HOW TO.

Configure Anti-passback in AXIS Camera Station Secure Entry.



December 3, 2024 Rev. 1.0 © Axis Communications AB

How To. Configure Anti-passback access solution in AXIS Camera Station

Contents

Introduction	3
Step 1 – Adding/updating & setting up devices	3
To add the devices	4
To update the devices	5
To setup the devices	6
Step 2 – How to create/edit a schedule	8
Creating/editing a schedule to use in Secure Entry	8
Step 3 – Creating a door	9
To create a door	9
Step 5– Creating a zone and applying Anti-passback	10
To create a Zone	10
Bonus Step –Exempt from Anti-passback	13
To configure exempt from anti-passback	13
Considerations and limitations	14

Introduction

This how to document will show you how to set up the selected device(s) to have Antipassback within Axis Camera Station.

Prerequisites

AXIS A1610/A1210 Door Controller x11.8.20.2 or later

AXIS Camera Station 5.57 or later

Door Position Sensor

Please note that Axis doesn't take any responsibility for how this configuration may affect your system. If the modification fails or if you get other unexpected results, you may have to restore the settings to default.

Step 1 – Adding/updating & setting up devices

Start by adding the unit(s) to Axis Camera Station and ensuring that they are running the latest firmware. For the devices used we require the use of HTTPS for end-to-end security, these devices should also use ACS as an NTP. Only the door controller is required to be added to Axis Camera Station, but the intercom or camera can be added. Ensure either way that all devices are on the latest firmware.

To add the devices

Follow these steps if you need to add the devices:

- 1. In Axis Camera Station open the configuration tab via the "+" symbol found at the top of the screen.
- 2. From the left menu select "Devices" and under this drop-down select "Add Devices"
- 3. On this page if the units are in your network, you should see them, if they are missing then you can try do a manual search via the button "Manual Search". If they still cannot be found, please check the units are powered and are on the same network.
- 4. If the units are greyed out, this means they require the password for the unit, this is entered by clicking on the "Enter password" under status for the unit.
- 5. Once you see the units you wish to add, you can hold down the "ctrl" key and select the units, then click add found on the bottom left.
- 6. Follow the pop-up wizard to add these devices

Add devices	?	-		×
Choose how to configure your devices				
Quick configuration				
O Site Designer configuration				
✓ Use hostnames instead of IP when possible				
Help < Back	Next >		Cance	2

To update the devices

Follow these steps to update your devices:

- 1. In Axis Camera Station open the configuration tab via the "+" symbol found at the top of the screen.
- 2. From the left menu select "Devices" and under this drop-down select "Management"
- 3. From this page hold "ctrl" and select the devices, once selected press the update firmware button.
- 4. In the popup select the latest firmware in the list for each device (for the A1601 ensure to select the latest Secure Entry track) and press "OK"
- 5. The update can be monitored via the "tasks"

			Upgrade Firmware			?	-		×
Select firmwa	ire versi	ons for u	ıpgrade						
Check for Updates	Browse								
Model	Quantity	Firmware	Upgrade		Туре				
AXIS A8207-VE	1	10.9.4	10.9.4 (Active, Download)	•	Standard 👻				
Select / Deselect a				Lates	t check for updates:	16/02/	/2022	11:09:	55
					Hala	or		Cana	
					нер	OK		Cance	a

To setup the devices

Follow these steps to setup your devices:

- 1. In Axis Camera Station open the configuration tab via the "+" symbol found at the top of the screen.
- 2. From the left menu select "Devices" and under this drop-down select "Management"
- 3. Right click on the device and select "Security HTTPS Enable/Update"

Manage dev P B E	vices 🐻 🕐 🐵 🛟 🐇	G	
Name	MAC address	Status	Address
AXIS A1601 SE	ACCC8EB362F8	ОК	192.168.1.219
	Assign IP Address Configure Devices User Management	•	
	Security	HTTPS	Enable/Update
	Upgrade Firmware	IEEE 802.1X •	Disable
	Set Date and Time	Certificates 🔸	
	Restart		
	Restore to Factory Settings		
	Install Application		
	Collect Device Data		
	Connection	<u> </u>	
	Reload		
	Tag Devices		

4. This will create a task in the task and alarms, once this has completed, HTTPS is enabled on this device.

Alarms Tasks			
Name	Start	Message	Owner Progress
Enable HTTPS	10/10/2022 09:58:31	Enabling HTTPS	AXISNVR-2ORNKR
			6

5. Next to setup is the time & date on the device, we do this but right clicking on the device in Devices – Management and selecting "Set Date and Time..."



