

HOW TO.

Configure Anti-passback in AXIS Camera Station Secure Entry.

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 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.

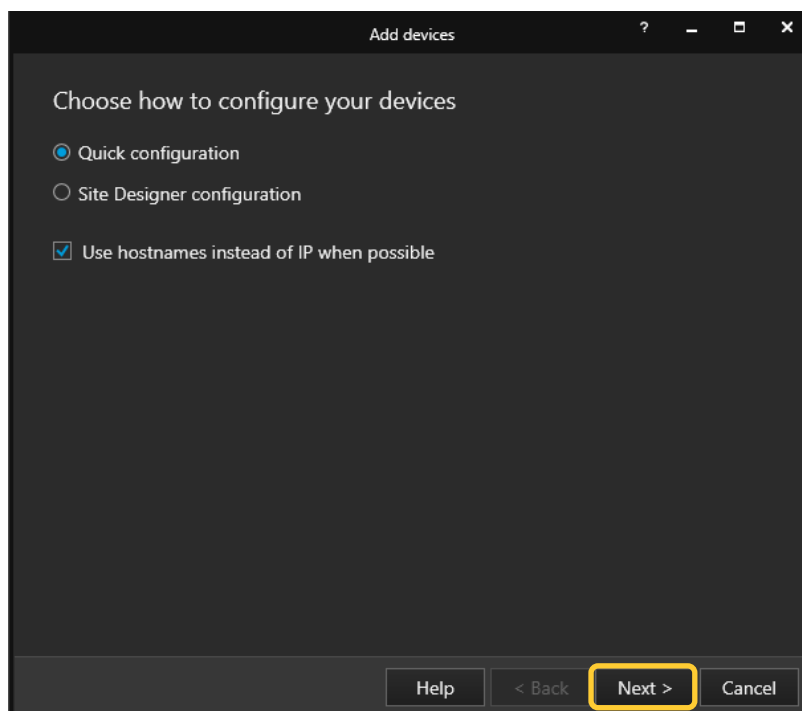
Step 1 – Adding/updating & setting up devices

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:

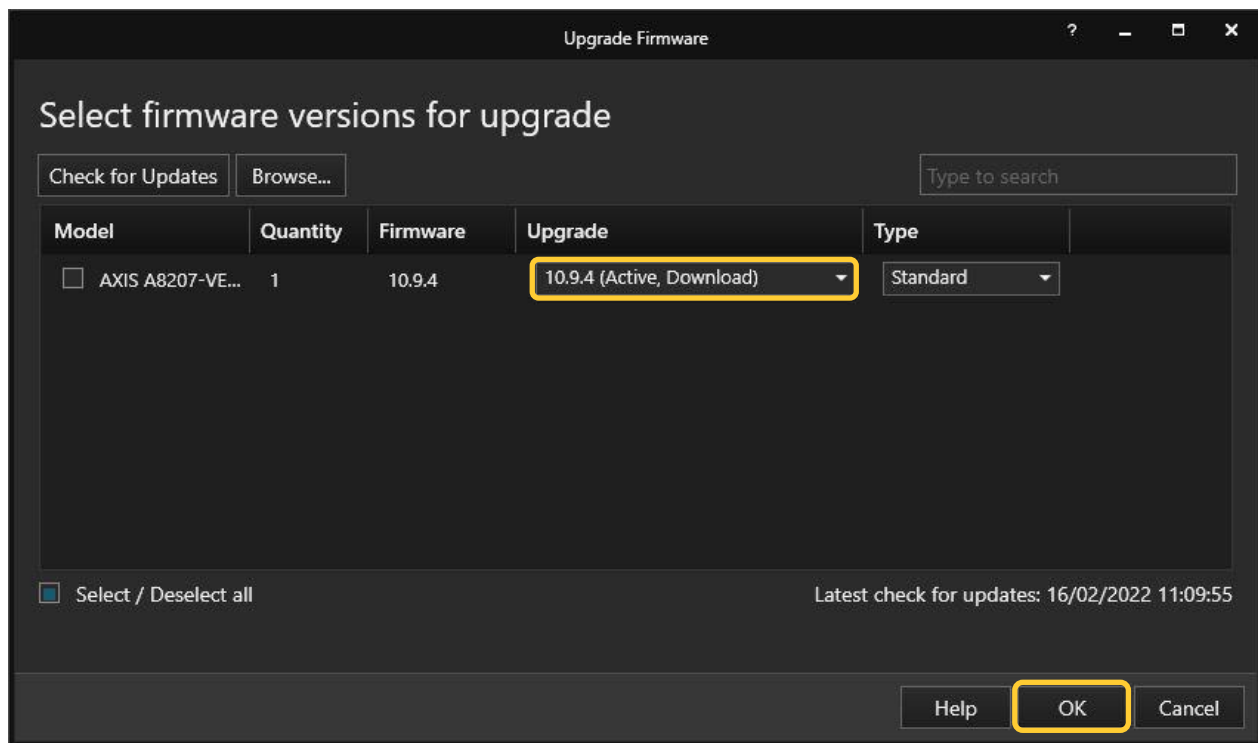
1. In Axis Camera Station open the configuration tab via the “+” symbol found at the top of the screen.
2. From the left menu select “Devices” and under this drop-down select “Add Devices”
3. On this page if the units are in your network, you should see them, if they are missing then you can try do a 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



