MAKE THE
WORLD SEE

Date: 20 July 2020

Manual

Milestone Honeywell Pro-Watch Access Control Integration v2.0

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 and HSDK software.
The operation part of this document is aimed at system administrators and also 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 2019 R3 (XProtect Management Client and XProtect Smart Client) help which contains detailed information about XProtect Access
- Honeywell Pro-Watch Installation Guide v4.5 SP1 which contains detailed information about installation of Pro-Watch access control system
- Honeywell Pro-Watch Software Suite v4.5 SP1 help which contains detailed information about configuration and use of Pro-Watch access control system
- Honeywell Security Developer Kit User's Guide v2.6.0.0 contains detailed information about installation, configuration and use of HSDK

and for system operators to check at least:

- Milestone XProtect 2019 R3 (XProtect Smart Client) help which contains detailed information about Milestone XProtect Access

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 make adjustments 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 Milestone Honeywell Pro-Watch Access Control 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 from Milestone XProtect including visual representation
- Badge Holders from Honeywell Pro-Watch access control system are integrated into Milestone XProtect

Solution overview

The integration consists of an XProtect Event Server plug-in which communicates with Honeywell Security Developer Kit (HSDK) as illustrated here:
<XProtect Event Server> <-> <HSDK> <-> <Pro-Watch access control system> <-> <Panel>

The machine running the XProtect Event Server must be able to connect to the HSDK/Pro-Watch system 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.

***Note**: The HSDK supports only a single system querying for events. This means that only a single XProtect Event Server must access the HSDK at a time. If more than one XProtect Event Server (or other application such as HSDK Test Client) tries to communicate with the HSDK, the receiving of events will become unpredictable.*

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
- Pro-Watch generated alarms are listed and visualized in the Alarms list
- Acknowledgement of the Pro-Watch generated alarms
- Centralized overview of Events/Doors/Cardholders in Access Control tab
- Access request notifications

Installation

Prerequisites

The Milestone Honeywell Pro-Watch Access Control Integration is compatible with:

- Milestone XProtect Corporate, Expert, Professional+, Express+ and Essential+ 2019 R3 or newer
- Honeywell Pro-Watch v4.5 SP1
- Honeywell Security Developer Kit (HSDK) v2.6.0.0

Installer

The Milestone Honeywell Pro-Watch Access Control Integration consists of one installation file supporting Windows 64-bit only:

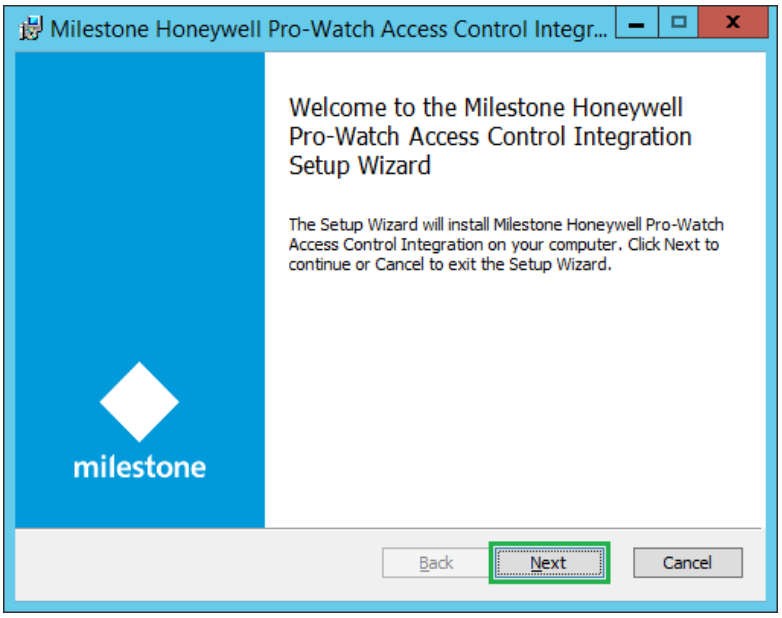
- *ProWatchInstallation_x64_2.0.XX.X.msi*

The Milestone Honeywell Pro-Watch Access Control 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

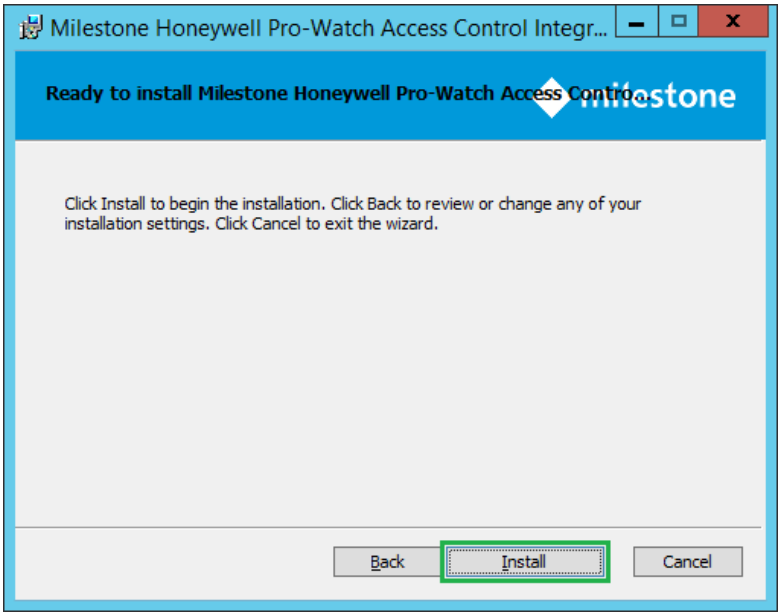
Installation steps

1. Start the installation by executing ***ProWatchInstallation_x64_2.0.XX.X.msi***.
2. Click **Next**.

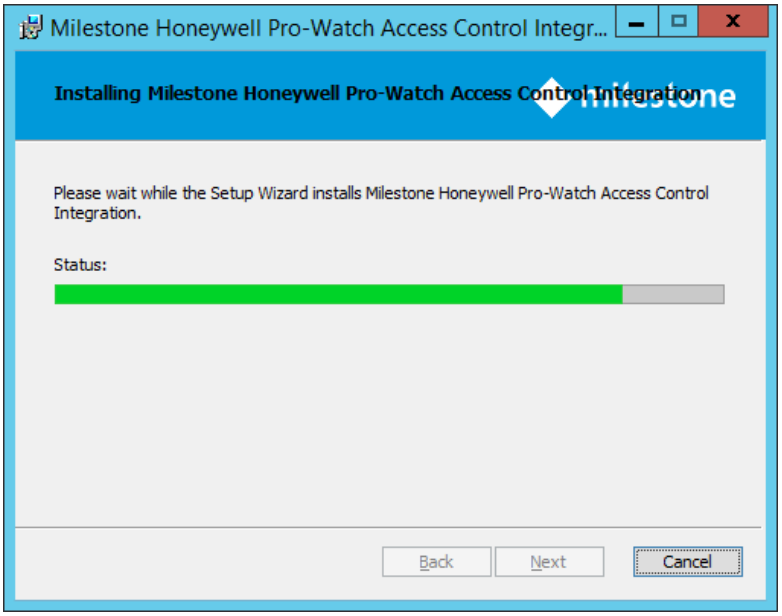


3. Read the license agreement carefully and select the **I accept the terms in the License Agreement** box. Click **Next**.

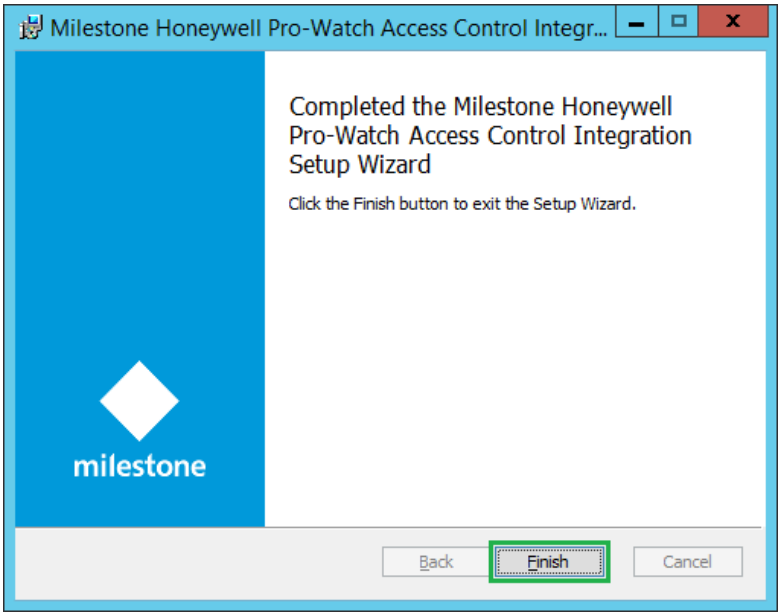
4. Click **Install**.



5. The next steps are executed automatically.



6. Click **Finish**.



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

License

The use of Milestone XProtect Access requires a **Base** license which allows accessing this feature.
An **Access control door** license is needed for each door which needs to be controlled.

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

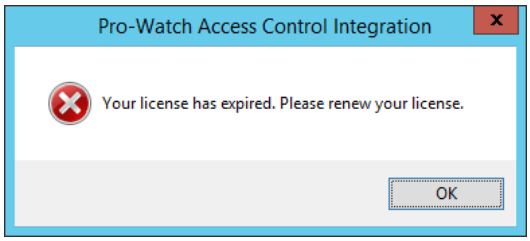
This solution does have also a build-in **MIP** license check that is locked to the software license code (SLC) of the XProtect installation of which it is a part.

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

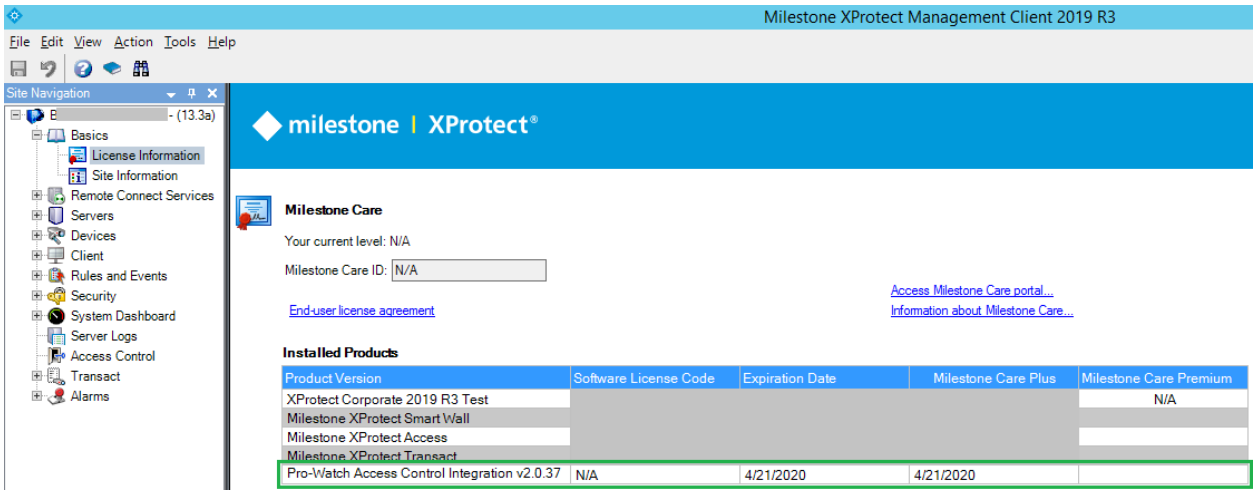
The permanent **MIP** license is free of charge for this solution.

The permanent **MIP** licenses are provided by the distributor. In order 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 plug-in will issue error messages and will have a reduced functionality.

