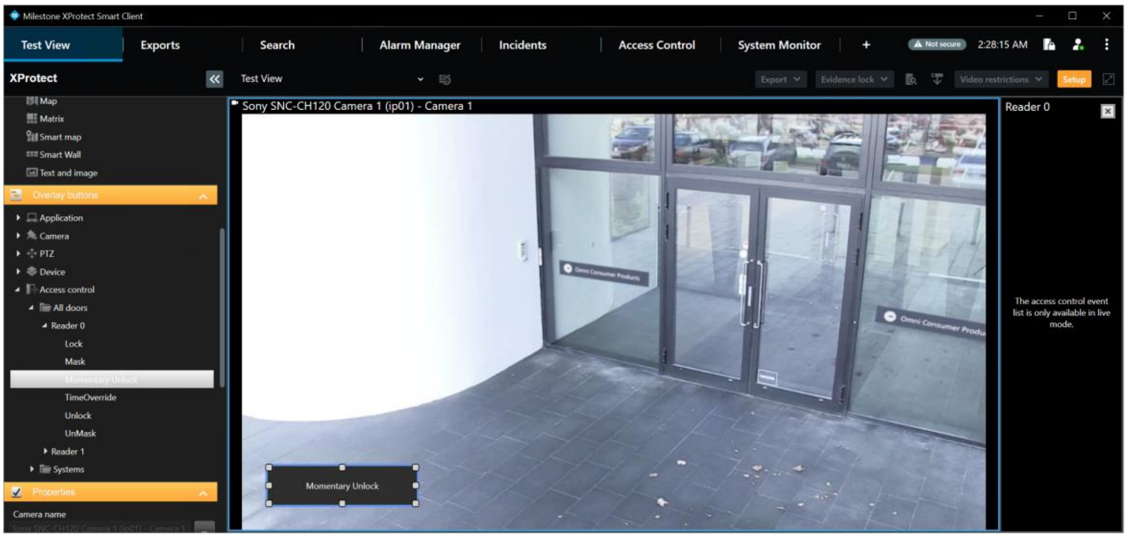
In the **Overlay buttons** panel, select and drag the action (command) in the view item. The following actions related to Pro-Watch doors are available:

Unit	Actions
Reader 0	Lock, Mask, Momentary Unlock, TimeOverride, Unlock, Unmask

Example:



The **Momentary Unlock** action for **Reader 0** is added to the **Access monitor** in the example below.



5. Click **Setup** to complete the configuration.

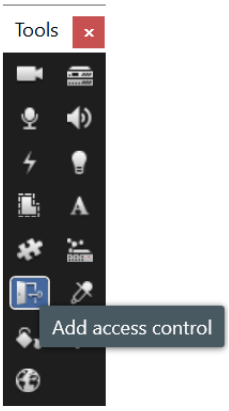
Add Pro-Watch system units on the map

The Pro-Watch system units integrate with the map features of XProtect Smart Client, and a visual representation of the units can be done using this feature:

1. Open XProtect Smart Client > **Live** tab.
2. Click **Setup** in the upper-right corner.
3. Add a **Group** and a **View**.
4. Add a map.

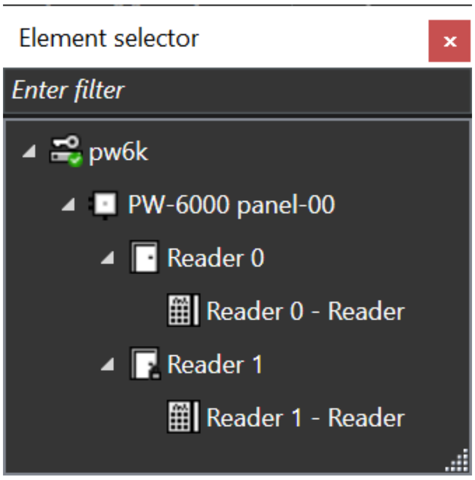
> **Note**: For detailed description on how to configure **Maps**, see the Milestone XProtect (XProtect Smart Client) help.

5. Click **Add access control** in the **Tools** dialog box.



6. In the **Element selector** dialog box, expand the Pro-Watch access control node. Drag and drop an element from the list to the map depending on the required configuration.

Example:

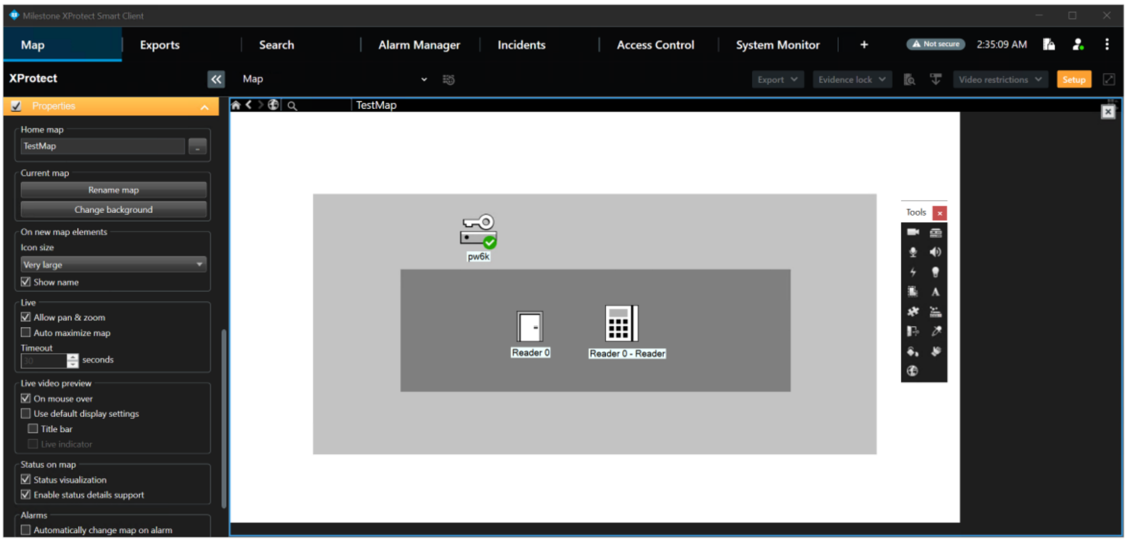


Element selector

Enter filter

- pw6k
  - PW-6000 panel-00
    - Reader 0
      - Reader 0 - Reader
    - Reader 1
      - Reader 1 - Reader

Reader 0 and **Reader 0 – Reader** are added in the example below.



Properties

Home map: TestMap

Current map: Rename map | Change background

On new map elements
Icon size: Very large
☑ Show name

Live
☑ Allow pan & zoom
☐ Auto maximize map
Timeout: 30 seconds

Live video preview
☑ On mouse over
☐ Use default display settings
☐ Title bar
☐ Live indicator

Status on map
☑ Status visualization
☑ Enable status details support

Alarms
☐ Automatically change map on alarm

7. Close the **Element selector** dialog box when you finish adding the elements.
8. Click **Setup** in the upper-right corner to complete the map configuration.

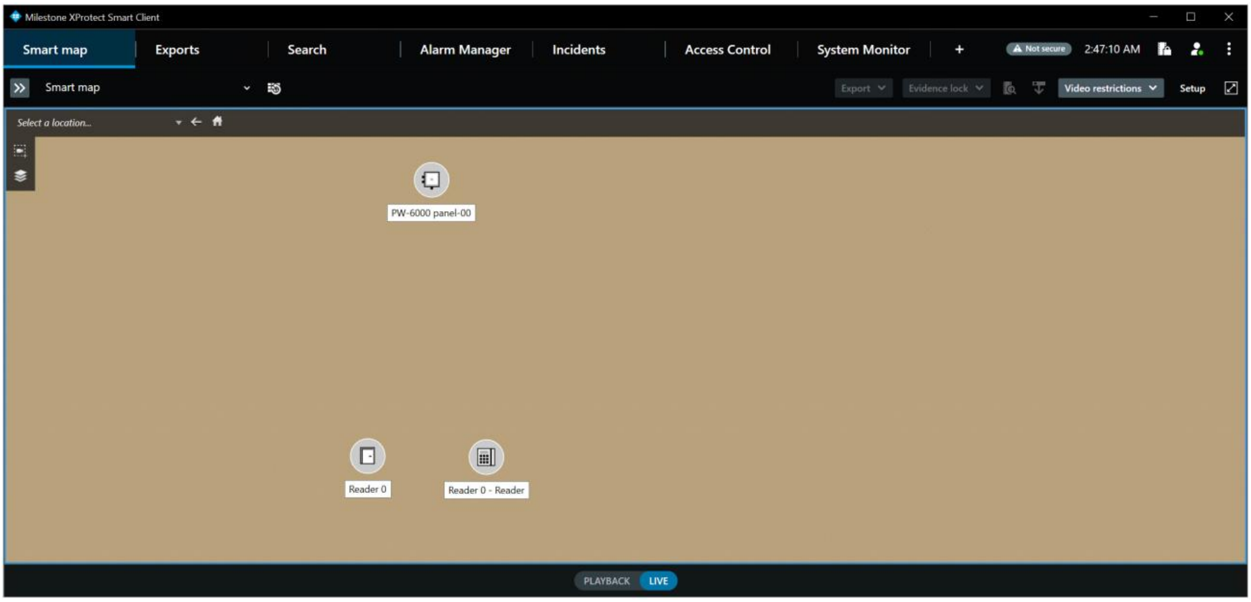
Add Pro-Watch system units on the Smart Map

The Pro-Watch system units integrate with the map features of XProtect Smart Client, and a visual representation of the units can be done using this feature:

1. Open XProtect Smart Client > **Live** tab.
2. Click **Setup** in the upper-right corner.
3. Add a **Group** and a **View**.
4. Add a **Smart map**.

Note: For detailed description on how to configure **Smart Maps**, see the Milestone XProtect (XProtect Smart Client) help.

The Pro-Watch system units are automatically available on the Smart map (based on the configuration made in chapter Pro-Watch Access Control Properties > GPS coordinates.

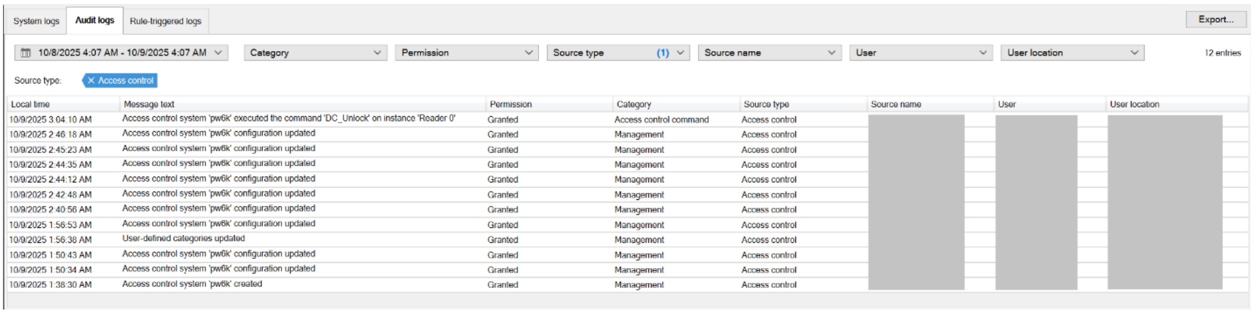


XProtect Management Client operation

Audit logs

Open XProtect Management Client > **Site Navigation** > **Server Logs** > **Audit logs**. The **Audit logs** contain information about the commands that each user performs over the doors using XProtect Smart Client.