To update the devices

Follow these steps to update your devices:

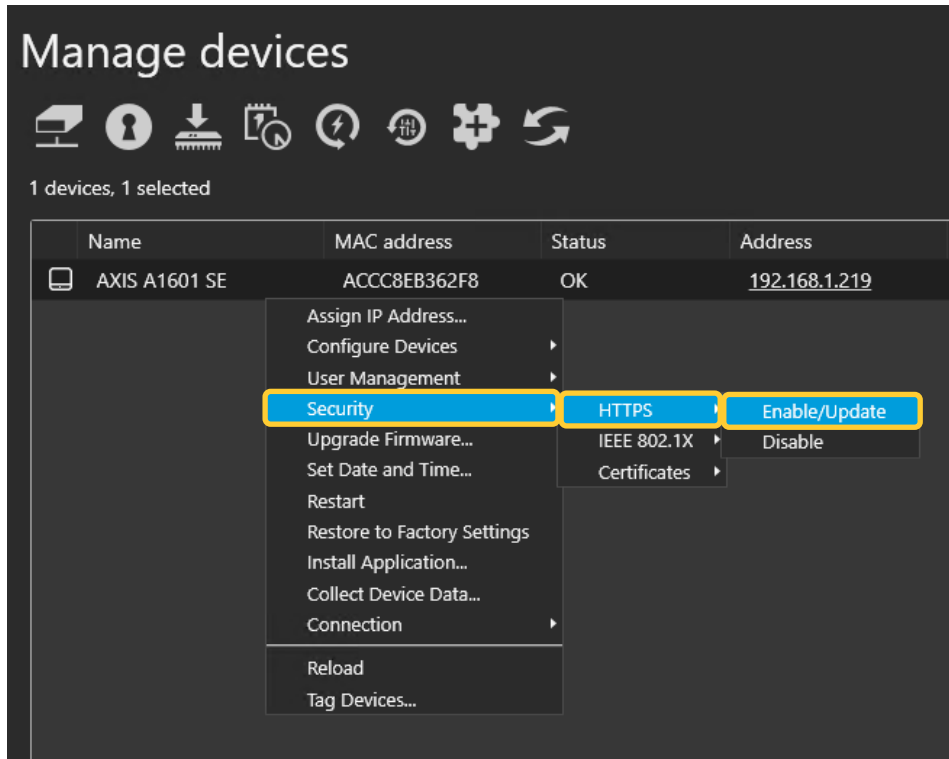
1. In Axis Camera Station open the configuration tab via the “+” symbol found at the top of the screen.
2. From the left menu select “Devices” and under this drop-down select “Management”
3. From this page hold “ctrl” and select the devices, once selected press the update firmware button.
4. In the popup 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”