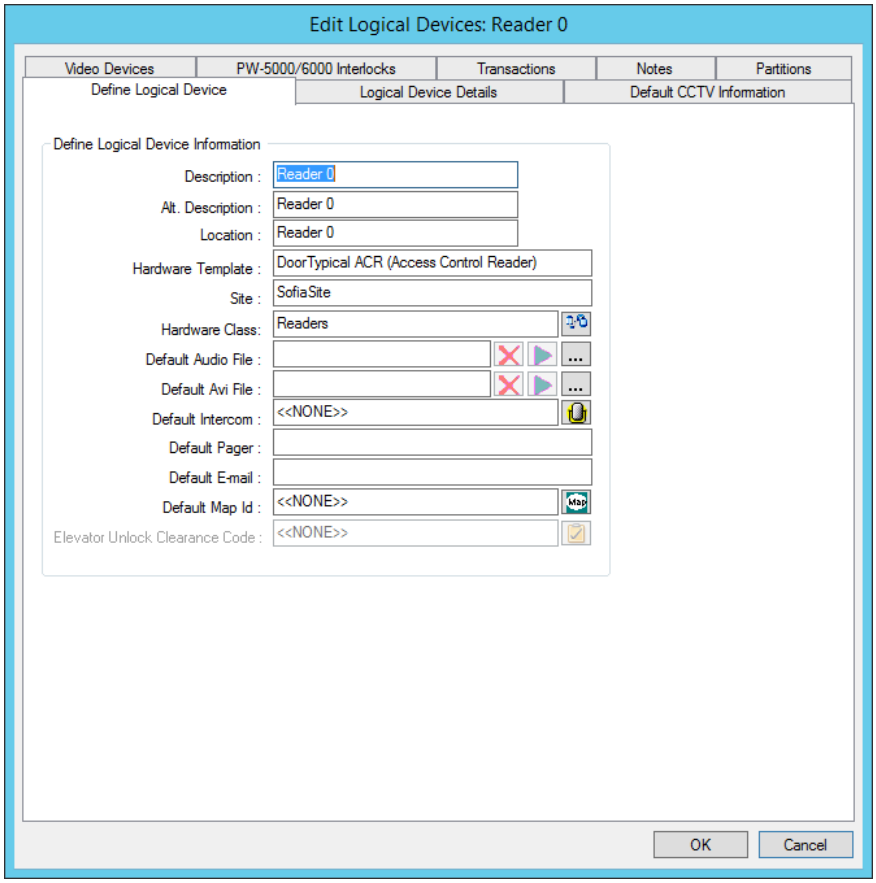


The license information can also be checked in the XProtect Management Client > **Site Navigation** > **Basics** > **License Information** > **Installed Products** > **Pro-Watch Access Control Integration v2.0.XX.X**

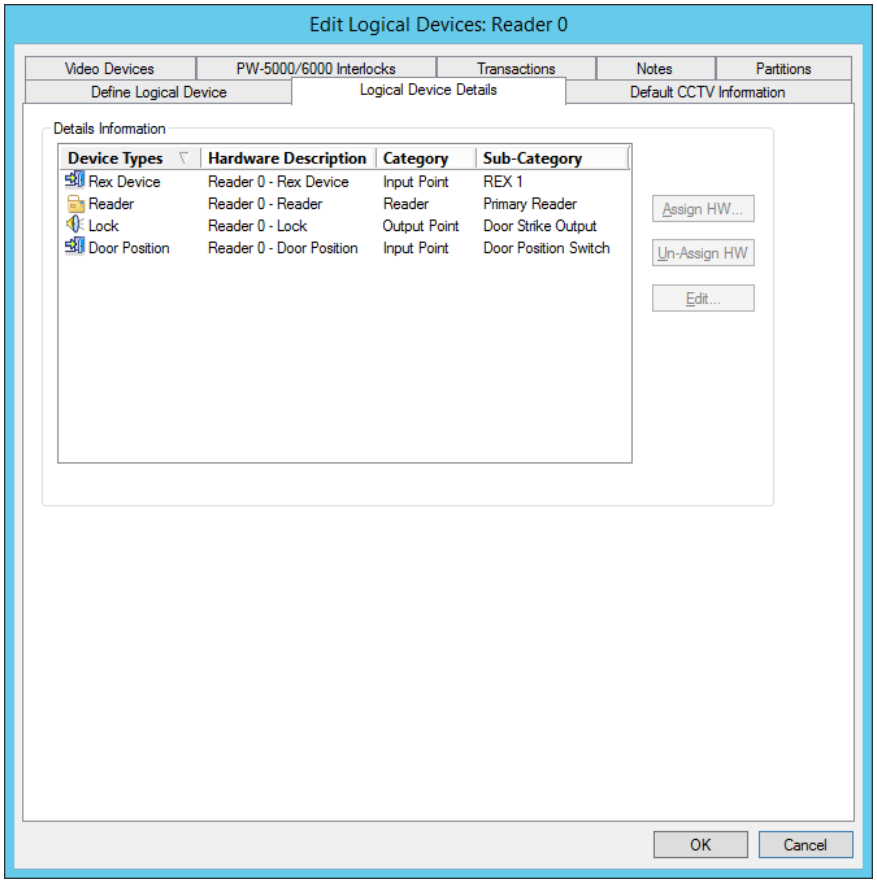


Pro-Watch and XProtect elements mapping

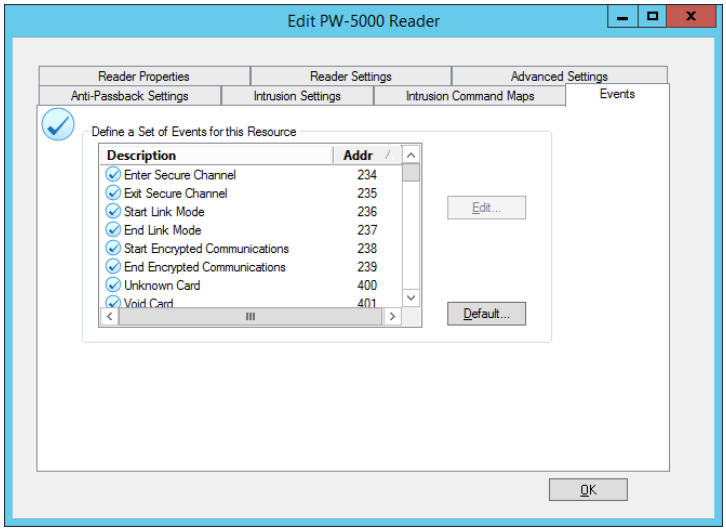
The hierarchy in the Pro-Watch system is usually **Site** > **Channel** > **Panel** > **Logical Devices**. The **Logical Devices** are based on **Hardware Templates** and **Hardware Classes**.



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



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.



The Milestone Honeywell Pro-Watch Access Control 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, Lock 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	Door 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 • The parent device (in this case Reader 0) takes over the ownership of the generated events
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

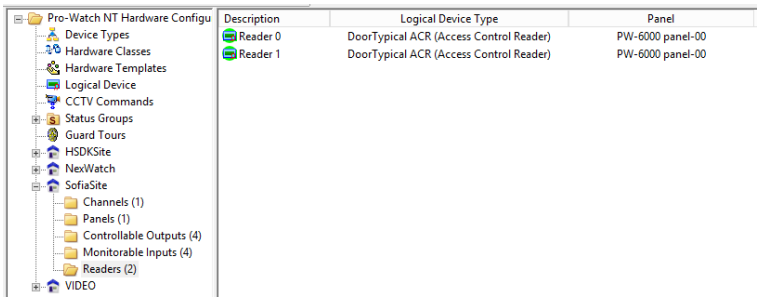
Pro-Watch configuration

General configuration

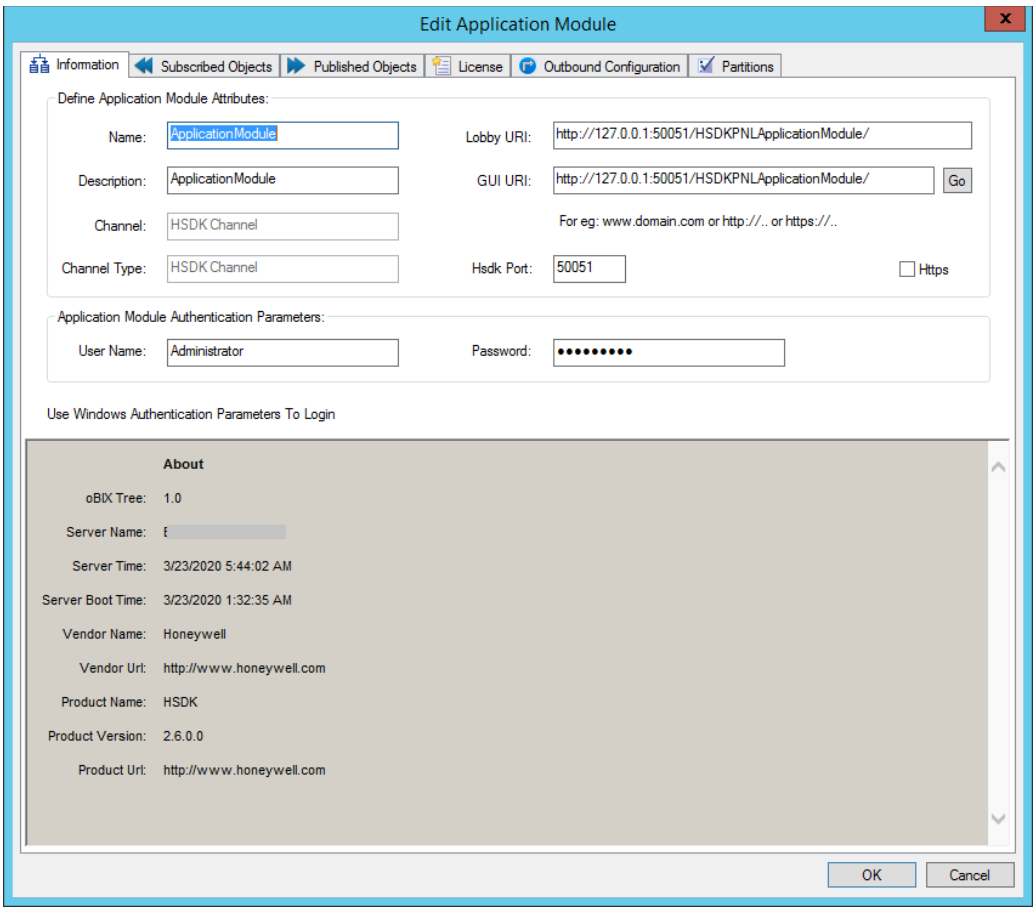
1. (Optional) Connect the Pro-Watch panel to the network and turn it on.

In the example below, a **PW-6000** panel is used.

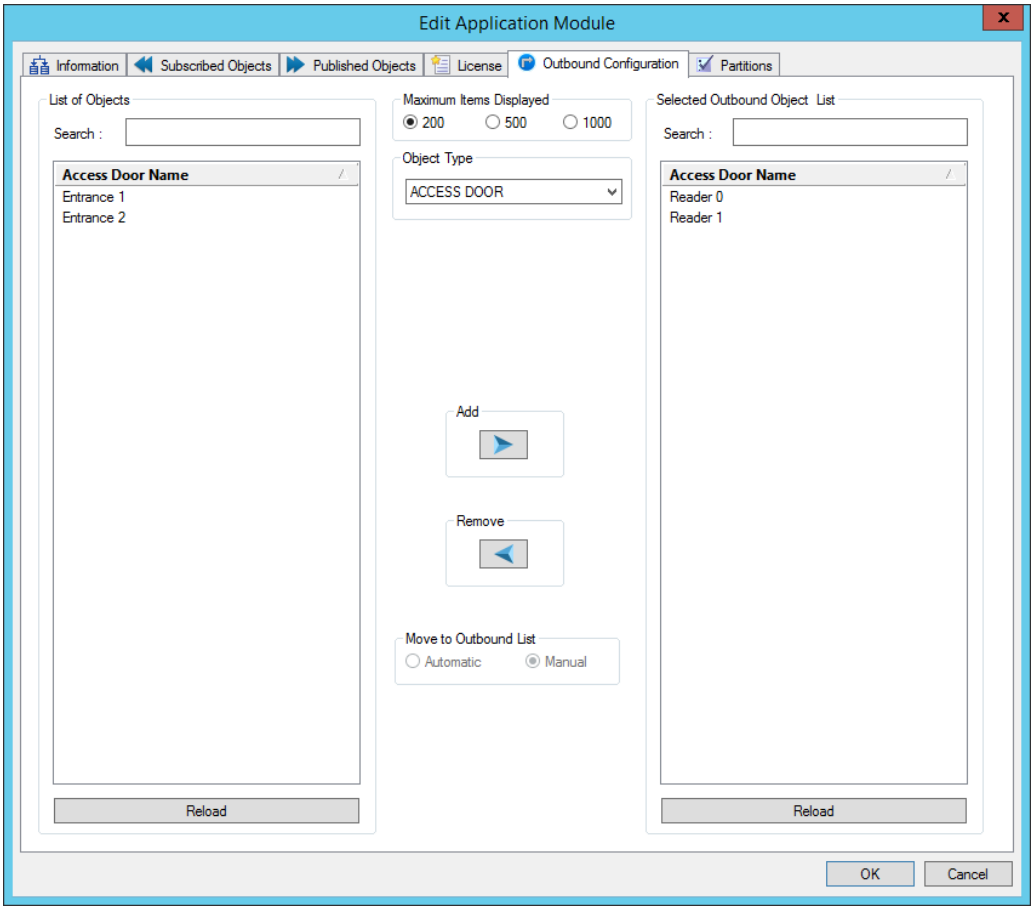
2. Create a **Site**, a **Channel**, and a **PW-6000** panel.
3. Add at least one **Reader** for the panel.
   In the example below, two **Readers** are created.