Example:



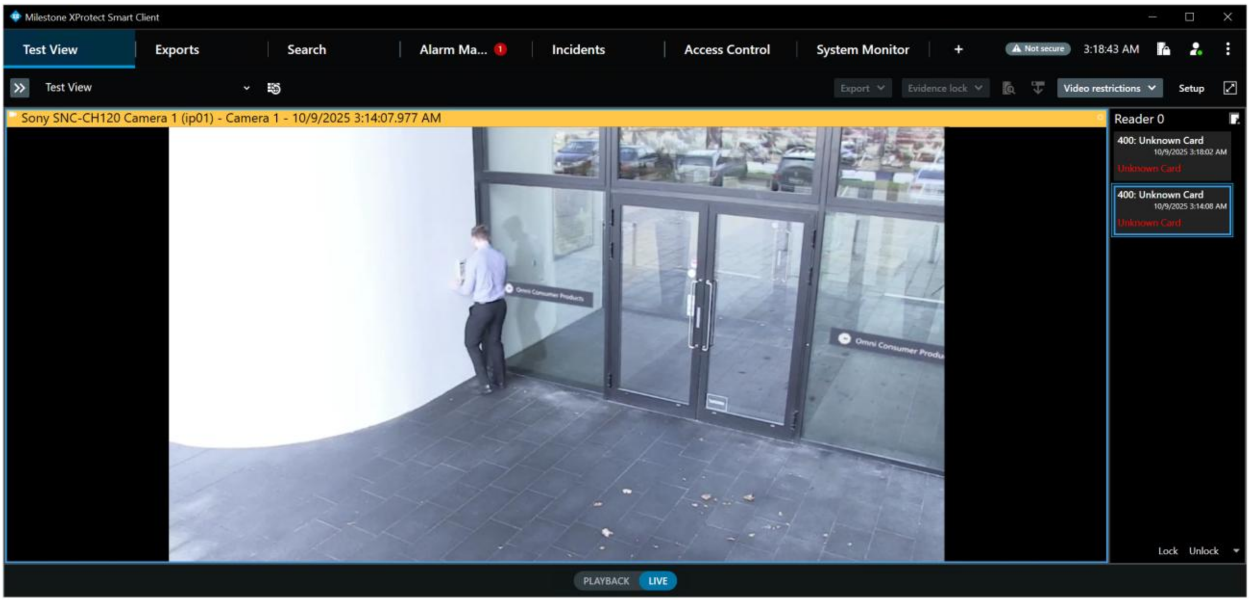
Local time	Message text	Permission	Category	Source type	Source name	User	User location
10/9/2025 3:04:10 AM	Access control system 'pw6k' executed the command 'DC_Unlock' on instance 'Reader 0'	Granted	Access control command	Access control	[redacted]	[redacted]	[redacted]
10/9/2025 2:46:18 AM	Access control system 'pw6k' configuration updated	Granted	Management	Access control	[redacted]	[redacted]	[redacted]
10/9/2025 2:45:23 AM	Access control system 'pw6k' configuration updated	Granted	Management	Access control	[redacted]	[redacted]	[redacted]
10/9/2025 2:44:35 AM	Access control system 'pw6k' configuration updated	Granted	Management	Access control	[redacted]	[redacted]	[redacted]
10/9/2025 2:44:12 AM	Access control system 'pw6k' configuration updated	Granted	Management	Access control	[redacted]	[redacted]	[redacted]
10/9/2025 2:42:48 AM	Access control system 'pw6k' configuration updated	Granted	Management	Access control	[redacted]	[redacted]	[redacted]
10/9/2025 2:40:56 AM	Access control system 'pw6k' configuration updated	Granted	Management	Access control	[redacted]	[redacted]	[redacted]
10/9/2025 1:56:53 AM	Access control system 'pw6k' configuration updated	Granted	Management	Access control	[redacted]	[redacted]	[redacted]
10/9/2025 1:56:38 AM	User-defined categories updated	Granted	Management	Access control	[redacted]	[redacted]	[redacted]
10/9/2025 1:50:43 AM	Access control system 'pw6k' configuration updated	Granted	Management	Access control	[redacted]	[redacted]	[redacted]
10/9/2025 1:50:34 AM	Access control system 'pw6k' configuration updated	Granted	Management	Access control	[redacted]	[redacted]	[redacted]
10/9/2025 1:38:30 AM	Access control system 'pw6k' created	Granted	Management	Access control	[redacted]	[redacted]	[redacted]

XProtect Smart Client operation

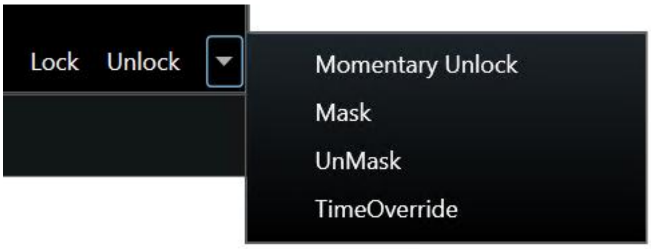
Live

Open XProtect Smart Client > **Live** tab. A list with generated events appears on the right side of the view (which was created in chapter XProtect Smart Client configuration > Add Pro-Watch Access monitor) if they are also assigned to an **Event Category**. When a single event is selected, the related video recording starts playing if the video exists and it is available.

