Manual

Milestone ASSA ABLOY ARX Access Control Integration v1.0





Table of Content

Target audience for this document	4
Copyright, trademarks & disclaimer	5
Copyright	5
Trademarks	5
Disclaimer	5
General description	6
Introduction	6
Solution overview	6
Installation	6
Prerequisites	6
Installer	7
Installation steps	7
License	11
ARX and XProtect elements mapping	12
ARX configuration	14
ARX Server	14
ARX Client	14
XProtect Management Client configuration	19
Add ARX Access Control	19
Remove ARX Access Control	23
ARX Access Control Properties	23
Alarms based on ARX Access Control events	25
Rules based on ARX Access Control events	27
XProtect Smart Client configuration	30



Add ARX Access Monitor	30
Add ARX Overlay Buttons	31
Add ARX devices on the map	33
XProtect Management Client operation	35
Audit logs	35
XProtect Smart Client operation	36
Live tab	36
Alarm Manager tab	36
Access Control tab	40
Access request notifications	40
Troubleshooting	41
XProtect Event Server and MIP logs	42
Limitations	43
Known issues	43



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

© 2020 Milestone Systems A/S.

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.







6. The next steps are executed automatically.

6	Milestone ASSA ABLOY ARX Access Control Integration Setup
	Installing Milestone ASSA ABLOY ARX Access Control Integration tone
	Please wait while the Setup Wizard installs Milestone ASSA ABLOY ARX Access Control Integration. Status:
	Back Next Cancel





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

Milestone XProtect Management Cli	lient 2019 R1				- 0
Eile Edit View Action Tools Help ☐ ♥ 3 ♥ ∰					
Site Navigation • 4 × • • • • • • (13.1a • • • • • • • • • • • • • • • • • • •	milestone The Open Platform Company				
Site Information Remote Connect Services Cervers Cent Cent Cent Cent Cent Security System Dashboard System Cags			A In	ccess Milestone Care portal formation about Milestone Care	
Diff Access Control Diff. Transact Diff. Alarms	Product Version XProtect Corporate 2019 R1 Test Milestone XProtect Smart Vall Milestone XProtect Access Milestone XProtect Transact	Software License Code	Expiration Date	Milestone Care Plus	Milestone Care Premium N/A
	ARX Access Control Integration v1.0.29.1	N/A	6/17/2020	6/17/2020	

milestone

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	N/A	Not visible in XProtect Management Client
nodes (Keypad		Not visible in XProtect Smart Client
Reader)		
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.

Edit system properties				×
Integration server set	tings			
The TCP ports to which	the integration server should l	isten.		
For security reasons it i	s recommended to only use HT	TPS.		
'Server address' can no	rmally be left empty.			
Integration HTTP pe	and a state			
On: Port:	Server address:			
⊂ Integration HTTPS	port			
On: Port:	5003 Server address:			
			Save	Cancel
				Gander

ARX Client

- 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.



*		ARX			_ _ _ ×
File <u>E</u> dit Tools System Window Help					
Persons Access Schedules Access	Door Installation	Alarm Firmware	Logs	Resource	() Status
categories areas	types			tree	overview
💐 Installation tree 🗙					
□ · ā + •					
 Test Folder Test Controller Test Controller Test Controller Test Door (1) In (0) Keypad Reader (31e4c) 	Settings Modem Controller type LC Name Te Description Serial number 00 Time zone Eu Z Active Offline updater No Update process info Current state: Last update duration: Cards added/updated	U 9016/17 II/III (16 d ist Controller i:06:8e:30:c8:b9 irope/Sofia one Waiting 1 May 20, 0:00:00. 1 I/removed: 0/0/0	v v or changes t 2020 7:03:35	o process P PM	
				ок	Cancel Apply
L]
(Milestone) - master@127.0.0.1					

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

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

*	ARX	_ 🗆 ×
File Edit Tools System Window Help		
Persons Access categories Schedules Access areas	Door types	Status overview
Image: Second system Image: Second system	Settings Inputs Relay outputs Lost connection Times Door codes Functions Hi-O Type of door Type of door Test Door Description External ID ID:1_20200518_154740 Address 1 Active Active Hi-O Service interval (door openings) O Change Passed service intervals 0 Force pon Off Force block Off Show door in access area OK Cancel	
(Milestone) - master@127.0.0.1		



Connected HI-O nodes:

In (0) is added (Credential format: External). Keypad Reader (31e4c) is added.

