MAKE THE
WORLD SEE

Date: 21 May 2020

Manual

Milestone ASSA ABLOY ARX Access Control Integration v1.0

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 and ASSA ABLOY ARX 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 ASSA ABLOY ARX, it is recommended for system administrators to check the following sources of information:

- Milestone XProtect (XProtect Management Client and XProtect Smart Client) help which contains detailed information about XProtect Access
- ASSA ABLOY ARX Installation Guide, LCU9016II/LCU9017II which contains detailed information about installation and configuration of ARX access control system and LCU9016II/LCU9017II hardware
- ASSA ABLOY ARX User Guide v3.1 (i.e. integrated help) which contains detailed information about configuration and use of ARX access control system

and for system operators to check at least:

- Milestone XProtect (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 ASSA ABLOY ARX Access Control Integration is a Milestone XProtect Access plug-in, which supports a number of features including:

- Events generated by doors from ASSA ABLOY ARX 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 (Persons) from ASSA ABLOY ARX access control system are integrated into Milestone XProtect

Solution overview

The integration consists of an XProtect Event Server plug-in which communicates with ARX Server as illustrated here:
<XProtect Event Server> <-> <ARX Server> <-> <ARX control unit>

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

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

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

The integrated features in the XProtect Smart Client include:

- Adding the ARX system doors as Access Monitor for live monitoring of the events
- Adding the ARX system actions as Overlay Buttons
- Map feature integration used for control, monitoring and visual representation of the ARX system doors
- Centralized overview of Events/Doors/Cardholders in Access Control tab
- Access request notifications

Installation

Prerequisites

The Milestone ASSA ABLOY ARX Access Control Integration is compatible with:

- Milestone XProtect Corporate, Expert, Professional+, Express+ and Essential+ 2019 R1 or newer
- ASSA ABLOY ARX v4.1.3

Installer

The Milestone ASSA ABLOY ARX Access Control Integration consists of one installation file supporting Windows 64-bit only:

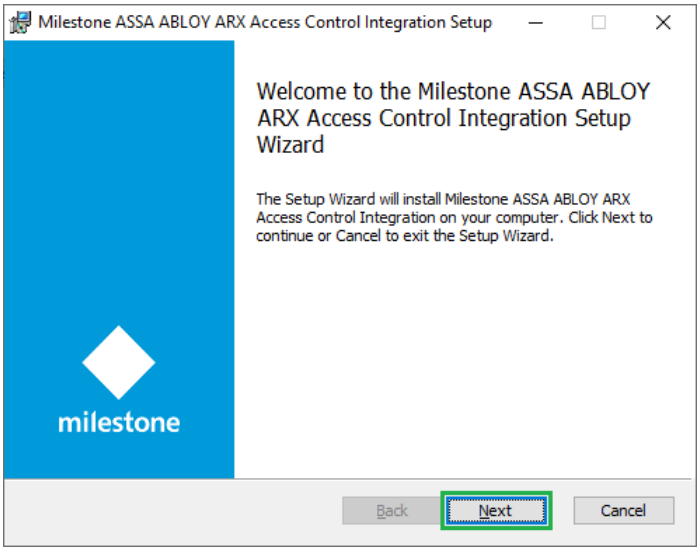
- *AssaAbloyAccessControl_1.0.XX.X.msi*

The Milestone ASSA ABLOY ARX Access Control Integration must be installed on the following computers:

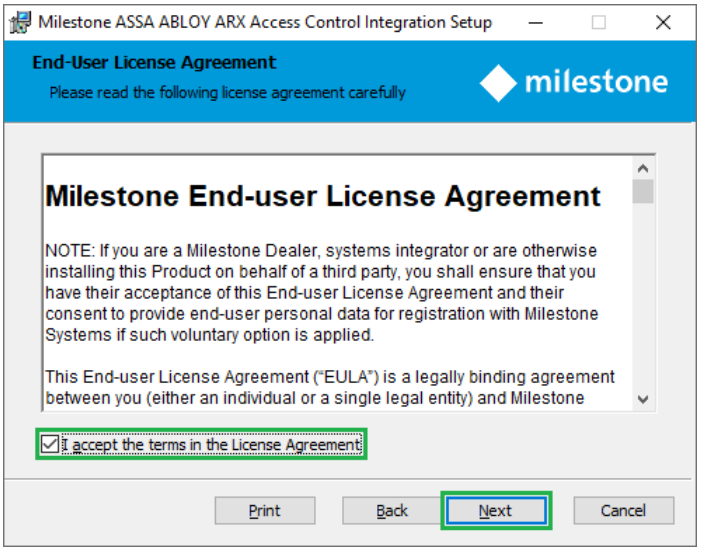
- On the computer where the Milestone XProtect Event Server is installed
- On the computers where the Milestone XProtect Management Client is installed

Installation steps

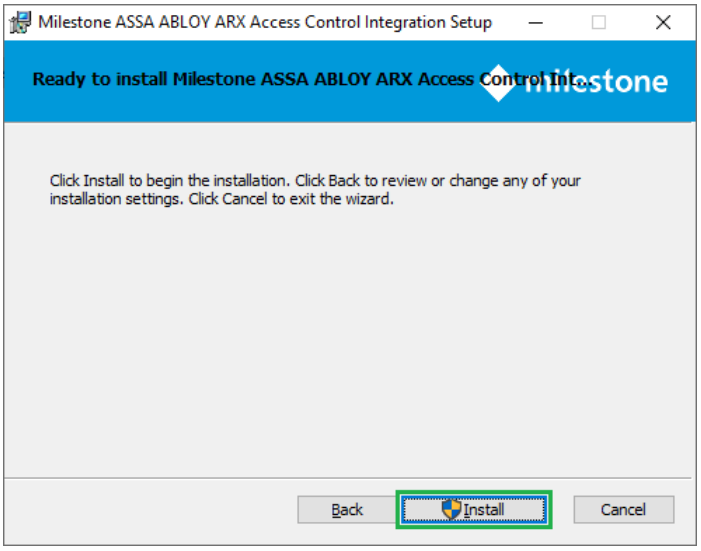
1. Start the installation by executing ***AssaAbloyAccessControl_1.0.XX.X.msi***.
2. Click **Next**.



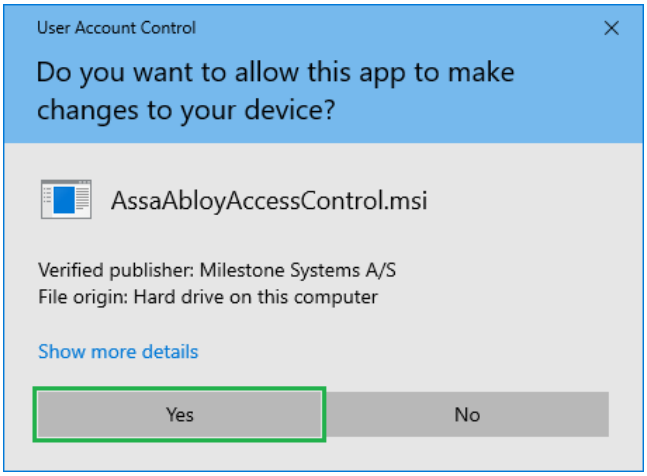
3. Read the license agreement carefully and select the **I accept the terms in the License Agreement** box. Click **Next**.



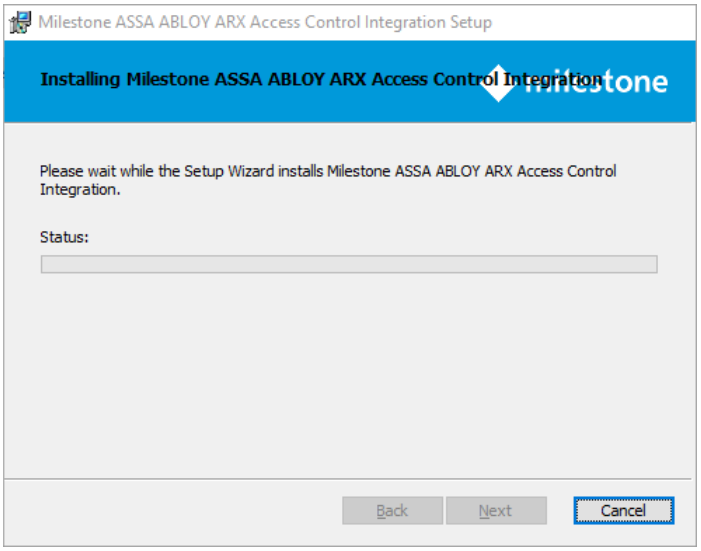
4. Click **Install**.



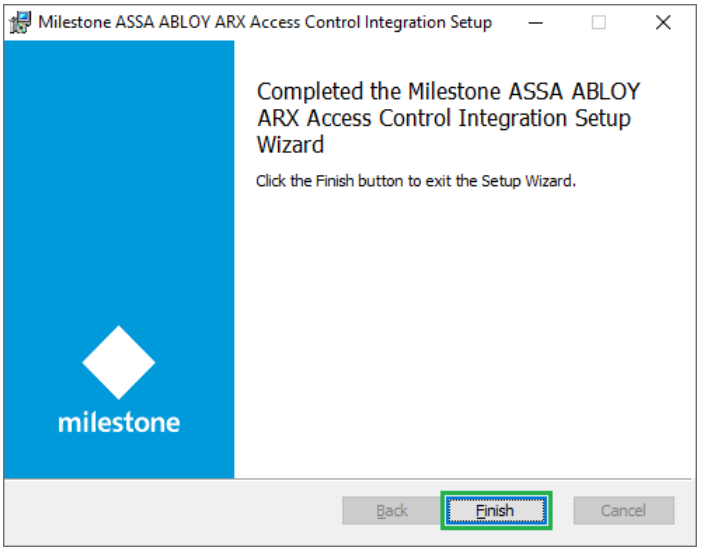
5. Click **Yes**, in case the following message appears on the screen:



6. The next steps are executed automatically.



7. Click **Finish**.



8. 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.

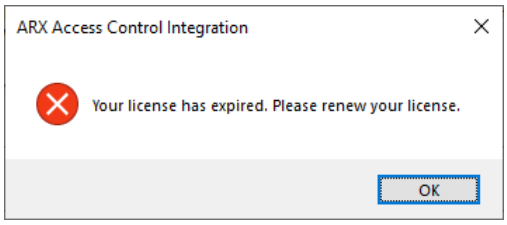
This solution does have also a build-in **MIP** license check that is locked to the software license code (SLC) of the XProtect installation of which it is a part.

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.

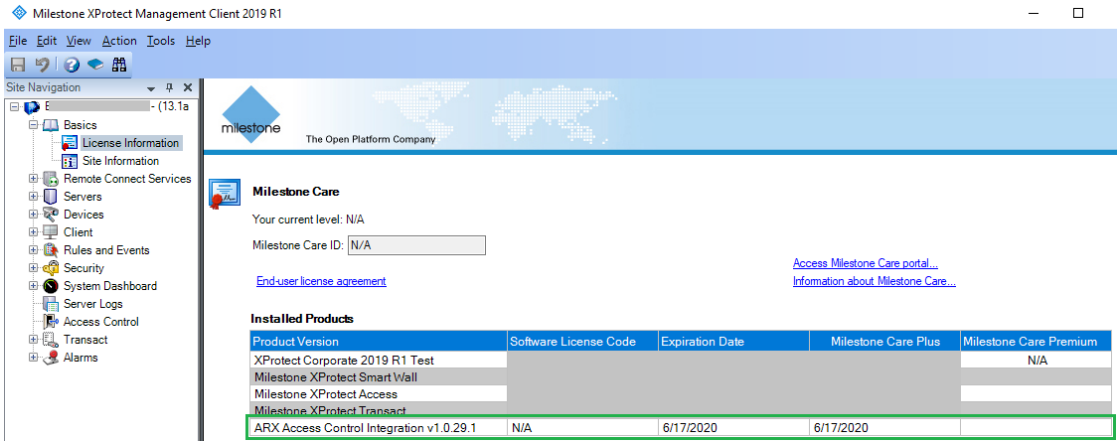
The permanent **MIP** license is free of charge for this solution.

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** > **ARX Access Control Integration v1.0.XX.X**



ARX and XProtect elements mapping

The hierarchy in the ARX system is usually **Installation tree** > **Folder** > **Controller** > **Door**.
Each **Controller** is specified with **Controller type** and **Serial number**.
Each **Door** is specified with **Type of door** and **Address**, and can include several devices like **Connected HI-O nodes** and **Readers**.

