HOW TO.

Configure Anti-passback in AXIS Camera Station Secure Entry.



February 29, 2024 Rev. 1.0 © Axis Communications AB

How To. Configure Anti-passback access solution in AXIS

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	15

Introduction

This how to document will show you how to set up the selected device(s) to have Anti-passback 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 >	Cancel

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	
					Help	ОК		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"

(7	nage de B 📥 ces, 1 selected		es 🕐 🐵 <table-cell-rows> 🐇</table-cell-rows>	5				
		Name		MAC address	St	atus		Address	
		AXIS A1601 SE		ACCC8EB362F8	c	Ж		<u>192.168.1.219</u>	
			c	Assign IP Address Configure Devices Jser Management	•				
			S	ecurity		HTTPS		Enable/Update	
				Jpgrade Firmware		IEEE 802.1X		Disable	
				et Date and Time		Certificates	•		
				lestart					
				lestore to Factory Settings					
				nstall Application					
				Collect Device Data					
				Connection	-				
			F	leload					
			T	ag 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	

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	?	×
Device time 10/10/2022 10:07:18		
Time zone		
(UTC+01:00) Amsterdam, Berlin, 🔻		
Automatically adjust for daylight saving time c		s.
Time mode		
Synchronize with server computer time		
10/10/2022 10:07:21		
O Synchronize with NTP server		
192.168.1.194		
O Set manually		
10/10/2022 10:06:15		
	Cance	

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 Ret
Name: Office Hours	Schedule on Schedule off	
Name: Office Hours	Schedule on Schedule off	
Week schedule	Override schedule Add	
06:00 03:00 06:00 09:00 12:00 15:00 18:00 21:00 06:00 Monday		
Tuesday		
Wednesday		
Thursday		
Friday		
Saturday		
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".

The construction See of the constru	Configuration X Access management	A1210 Assist and Monitor A				Ĕ
Next Matched Mathdhdd Mathhdd M	Type to filter					
Out of the data was in the data was	-					
Out of the state of		Overview Door settings O			Sensors	
Single image ima						
Terminant Construction Starty Starty						
<pre>segure is a use is is</pre>			840-0084440E3118		Door position sensor	
Married Married Married Soroge Recording and evels Call Soroge						
Image definition of the second services Society Socity Society <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>						
Security Secu	External data sources					
<pre>k Roonding and events C Generation services Server L Generation and main Server S</pre>	Time synchronization					
<pre>State S</pre>	🛢 Storage					
<pre>State S</pre>	Recording and events					
Security Security A consecutive start forme If M and the mean Security A consecutive start forme A consecutive start forme If M and the mean Security A consecutive start forme A consecutive start forme If M and the mean Security Security A consecutive start forme If M and the mean Security Security						
Server Serve						
L kcrese Security A ccress control Mediationer prifin Carl forma and With Pripage communication Mid service System Health Monitoring	Connected services					
E Lenses Δ scess contol Mark scess contol Mark scess contol Second control Second contol Second control	E Server	C EI COR conter				
 scrift Scrift Create and a read Scrift Constant and RR Scrift Scrift Scrift	Licenses					
Access control Not and area Not because at 200 The period of the interview Actes Decays ettings System Health Monitoring TE De able for Anti-passback to be used, α door monitor						
Constant Use difficunt profiles Cast format safe N System Health Monitoring C S mart safe λ * * System Health Monitoring * CE See able for Antii-passback to be used, a door monitor	-					
Cut forma and PN Cut format and PN Cropped connectation Missiver ⁴⁷ Active freetoy stript ⁴⁷ C Smart search 2 + System Health Monitoring CE De able for Anti-passback to be used, α door monitor	·					
Start search P Start search 2						
Frequencies Stratt search 2 * System Health Monitoring TE De able for Anti-passback to be used, a door monitor						
Mistores ^{an} Associationed by attracting * System Health Monitoring TE De able for Anti-passback to be used, a door monitor						
A Atter Detectory setting ²⁸ S snart search 2 * System Health Monitoring TE be able for Anti-passback to be used, a door monitor						
^Q Smart search 2 * System Health Monitoring TE be able for Anti-passback to be used, a door monitor						
* System Health Monitoring TE De able for Anti-passback to be used, a door monitor						
TE be able for Anti-passback to be used, a door monitor						
be able for Anti-passback to be used, a door monitor	- System Health Monitoring					
be able for Anti-passback to be used, a door monitor						
be able for Anti-passback to be used, a door monitor						
be able for Anti-passback to be used, a door monitor						
be able for Anti-passback to be used, a door monitor						
be able for Anti-passback to be used, a door monitor						
be able for Anti-passback to be used, a door monitor						
be able for Anti-passback to be used, a door monitor						
be able for Anti-passback to be used, a door monitor						
be able for Anti-passback to be used, a door monitor						
be able for Anti-passback to be used, a door monitor	0.72)	
	16				I	
					I	
					I	
					I	
	a able for	Anti-nas	shack to b	ob n heau e	or monitor	
equired.	le aple IOI	. Ann-pus	SDUCK IO D	e useu, u uo		
equirea.	a averativa al					
	equirea.					
	-					