Example:


Milestone XProtect Smart Client
Test View
Exports
Search
Alarm Ma...
Incidents
Access Control
System Monitor
Not secure
3:18:43 AM
Test View
Export
Evidence lock
Video restrictions
Setup
Sony SNC-CH120 Camera 1 (ip01) - Camera 1 - 10/9/2025 3:14:07.977 AM
Reader 0
400: Unknown Card 10/9/2025 3:18:02 AM Unknown Card
400: Unknown Card 10/9/2025 3:14:08 AM Unknown Card
Lock
Unlock
PLAYBACK
LIVE

Also, the door commands are available in the bottom-right corner:



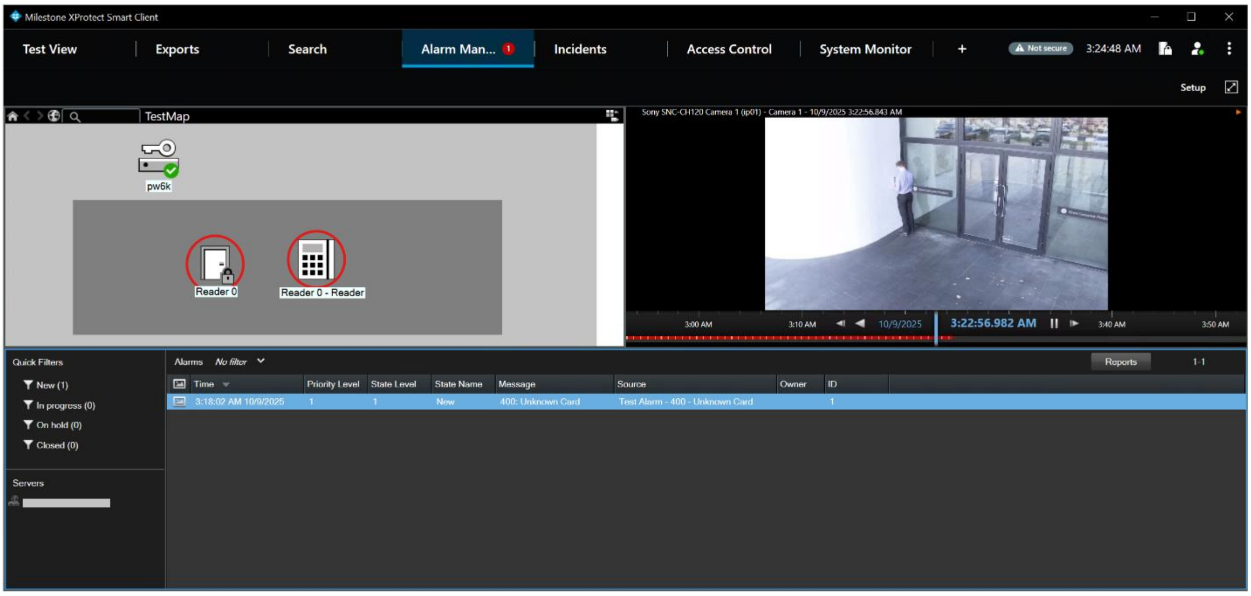
Alarm Manager

Pro-Watch system units on the map

Open XProtect Smart Client > **Alarm Manager** tab.
The map in the example shows:

- **pw6k, Reader 0** and **Reader 0 - Reader** and their current state.
- **Test Alarm - 400 - Unknown Card** (which was created in chapter XProtect Management Client configuration > Alarms based on Pro-Watch Access Control events) is generated.
- **Reader 0** is currently in state **Alarms**.

Note: The correctness of the door initial state is not guaranteed.



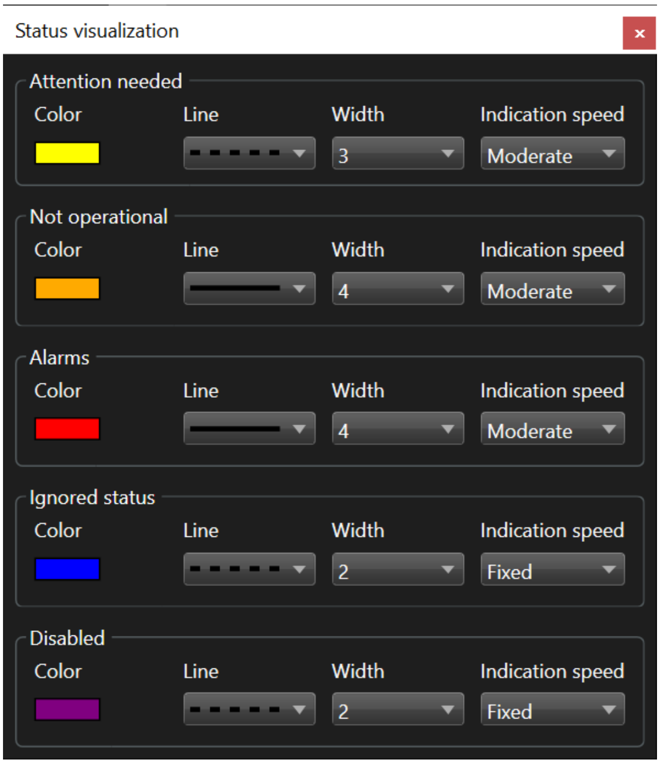
Servers [redacted]