An **Area** must be defined in **Access areas** and each door must be added there, based on a **Door Type**.

***Note**: The Milestone ASSA ABLOY ARX Access Control integration supports **Controller type**: **LCU 9016/17 II/II (16 doors)**. The integration may work with **Controllers** based on other **Controller types**, but Custom Development does not guarantee that.*

The table below contains the mapping between the ARX system devices and the XProtect Access devices:

ARX	XProtect Access	Notes
Controller	Controller	• Visible in XProtect Management Client • Visible in XProtect Smart Client • Events are not supported
Door	Door	• Visible in XProtect Management Client • Visible in XProtect Smart Client • Events are supported • Actions from the ARX system are transferred into actions in the XProtect system
Connected HI-O nodes (Keypad Reader)	N/A	• Not visible in XProtect Management Client • Not visible in XProtect Smart Client
Reader	Door Access Point	• Visible in XProtect Management Client • Camera (s) can be associated with each Door Access Point • Visible in XProtect Smart Client • Events are not supported

The table below contains the mapping between the ARX system events and the XProtect Access events:

ARX	XProtect Access
controller.access.card.duress	Access Card Duress
controller.access.card.invalid.door	Access Card Invalid Door
controller.access.card.invalid.format	Access Card Invalid Format
controller.access.card.invalid.inhibited	Access Card Invalid Inhibited
controller.access.card.invalid.operatorcontrol	Access Card Invalid Operator Control
controller.access.card.invalid.pin	Access Card Invalid Pin
controller.access.card.invalid.pinattempts	Access Card Invalid Pin Attempts

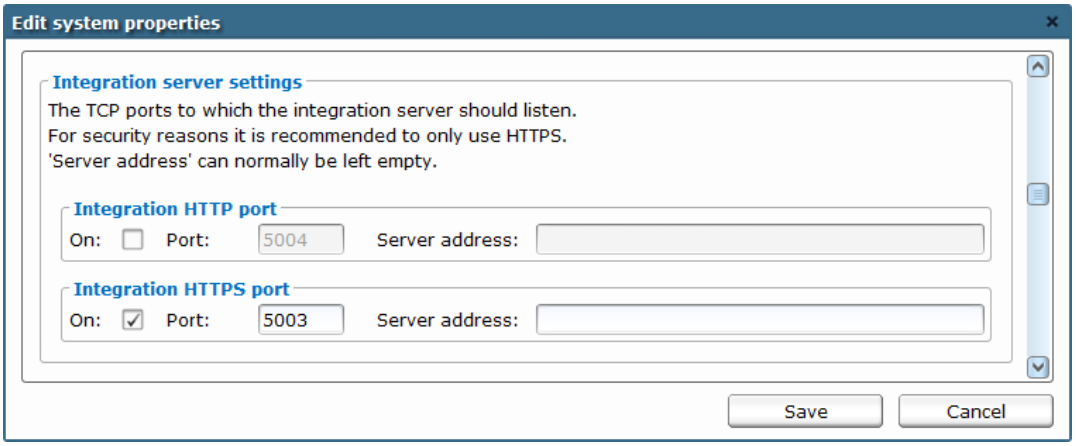
controller.access.card.invalid.pintimeout	Access Card Invalid Pin Timeout
controller.access.card.invalid.schedule	Access Card Invalid Schedule
controller.access.card.invalid.standard	Access Card Invalid Standard
controller.access.card.invalid.areaarmed	Access Card Invalid Area Armed
controller.access.card.invalid.time.antipassback	Access Card Invalid Anti-passback
controller.access.card.pinrequest	Access Card Pin Request
controller.access.card.valid.standard	Access Card Valid Standard
controller.notification.tamper.active	Tamper Notification Active
controller.notification.tamper.restored	Tamper Notification Restored
controller.dac.tamper.active	Dac Tamper Active
controller.dac.tamper.restored	Dac Tamper Restored
controller.door.closed	Door Closed
controller.door.forcedopen	Door Forced Open
controller.door.lock	Door Lock
controller.door.notclosed	Door Not Closed
controller.door.opened	Door Opened
controller.door.pulseopenrequest	Door Pulse Open Request
controller.door.requesttoexit	Door Request to Exit
controller.door.unlock	Door Unlock
controller.door.pulseopen	Door Pulse Open
controller.door.forcedlock	Door Forced Lock
controller.door.forcedunlock	Door Forced Unlock
controller.door.mode.access.accessinhibited	Door Mode Access (Access) Inhibited
controller.door.mode.access.dualcardsrequired	Door Mode Access Dual Cards Required
controller.door.mode.access.modepinrequired	Door Mode Access Mode Pin Required
controller.door.mode.access.pincardnumber	Door Mode Access Pin Card Number
controller.door.mode.access.pinonlyallowed	Door Mode Access Pin Only Allowed
controller.door.mode.maintainedlock	Door Mode Maintained Lock
controller.door.mode.maintainedunlock	Door Mode Maintained Unlock
controller.door.mode.unlocked	Door Mode Unlocked
controller.door.mode.locked	Door Mode Locked
controller.door.motorlock.daylocked	Door Motorlock Day Locked
controller.door.motorlock.error.failedtolock	Door Motorlock Error Failed to Lock
controller.door.motorlock.error.failedtounlock	Door Motorlock Error Failed to Unlock
controller.door.motorlock.error.problematlock	Door Motorlock Error Problem at Lock
controller.door.motorlock.error.problematunlock	Door Motorlock Error Problem at Unlock
controller.door.motorlock.locked	Door Motorlock Locked
controller.door.motorlock.unlocked	Door Motorlock Unlocked
acs.door.forcedblockon	Door Forced Block On
acs.door.forcedblockoff	Door Forced Block Off
acs.door.forcedopenon	Door Forced Open On
acs.door.forcedopenoff	Door Forced Open Off
acs.dac.update	Dac Update

ARX configuration

ARX Server

1. Enable **Integration HTTPS port**. By default, it is **5003**.

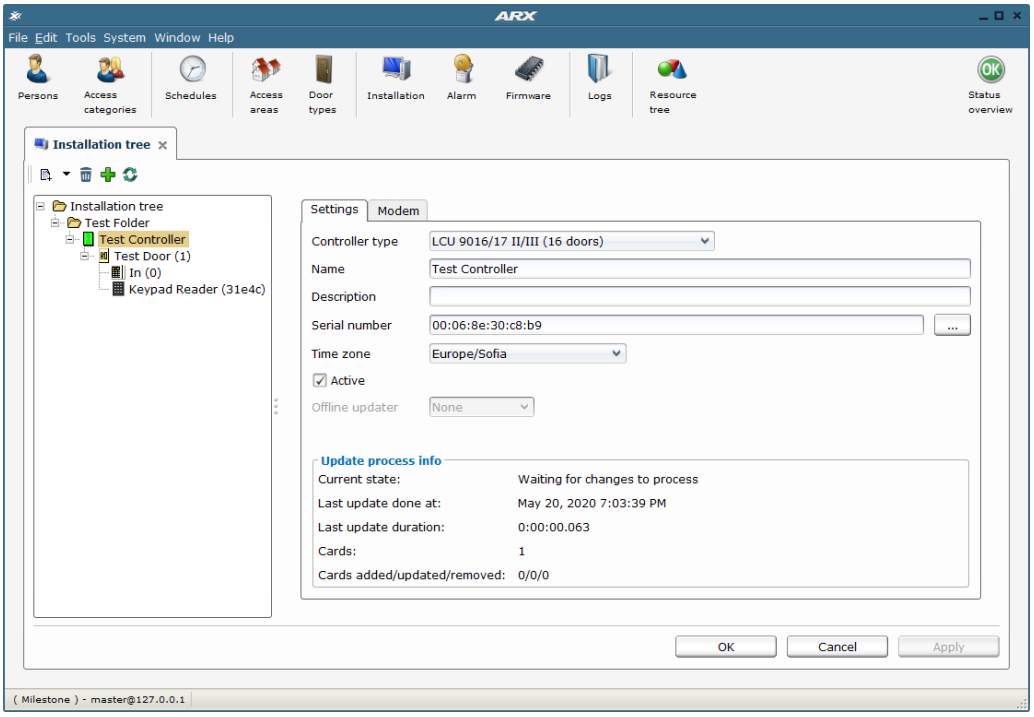
   ***Note**: Only **HTTPS** communication is supported between ARX Server and XProtect Access.*



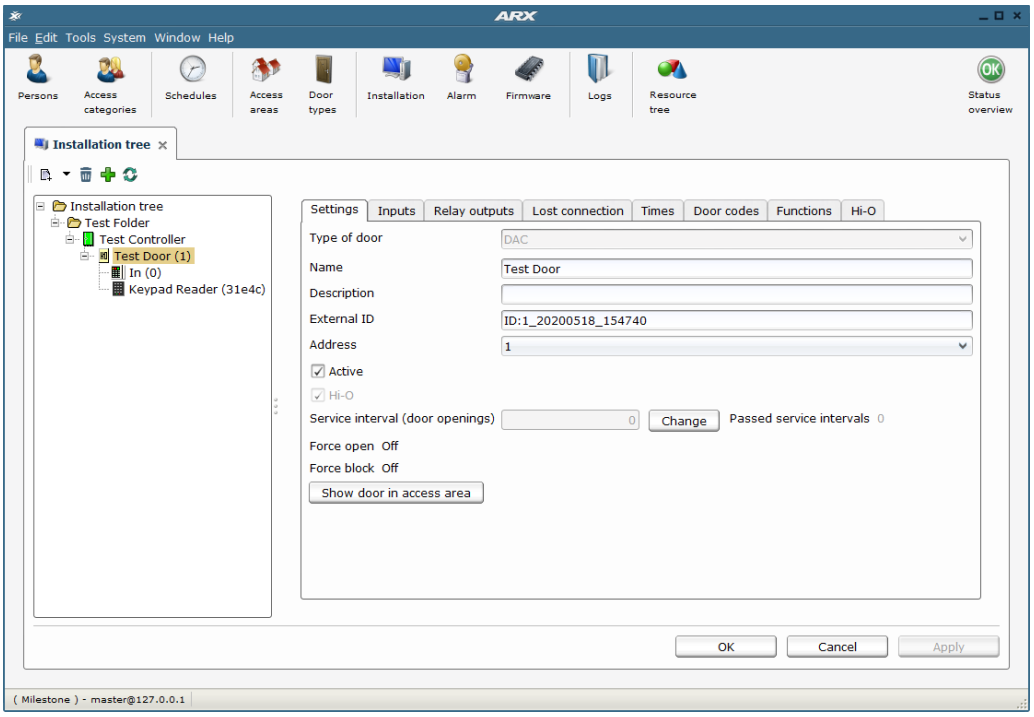
ARX Client

1. Connect the ARX control unit to the network and turn it on.
   In the example below, an **LCU 9016/17 II/III (16 doors)** control unit is used.
2. Create a **Folder** and then add a **Controller**, a **Door**, and **Connected HI-O nodes**.
   In the example below:
   Test Folder is created.

Test Controller is added (**Controller type**: **LCU 9016/17 II/III (16 doors)**).