*	AF	ex in the second s	_ 🗆 ×
File <u>E</u> dit Tools System Window Help			
Persons Access categories Schedules Access areas	Door Installation Alarm Fir	Ware Logs Resource tree	Status overview
Installation tree ×			
Installation tree	Name		
Test Controller	Address In passag	e (0)	~
□ □ □ Test Door (1)	Number of digits 9		
Keypad Reader (31e4c)	Credential format		
	External		
	Change credential format for reader]	
		OK Cancel	Apply
(Milestone) - master@127.0.0.1			

3. Create a **Door type**.

In the example below, **Test Door Type** is created:

ns Access Schedules Ar categories an	ccess Door Installation Alarm Firmware Logs Resource tree	St
Door Types 🗙 📕 Door Type - T	iest Door Type X	
Name	Test Door Type	
Description		
Domains	default	~
Door		
Unlocked	Always off	✓ Show
Buzzer	Always on	✓ Show
Motor lock day	Always off	✓ Show
Buy alarm time	Always off	✓ Show
Unlock from reader	Always on	✓ Show
Lock from reader	Always on	✓ Show
Open button	Always on	✓ Show
Latched open button	Always on	✓ Show
Reader		
Security level in	Credential Always	✓ Show
Security level out	Credential Always	✓ Show



 Create an Access area and add a Door. In the example below:

Test Area is created.

*	ARX	_ 🗆 ×
File <u>E</u> dit Tools System Window Help		
Persons Access categories Column Schedules Schedules areas	Door Installation Alarm Firmware Logs Resource tree	Status overview
Access areas x Access areas x Clear Clear	Name Test Area Description D D D:3_20200518_155816 Area Area Area Category Schedule Disabled Unlock/lock Arm Disarm Caretaker Add Remove Exception Clear	
Free door licenses: 3 Used door licenses: 1	OK Cancel Ap	ply
(Milestone) - master@127.0.0.1		

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

						ARX				
Edit Tools Systen	n Window Help	p								
sons Access categories	Schedules	Access areas	Door types	Installation	Alarm	Firmware	Logs	Resource tree		(Sta
Access areas : Access areas : Domains Domains Domains C Test Ar Test Ar	Clear Clear	Search/Next	Na t De	me Test scription	Door			-		
			000	Door Type	Fest Door	Туре	Ahumu		New	Change
				Buzzer			Always	s on	Exception	Clear
				Motor lock	day		Always	s off	Exception	Clear
				Buy alarm t Unlock from	time n reader		Always	s off	Exception	Clear
										, 💟

5. Create a **Person**.

In the example below, **Test User** is created:





Access Categories tab:

dit Toole System					ARX			-
tale roois system	Window Help							
24		M 🛛		2	1000		A	(
ons Access categories	Schedules Ac	eas types	Installation	Alarm	Firmware	Logs	Resource tree	Stat
Editing person T	fest User ×							
irst name	Test							
ast name	User							
escription								
o	ID:1_20200519_	033712						
omains	default			~				
IN code								
	Require PIN ch	ange within	da	ys				
	Disabled perso	on						
atest passage	May 19, 2020							
atest passage	May 19, 2020 Show log (30 d	ays)					🛄 Browse 💼 Delete	
atest passage Access Categorie	May 19, 2020 Show log (30 d	ays)	My pages	Unlock	function for of	line doors	📕 Browse 🗑 Delete	
Access Categorie	May 19, 2020 Show log (30 d es Detailed acces	ays) ss Credentials	5 My pages To	Unlock	function for of	iline doors ange date	Browse To Delete	Add
Access Categorie	May 19, 2020 Show log (30 d es Detailed acces From	ays) ss Credentials	My pages	Unlock	function for of Ch 5/:	fline doors ange date 19/20 3:37	Browse Delete Delete Operator AM master	Add
Access Categorie Name Full access	May 19, 2020 Show log (30 d. es Detailed acces From	ays) ss Credentials	My pages To	Unlock	function for of Ch 5/:	iline doors ange date 19/20 3:37	Browse To Delete Operator AM master	Add
Access Categorie Name Full access	May 19, 2020 Show log (30 d es Detailed acces From	ays) is Credentials	My pages To	Unlock	function for of Ch 5/:	fline doors ange date 19/20 3:37	Browse To Delete Operator AM master	Add Remove Set validity
Access Categoria	May 19, 2020 Show log (30 d es Detailed access From	ays)	My pages To	Unlock	function for of Ch 5/:	fline doors ange date 9/20 3:37	Browse To Delete Operator AM master	Add Remove Set validity
Access Categorie Access Categorie Name Full access	May 19, 2020 Show log (30 d es Detailed acces From	ays)	7 My pages To	Unlock	function for of Ch 5/3	iline doors ange date 19/20 3:37	Browse To Delete Operator AM master	Add Remove Set validity
Access Categorie Name Full access	May 19, 2020 Show log (30 d es Detailed acces	ays)	My pages To	Unlock	function for of Ch 5/:	ine doors ange date 9/20 3:37 Save 8	Browse To Delete	Add Remove Set validity el Apply