4. (Optional) Verify that there is a connection between the **PW-6000** panel and **Pro-Watch Software Suite**.
5. Create a **HSDK Site**, a **Channel**, and a **HSDK Panel**.
6. Create an **Application Module** using the **HSDK Channel** and the **HSDK Panel** from the previous step.



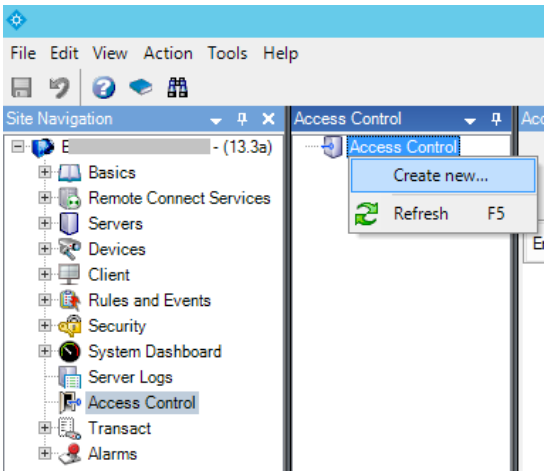
7. Add a **Reader** (part of object type **ACCESS DOOR**) to the **Outbound Object List**. In the example below, two **Readers** are added.



XProtect Management Client configuration

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 **Honeywell Pro-Watch** from the **Integration plug-in** dropdown. The following connection details appear and need to be specified:

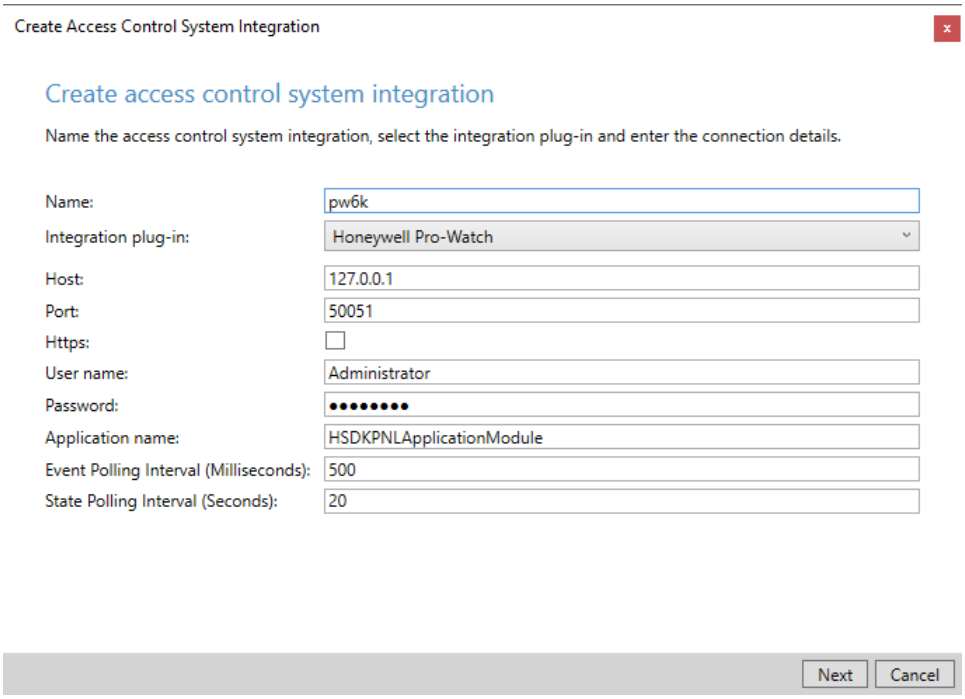
***Note**: In case HSDK and Milestone XProtect are installed on different computers and **https** connection type is used, it is mandatory to open the certificate stores on the computer where the HSDK is installed and export **HSDK Root CA** (located in **Certificates (Local Computer)** > **Trust Root Certification Authorities** > **Certificates**) and **computer certificate issued by HSDK Root CA** (located in **Certificates (Local Computer)** > **Personal** > **Certificates**). Then import both certificates in the same certificate stores on the computer where the Milestone XProtect Event Server is installed.*

Host: The IP address or the computer name of the **HSDK Lobby URI**.

***Note**: In case HSDK and Milestone XProtect are installed on different computers and **https** connection type is used, it is mandatory to use the computer name (instead of the IP address).*

Port: The port number of **HSDK Lobby URI** also known as **Hsdk port**.
Https: The connection type will be changed to **https**. The port should be adjusted properly depending on the connection type.
User name: The user with the administrative rights for the Pro-Watch system.
Password: The password of the user.
Application name: The name of the HSDK application module.
Event Polling Interval (Milliseconds): Defines the event polling interval. It is recommended to use the default value.
State Polling Interval (Seconds): Defines the state polling interval. It is recommended to use the default value.

Example:



Click **Next**.

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

Example:

In the example below, the following items are added:

Doors (2): The doors which are added to the **Outbound Configuration** (step 6, chapter Pro-Watch configuration – General configuration):

Reader 0

Reader 1

Units (2): The units (door access points) which are related to the added doors.

Reader 0 – Reader

Reader 1 – Reader

Servers (1): The Pro-Watch system.

Server

Events (179): A list with supported events.

1: EV_LOG Threshold Limit Exceeded	430: Invalid Card - Before Activation
2: Database record Add	431: Denied - Building not open
3: Database record updated	432: Building Close Fail- Key
4: Database record deleted	433: Sensor Fail
5: Database queryset	434: Coax Failure

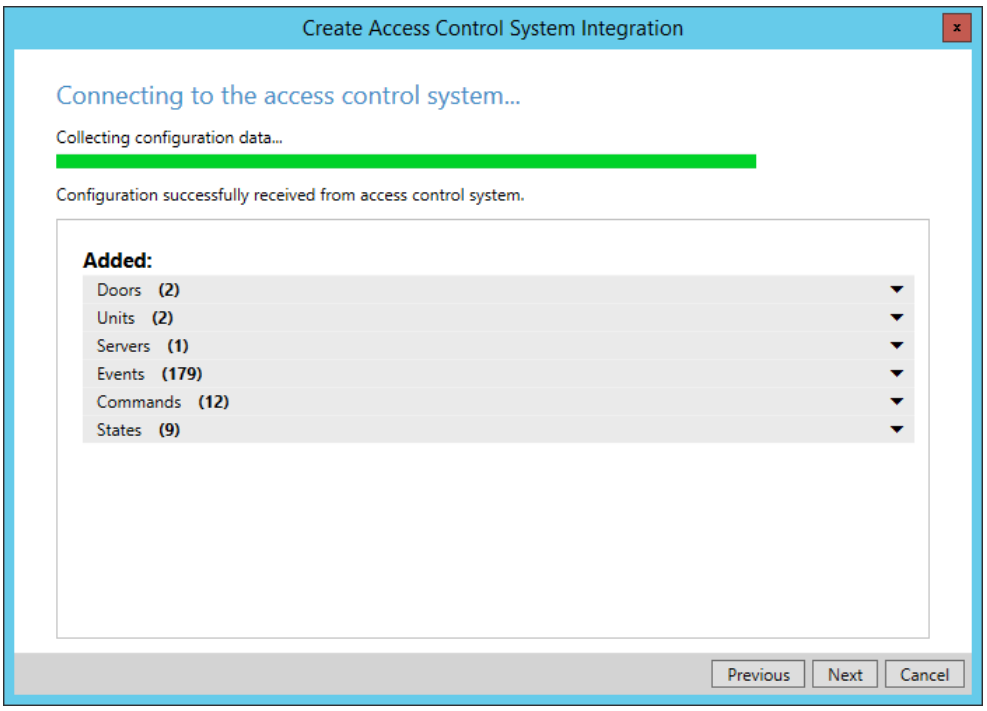
6: Operator has logged in	435: Exit Granted
7: Operator has logged off	436: Exit Denied
8: Report has been requested	437: Auto unlocked
9: Operator log is filling up	438: Auto locked
10: Event Occured	439: Coax shunted
11: Alarm response has been entered	440: Sensor shunted
12: Alarm has been acknowledged	441: Denied - ABA Site Code
13: Alarm has been cleared	442: Denied - ABA card expired
14: CCTV command has been requested	443: VIP Tamper Shunt
15: Page has been issued	444: VIP Tamper unshunt
16: Alarm beeper has been silenced	445: VIP Tamper
17: Alarm has been cleared without a normal	446: MSM Failure
18: Maps have been rebuilt	447: Building Close Fail- User
19: System procedure has been executed	448: Reader/Device Comm Fail
20: Intercom Request	449: Reader/Device Tamper
50: Download request	450: Keypad Failure
51: Mask an alarm point	451: Host denied access (Verification Viewer)
52: Arm an alarm point	452: Biometric Verification Failed
53: Door locked	453: Biometric Verification Failed: No Record
54: Door unlocked	454: Biometric Verification Failed: No Device
55: Door in access mode	455: Auto-Disabled Card
56: Timed override issue	456: Wireless Rdr Tamper Active
57: Momentary Unlock	457: Wireless Rdr Tamper Inactive
58: Output activate request	458: Tamper - Wireless Rdr Low Batt
59: Output deactivate request	459: Tamper - Wireless Rdr R/F Loss
60: Output momentary pulse	460: Tamper - Wireless Rdr Motor
61: Threat level change request	461: Wireless Reader Key Override
62: Void card request	462: Incomplete Card/PIN Sequence
63: Archive Start	463: Tamper Rdr R/F Jammed
64: Archive has completed	464: Tamper Rdr Offline
65: Restore has started	465: Tamper Rdr Lock Jammed
66: Restore has completed	466: Tamper Rdr Fault
70: Invalid Operator ID	467: Tamper Rdr No Signal
71: Invalid password	500: Access Granted
72: Invalid workstation	501: HostGrant
73: Invalid operator class	502: Executive Privilege
74: Operator ID has expired	503: Timed override enabled
75: Too Many Active Users	504: Timed override disabled
76: EV_LOG Limit Exceeded	505: Timed override enabled by host
77: Door Reenabled	506: Timed override disabled by host
78: Group Access Project Started	507: Timed override expired
79: Group Access Project Ended	508: Opened Unlocked Door
80: Remote Server is Offline	509: Local Grant - Duress - Not Used

81: Intrusion Group control request	512: Local Grant - APB Error - Not Used
82: Intrusion Zone List control request	513: Local Grant - APB Error - Used
83: Intrusion Zone control request	514: Local Grant - Duress - Used
84: Portal Lock control request	515: Local Grant - Door not used
100: Communication Break	516: Access terminated
101: Loop Command error	517: Host Grant (Verification Viewer)
102: Checksum error occurred	518: Pre-Grant: Local Grant in Progress
103: Message termination error	519: Pre-Grant: Host Grant in Progress
104: Unexpected Disconnect	600: Reader has been disabled
105: Connection Started	601: Reader has been unlocked
106: Connection successful	602: Reader has been locked
107: Connection failed	603: Reader in facility code mode only
114: Disconnect complete	604: Reader in card only mode
400: Unknown Card	605: Reader in PIN only mode
401: Void Card	606: Reader Card+PIN mode
402: Expired Card Attempt	607: Reader in Card OR PIN mode
403: Card Trace	608: Rex Pressed, Non-verified
404: Host denied access	609: Rex Pressed, Door not used
405: Valid Card at an unauthorized reader	610: Rex Pressed, Door used
406: Lost Card Attempt	611: Host Rex, Non-verified
407: Stolen Card Attempt	612: Host Rex, Door not used
408: Unaccounted for Card Attempt	613: Host Rex, Door used
409: Deactivated Card Attempt	614: Guard Arrived Early
410: Terminated Card Attempt	615: Guard Arrived Late
411: Valid Card presented at wrong time	616: Guard Never Arrived
412: Invalid Reader Time Zone	617: Guard Is Now Late
413: Invalid Pin	900: Input point in alarm
414: Invalid Facility Code	10900: Input point in alarm, RTN return to normal
415: Valid card with an incorrect issue level	901: Input point in short condition
416: Invalid Timed override	902: Input point is open
417: Invalid IN-X-IT status	903: Input point held past shunt time
418: Invalid threat level	904: Input point in trouble
419: Antipassback error	905: Input point masked for Entry Delay
420: Pincode Retry Exceeded	906: Input Point Masked for Exit Delay
421: Invalid Forward Card Read	907: Input point fault detected
422: Invalid Reverse Card Read	908: Input point status unknown
423: Attempt to open Locked Door	910: Input point disconnected
425: Duress Detected - Access Denied	911: Monitor Input Alarm
426: Second not presented	950: Output point is active
427: Access denied - Occupancy limit reached	Lost connection
428: Access denied - Area disabled	Reconnected
429: Access denied - Use limit reached	