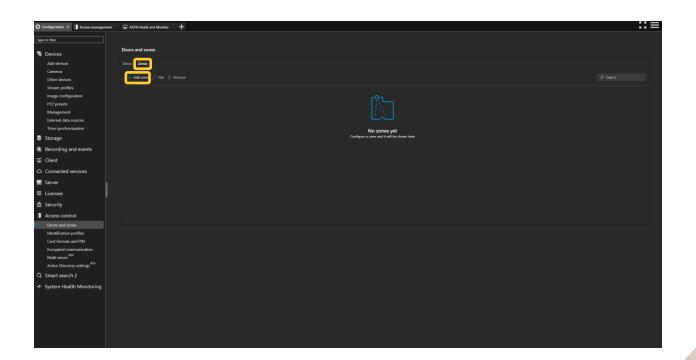
Step 5– Creating a zone and applying Anti-passback

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 X Access management	🖵 A1210 Assist and Monitor 🛛 🕂					
Type to filter	Save 🗙 Cancel 🧠 Security level	Add				
	Zones > New Zone					Search
Services	Name	Name 🕆	Door controller	Side A	Side 8	Address
Add devices Cameras	Main Entry	✓ A1210	AXIS A1210	Available	Available	axis-b8a44f625f7a
Cameras Other devices		Intrusion Control	AXIS A1610	Available	Available	axis-b8a44495455
Stream profiles	+ Add door	Wireless	AXIS A1610	Available	Available	axis-b8a444495455
Image configuration						
PTZ presets						
Management External data sources						
Time synchronization						
Storage						
Recording and events						
떂 Client						
Connected services						
E Server						
Licenses						
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						
		Add				
						,