Time	Priority Level	State Level	State Name	Message	Source	Owner	ID
3:18:02 AM 10/9/2025	1	1	New	400: Unknown Card	Test Alarm - 400 - Unknown Card		1

The default XProtect states for the Pro-Watch system units are described in the table below:

State	Description
Attention needed	Currently not supported.
Not operational	Currently not supported.
Alarms	An alarm involving the Pro-Watch system / door is generated and listed in the **Alarms** list.
Ignored status	Currently not supported.
Disabled	Currently not supported.

Status Visualization option in XProtect Smart Client for configuring the desired visualization for each default XProtect state (right click on the map in **Setup** mode > **Status visualization**):



Status visualization ×

Attention needed

Color	Line	Width	Indication speed
🟨	- - - - - -	3	Moderate

Not operational

Color	Line	Width	Indication speed
🟧	———	4	Moderate

Alarms

Color	Line	Width	Indication speed
🟥	———	4	Moderate

Ignored status

Color	Line	Width	Indication speed
🟦	- - - - - -	2	Fixed

Disabled

Color	Line	Width	Indication speed
🟪	- - - - - -	2	Fixed

The Pro-Watch system states based on the integration are described in the table below:

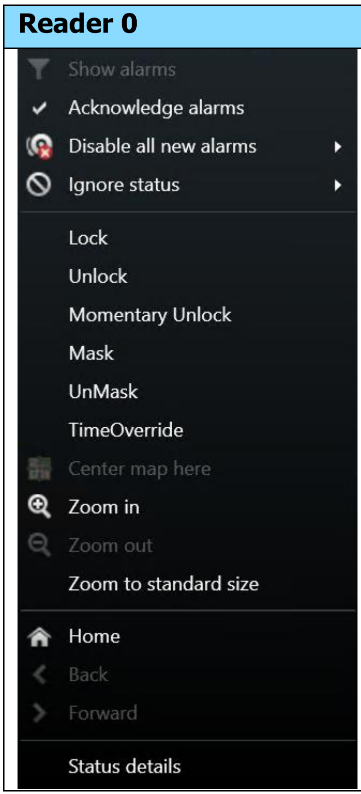
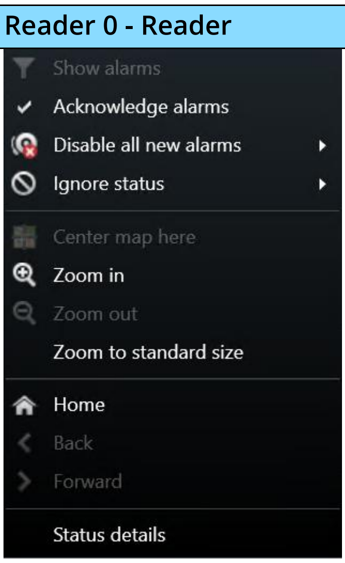
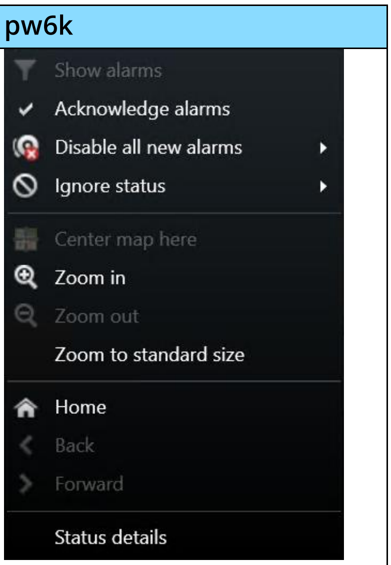
Pro-Watch system state image	Description
🔑✓	Connected
🔑✗	Disconnected

The door states based on the integration are described in the table below:

Door state image	Description
🚪	Open
🚪	Closed
🚪🔒	Locked
🚪	Unlocked

Context menu on the map

If you right-click on the ProWatch system / door, you will see several standard actions / options plus the integration specific:

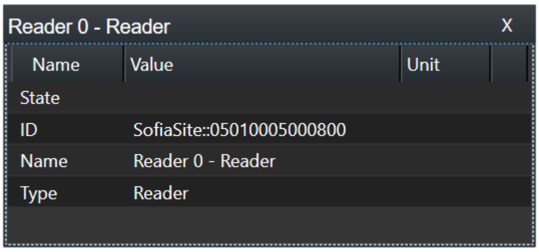
Reader 0	Reader 0 - Reader	pw6k
 Show alarms Acknowledge alarms Disable all new alarms Ignore status Lock Unlock Momentary Unlock Mask UnMask TimeOverride Center map here Zoom in Zoom out Zoom to standard size Home Back Forward Status details	 Show alarms Acknowledge alarms Disable all new alarms Ignore status Center map here Zoom in Zoom out Zoom to standard size Home Back Forward Status details	 Show alarms Acknowledge alarms Disable all new alarms Ignore status Center map here Zoom in Zoom out Zoom to standard size Home Back Forward Status details

The most important ones are described in the table below:

Action	Description	Reader 0	Reader 0 - Reader	pw6k
Show alarms	Currently not supported.	NA	NA	NA
Acknowledge alarms	This action changes the **State Name** of an alarm from **New** to **In Progress**.	Available	NA	Available
Disable all new alarms	Currently not supported.	NA	NA	NA
Ignore status	Currently not supported.	NA	NA	NA
Lock, Unlock, Momentary Unlock, Mask, Unmask, TimeOverride	Pro-Watch system actions related to doors.	Available	NA	NA

Status Details	This option shows the current status of the unit, including several properties and their values.	Available	NA	Available

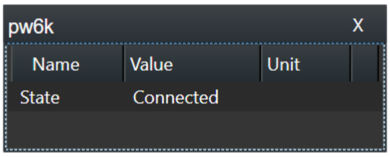
In the example below, the **Reader 0 - Reader** status is shown:



Reader 0 - Reader X

Name	Value	Unit
State		
ID	SofiaSite::05010005000800	
Name	Reader 0 - Reader	
Type	Reader	

In the example below, the **pw6k** status is shown:



pw6k X

Name	Value	Unit
State	Connected	

Alarms

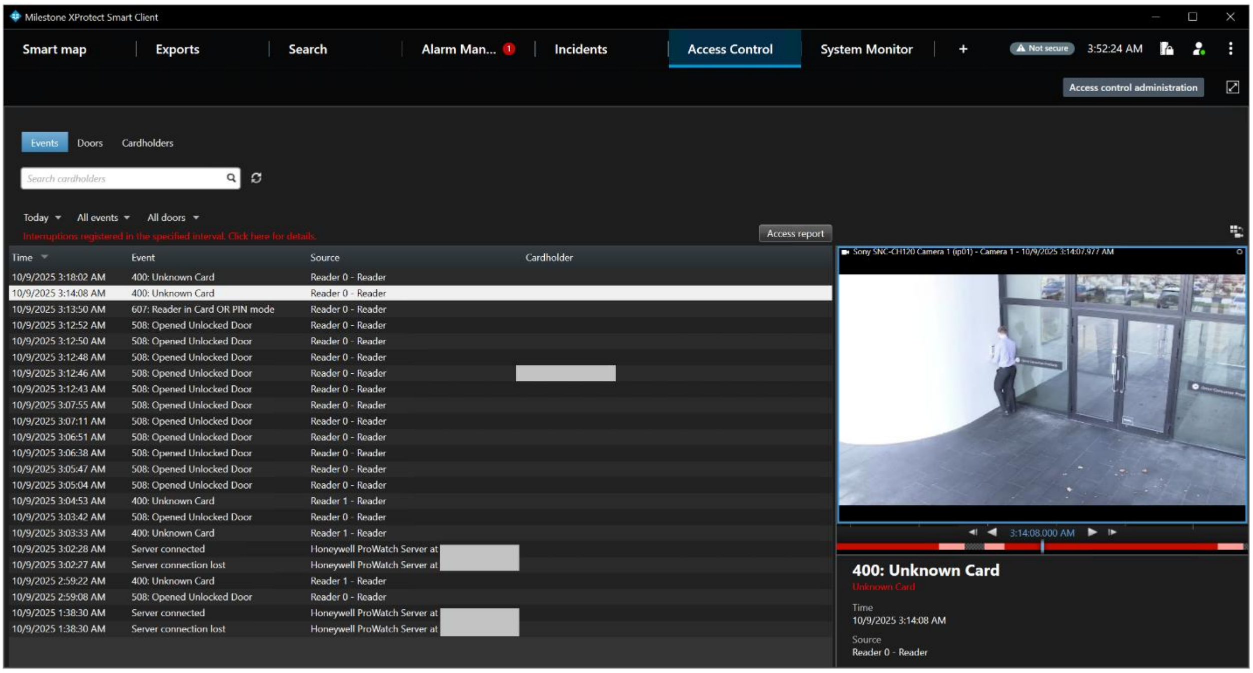
Alarms from Pro-Watch that are acknowledged or closed in XProtect Smart Client will also be acknowledged in Pro-Watch system. XProtect also has a state named **On hold**. Setting Pro-Watch alarms to this state in XProtect Smart Client will not change their state in Pro-Watch system.

Note: Pro-Watch system events are only registered when the XProtect Event Server is running, and the integration is loaded. Moreover, the past Pro-Watch system events cannot be read by the integration. That means that in case the XProtect Event Server has stopped, the Pro-Watch system events generated meanwhile will not be shown in XProtect Smart Client and also will not be displayed when the XProtect Event Server is restarted.

Access Control

Note: For detailed description, see the Milestone XProtect (XProtect Smart Client) help.

Example:



Interruptions registered in the specified interval. Click here for details.