Commands (12): A list of supported actions (commands) for the doors added: Mask, UnMask, TimedMask, Lock, MomentaryUnlock, Re-Enable, TimeOverride, Unlock, MaskTamperAlarm, UnMaskTamperAlarm, EnterCypher, ExitCypher

***Note**: For detailed Hardware Actions description, see the Honeywell Pro-Watch Software Suite v4.5 SP1 help.*

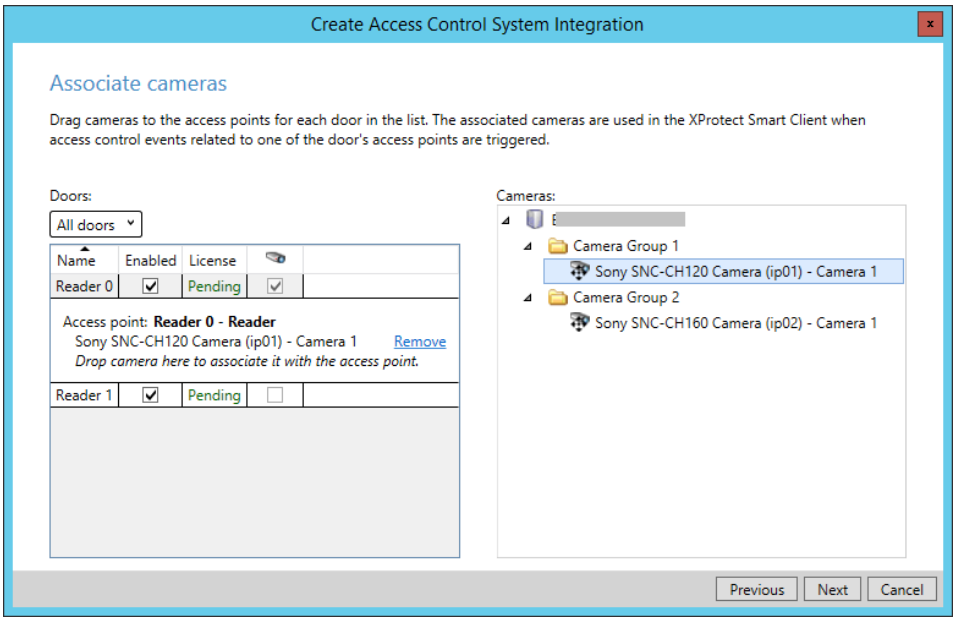
States (9): A list of supported states for the added doors and panel: Closed, Open, Unknown, Locked, Unlocked, Fault, Unknown, Connected, Disconnected



Click **Next**.

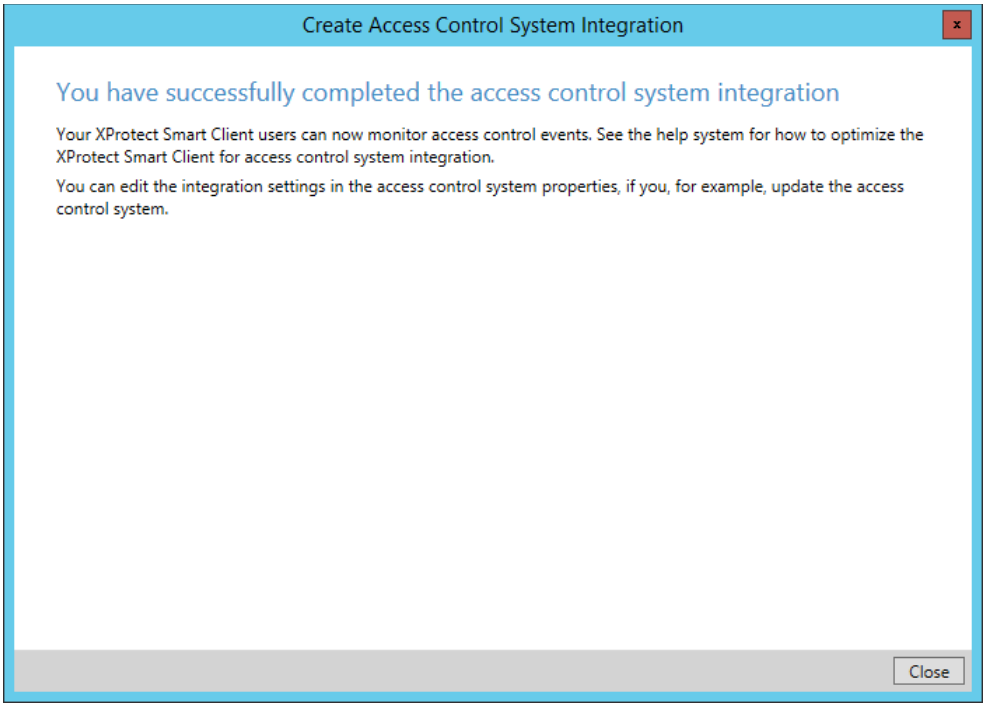
5. (Optional) Drag and drop cameras to the door access points for each door in the list. The associated cameras are used in XProtect Smart Client when access control events related to each door are triggered.

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



Click **Next**.

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



Remove Pro-Watch 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.

Pro-Watch Access Control Properties

***Note**: See the Milestone XProtect (XProtect Management Client) help for the **Access control** properties.*

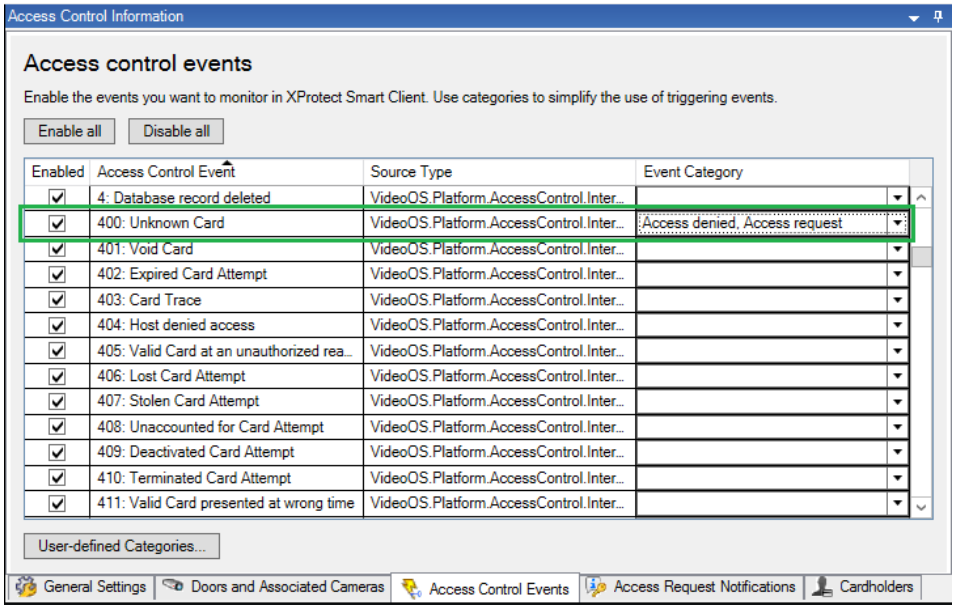
General Settings tab

***Note**: Operator login required option (differentiated user rights) is not supported.*

Access Control Events tab

***Note**: All listed events are enabled, but not assigned to an **Event Category** by default.*

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.



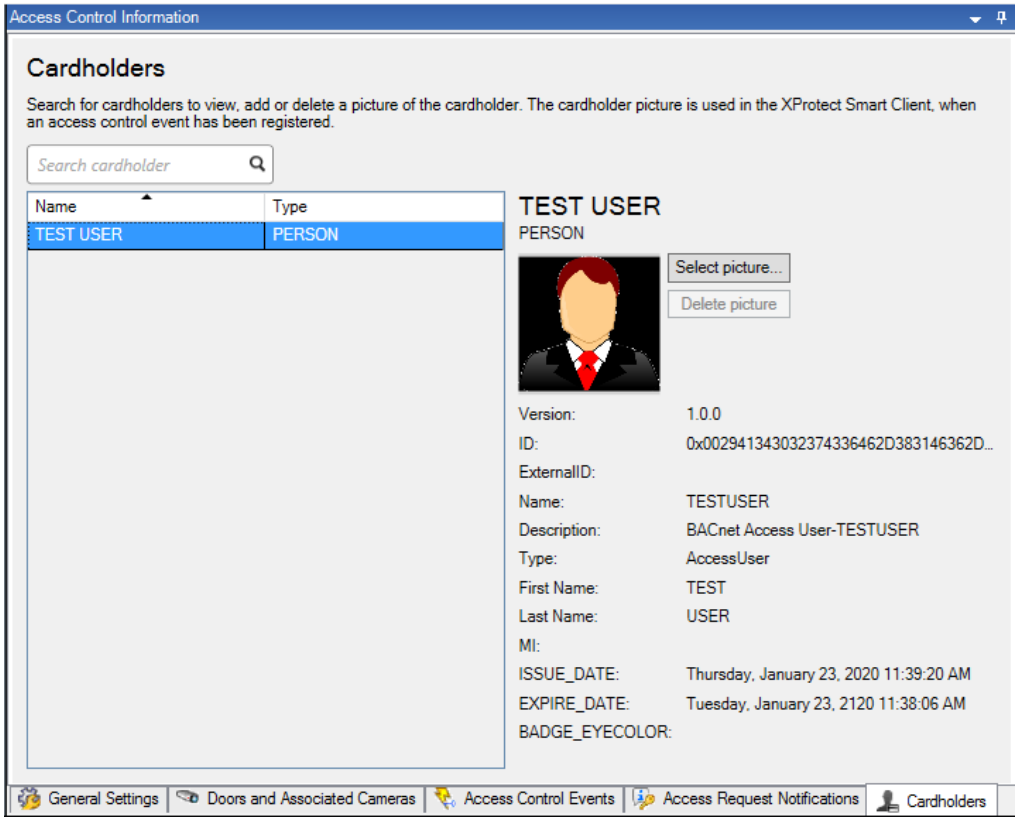
Access Request Notifications tab

***Notes**: By default, **Access denied** is not associated with **Access request** which means that the association should be configured additionally.*

Cardholders tab

Badge Holders from the Pro-Watch 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.

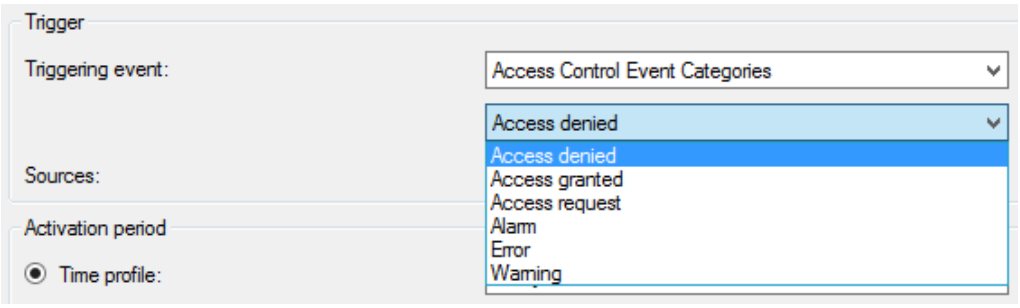


Alarms based on Pro-Watch Access Control events

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 description on how to configure **Alarm Definitions**, see the Milestone XProtect (XProtect Management Client) help.*

3. On the **Properties** 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.

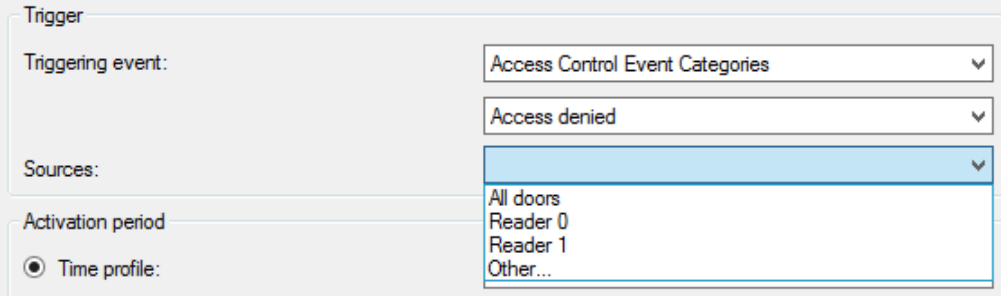


In the example, **Access denied** is selected.