6. In the pop-up select yes, In the next pop-up under "Time Mode" choose the first option, "Synchronize with server computer time"

Date and Time Settings ? X
Device time
10/10/2022 10:07:18
Time zone
Automatically adjust for daylight saving time changes.
Time mode
Synchronize with server computer time
Synchronize with server computer time
 Synchronize with server computer time 10/10/2022 10:07:21 O Synchronize with NTP server
 Synchronize with server computer time 10/10/2022 10:07:21 O Synchronize with NTP server
 Synchronize with server computer time 10/10/2022 10:07:21 Synchronize with NTP server
 Synchronize with server computer time 10/10/2022 10:07:21 Synchronize with NTP server 192.168.1.194 Set manually 10/10/2022 10:06:15

7. This will then add a task in the task and alarms, once completed the time will now be synched with the computer server time.

Alarms Tasks				
Name	Start	Message	Owner	Progress
➡ Set date and time	10/10/2022	10:08:41 Restarting devices	AXISNVR-2ORNKR	

Step 2 - How to create/edit a schedule

Creating/editing a schedule to use in Secure Entry

These schedules would be used for setting specified time periods for identification profiles and access times for cardholders or door unlock schedules.

Follow these steps to create a schedule:

- 1. In Axis Camera Station open the configuration tab via the "+" symbol found at the top of the screen.
- 2. From the left menu select "Recording and events" and under this drop-down select "Schedules"
- 3. To edit a schedule, highlight the schedule you wish to edit, if you wish to create a new schedule, press new.
- 4. To edit this schedule hold and drag the cursor along the time for each day that you want the schedule to be running. Blue highlighted will be the active times on each day.
- 5. Once you are happy with your schedule you can provide it with a new name in the name field and click apply.

Schedules		Type to search
Name Used		
Office Hours		
Weekends		
New schedule		
		New Remove
Name: Office Hours	Schedule on Schedule off	
Week schedule	Override schedule Add	
00.00 03.00 06:00 09:00 12:00 15:00 18:00 21:00 00:00		
Monday		
Tuesday		
Wednesday		
Thursday		
Friday		
Caburday		
Sunday		
	Apply	

Step 3 - Creating a door

To create a door

If you already have a door in your system that you wish to apply Anti-passback too, please move to the next step.

Follow these steps to create a door:

- 1. In Axis Camera Station open the configuration tab via the "+" symbol found at the top of the screen.
- 2. From the left menu select "Access control" and under this drop-down select "Doors and zones"
- 3. On this page press "+ Add door" and in the pop-up give the door a relative name and select the A1601 door controller in the second drop down, then press "Next"
- 4. Proceed to configure the locks with the correct relay, door monitors and readers, then press "Save".

Type to filter					
	Save Cancel 🗅 Copy configuration 🗸				
Sevices	Doors > Edit door				
Add devices	Overview Door settings O			Sensors	
Cameras				+ Add \checkmark // Edit 🛞 Remove	
Other devices	Door controller	IP address min.b8a4462567a	Door type Door		
Image configuration	Dograma	0.00 00014002.018		U El Loter position sensor	
PTZ presets	A1210				
Management	Identification profile				
External data sources					
Storage					
e storage					
Recording and events					
🙄 Client	Side A			Side B	
Connected services					
Server	IEI OSDP reader			f. REX device	
Licenses					
Ĝ Security					
Access control					
Doors and zones					
Identification profiles					
Card formats and PIN					
Encrypted communication					
Active Directory settings					
Q Smart search 2					
C Smart search 2					
Q Smart search 2					
 Q Smart search 2 ≁ System Health Monitoring 					
 Q. Smart search 2 ➔ System Health Monitoring 					
Q. Smart search 2 → System Health Monitoring					
Q. Smart search 2 + System Health Monitoring					
Q: Smart search 2 → System Health Monitoring					
Q: Smart search 2 → System Health Monitoring					
Q. Smart search 2 → System Health Monitoring					
Q. Smarts search 2 → System Health Monitoring					
Q. Smart search 2					
Q. Smart search 2					
Q. Smarts search 2 → System Health Monitoring					
Q. Smarts search 2 → System Health Monitoring					
© Smart search 2 → System Health Monitoring 'E De able for /	Anti-nassh	back to be	used, a door n	nonitor is	
© Smarts search 2 ★ System Health Monitoring 'E)e able for A	Anti-passb	ack to be a	used, a door n	nonitor is	
C Smart search 2 → System Health Monitoring 'E)e able for A 1ired.	Anti-passb	ack to be a	used, a door n	nonitor is	
G Smart search 2 → System Health Monitoring 'E)e able for A lired.	Anti-passb	ack to be	used, a door n	nonitor is	
© Smart search 2 → System Health Monitoring 'E)e able for A lired.	Anti-passb	ack to be a	used, a door n	nonitor is	

Step 5- Creating a zone and applying Anti-passback

To create a Zone

If you already have a Zone in your system that you wish to apply Anti-passback too, please highlight your zone and click edit, then follow from step 5.

Follow these steps to create a door:

- 1. In Axis Camera Station open the configuration tab via the "+" symbol found at the top of the screen.
- 2. From the left menu select "Access control" and under this drop-down select "Doors and zones"
- 3. On this page Press on "Zones" then press "Add zone"



4. Provide the zone a name and click the "+ add door" button, in the new popup select the doors you would like to have in the zone, then click add.