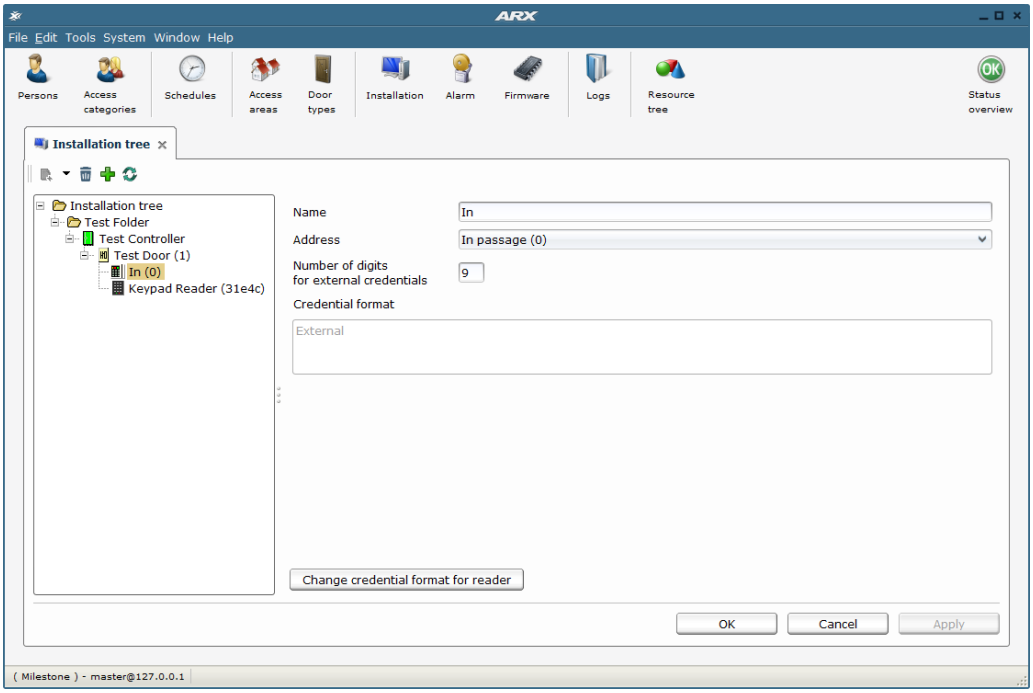
Test Door is added (**Type of door**: **DAC**).



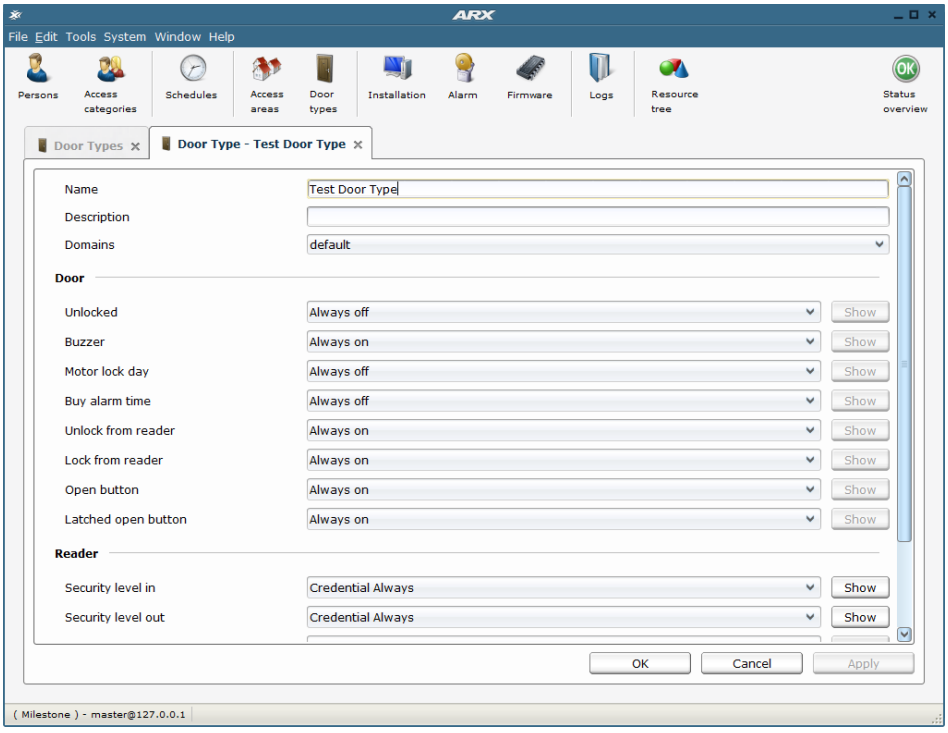
Connected HI-O nodes:

In (0) is added (**Credential format**: **External**).

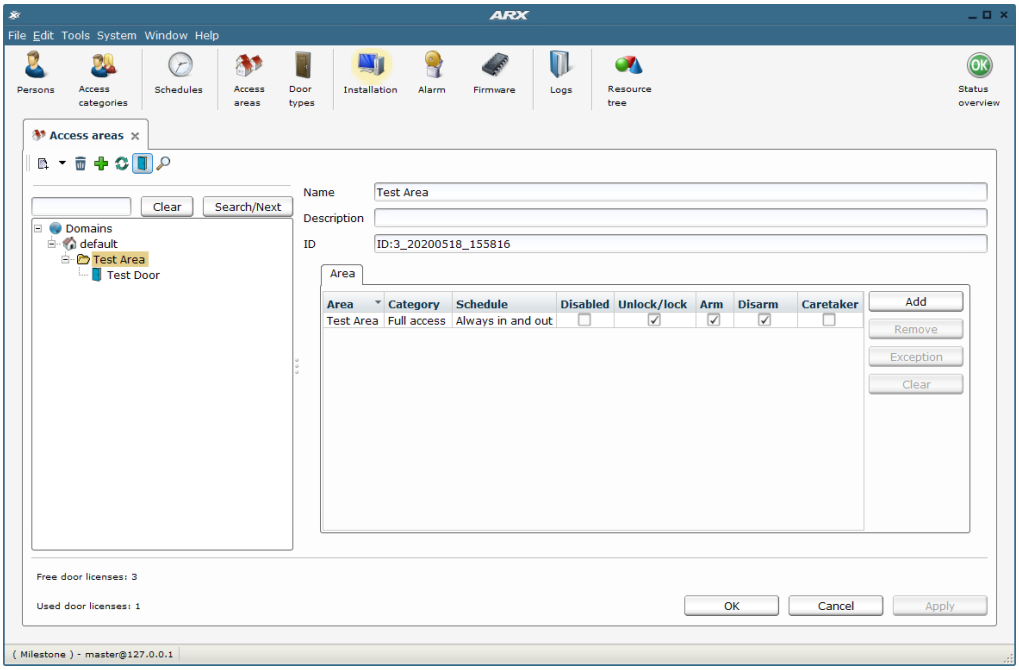
Keypad Reader (31e4c) is added.



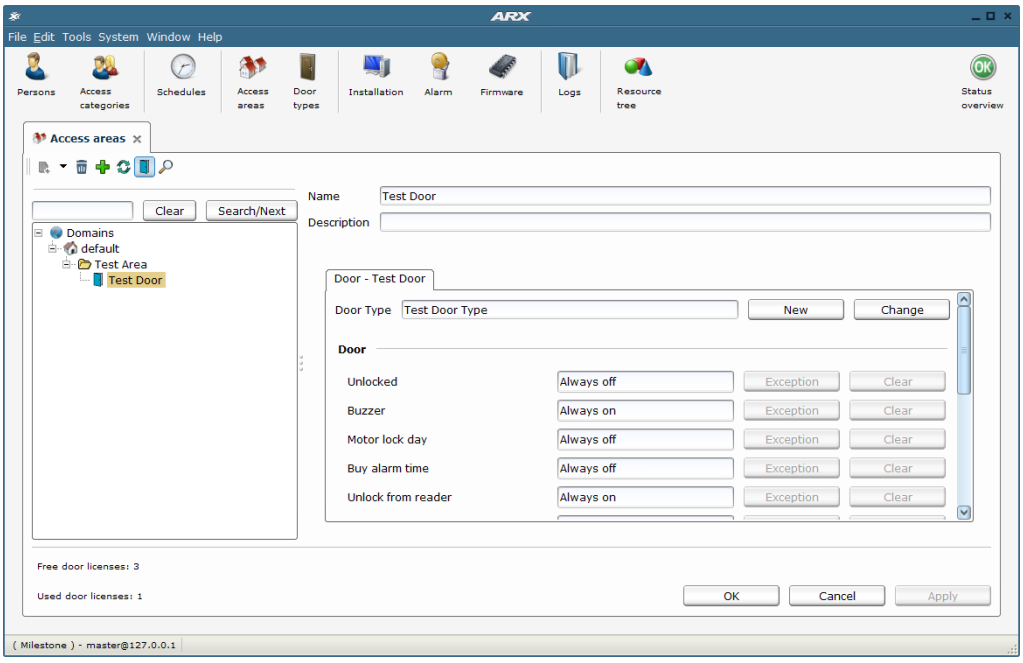
3. Create a **Door type**.
   In the example below, **Test Door Type** is created:



4. Create an **Access area** and add a **Door**.
   In the example below:
   Test Area is created.

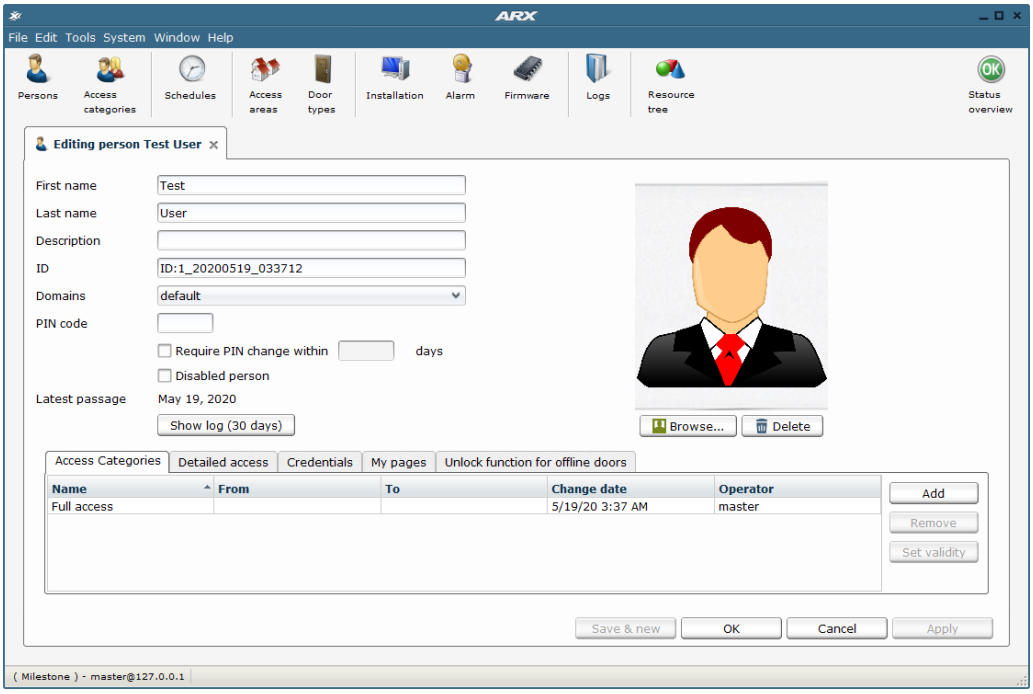


Test Door is added (**Door Type**: **Test Door Type**).

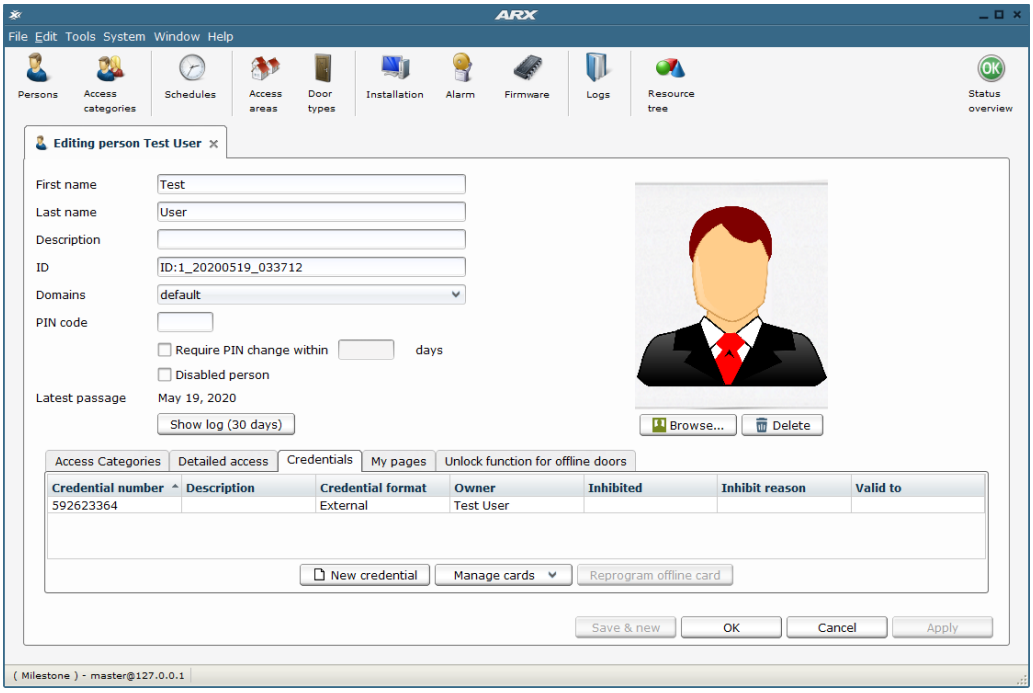


5. Create a **Person**.
   In the example below, **Test User** is created:

Access Categories tab:



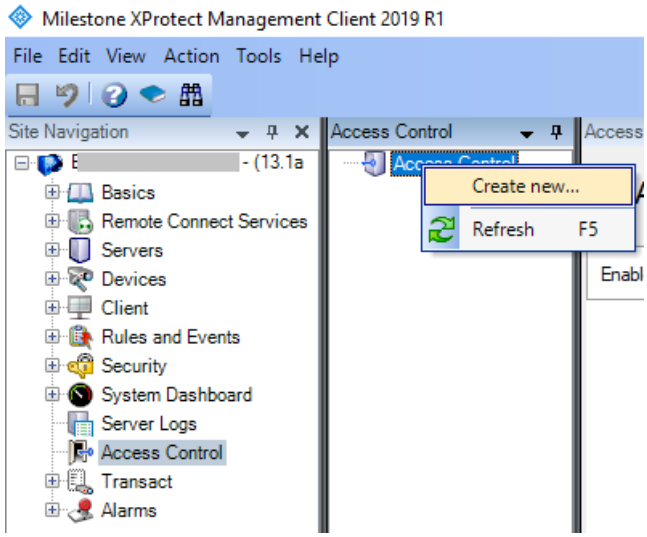
Credentials tab:



XProtect Management Client configuration

Add ARX 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 **ARX Access Control Integration** from the **Integration plug-in** dropdown. The following connection details appear and need to be specified:

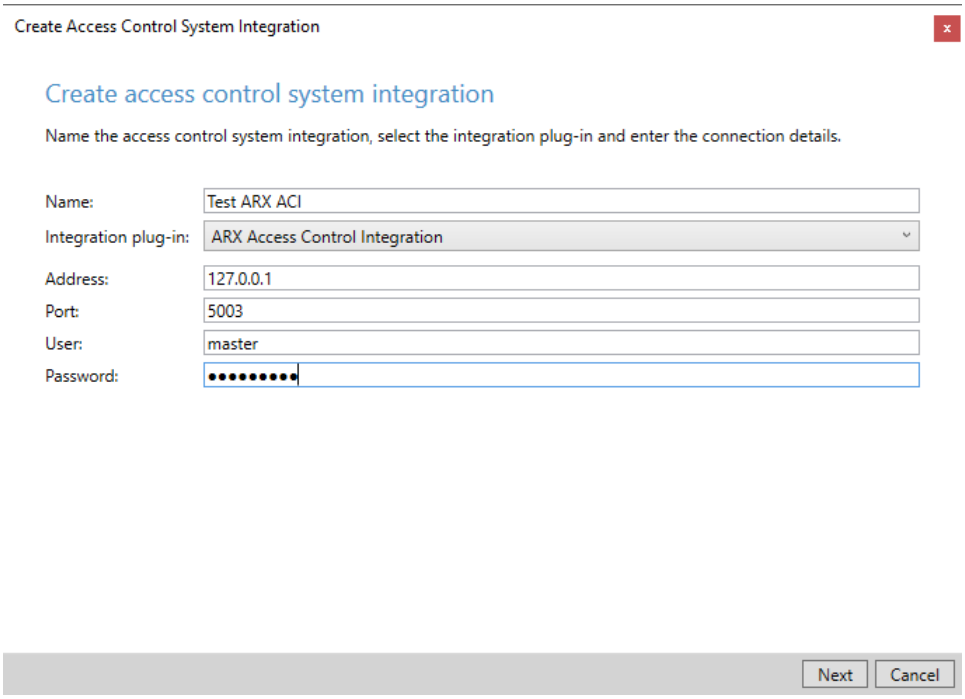
   Address: The IP address of the **ARX Server**.

   Port: The **Integration HTTPS port** number of **ARX Server** from subchapter ARX Server.

   User: The user with the administrative rights for the ARX system.

   Password: The password of the user.

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 ARX system:

Example:

In the example below, the following items are added:

Doors (1):

Test Door

Units (3): The units which are related to the added doors.

Controller: 1

Entry: Test Door

Exit: Test Door

Servers (1):

ARX System on 127.0.0.1

Events (50): A list with supported events.

1	Access Card Duress	26	Door Unlock
2	Access Card Invalid Door	27	Door Pulse Open
3	Access Card Invalid Format	28	Door Forced Lock
4	Access Card Invalid Inhibited	29	Door Forced Unlock
5	Access Card Invalid Operator Control	30	Door Mode Access (Access) Inhibited
6	Access Card Invalid Pin	31	Door Mode Access Dual Cards Required
7	Access Card Invalid Pin Attempts	32	Door Mode Access Mode Pin Required

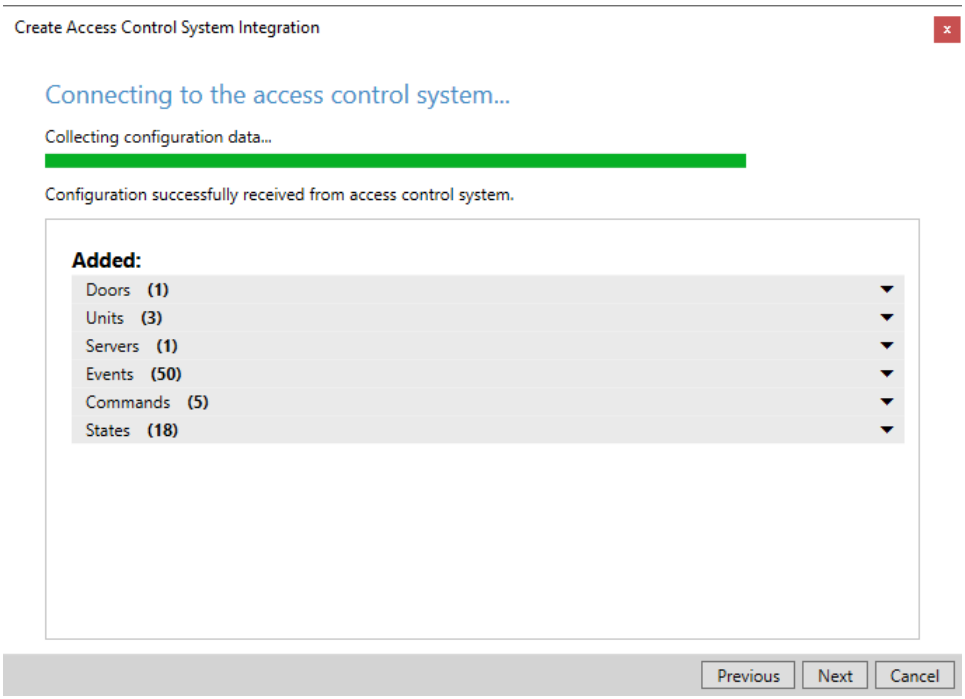
8	Access Card Invalid Pin Timeout	33	Door Mode Access Pin Card Number
9	Access Card Invalid Schedule	34	Door Mode Access Pin Only Allowed
10	Access Card Invalid Standard	35	Door Mode Maintained Lock
11	Access Card Invalid Area Armed	36	Door Mode Maintained Unlock
12	Access Card Invalid Anti-passback	37	Door Mode Unlocked
13	Access Card Pin Request	38	Door Mode Locked
14	Access Card Valid Standard	39	Door Motorlock Day Locked
15	Tamper Notification Active	40	Door Motorlock Error Failed to Lock
16	Tamper Notification Restored	41	Door Motorlock Error Failed to Unlock
17	Dac Tamper Active	42	Door Motorlock Error Problem at Lock
18	Dac Tamper Restored	43	Door Motorlock Error Problem at Unlock
19	Door Closed	44	Door Motorlock Locked
20	Door Forced Open	45	Door Motorlock Unlocked
21	Door Lock	46	Door Forced Block On
22	Door Not Closed	47	Door Forced Block Off
23	Door Opened	48	Door Forced Open On
24	Door Pulse Open Request	49	Door Forced Open Off
25	Door Request to Exit	50	Dac Update

Commands (5): A list of supported actions (commands) for the doors added:

Pulse Open
Force Open On,
Force Open Off
Force Close On
Force Close Off

States (18): A list of supported states for the added doors and panel:

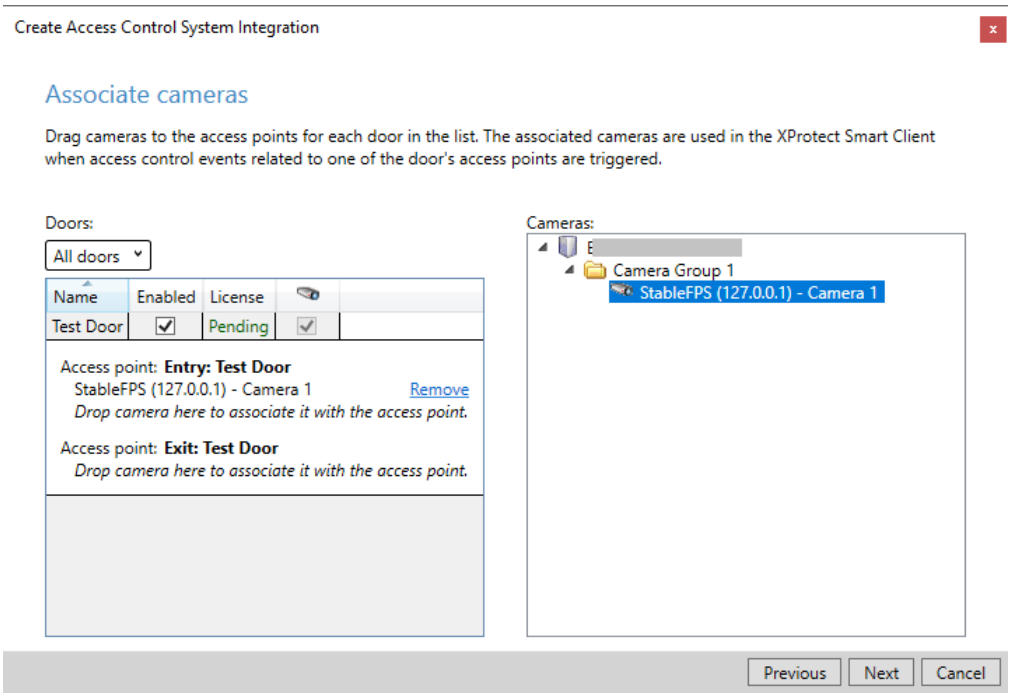
1	Open State: Open	10	Locked State: Tub Turned
2	Open State: Closed	11	Locked State: Communication Failure
3	Open State: Unknown	12	Locked State: Day Locked
4	Open State: Open too Long	13	Locked State: Failed to Lock
5	Open State: Forced Open	14	Locked State: Failed to Unlock
6	Locked State: Unknown	15	Locked State: Locked - Force Close On
7	Locked State: Unlocked	16	Locked State: Unlocked - Force Open On
8	Locked State: Locked	17	Connected
9	Locked State: Security Locked	18	Disconnected



Click **Next**.