Credentials tab:

							ARX					_ 0
e <u>E</u> dit T	ools System	Window Help)									
2 Persons	Access categories	Schedules	Access areas	Door types	Installation	Alarm	Firmware	Logs	Resource tree			Status overview
🕹 Edi	iting person T	est User 🗙										
First n	iame	Test										
Last n	iame	User										
Descri	ption											
ID		ID:1_20200	519_03371	2								
Domai	ins	default				~						
PIN co	ode									~		
		🗌 Require P	IN change v	within	da	ays						
		Disabled	person									
Latest	t passage	May 19, 202	D									
		Show log (30 days)						Browse	📅 Delete		
Aci	cess Categorie	es Detailed	access C	redentials	My pages	Unlock	function for o	ffline doors				
Cre	dential numb	er ^ Descrin	tion	Crede	ential format	Own	er	Inhibite	ed Inhi	hit reason	Valid to	
592	2623364	er besenp	tion	Exter	nal	Test	User			bit i cuson	vulla to	
				D Nev	v credential	Mana	age cards 👻	Reprog	ram offline card			
							-					
								Save &	new OK	Car	rel	apply
								Save &	or new OK	Car	icel	Apply



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 <u>ARX Server</u>.
User: The user with the administrative rights for the ARX system.

Password: The password of the user.



x

Example:

Create Access Control System Integration

Create access control system integration

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

Name:	Test ARX ACI	_
Integration plug-in:	ARX Access Control Integration	v
Address:	127.0.0.1	
Port:	5003	_
User:	master	_
Password:	•••••	_

Next Cancel

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



Create Access Control System Integration	x
Connecting to the access control system	
connecting to the access control system	
Collecting configuration data	
Configuration successfully received from access control system	
Added	
Doors (1)	-
Units (3)	•
Servers (1)	•
Events (50)	•
Commands (5)	•
States (18)	•
	Previous Next Cancel

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.

Create Access Control System Integration	x
Associate cameras Drag cameras to the access points for each door in the list. The a when access control events related to one of the door's access p	associated cameras are used in the XProtect Smart Client joints are triggered.
All doors Name Enabled License Test Door Pending Image: Comparison of the second	Cameras: Camera Group 1 Camera Group 1 StableFPS (127.0.0.1) - Camera 1
	Previous Next Cancel

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 <u>Alarms based on ARX Access Control events</u> and <u>Access request notifications</u>.