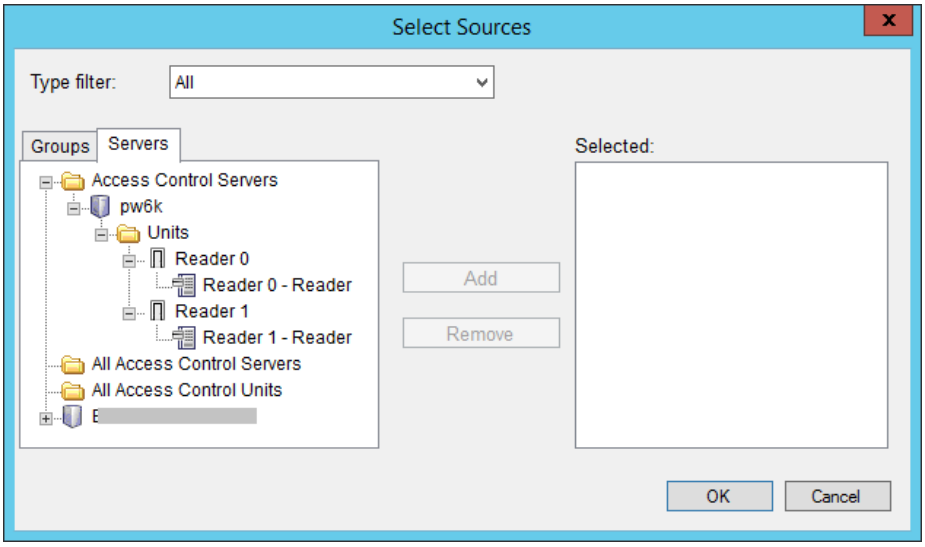
5. From the **Sources** dropdown list, select a proper source depending on the required configuration. The default options are:
   All doors: This option will select all added doors as a source for triggering the alarm.
   <door 1>: This option will select only **door 1** as a source.
   <door 2>: This option will select only **door 2** as a source.
   ..
   <door n>: This option will select only **door n** as a source.
   Other...: This option opens the **Select Sources** dialog. The following three options are available:
   Access Control Servers: This option will list all added access control systems and related access control units.
   All Access Control Servers: This option will select all added access control servers as sources.
   All Access Control Units: This option will select all added access control units as sources.

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

   The following options are available in the example below:
   All doors, Reader 0, Reader 1, Other...

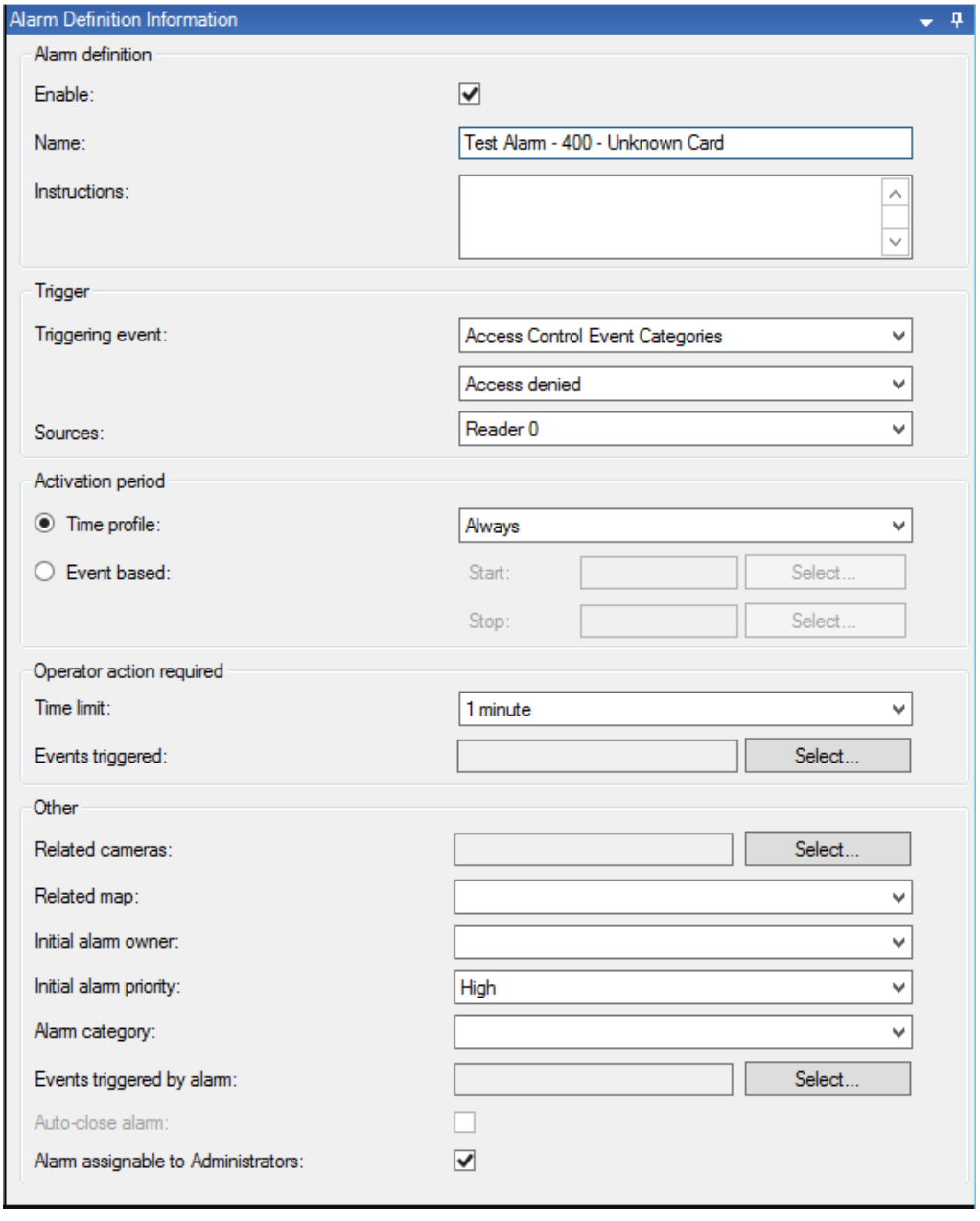


The **Other...** option



Reader 0 from the initial listings is selected in the example above. Click **OK**.

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



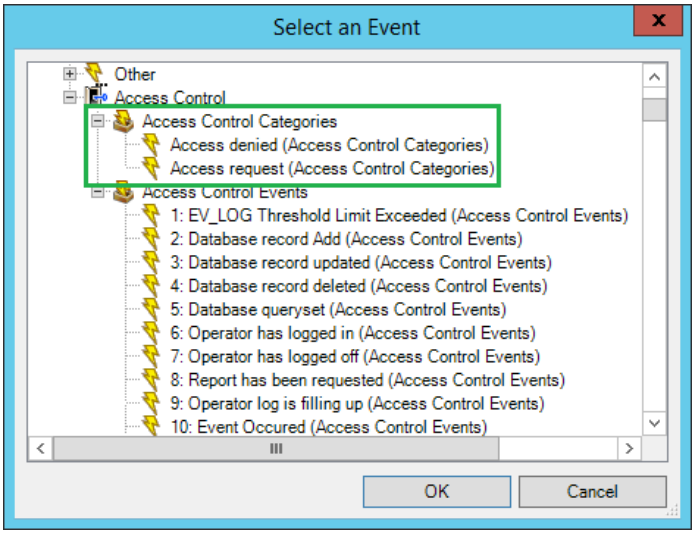
Rules based on Pro-Watch Access Control events

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...**.

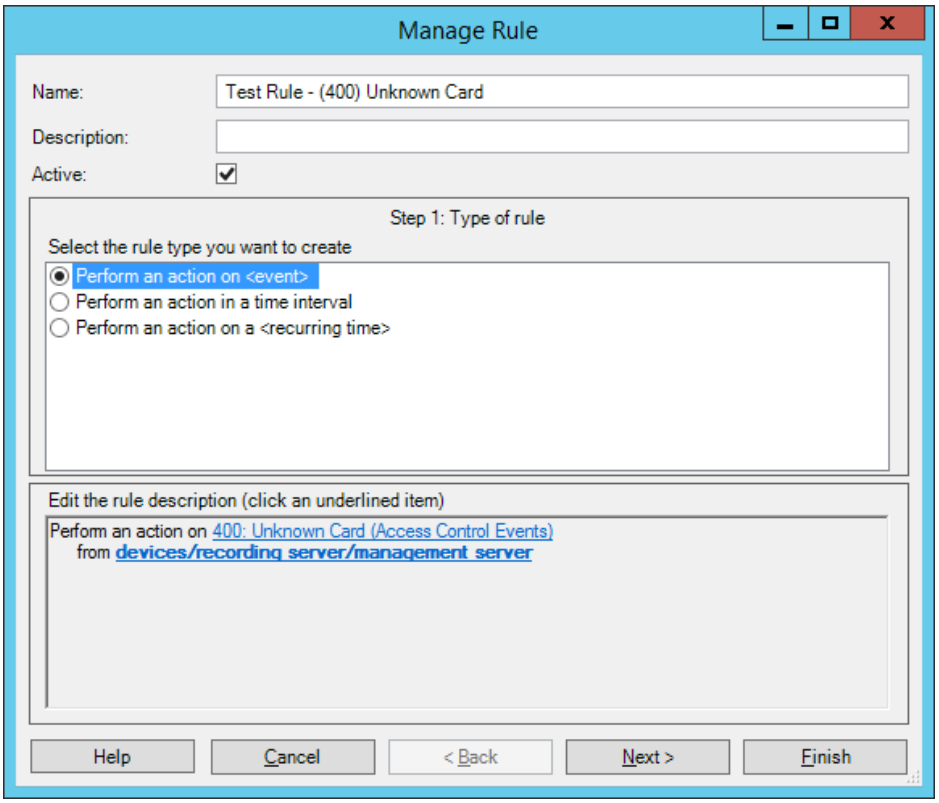
***Note**: For detailed description on how to configure **Rules**, see the Milestone XProtect (XProtect Management Client) help.*

3. In the **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** > **Access Control Events**, and select an event as per your requirements.

***Note**: An **Access Control Categories** root will appear in this tree if an event is assigned to **Event Category** in the Pro-Watch Access Control Properties.*

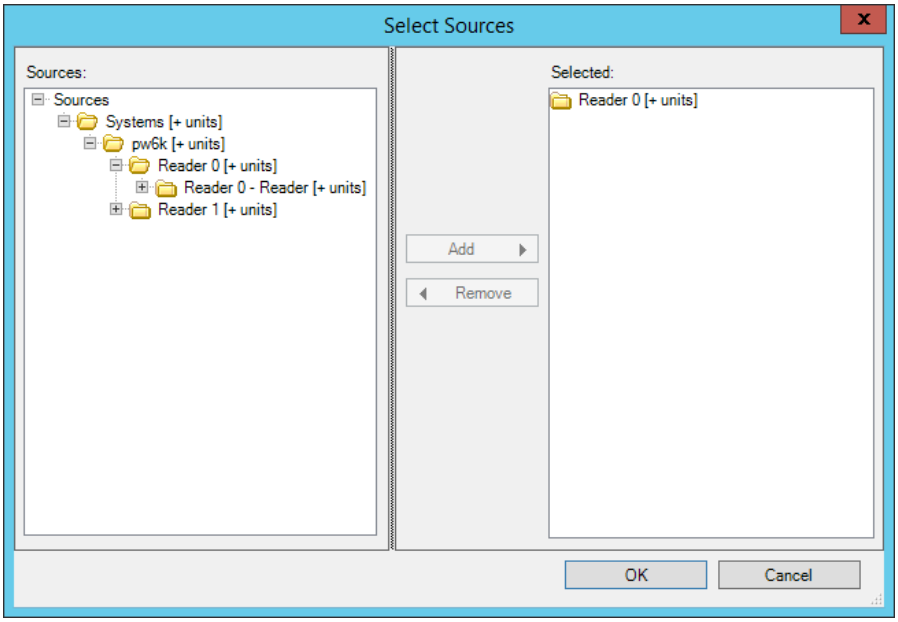


400: Unknown Card (Access Control Events) is selected in the example above. Click **OK**.

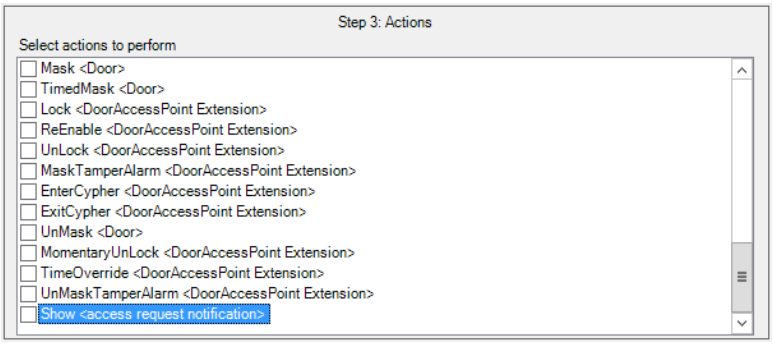


6. In the **Edit the rule description section (click an underlined item)**, click **devices/recording server/management server**.
7. In the **Select Sources** dialog box, select **Systems [+ units]** or expand it, and select devices as per your requirements. Click **OK**.