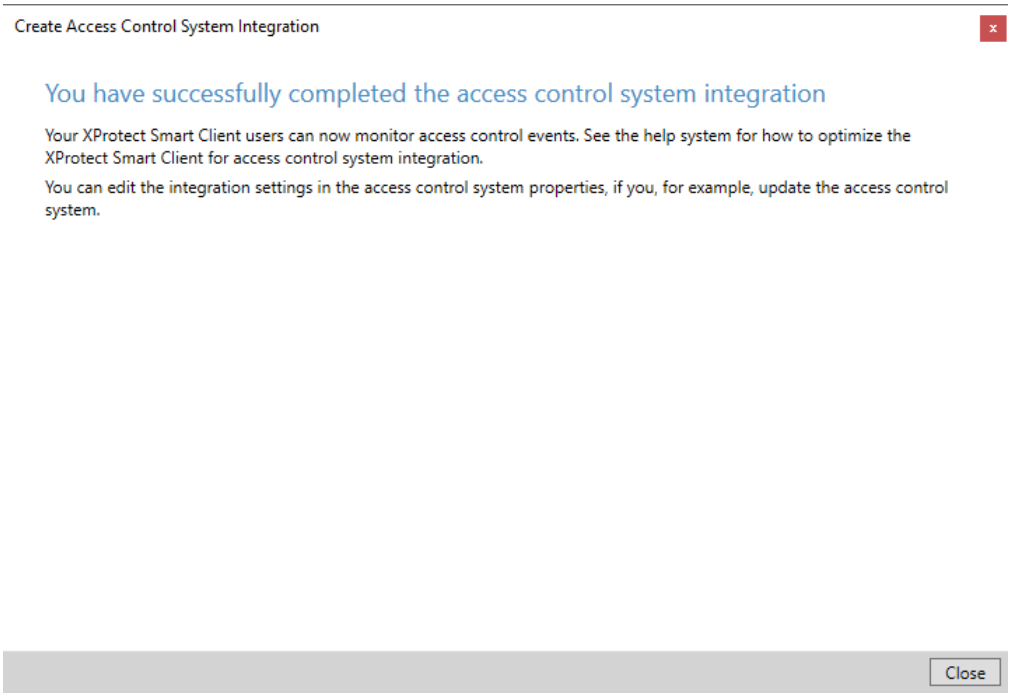
5. (Optional) Drag and drop cameras to the door access points for each door in the list. The associated cameras are used in XProtect Smart Client when access control events related to each door are triggered.

   In this example, **StableFPS (127.0.0.1) – Camera 1** is associated to **Entry: Test Door**.



Click **Next**.

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



Remove ARX 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.

ARX Access Control Properties

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

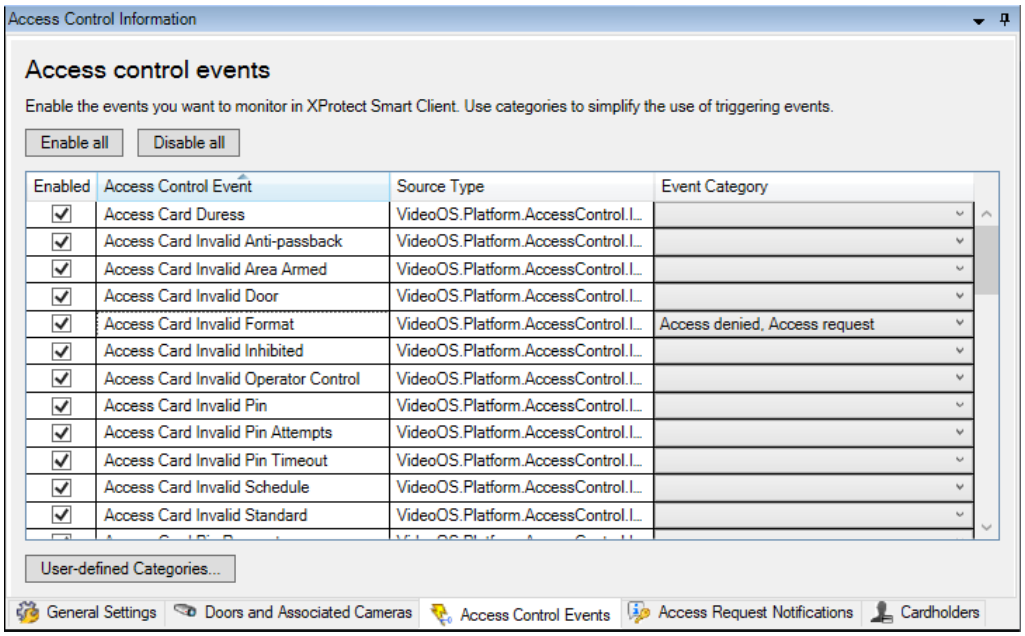
General Settings tab

***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 **Access Card Invalid Format** in this example as this access control event will be used in chapters Alarms based on ARX Access Control events and Access request notifications.



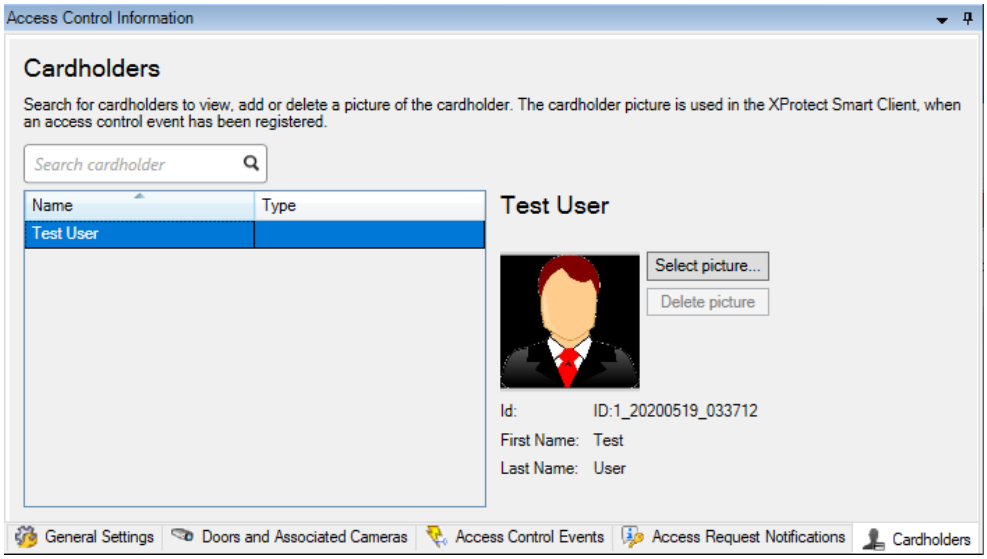
Access Request Notifications tab

***Notes**: By default, **Access denied** is associated with **Access request**.*

Cardholders tab

Badge holders (i.e. **Persons**) from the ARX 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.

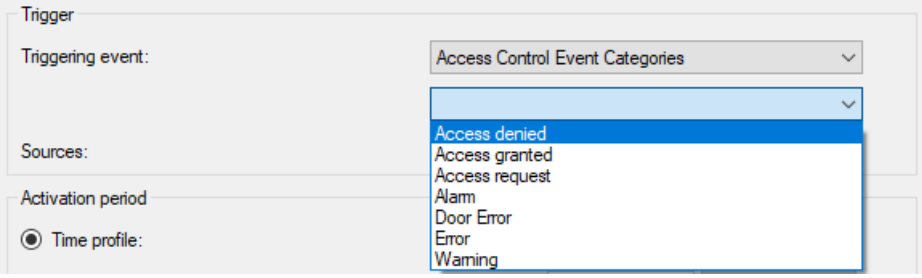


Alarms based on ARX Access Control events

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.*

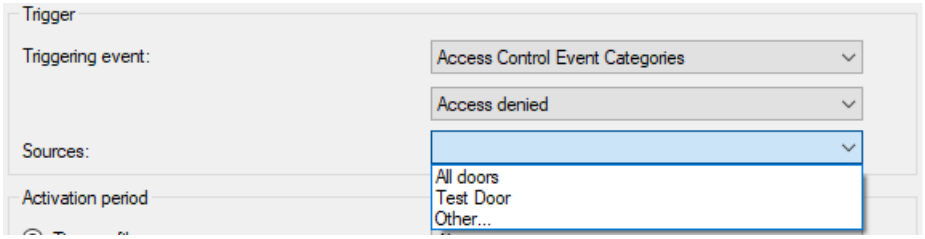
3. On the **Properties** page, locate the group of settings called **Trigger**.
4. Specify the **Triggering event** by selecting from the top dropdown list the **Access Control Event Categories** event group, and from the next dropdown list, select the appropriate **Event Category**. The default **Event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



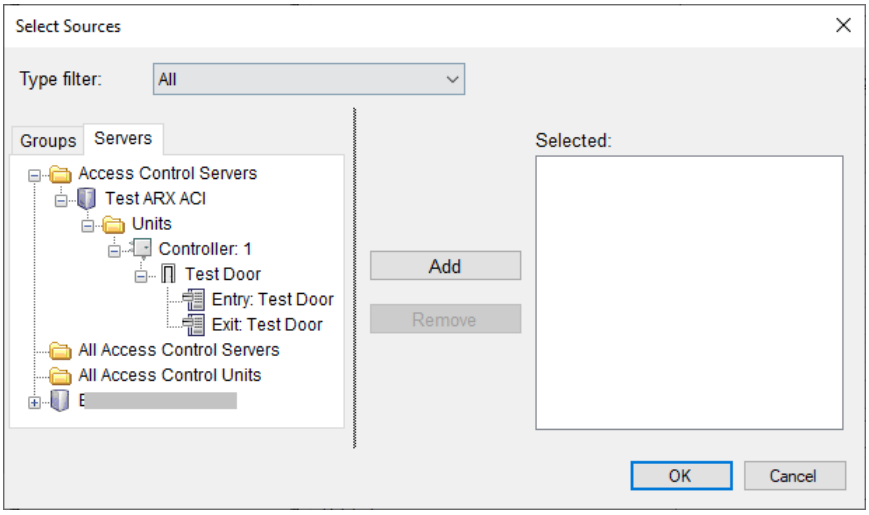
   In the example, **Access denied** is selected.
5. From the **Sources** dropdown list, select a proper source depending on the required configuration. The default options are:
   All doors: This option will select all added doors as a source for triggering the alarm.
   <door 1>: This option will select 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, **Test Door**, **Other...**

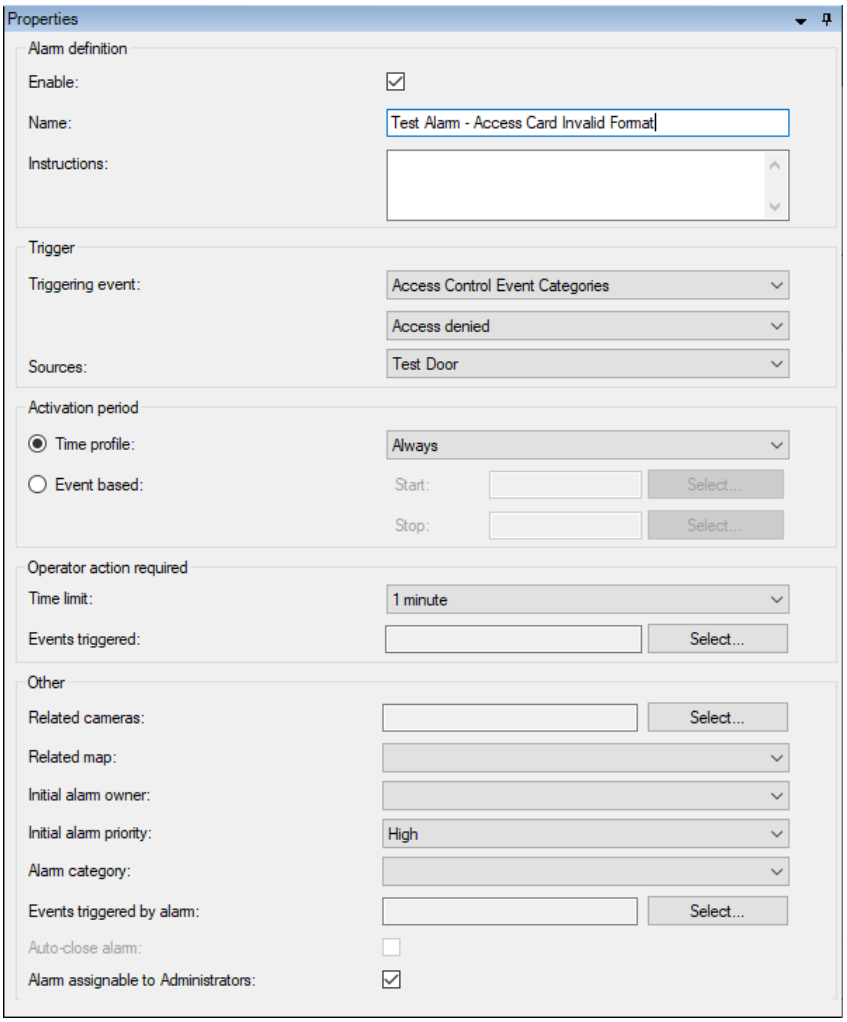


The **Other...** option



Test Door from the initial listings is selected in the example above. Click **OK**.