Time	Event	Source	Cardholder
10/9/2025 3:18:02 AM	400: Unknown Card	Reader 0 - Reader	
10/9/2025 3:14:08 AM	400: Unknown Card	Reader 0 - Reader	
10/9/2025 3:13:50 AM	607: Reader in Card OR PIN mode	Reader 0 - Reader	
10/9/2025 3:12:52 AM	508: Opened Unlocked Door	Reader 0 - Reader	
10/9/2025 3:12:50 AM	508: Opened Unlocked Door	Reader 0 - Reader	
10/9/2025 3:12:48 AM	508: Opened Unlocked Door	Reader 0 - Reader	
10/9/2025 3:12:46 AM	508: Opened Unlocked Door	Reader 0 - Reader	[redacted]
10/9/2025 3:12:43 AM	508: Opened Unlocked Door	Reader 0 - Reader	
10/9/2025 3:07:55 AM	508: Opened Unlocked Door	Reader 0 - Reader	
10/9/2025 3:07:11 AM	508: Opened Unlocked Door	Reader 0 - Reader	
10/9/2025 3:06:51 AM	508: Opened Unlocked Door	Reader 0 - Reader	
10/9/2025 3:06:38 AM	508: Opened Unlocked Door	Reader 0 - Reader	
10/9/2025 3:05:47 AM	508: Opened Unlocked Door	Reader 0 - Reader	
10/9/2025 3:05:04 AM	508: Opened Unlocked Door	Reader 0 - Reader	
10/9/2025 3:04:53 AM	400: Unknown Card	Reader 1 - Reader	
10/9/2025 3:03:42 AM	508: Opened Unlocked Door	Reader 0 - Reader	
10/9/2025 3:03:33 AM	400: Unknown Card	Reader 1 - Reader	
10/9/2025 3:02:28 AM	Server connected	Honeywell ProWatch Server at [redacted]	
10/9/2025 3:02:27 AM	Server connection lost	Honeywell ProWatch Server at [redacted]	
10/9/2025 2:59:22 AM	400: Unknown Card	Reader 1 - Reader	
10/9/2025 2:59:08 AM	508: Opened Unlocked Door	Reader 0 - Reader	
10/9/2025 1:38:30 AM	Server connected	Honeywell ProWatch Server at [redacted]	
10/9/2025 1:38:30 AM	Server connection lost	Honeywell ProWatch Server at [redacted]	

400: Unknown Card
Unknown Card

Time
10/9/2025 3:14:08 AM

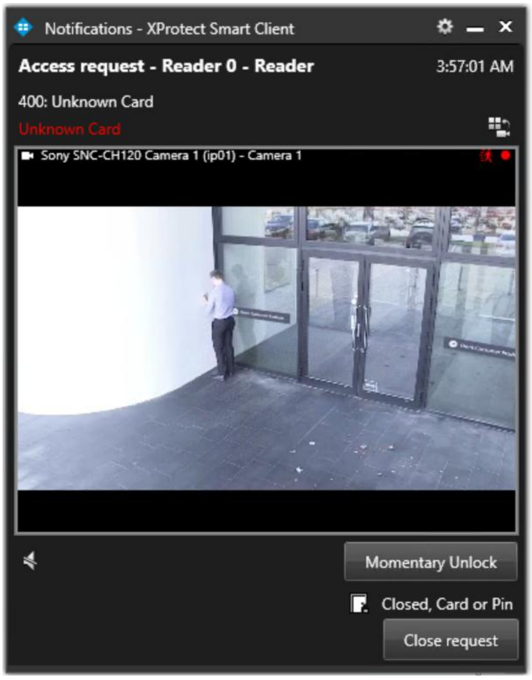
Source
Reader 0 - Reader

Access request notifications

Access request notifications appear as a pop-up in the bottom-right corner of the screen. Each notification contains the following information:

- Source (door)
- Local Time
- Event name
- Live video from the associated camera
- Button to Toggle playing of incoming audio
- Actual state of the door
- Button **Close request**

In the example below, an access request notification for **400: Unknown Card** event is shown:



Notifications - XProtect Smart Client

Access request - Reader 0 - Reader 3:57:01 AM

400: Unknown Card

Unknown Card

Sony SNC-CH120 Camera 1 (ip01) - Camera 1

Closed, Card or Pin

Troubleshooting

This section provides information which helps the administrator solve cases where the integration fails working. For detailed troubleshooting Log files should be inspected.

Case: **XProtect Pro-Watch Integration** is not listed as an option in **Integration plug-in** when adding the Pro-Watch Access Control to the XProtect system.

Cause	Action
The XProtect Event Server and XProtect Management Client have not been restarted after the installation of the plug-in.	Restart the XProtect Event Server and XProtect Management Client after the installation of the plug-in.

Case: Alarms in XProtect are not detected. Map displays errors/warnings.

Cause	Action
XProtect Event Server is not running.	Open Windows Services and check the status of Milestone XProtect Event Server. Try to start it. Check the XProtect Event Server logs, if it fails to start.

XProtect ProWatch Integration is not loaded by the XProtect Event Server.	Check the XProtect Event Server log. Look for an entry resembling: “2025-10-09 03:02:13.823+03:00 [9] INFO - PluginHandler Access Control plugin loaded: XProtect Pro-Watch Integration v3.0 - Milestone Systems A/S” Note that this message is produced only occurs while the XProtect Event Server is starting. Verify that the plug-in has been installed correctly if no log entries are found. It should be typically located in: *C:\Program Files\Milestone\MIPPlugins\XProtect Pro-Watch Integration*
MIP License has expired or is not activated.	First, consider re-activation of the license either online or offline. Check the license details in XProtect Management Client.