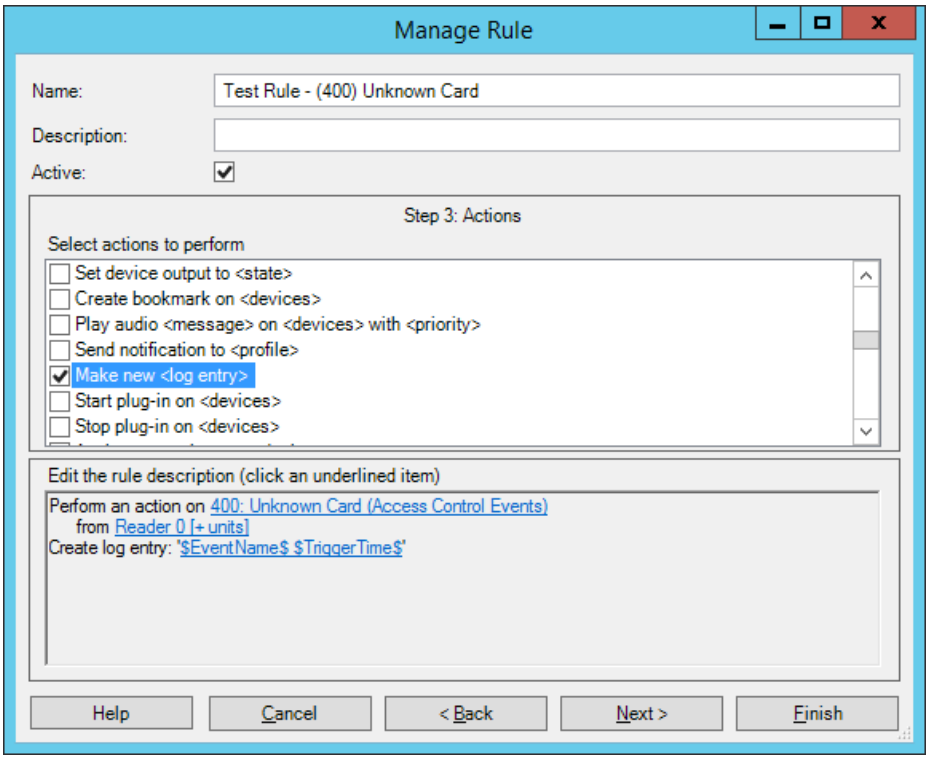
   Reader 0 [+ units] is selected in the example below. Click **OK**.



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):
   Mask <Door>
   TimedMask <Door>
   Lock <DoorAccessPoint Extension>
   ReEnable <DoorAccessPoint Extension>
   UnLock <DoorAccessPoint Extension>
   MaskTamperAlarm <DoorAccessPoint Extension>
   EnterCypher <DoorAccessPoint Extension>
   ExitCypher <DoorAccessPoint Extension>
   UnMask <Door >
   MomentaryUnlock <DoorAccessPoint Extension>
   TimeOverride <DoorAccessPoint Extension>
   UnMaskTamperAlarm <DoorAccessPoint Extension>
   Show <access request notification>



In the example one of the default XProtect actions is selected – **Make new <log entry>** with variables **Reader 0 - $TriggerTime$**. In this way, a new log entry is created in the **Rule-triggered logs** when the event is triggered.



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

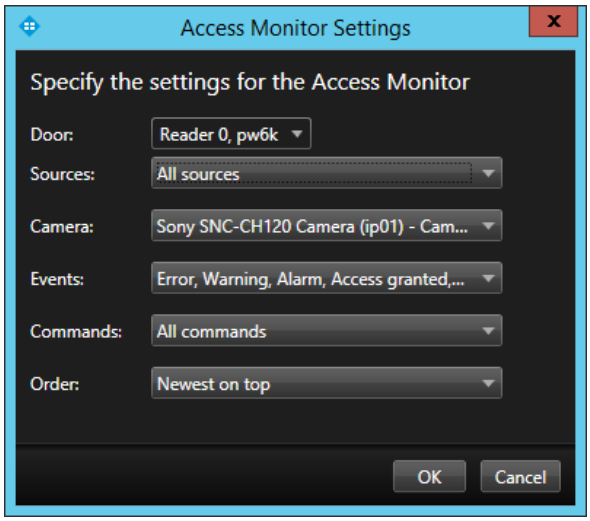
XProtect Smart Client configuration

Add Pro-Watch Access Monitor

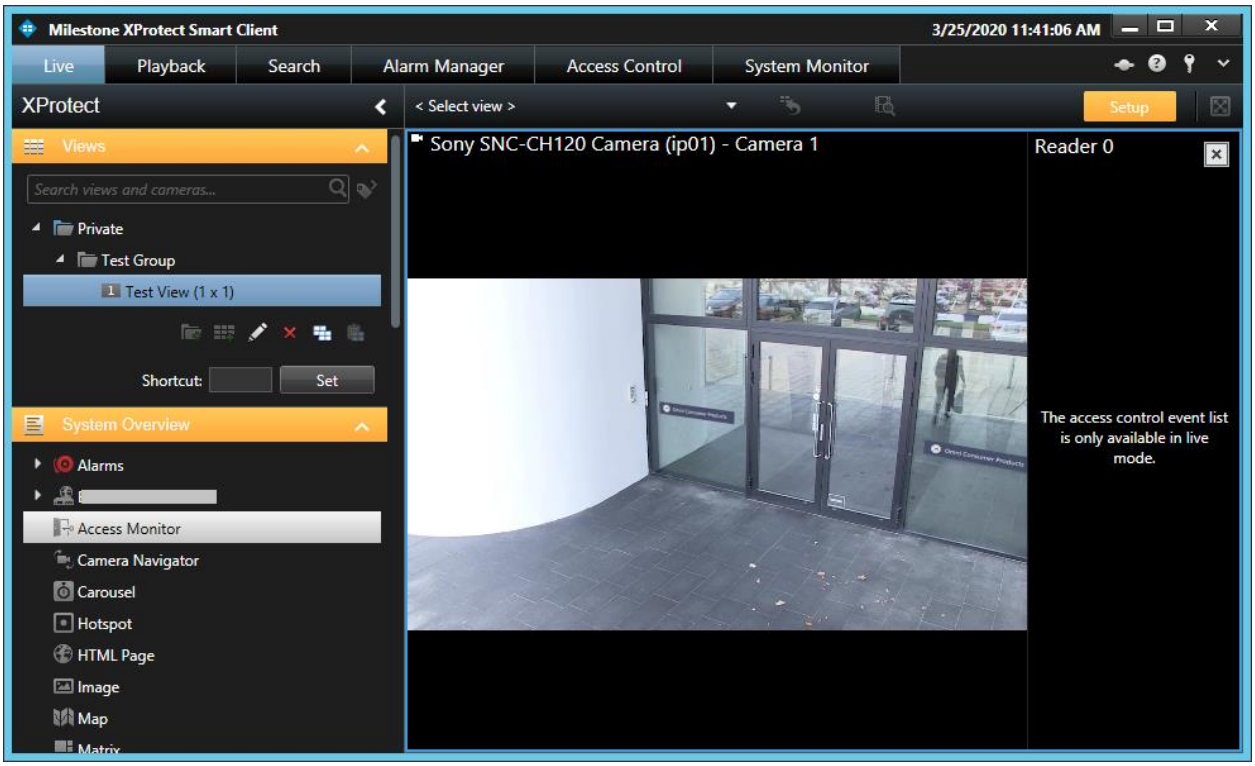
1. Open XProtect Smart Client > **Live** tab.
2. In the upper-right corner, click **Setup**.
3. Add a **Group** and a **View**.

   ***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**.



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.



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

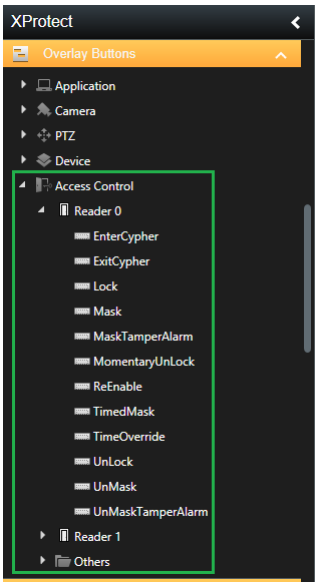
Add Pro-Watch Overlay Buttons

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

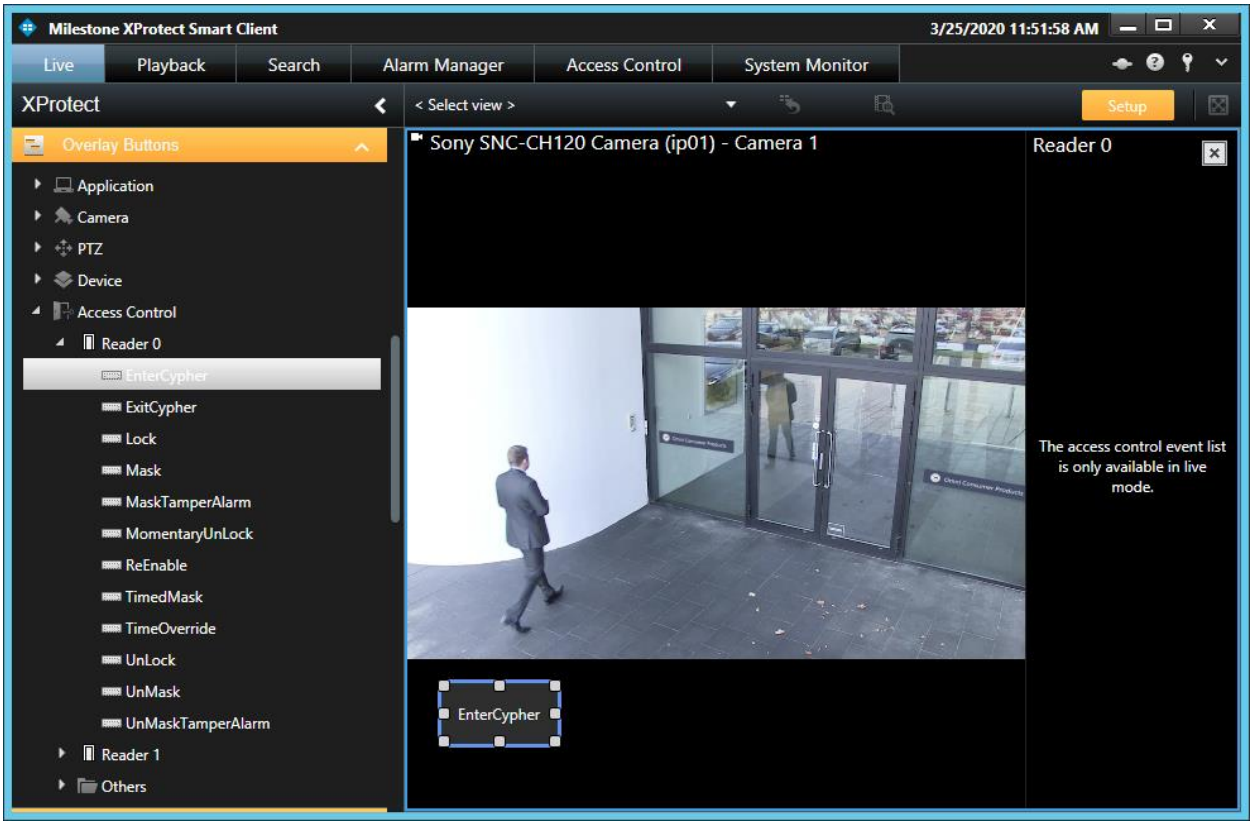
3. Add a **Group** and a **View**.
4. Add a **Camera** or **Access Monitor**

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

5. In the **Overlay Buttons** panel, select and drag the action on the camera position. The following actions related to Pro-Watch doors are available: EnterCypher, ExitCypher, Lock, Mask, MaskTamperAlarm, MomentaryUnlock, ReEnable, TimedMask, TimeOverride, Unlock, UnMask, UnMaskTampterAlarm (These actions were added when Pro-Watch Access Control is added to XProtect).



The **EnterChypher** action for **Reader 0** is added to the camera in the example.