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



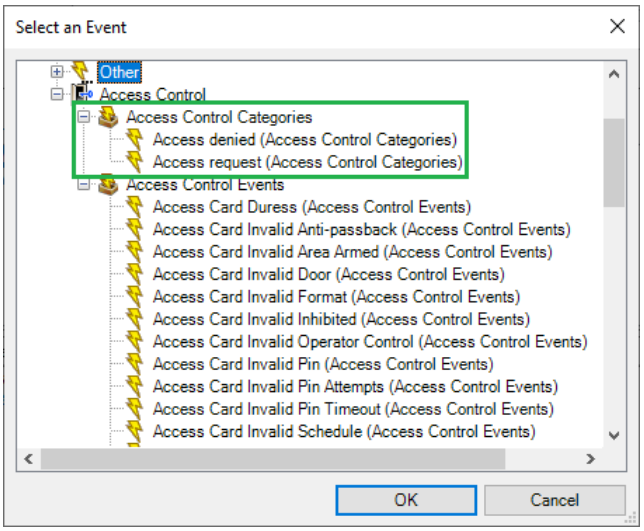
Rules based on ARX Access Control events

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...**.

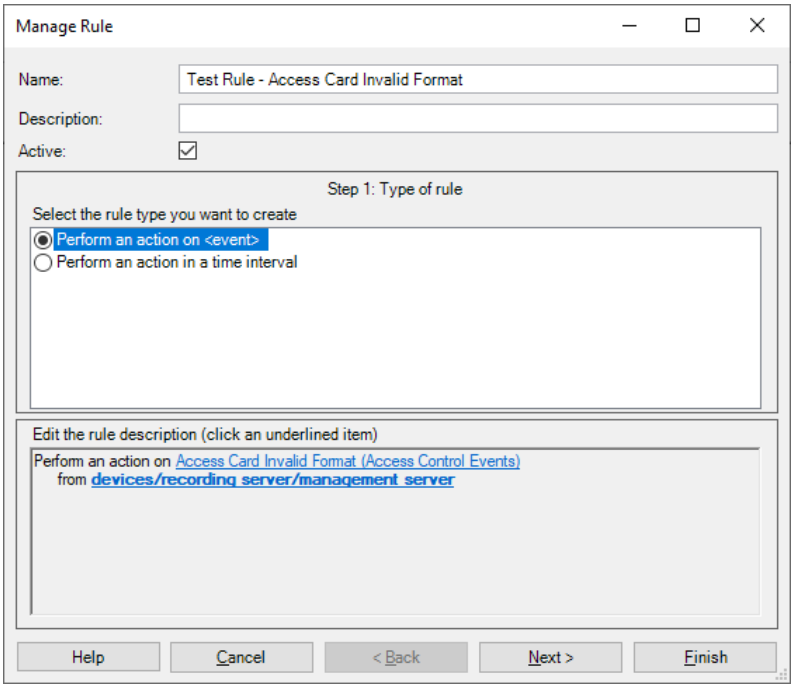
   ***Note**: For detailed description on how to configure **Rules**, see the Milestone XProtect (XProtect Management Client) help.*

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 ARX Access Control Properties.*

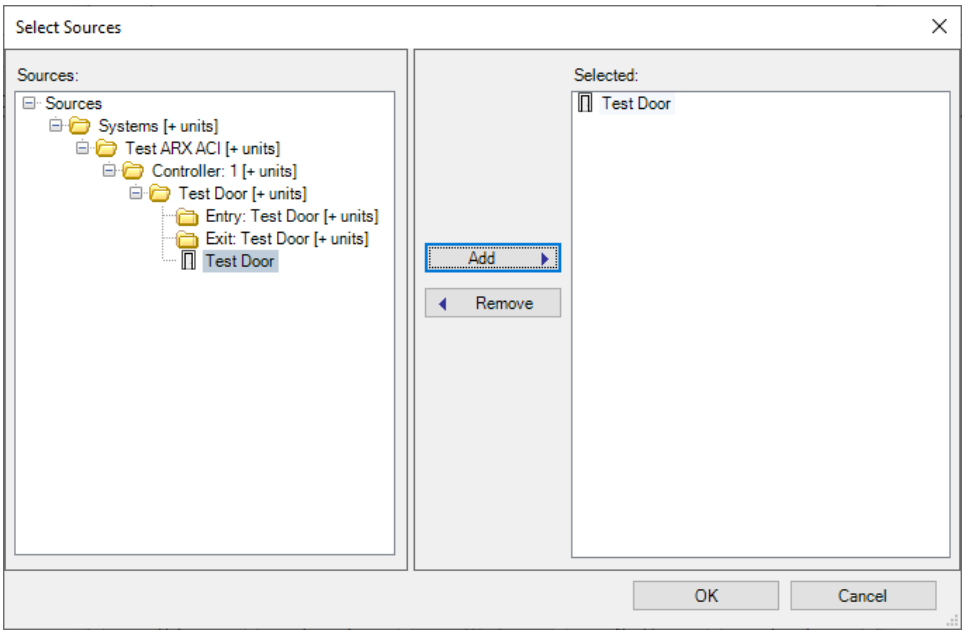


Access Card Invalid Format (Access Control Events) is selected in the example above. Click **OK**.

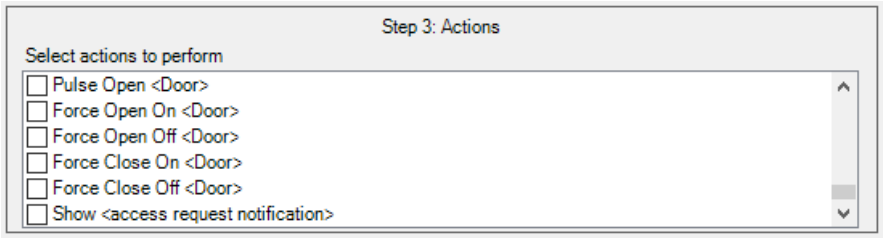


6. In the **Edit the rule description section (click an underlined item)**, click **devices/recording server/management server**.
7. In the **Select Sources** dialog box, select **Systems [+ units]** or expand it, and select devices as per your requirements. Click **OK**.

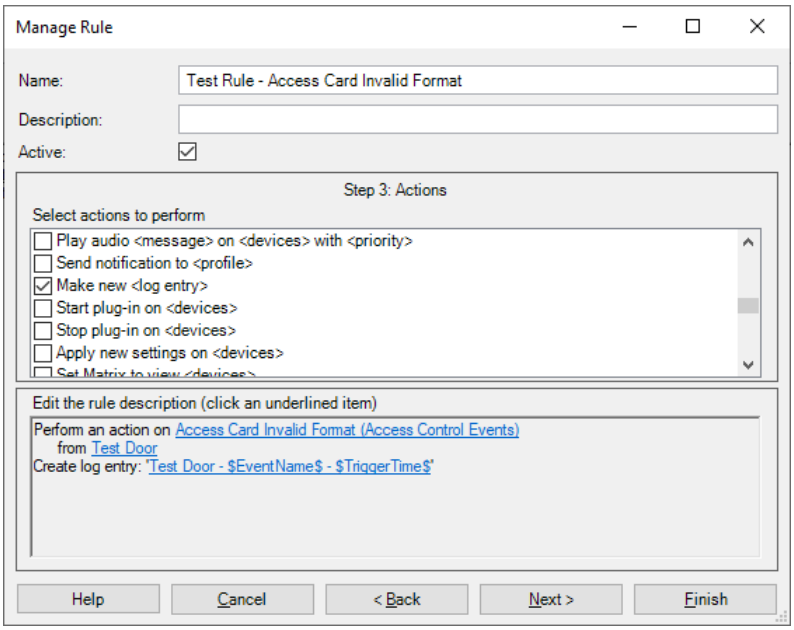
   Test Door is selected in the example below. Click **OK**.



8. In **Step 2: Conditions**, select conditions if those are required and click **Next**.
   Conditions are not selected in the example.
9. In **Step 3: Actions**, following actions are added based on the integration (These actions were added when ARX Access Control is added to XProtect):
   Pulse Open <Door>
   Force Open On <Door>
   Force Open Off <Door>
   Force Close On <Door>
   Force Close Off <Door>
   Show <access request notification>



In the example one of the default XProtect actions is selected – **Make new <log entry>** with variables **Test Door - $EventName$ - $TriggerTime$**. 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**.

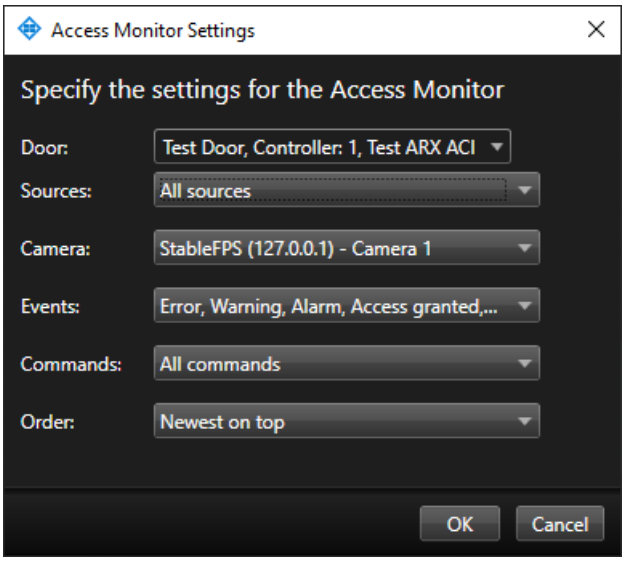
XProtect Smart Client configuration

Add ARX Access Monitor

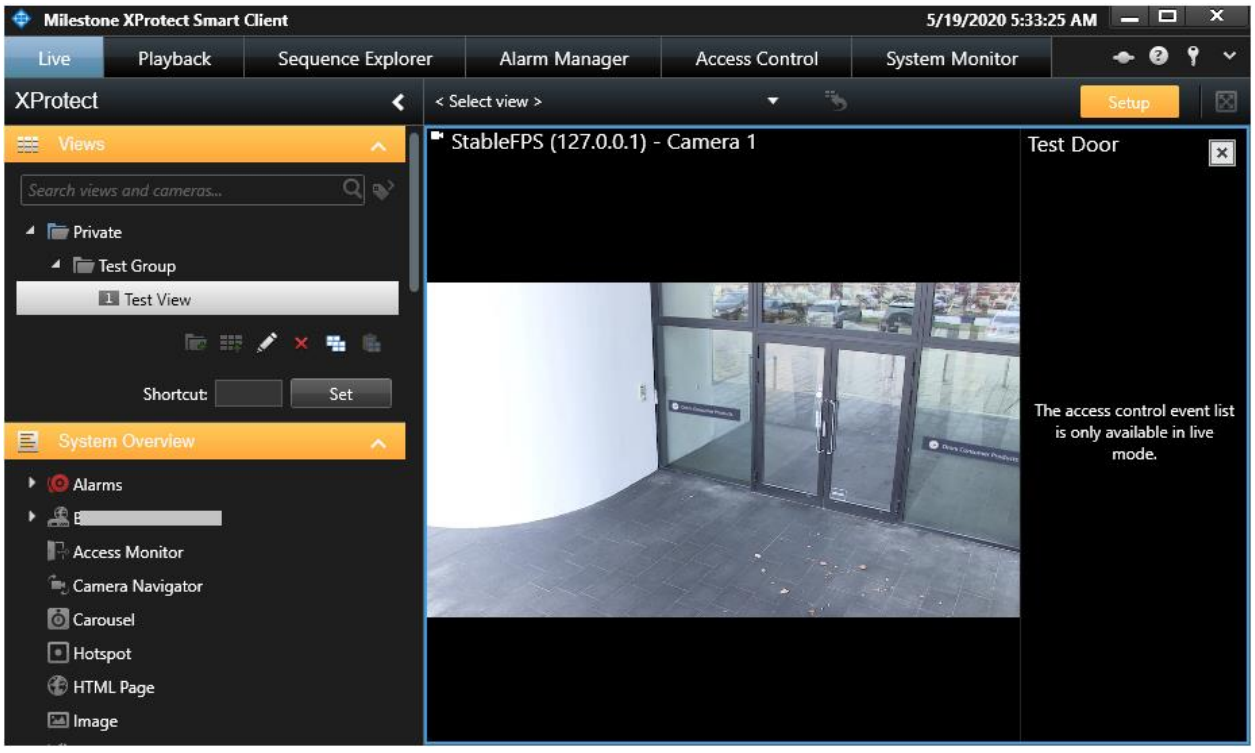
1. Open XProtect Smart Client > **Live** tab.
2. In the upper-right corner, click **Setup**.
3. Add a **Group** and a **View**.