Configuration × Access manager	ment 🖵 A1210 Assist and Monitor 🕂					
Type to filter	🗟 Save 🗙 Cancel 🤜 Security level	Add				
S Devices	Zones > New Zone					P Search
Add devices	Name	Name 🕆	Door controller	Side A	Side 8	Address
Cameras	Main Entry	A1210	AXIS A1210	Available	Available	axis-b8a446625f7a
Other devices		Intrusion Control	AXIS A1610	Available	Available	axis-b8a444495455
Stream profiles	+ Add door	Wireless	AXIS A1610	Available	Available	axis-b8a44495455
Image configuration						
PTZ presets						
External data sources						
Time synchronization						
🛢 Storage						
Recording and events						
덮 Client						
Connected services						
Server						
Licenses						
Security						
Access control						
Doors and zones						
Identification profiles						
Card formats and PIN						
Multi server						
Active Directory settings						
Q Smart search 2						
+ System Health Monitoring						
		Cancel				

5. Next from the Edit Zone page click on the "security level" button at the top of the screen.

Type to filer Sever X Canal Security Invest	
Zones > Edit Zone Add devices Name Add devices Main fatty Cameras Mon fatty Other devices Cameras	
Stream profiles + Add door @ Remove /	
Image configuration	
Pf2 precisis Name + Dour controllor Dour controllor Management Out and the second sec	
nengyonia orosa da 21/20 da	
Time synchronization	
Storage	
€ Recording and events	
g Client	
Connected services	
2 Server	
🖾 Lienses	
â Security	
Access control	
Doors and zones	
leartification profile Carl format and BN	
Encypted communication	
non seres Ache Directory settings #X	
Q. Smart search 2	
★ System Health Monitoring	

6. In the side pop-up, enable the anti-passback toggle then choose the mode you wish to use, and enter a timeout if you wish to have. If you are editing an active zone, you can use the tickbox to clear the current cardholders entered if necessary. Then click "Add".

Configuration × 🗍 Access managem	nt 🖵 A1210 Assist and Monitor 🕂		£3 ≡
Type to filter			Security level $ imes$
Se Devices Add devices Cameras	Zones > Edit Zone Name Main Intry		Anti-Resback Anti-passback prevents people from using the same oredentials as someone who entered an area before them. It enforces that a person must first cell the area before they can use their ordentimits again.
Other devices Stream profiles Image configuration			Mode Log violation only (Soft) Dery access (Hard)
Management External data sources Time synchronization		Enter from side A	User timeout (sec) 30(Cear cardholders in current anti-
 Storage Recording and events 			passback zone
 Client Connected services 			
Server			
Licenses			
Security			
Access control			
Doors and zones Identification profiles Card formats and PIN Encrypted communication Multi server ^{HIN} Active Directory settings ^{HTN}			
C Smart search 2			
+ System Health Monitoring			Const.

7. Now check you see the Anti-passback green tag next to the name, and the doors are configured for the correct "door usage". Once correct click "Save".

Configuration × Access manager	nent 😓 A1210 Assist and Monitor 🕂			$\Box \equiv$
Turne to filter	Save Cancel 🖘 Security level			
Devices Add devices Cameras	Zones > Edit Zone Name Main Entry			
Other devices Stream profiles Image configuration	+ Add door 🛞 Remove			Search
PTZ presets	Name *	Door controller	Door usage	
Management			Enter from side A	
Time synchronization				
🛢 Storage				
Recording and events				
🛱 Client				
 Connected services 				
Server				
Licenses	I			
Security				
Access control				
Doors and zones Identification profiles Card formats and PIN Encrypted communication Multi server				
Active Directory settings				
Q Smart search 2				
+ System Health Monitoring				

Bonus Step -Exempt from Anti-passback

To configure exempt from anti-passback

If you have a cardholder who should not trigger this rule, please follow to allow them to be exempt.

Follow these steps to make a cardholder exempt:

- 1. In Axis Camera Station open the Access management via the "+" symbol found at the top of the screen.
- 2. From this screen highlight the cardholder then click edit.

Cardholders and groups								
👸 Cardholders								
+ Add 🖉 Edit 🖞 Delete 😞 Suspend 👂 Credentials ~								
1 selected								
🔲 First name 个	Last name	Group	Status	Origin				
Alexander	Strandberg	0						
Ashley	Rios	0						

3. On this page select "advanced" and tick the "Exempt from anti-passback" tickbox then click "Apply".



Considerations and limitations

- 1. The use of the A1610/A1210 requires HTTPS to be enabled.
- 2. Anti-passback cannot be configured directly on a door, it is configured on a zone level.
- 3. Anti-passback requires a door monitor for all doors used.
- 4. If enabling hard violation, a timeout or exit reader should be configured.
- 5. If no exit readers are used, a timeout is recommended.