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

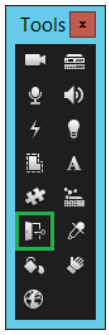
Add Pro-Watch devices point on the map

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

1. Open XProtect Smart Client > **Alarm Manager** tab.
2. Click **Setup** in the upper-right corner.
3. Add a map.

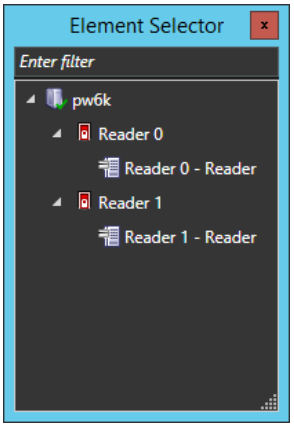
   ***Note**: For detailed description on how to configure **Maps**, see the Milestone XProtect (XProtect Smart Client) help.*

4. Click **Add Access Control** in the **Tools** dialog box.

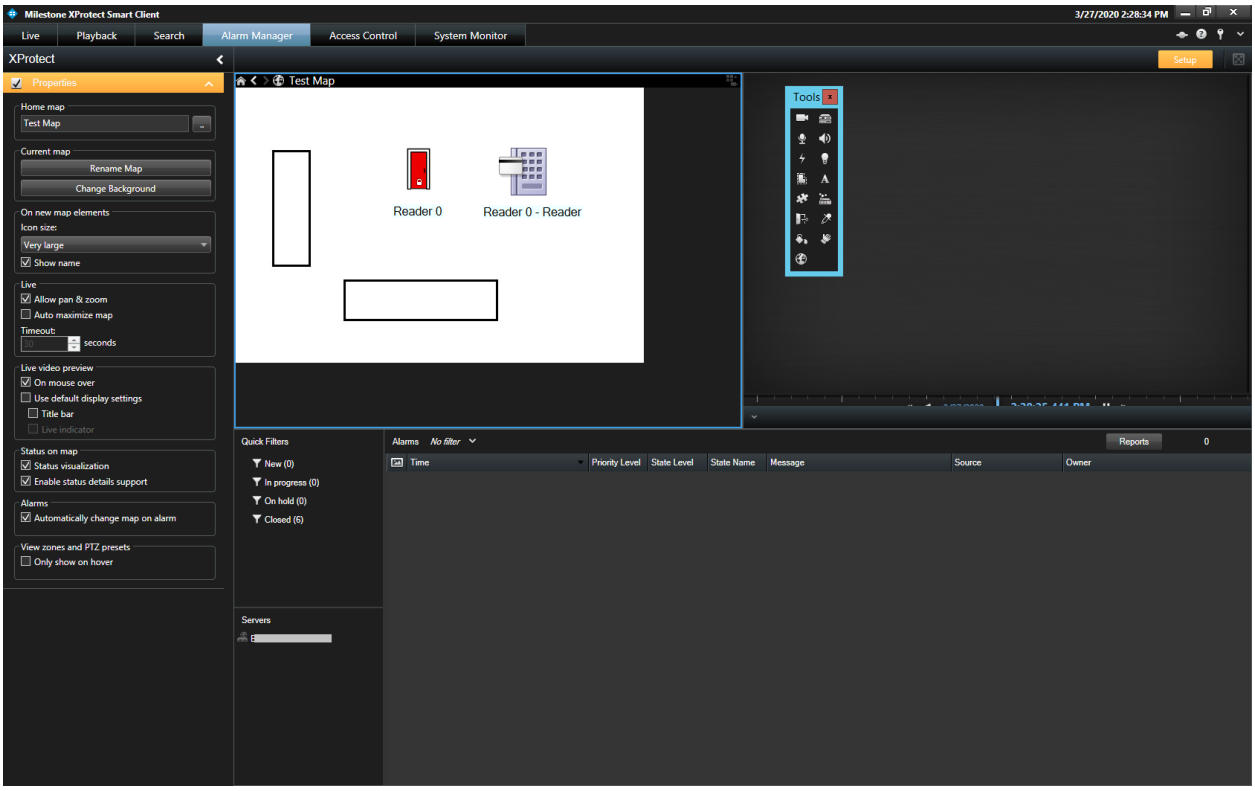


5. In the **Element Selector** dialog box, expand the Pro-Watch access control node. Drag and drop an element (door and/or door access point) from the list to the map depending on the required configuration.

   ***Note**: The panel is not supported.*



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



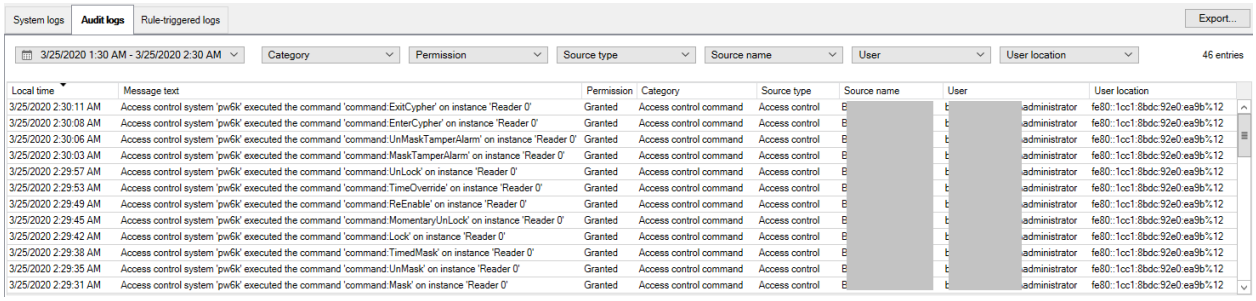
6. Close the **Element Selector** dialog box when you finish adding the Pro-Watch system doors.
7. Click **Setup** in the upper-right corner to complete the map configuration.

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.

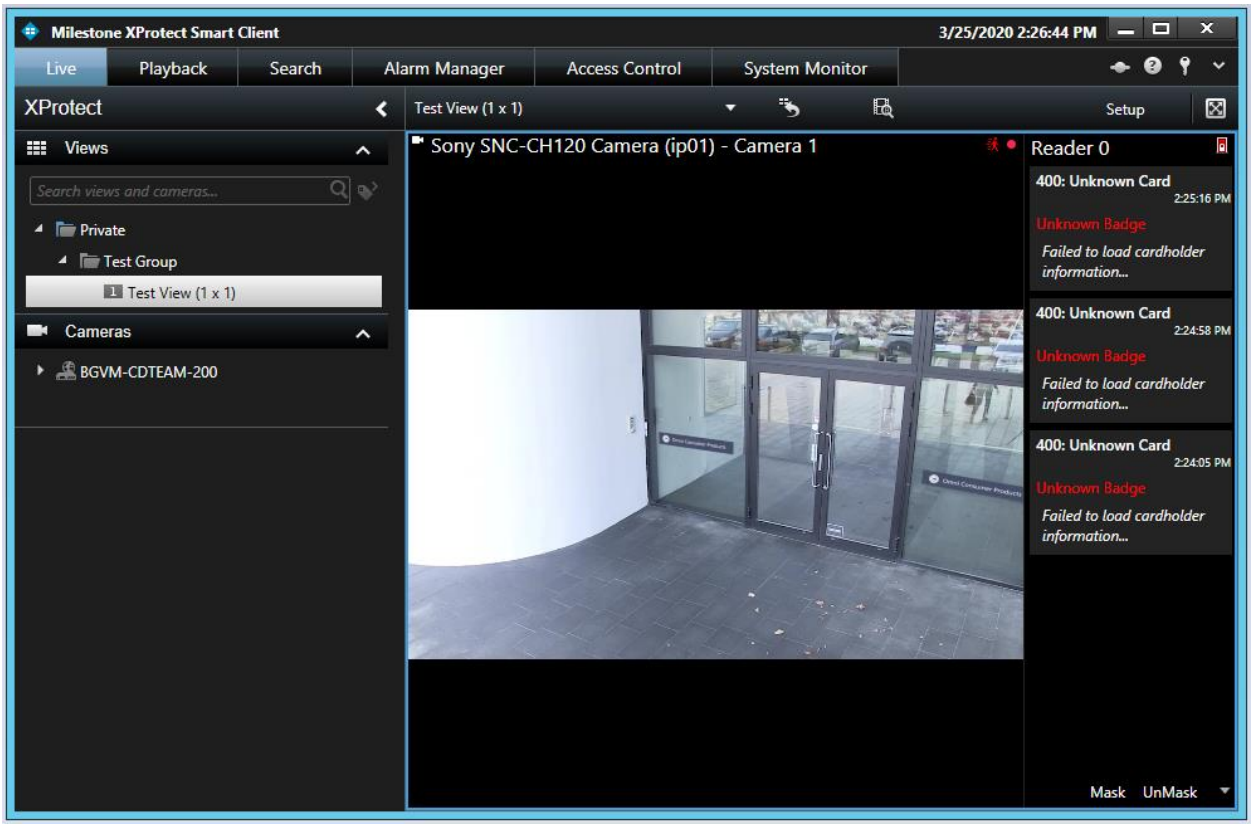
Example:



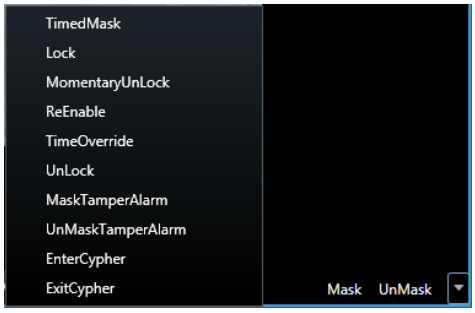
XProtect Smart Client operation

Live tab

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.



A list with available actions is displayed in the bottom-right corner (These actions were added when Pro-Watch Access Control is added to XProtect).

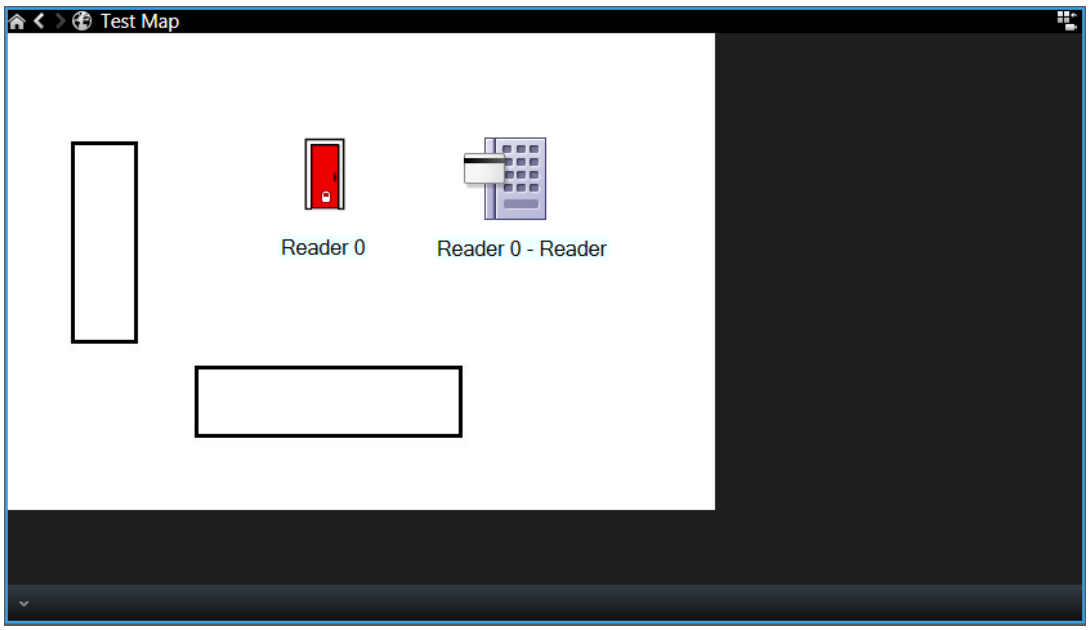


Alarm Manager tab

Pro-Watch devices on the map

Open XProtect Smart Client > **Alarm Manager** tab.
The map in the example shows **Reader 0** and **Reader 0 - Reader** (which were added in chapter XProtect Smart Client configuration - Add Pro-Watch devices on the map)

***Note**: The correctness of the initial state of a door cannot be guaranteed. Initially, it will be set to **Locked**, **Closed**.*

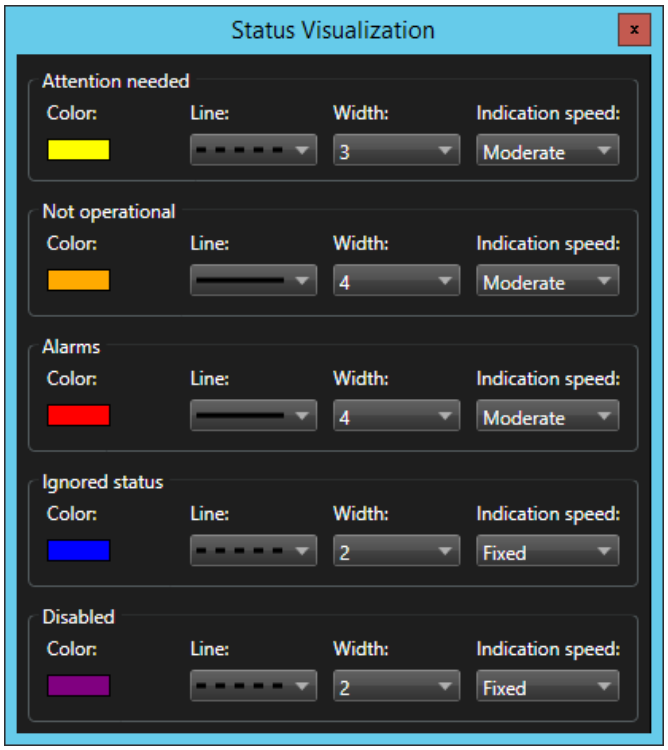


The other default XProtect states for the doors/door access points are described in the following table:

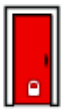
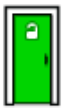
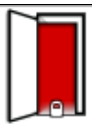
.