   ***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, **Test Door** 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.

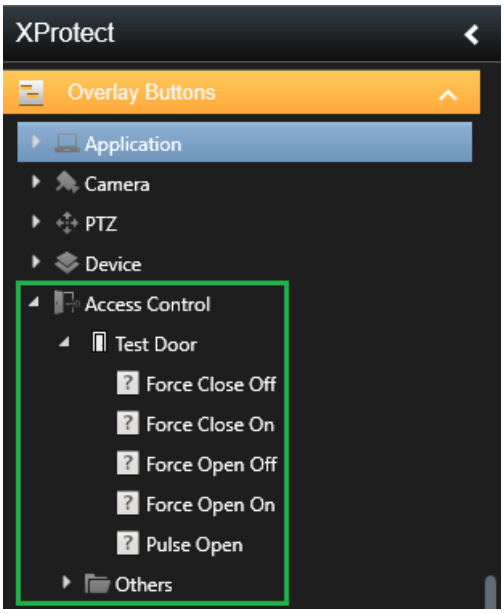
Add ARX Overlay Buttons

1. Open XProtect Smart Client > **Live** tab.

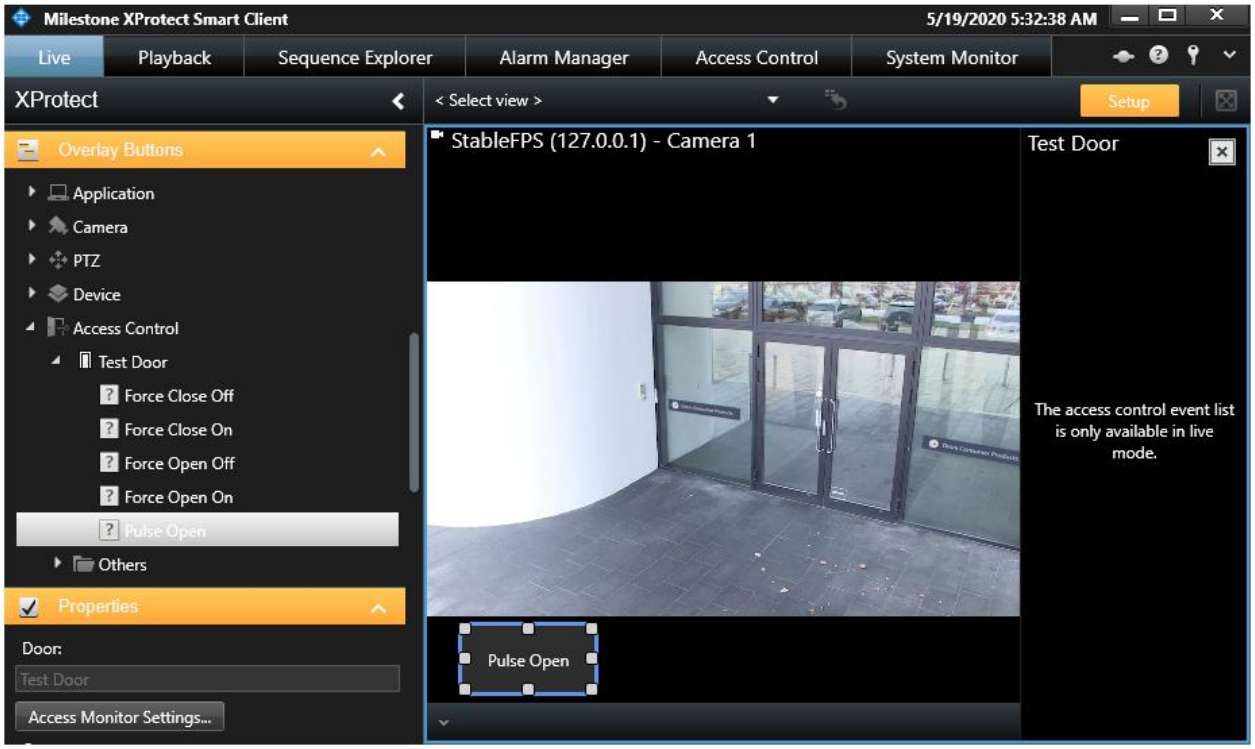
2. Click **Setup** in the upper-right corner.
3. Add a **Group** and a **View**.
4. Add a **Camera** or **Access Monitor**

   ***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 ARX doors are available: Force Close Off, Force Close On, Force Open Off, Force Open On, Pulse Open (These actions were added when ARX Access Control is added to XProtect).



The **Pulse Open** action for **Test Door** is added to the camera in the example.



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

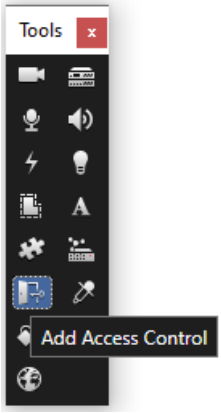
Add ARX devices on the map

The ARX 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.

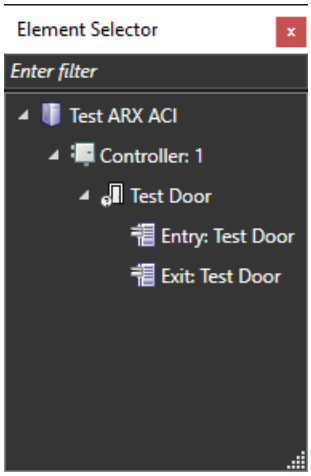
   ***Note**: For detailed description on how to configure **Maps**, see the Milestone XProtect (XProtect Smart Client) help.*

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

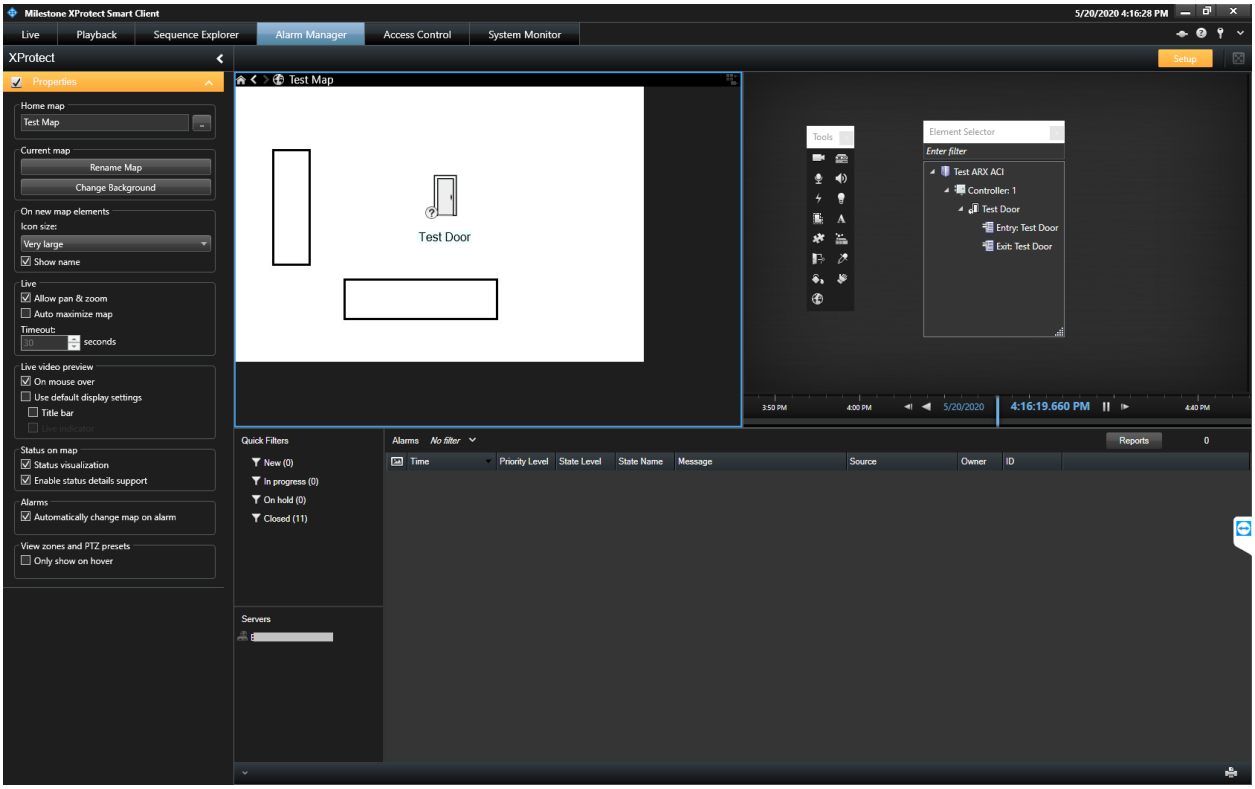


5. In the **Element Selector** dialog box, expand the ARX access control node. Drag and drop an element (door) from the list to the map depending on the required configuration.

   ***Note**: Currently events (and alarms based on those events) are received only for **Doors**. **Server**, **Controller** and **Door Access Points** are not supported.*



Test Door is added in the example.



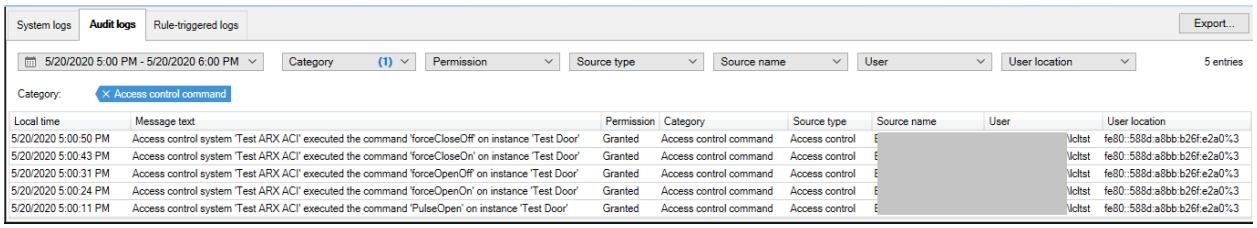
6. Close the **Element Selector** dialog box when you finish adding the ARX system doors.
7. Click **Setup** in the upper-right corner to complete the map configuration.

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.

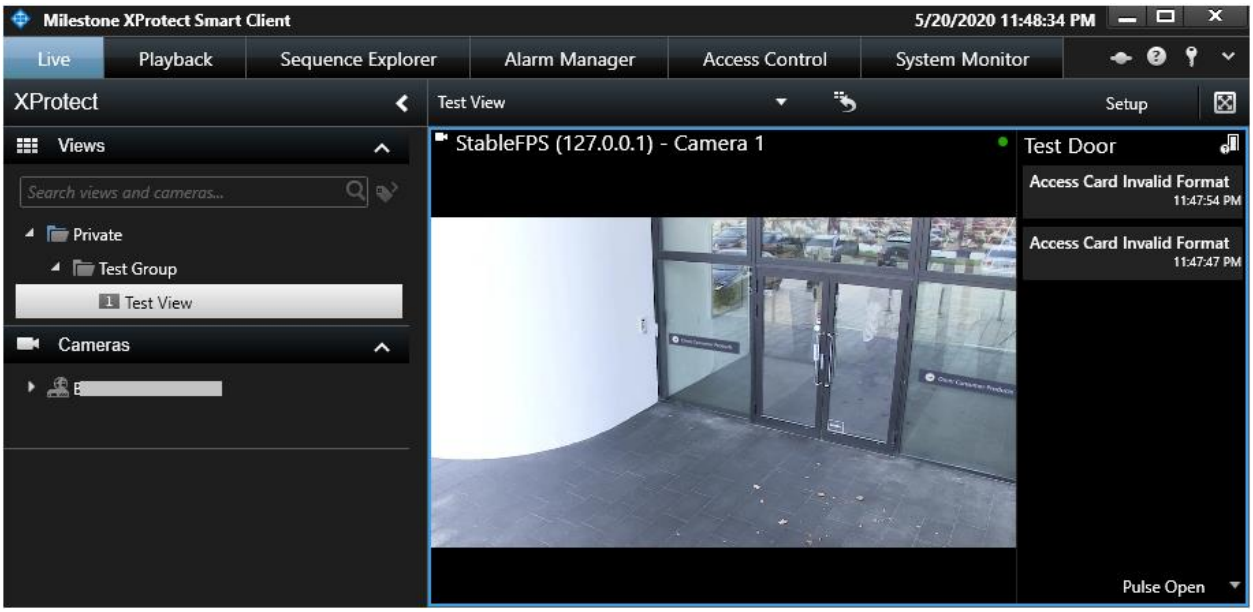
Example:



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 ARX 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.