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

Centry of a Normany of Centry of a NOP Ander and Maxim Name to Many of a Normany of A NOP Ander and Maxim Name to Many of a Normany of A NOP Ander and Maxim Name to Many of A NoP Ander and Maxim Name to Many of A NoP Ander and Maxim Name to Many of A NoP Ander and Maxim Name to Many of A NoP Ander and Maxim Name to Many of A NoP Ander and Maxim Name to Many of A NoP Ander and Maxim Name to Many of A NoP Ander
Dreices Add drok one Add drok one Other drok Other drok Other drok Other drok Image one fix one set PT2 presist Management Index offices Inde
Porteises Image: Control of deficients Other deficient Image: Control of deficients Proprests Image: Add dow © Remont Madage: Strang data sources Image: Add dow © Remont Strang deficient data sources Image: Add dow © Remont Strang deficient data sources Image: Add dow © Remont Strang deficient data sources Image: Add dow © Remont Strang deficient data sources Image: Add dow © Remont Strang deficient data sources Image: Add dow © Remont Strang deficient data sources Image: Add dow © Remont Strang deficient data sources Image: Add dow © Remont Strang deficient data sources Image: Add dow © Remont Strang deficient data sources Image: Add dow © Remont Strang deficient data sources Image: Add dow © Remont Strang deficient data sources Image: Add dow © Remont Strang deficient data sources Image: Add dow © Remont Strang deficient data sources Image: Add dow © Remont Strang deficient data sources Image: Add dow © Remont Strang deficient data sources Image: Add dow © Remont Strang deficient data sources Image: Add dow @ Remont S
Cancal Mage configuration Image configuration <td< th=""></td<>
Obter devices Image configuration Image confige configuratio
Strang profile
mage configuration P for protein Mage configuration B formal data sources Three synthetication S formal data sources C format data sources L format data
Pipedia image image image Management image Attria Attria image imagement imagement imagement imagement imagement imagement imagement imagement imagement imagement <td< th=""></td<>
Maragement At20 At20 Tele semant data sances Time septement Imagement Imagement Imagement Imagement Imagement
Event data sources Image: Control of
 Storage Recording and events C lient Conected services Server Lients Access control Joccss control Lients and access and acc
Connected services Server Connected services Access control Access control Identification profile
Licenses Security Access control Does and zones leantification profiles
Security Access control Door and zones leditification profiles
Access control Doors and zone Identification profiles
Doors and zones Identification profiles
Doors and zones Identification profiles
Identification profiles
Card formats and PIN
Encrypted communication
Multi seren ^{era}
Active Directory settings ^{the}
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 management	N A1210 Assist and Maniltor		[] =
Type to filter	Save X Cancel Security level		Security level ×
	Zones > Edit Zone		Anti-Passback
Services			Anti-passback prevents people from using the
Add devices			same credentials as someone who entered an area before them. It enforces that a person
Cameras			must first exit the area before they can use their credentials again.
Other devices Stream profiles			Mode
Image configuration			Log violation only (Soft)
PTZ presets			O Deny access (Hard)
Management			User timeout (sec)
External data sources			
Time synchronization			Clear cardholders in current anti- passback zone
🛢 Storage			passoccume
Recording and events			
🛱 Client			
 Connected services 			
Server			
Licenses			
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			
system nearth monitoring			
			Add Cancel

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 X Access manageme	eent 🖵 A1210 Assist and Monitor 🕂			К Я К Я
Type to filter	Save Cancel Security level			
Sevices	Zones > Edit Zone			
Add devices	Name			
Cameras	Main Entry	Anti-Pansback		
Other devices				
Stream profiles	🕂 Add door 🛞 Remove			🔎 Search
Image configuration				
PTZ presets	Name †	Door controller	Door usage	
Management External data sources		AXIS A1210	Enter from side A	
Time synchronization				
Storage				
 Recording and events 				
⊈ Client				
 Connected services 				
Server				
Licenses				
Security				
Access control				
Doors and zones				
Identification profiles				
Card formats and PIN				
Encrypted communication Multi server				
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 click the three dots next to the cardholder then click edit.

Configura	ion 📳 Access management 🗶 🖵 A1210 Assist and Monitor 🛛 🕂					$\Box \equiv$
Ē	Cardholders Groups	Q, ashiey				+
٥	Ashley Rios Bd58b165-c934-4a0b-bc1c-ee3689bd8b90		:	I Axis	🛓 3 cardholder(s) 👔 1 door(s)	
				I Intrusion	2 7 cardholder(s) 1 door(s)	
				I Work Day	±1 ±1]2	
				Doors Zones		
				A1210		1
				Intrusion Control		1
				Wirotess		1

3. On this page press on the "More" expansion menu and tick the "Exempt from antipassback tickbox then click "Apply".

🗘 Configura	tion 🗍 Access management × 🖵 A1210 Assist and Monitor 🕂				::≡
Ē	× Edit cardholder				
٠	Lardholder		Credentials		
r.	Fetham				
	Ashley	PIN credential			
	Rios				
	Carabase 10 Básšíb 165 c334 4alob boto: ee03688kobb/90 Email address				
	Email address				
	Groups 🗸				
	∧ More				
	Suspond cardholder	Recent transact	Recent transactions		
	Long access time		Date	Time	
	Exempt from lockdown				
	22 Exemptition anti-passback				

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.