Logs

Logger configuration

1. Open simple text editor (such as Microsoft Notepad) as Administrator.
2. Open *C:\ProgramData\Milestone\XProtect Pro-Watch Integration\XProtect Pro-Watch Integration_LoggerConfig.config*

   The file does have the following structure by default:

```
<LoggerConfiguration>
  <ManagementClientPlugin>
    <LogLevel>Normal</LogLevel>
    <MaxLogFileSizeInMb>100</MaxLogFileSizeInMb>
    <LogFilesRetentionTimeInDays>30</LogFilesRetentionTimeInDays>
  </ManagementClientPlugin>
  <SmartClientPlugin>
    <LogLevel>Normal</LogLevel>
    <MaxLogFileSizeInMb>100</MaxLogFileSizeInMb>
    <LogFilesRetentionTimeInDays>30</LogFilesRetentionTimeInDays>
  </SmartClientPlugin>
  <EventServerPlugin>
    <LogLevel>Normal</LogLevel>
    <MaxLogFileSizeInMb>100</MaxLogFileSizeInMb>
    <LogFilesRetentionTimeInDays>30</LogFilesRetentionTimeInDays>
  </EventServerPlugin>
  <WindowsService>
    <LogLevel>Normal</LogLevel>
    <MaxLogFileSizeInMb>100</MaxLogFileSizeInMb>
    <LogFilesRetentionTimeInDays>30</LogFilesRetentionTimeInDays>
  </WindowsService>
  <WindowsServiceTray>
    <LogLevel>Normal</LogLevel>
    <MaxLogFileSizeInMb>100</MaxLogFileSizeInMb>
    <LogFilesRetentionTimeInDays>30</LogFilesRetentionTimeInDays>
  </WindowsServiceTray>
</LoggerConfiguration>
```

Note: **WindowsService** and **WindowsServiceTray** nodes are not used in the XProtect Pro-Watch Integration.

The file contains the configuration parameters for each of the XProtect Pro-Watch Integration components. Each parameter consists of a key which identifies the parameter and a value which corresponds to the value of the parameter.

Parameter	Description
LogLevel	The level of logging information. The possible values are: • **Normal**: This level enables logging of info and error messages related to the component functioning. This is the default value for this parameter. • **Debug**: This level enables full logging. It is not recommended when running in a production environment, but it is intended for deep troubleshooting.
MaxLogFileSizeInMb	The maximum size in MB of a single log file. It is **100 MB** by default.
LogFilesRetentionTimeInDays	The retention days for the log files. It is **30 days** by default.

Change the values of the parameters based on your requirements.

3. Save the changes and restart the component(s) for which you have changed the parameter value(s).

Log files

The log files are typically located in the following folder:
C:\ProgramData\Milestone\XProtect Pro-Watch Integration
New log files are created on a daily basis. The content of the files can be viewed using a simple text viewer such as Microsoft Notepad.

The following types of logs can be produced:

Logs folder	Description
ManagementClientPluginLogs	This folder contains log files related to the XProtect Managment Client plug-in component of the XProtect Pro-Watch Integration.
SmartClientPluginLogs	This folder contains log files related to the XProtect Smart Client plug-in component of the XProtect Pro-Watch Integration..

EventServerPluginLogs	This folder contains log files related to the Xprotect Event Server component of the XProtect Pro-Watch Integration..

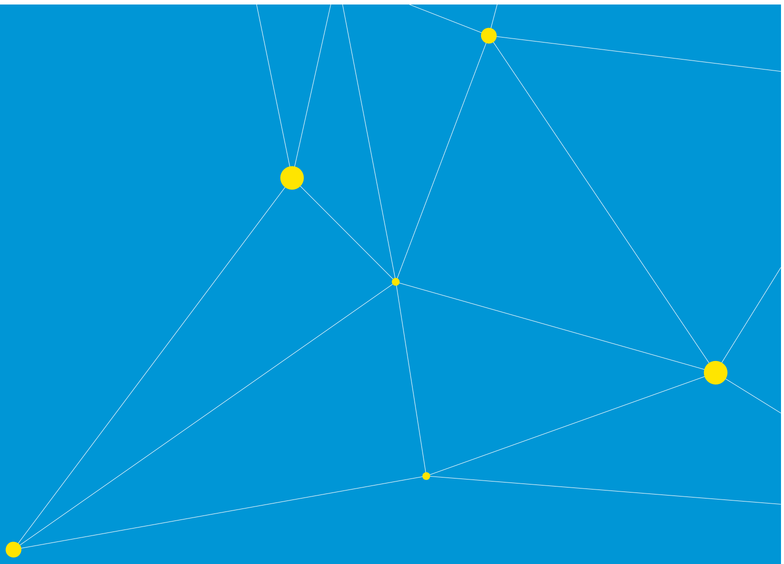
Limitations

1. The XProtect Pro-Watch Integration supports only the logical devices based on **Hardware Template**: **DoorTypicalACR (Access Control Reader)** and **Hardware Class**: **Reader**, their device types (resources) and the defined set of events for these resources. The integration may work with logical devices based on other **Hardware Templates** and **Hardware Classes**, but Custom Development does not guarantee that.

2. XProtect Pro-Watch Integration has been tested in the following environment(s):
   - Milestone XProtect Corporate 2025 R2
   - Honeywell Pro-Watch v6.5.1
   - Honeywell Pro-Watch API Service v6.5.2 with Rest API v2
   - Honeywell PW-6000 panel
3. Pro-Watch system events are only registered when the XProtect Event Server is running, and the integration is loaded. Moreover, the past Pro-Watch system events cannot be read by the integration. That means that in case the XProtect Event Server has stopped, the Pro-Watch system events generated meanwhile will not be shown in XProtect Smart Client and also will not be displayed when the XProtect Event Server is restarted.
4. Pro-Watch RTN events are currently not supported.
5. The correctness of the door initial state is not guaranteed.
6. In order to reset the reader to its default mode, the Re-Enable (Default Mode) command needs to be executed from the Pro-Watch client application.
7. The HTTPS connection to the Pro-Watch API is currently not supported.

Known issues

There are no known issues at the time of the release.



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.