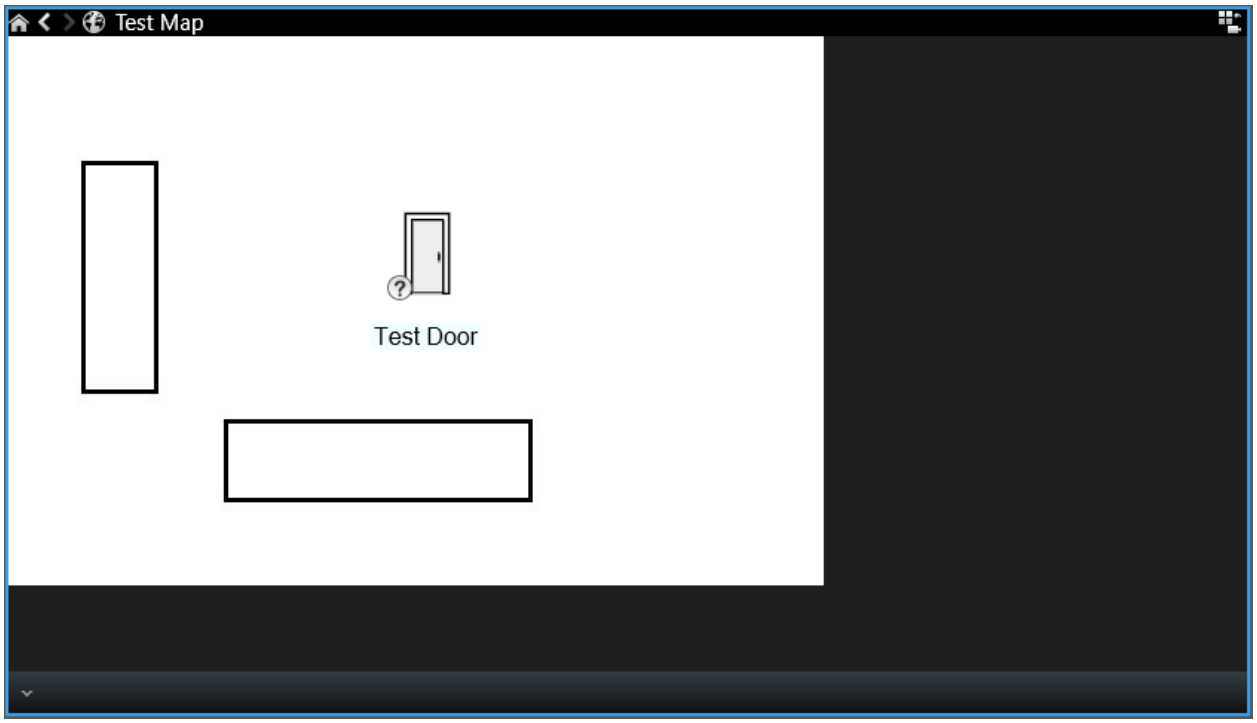


A list with available actions is displayed in the bottom-right corner (These actions were added when ARX Access Control is added to XProtect).

Alarm Manager tab

ARX devices on the map

Open XProtect Smart Client > **Alarm Manager** tab.
The map in the example shows **Test Door** (which was added in chapter XProtect Smart Client configuration - Add ARX devices on the map).

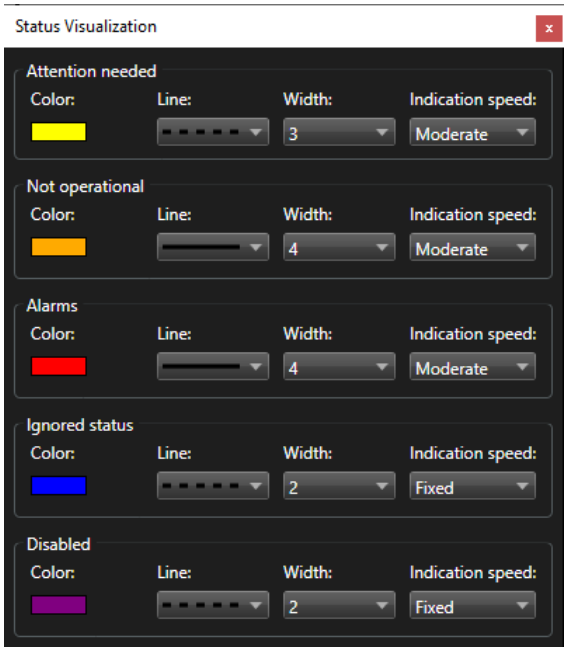


The other default XProtect states for the doors are described in the following table:

.

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**):



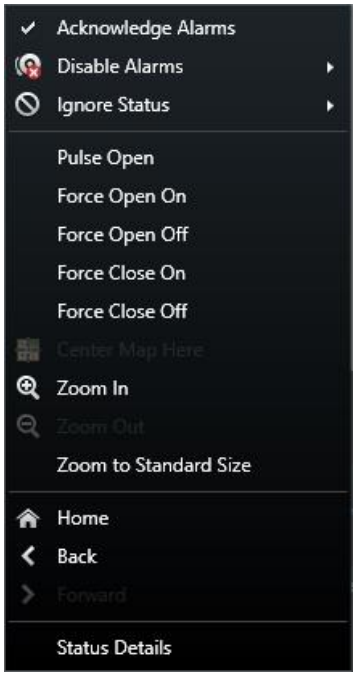
Based on the integration, common door states and related icons are described in the following table:

***Note**: The correctness of the initial state of a door cannot be guaranteed. Initially, it will be set to **Open State: Unknown**, **Locked State: Unknown**.*
*The icon will not be updated if only the **Locked State** is changed while the **Open State** remains **Unknown**. The icon will be updated once the **Open State** is changed from **Unknown** to other state.*

Icon	State description
	Open State: Unknown, Locked State: Unknown
	Open State: Open, Locked State: Unlocked
	Open State: Open, Locked State: Locked
	Open State: Closed, Locked State: Unlocked
	Open State: Closed, Locked State: Locked

Context menu

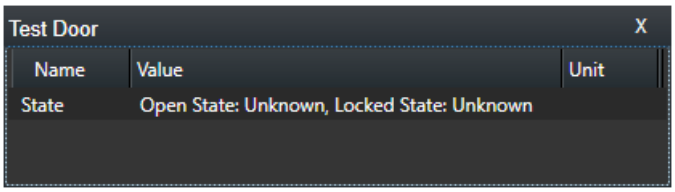
If you right-click on the door, you will see several standard actions plus the integration specific:



The most important ones are described in the following table:

Action	Description	Door
Acknowledge Alarms	This action changes the **State Name** of an alarm from **New** to **In Progress**.	Available
Disable Alarms	Currently not supported.	Available
Ignore Status	Currently not supported.	Available
Pulse Open Force Open On Force Open Off Force Close On Force Close Off	ARX system actions related to doors (These actions were added when ARX Access Control is added to XProtect). ***Note**: For detailed description, see the ASSA ABLOY ARX User Guide v3.1 (i.e. integrated help)*	Available
Status Details	This action shows the current status of a door.	Available

In the example below, the **Test Door** status is shown:



Access Control tab

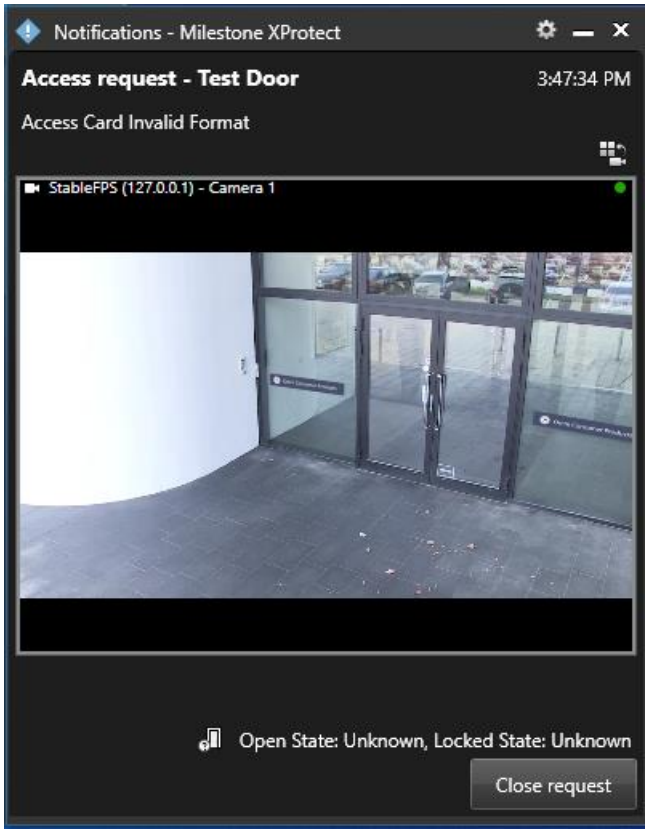
***Note**: For detailed description, see the Milestone XProtect (XProtect Smart Client) help.*

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)
- Local Time
- Event
- Live video from the associated camera
- Actual state of the door
- Button **Close request**

In the example, an access request notification for **Access Card Invalid Format** 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: **ARX Access Control Integration** is not listed as an option in **Integration plug-in** when adding the ARX 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 ASSA ABLOY ARX Access Control Integration is not loaded by the XProtect Event Server.	Check the XProtect Event Server log. Look for an entry resembling: "2020-05-20 1:47:48 PM UTC+02:00 Info ESEnvironmentManager Access Control plugin loaded: Assa Abloy v1.0a – 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\Assa Abloy
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 ASSA ABLOY ARX 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\Assa Abloy\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, error. "debug" = Highest level of logging,  "error" logs least-->
```

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

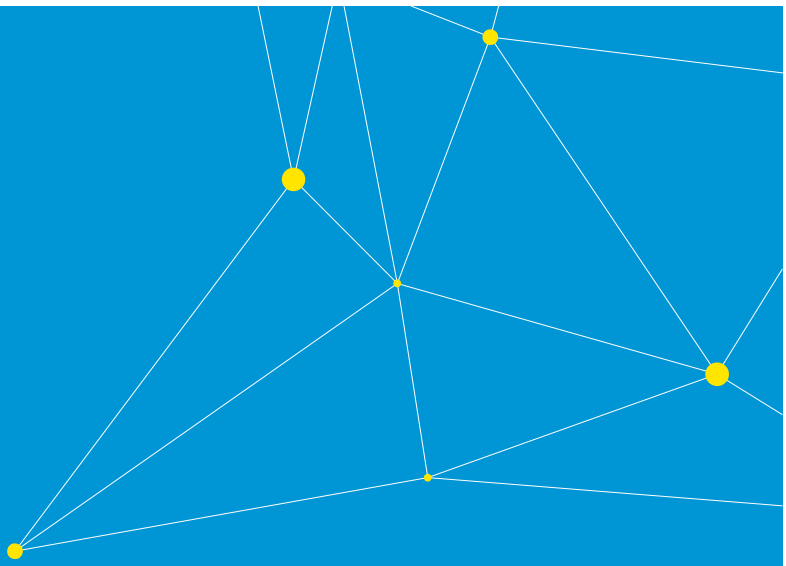
***Note**: XProtect Event Server must be restarted in order to load the new configuration whenever changing the value of the parameters.*

Limitations

- The Milestone ASSA ABLOY ARX Access Control integration supports **Controller type**: **LCU 9016/17 II/II (16 doors)**. The integration may work with **Controllers** based on other **Controller types**, but Custom Development does not guarantee that
- Only **HTTPS** communication is supported between ARX Server and XProtect Access
- **Alarms** from ARX system are not supported in XProtect Access
- **Badge holders** (i.e. **Persons**) pictures are not updated in ARX system if they are changed in XProtect Access

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.