nable the Enable a	e events you want to monitor in XProtect S all Disable all	mart Client. Use categories to simplify t	he use of triggering events.		
Enabled	Access Control Event	Source Type	Event Category		
✓	Access Card Duress	VideoOS.Platform.AccessControl.I		v	\sim
✓	Access Card Invalid Anti-passback	VideoOS.Platform.AccessControl.I		×	1
✓	Access Card Invalid Area Armed	VideoOS.Platform.AccessControl.I		v	
<	Access Card Invalid Door	VideoOS.Platform.AccessControl.I		Ŷ	
✓	Access Card Invalid Format	VideoOS.Platform.AccessControl.I	Access denied, Access request	~]
-	Access Card Invalid Inhibited	VideoOS.Platform.AccessControl.I		Ŷ]
✓	Access Card Invalid Operator Control	VideoOS.Platform.AccessControl.I		~	1
~	Access Card Invalid Pin	VideoOS.Platform.AccessControl.I		v	1
✓	Access Card Invalid Pin Attempts	VideoOS.Platform.AccessControl.I		~	1
~	Access Card Invalid Pin Timeout	VideoOS.Platform.AccessControl.I		~	1
✓	Access Card Invalid Schedule	VideoOS.Platform.AccessControl.I		~	1
✓	Access Card Invalid Standard	VideoOS.Platform.AccessControl.I		Ŷ	1
User-de	fined Categories				1.

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.

Access Control Information **→** 7 Cardholders Search for cardholders to view, add or delete a picture of the cardholder. The cardholder picture is used in the XProtect Smart Client, when an access control event has been registered. Q Search cardholder Test User Name Туре Test Us Select picture ... Delete picture ID:1_20200519_033712 ld: First Name: Test Last Name: User 🚳 General Settings 👒 Doors and Associated Cameras 🍖 Access Control Events 뒞 Access Request Notifications 🤰 Cardholders

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**.
- 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.

ngger		
Triggering event:	Access Control Event Categories	~
		~
Courses	Access denied	
Sources.	Access granted	
Activation period	Alam	
Activation period	Door Error	
Time profile:	Error	
	Warning	

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.

••

Tringer

<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...



Ingger		
Triggering event:	Access Control Event Categories	~
	Access denied	~
Sources:		~
Activation period	All doors Test Door	-
0.7 "	Other	

The **Other...** option

Select Sources	×
Type filter: All	~
Groups Servers	Add Remove OK Cancel

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

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



Properties		▼ ₽
Alarm definition		
Enable:	\checkmark	
Name:	Test Alarm - Access Card Invalid Fo	rmat
Instructions:		^
		×
Trigger		
Triggering event:	Access Control Event Categories	~
	Access denied	~
Sources:	Test Door	~
Activation period		
Time profile:	Always	~
O Event based:	Start:	Select
	Stop:	Select
Operator action may irred		
Time limit:	1 minute	~
Events triggered:		Select
Events trygered.		Jelect
Other		
Related cameras:		Select
Related map:		~
Initial alarm owner:		\sim
Initial alarm priority:	High	~
Alarm category:		~
Events triggered by alarm:		Select
Auto-close alarm:		
Alarm assignable to Administrators:	\square	

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 <u>ARX Access Control Properties</u>.





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

Manage Rule			-	- 1	n x
Name:	Test Rule - Access	s Card Invalid Format			
Description:					
Step 1: Type of rule Select the rule type you want to create Perform an action on <event> Perform an action in a time interval</event>					
	n n a une mervar				
Edit the rule descript	tion (click an underli	ned item)			
Perform an action on from <u>devices/re</u>	Access Card Invalid I scording server/ma	Format (Access Control F anagement server	<u>Events)</u>		
Help	<u>C</u> ancel	< <u>B</u> ack	<u>N</u> ext >		<u>F</u> inish

- 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 <u>ARX Access Control is added to XProtect</u>):

Pulse Open <Door> Force Open On <Door> Force Open Off <Door> Force Close On <Door> Force Close Off <Door> Show <access request notification>

Step 3: Actions	
Select actions to perform	
Pulse Open <door></door>	~
Force Open On <door></door>	
Force Open Off <door></door>	
Force Close On <door></door>	
Force Close Off <door></door>	
Show <access notification="" request=""></access>	×

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.



Manage Rule			-	-		×	
Name: Test Rule - Access Card Invalid Format							
Description:							
Active:							
		Step 3: Actions					
Select actions to pe	erform						
Play audio <message> on <devices> with <priority> Send notification to <profile> Make new (dop entry)</profile></priority></devices></message>							
Start plug-in on	<devices> <devices></devices></devices>						
Apply new settin	ngs on <devices></devices>					~	
Edit the rule descrip	otion (click an underlin	ied item)					
Perform an action or from <u>Test Door</u> Create log entry: ' <u>Te</u>	n <u>Access Card Invalid F</u> st Door - \$EventName\$	iomat (Access Control i § - \$TriggerTime\$*	<u>Events)</u>				
Help	<u>C</u> ancel	< <u>B</u> ack	<u>N</u> ext >		<u>F</u> inish		

- 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**.