State	Description
Attention needed	Currently not supported
Not operational	Currently not supported
Alarms	An alarm involving the 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 (right click on the map in **Setup** mode > **Status Visualization**):



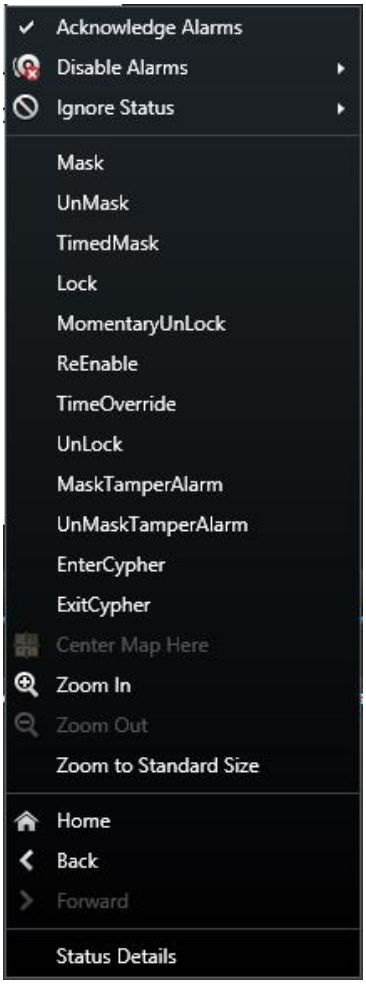
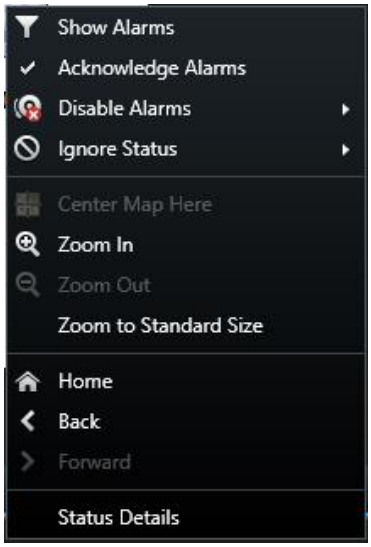
The door states based on the integration are described in the following table:

State	Description
	Locked, Closed
	Unlocked, Closed
	Locked, Open
	Unlocked, Open
	State is not available. That may happen if the door is disabled in XProtect Management Client.

There are not states for the door access points based on the integration.

Context menu

If you right-click on the door/door access point, you will see several standard actions plus the integration specific:

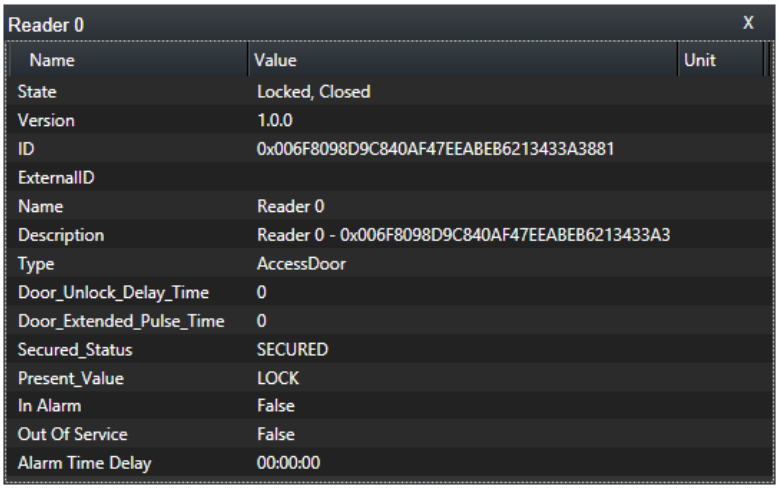
Door (Reader 0)	Door Access Point (Reader 0 - Reader)
	

The most important ones are described in the following table:

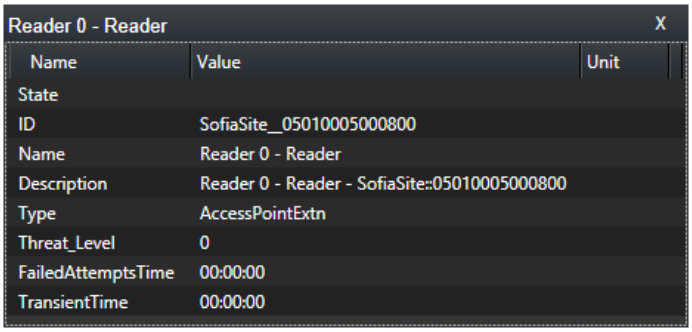
Action	Description	Door	Door Access Point
Acknowledge Alarms	This action changes the **State Name** of an alarm from **New** to **In Progress**.	Available	Available
Disable Alarms	Currently not supported.	Available	Available
Ignore Status	Currently not supported.	Available	Available

Mask, UnMask, TimedMask, Lock, MomentaryUnlock, ReEnable, TimeOverride, UnLock, MaskTamperAlarm, UnMaskTamperAlarm, EnterCypher, ExitCypher	Pro-Watch system actions related to doors (These actions were added when Pro-Watch Access Control is added to XProtect). ***Note**: For detailed description, see the Honeywell Pro-Watch Software Suite v4.5 SP1 help.*	Available	Not Available
Status Details	This action shows the current status of a door, including several properties and their values.	Available	Available

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



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



Alarms

Pro-Watch alarms are only registered when the XProtect Event Server is running, and the integration is loaded. Moreover, the past Pro-Watch alarms cannot be read by the integration. That means that in case

the XProtect Event Server has stopped, the Pro-Watch alarms generated meanwhile will not be shown in XProtect Smart Client and also will not be displayed when the XProtect Event Server is restarted.

Alarms from Pro-Watch that are acknowledged or closed in XProtect Smart Client will also be acknowledged in Pro-Watch. 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.

Access Control tab

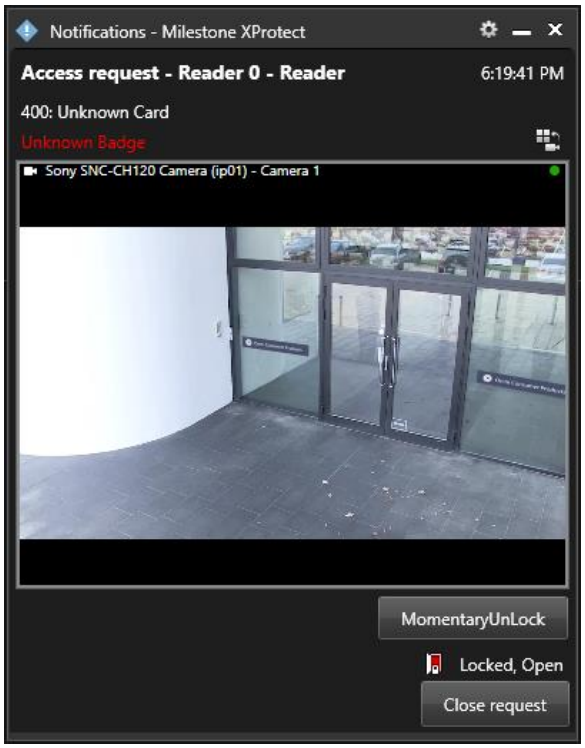
***Note**: For detailed description, see the Milestone XProtect (XProtect Smart Client) help.*

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/door access point)
- Local Time
- Event
- Live video from the associated camera
- A with action
- Actual state of the door
- Button **Close request**

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



Troubleshooting

This section provides information, which helps the administrator solve cases where the integration fails working. For detailed troubleshooting XProtect Event Server and MIP logs should be inspected.

Case: **Honeywell Pro-Watch** 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 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.
Milestone Honeywell Pro-Watch Access Control Integration is not loaded by the XProtect Event Server.	Check the XProtect Event Server log. Look for an entry resembling: "2020-03-25 9:47:48 PM UTC+02:00 Info ESEnvironmentManager Access Control plugin loaded: Honeywell Pro-Watch v2.0a – Milestone A/S" Note that this only occurs while the XProtect Event Server is starting. If no log entries are found, then verify that the plug-in has been installed correctly. It should be typically located in: C:\Program Files \Milestone\MIPPlugins\ProWatchAccessControlPlugin
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.

XProtect Event Server and MIP logs

The Milestone Honeywell Pro-Watch Access Control integration is driven by the XProtect Event Server and initializes whenever the server is restarted. This server produces logging information, which also includes status and error messages from the integration. There are two types of logs:

- **XProtect Event Server logs:** The log files are typically located in the following folder:
  C:\ProgramData\Milestone\XProtect Event Server\logs
  A new log-file is created on a daily basis and is named following this format: ***C<date>.log***. The content of the file can be viewed using a simple text viewer such as Microsoft Notepad

- **MIP logs**: The log files are typically located in the following folder:
  C:\ProgramData\Milestone\XProtect Event Server\logs\MIPLogs
  A new log-file is created on a daily basis and is named following this format: ***MIP<date>.log***. The content of the file can be viewed using a simple text viewer such as Microsoft Notepad.

  Log details
  The level of details being logged in the **MIP logs** can be controlled from the configuration file, which is included with the plug-in. The configuration file is located in:
  C:\ProgramData\Milestone\MIPPlugins\ProWatchAccessControlPlugin\LogLevel.xml

  The file can be edited with a simple text editor such as Microsoft Notepad. The default content of the configuration file is the following:

  <?xml version="1.0" encoding="utf-8" ?>
  <LogLevel>
  Error
  </LogLevel>
  <!-- Possible values: Debug, Warn, Error. Debug = Highest level of logging, Error logs least level -->

  The **LogLevel** parameter value specifies the level of logging information. The possible values are as described: **Debug**, **Warn**, **Error**, where **Debug** gives the most detailed information about the received Pro-Watch events and alarms. This level is not recommended when running in a production environment but is intended for detailed troubleshooting.

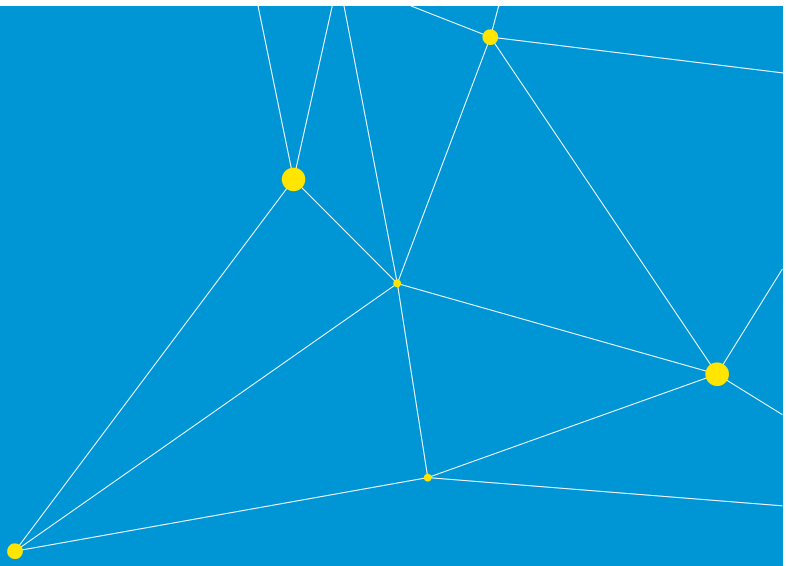
  ***Note**: XProtect Event Server must be restarted in order to load the new configuration whenever changing the value of the parameters.*

Limitations

The Milestone Honeywell Pro-Watch Access Control 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.

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.