Access Monitor Settings ×				
Specify the	settings for the Access Monitor			
Door:	Test Door, Controller: 1, Test ARX ACI 🔻			
Sources:	All sources			
Camera:	StableFPS (127.0.0.1) - Camera 1 🔹 🔻			
Events:	Error, Warning, Alarm, Access granted, 🔻			
Commands:	All commands 🔹			
Order:	Newest on top 🔹			
	ОКС	ancel		

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 <u>XProtect Smart Client</u> <u>operation - Live</u> 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 <u>ARX Access Control is added to XProtect</u>).







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.

Line Nytak Sequence Explore Aum Manage Acces Control System Manales XProtect Image: Sequence Explore Image: Sequence Explore Image: Sequence Explore Image: Sequence Explore Image: Sequence Explore Image: Sequence Explore Image: Sequence Explore Image: Explore Image: Explore I	28 PM — 🗗 🗙	5/20/2020 4:16				t Client	XProtect Smart	💠 Mileston
XPdact I mark I mark	- • 0 ° ×		System Monitor	Access Control	Alarm Manager	Sequence Explorer	Playback	Live
Image: Construint Image: Construint	Setup 🛛 🔀					<		XProtect
Here nig Interest Rig Interest Rig <t< td=""><td></td><td></td><td></td><td></td><td>🏫 < > 🤁 Test Map</td><td>^ 1</td><td>ies</td><td>V Proper</td></t<>					🏫 < > 🤁 Test Map	^ 1	ies	V Proper
□ the bar 23574 400 M 4 9/20/2020 4.16.13.660 PM II II ► Static source Oxick Filters Atoms Mo Siter ~ Reports Static source Time Priority Level State Level State Name Message Source Owner D Atoms Addresses Source Owner D Image: D Source Owner D View zones and PIZ prests Servers Image: D Servers Image: D Servers Image: D		Tools Eternett Selector • • •	, 	Test Door		tep Inpound	p Rename Ma Change Backgr pp elements ame am & zoom am & zoom am & zoom am & zoom as seconds seconds seconds	Home may Test Map Current m kon size: Very large Ø Show r Uve Ø Alow auto m Timeout: 20 Vive video U Ø on mo
Interstand Adarms Adarms No filter ∨ Reports Status visualization Vew (0) Time Pointy Level State Name Message Source Owner ID Adarms Adarms Time Pointy Level State Level State Name Message Source Owner ID View zones and PIZ presets On hold (0) T Cased (11) Servers Servers Servers Servers Servers Servers Servers Servers Servers Servers	4:40 PM	350 FM 4:00 FM ◀ 5/20/2020 4:16:19.660 PM Ⅱ IF				ngs	ault display setting	Use de
Status on map Ouder Filters Atama No filter * Regords I status visualization I nongenes (0) I nongenes (0) I nongenes (0) I no that (0) I constantially change map on alarm Image: Status visualization Status visualization Status visualization Status visualization Status visualization Image: Status visualitation Image: Statusvisualitation Image						L	xar 1dicator	Live i
M Statu visualization Image may on slam Image may on slam Image may on slam Image may on slam View zones and PTZ presets Image may on slam Servers	ts O	Repo		Alarms No filter ∨	Quick Filters		пар	Status on
Alarms ✓ Alarms ✓ Alarms ✓ On hold (0) ✓ Closed (11) ✓ Closed (11) Servers Servers ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓		State Name Message Source Owner ID	Phonty Level State Le	Ilme	▼ New (0) ▼ In progress (0)	nort	isualization status details suon	✓ Status ✓ Enable
☑ Automatically change map on alarm ▼ Closed (11) 'View zones and PTZ presets Image: Closed (11) □ Chly show on hove: Servers Image: Closed (11) Image: Closed (11) Servers Image: Closed (11)					T On hold (0)			Alarms
View zones and PTZ presets C Only show on hover Servers	F				T Closed (11)	ap on alarm	itically change map	Autom
					Servers		and PTZ presets cow on hover	View zone Only st

- 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:

System logs	Audit logs	Rule-triggered logs	5													[Export
₫ 5/20/20	20 5:00 PM	- 5/20/2020 6:00 PM	1 ~	Category	(1) ~	Permission	1	 ✓ Sou 	rce type	~	Source name	~	User	V User locatio	on	~	5 entries
Category:	× Acces	s control command															
Local time	N	lessage text							Permission	Category		Source type	Source name	User		User location	
5/20/2020 5:00:	50 PM A	ccess control system '	Test ARX A	CI' executed the o	ommand 'ford	eCloseOff or	n instance '	Test Door'	Granted	Access con	trol command	Access control	E		Voltst	fe80::588d:a8bb:	b26f:e2a0%3
5/20/2020 5:00:4	43 PM A	ccess control system '	Test ARX A	Cl' executed the o	ommand 'ford	eCloseOn' or	n instance '	Test Door'	Granted	Access con	trol command	Access control	E		Voltst	fe80::588d:a8bb:	b26f:e2a0%3
5/20/2020 5:00:3	B1 PM A	ccess control system "	Test ARX A	Cl' executed the o	ommand 'ford	eOpenOff on	n instance '	Test Door'	Granted	Access con	trol command	Access control	E		Vicitst	fe80::588d:a8bb:	b26f:e2a0%3
5/20/2020 5:00:2	24 PM A	ccess control system '	Test ARX A	Cl' executed the o	ommand 'ford	eOpenOn' on	n instance '	Test Door'	Granted	Access con	trol command	Access control	E		Voltst	fe80::588d:a8bb:	b26f:e2a0%3
5/20/2020 5:00:1	11 PM A	ccess control system '	Test ARX A	Cl' executed the o	ommand 'Pul	seOpen' on in	stance 'Te	st Door'	Granted	Access con	trol command	Access control	E		Vicitist	fe80::588d:a8bb:	b26f:e2a0%3

milestone

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 <u>XProtect Smart Client configuration – Add ARX Access Monitor</u>) 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 <u>ARX</u> <u>Access Control is added to XProtect</u>).

Force Open On		
Force Open Off		
Force Close On		
Force Close Off	Pulse Open	•

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 <u>XProtect Smart Client</u> <u>configuration - Add ARX devices on the map</u>).



斎く〉登 Test Map	**
Test Door	
•	

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**):

.



Status Visualization ×				
Attention need	ed		1	
Color:	Line:	Width:	Indication speed:	
		3 🔻	Moderate 🔻	
Not operationa	I			
Color:	Line:	Width:	Indication speed:	
		4 🔻	Moderate 🔻	
Alarms				
Color:	Line:	Width:	Indication speed:	
		4 🔻	Moderate 🔻	
Ignored status				
Color:	Line:	Width:	Indication speed:	
		2 🔻	Fixed 🔻	
Disabled				
Color:	Line:	Width:	Indication speed:	
		2 🔻	Fixed 🔹	

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.

lcon	State description
<u>.</u>	Open State: Unknown, Locked State: Unknown
	Open State: Open, Locked State: Unlocked
	Open State: Open, Locked State: Locked
٩	Open State: Closed, Locked State: Unlocked
9	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	Available
	In Progress.	
Disable Alarms	Currently not supported.	Available
Ignore Status	Currently not supported.	Available
Pulse Open	ARX system actions related to doors (These actions were added	Available
Force Open On	when ARX Access Control is added to XProtect).	
Force Open Off		
Force Close On	<i>Note</i> : For detailed description, see the ASSA ABLOY ARX User Guide	
Force Close Off	v3.1 (i.e. integrated help)	
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 <u>XProtect Event Server and MIP logs</u> 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	Restart the XProtect Event Server and XProtect
Management Client have not been	Management Client after the installation of the plug-in.
restarted 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	Check the XProtect Event Server log. Look for an entry
Control Integration is not loaded by the	resembling:
XProtect Event Server.	
	"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	First, consider re-activation of the license either online or
activated.	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.