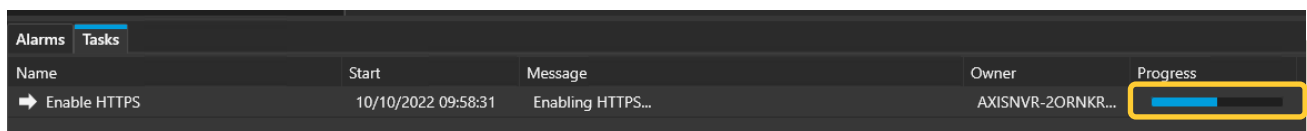
To setup the devices

Follow these steps to setup your devices:

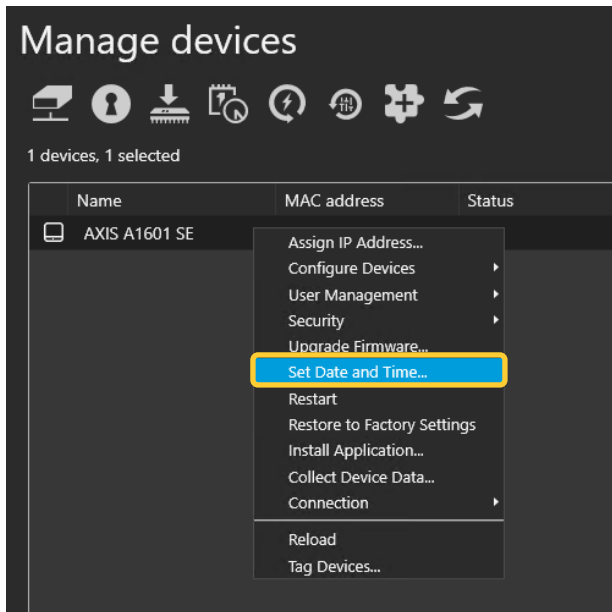
1. In Axis Camera Station open the configuration tab via the “+” symbol found at the top of the screen.
2. From the left menu select “Devices” and under this drop-down select “Management”
3. Right click on the device and select “Security – HTTPS – Enable/Update”



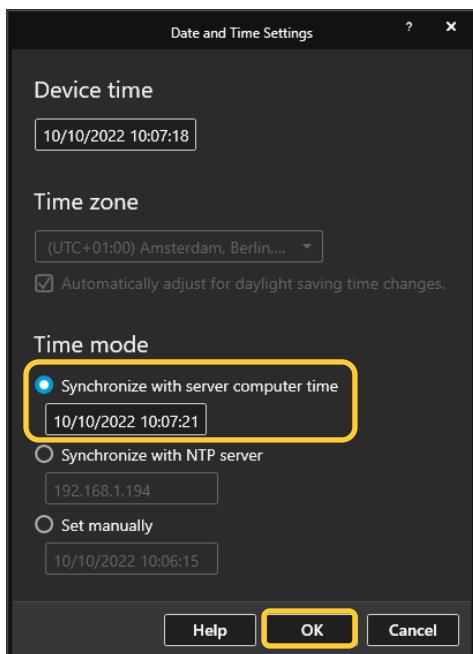
4. This will create a task in the task and alarms, once this has completed, HTTPS is enabled on this device.



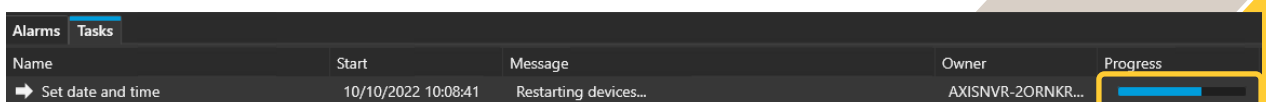
- Next to setup is the time & date on the device, we do this but right clicking on the device in Devices – Management and selecting “Set Date and Time...”



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



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



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.

The screenshot displays the 'Schedules' configuration page in Axis Camera Station. At the top, there is a search bar labeled 'Type to search'. Below it, a table lists existing schedules with columns for 'Name' and 'Used'. The 'Office Hours' schedule is highlighted. Below the table, there are 'New' and 'Remove' buttons. The main area shows the configuration for the 'Office Hours' schedule. It includes a 'Name' field containing 'Office Hours', a legend for 'Schedule on' (blue square) and 'Schedule off' (white square), and a 'Week schedule' grid. The grid shows the days of the week from Monday to Sunday, with time slots from 00:00 to 06:00. Blue bars indicate the active schedule periods. There is an 'Override schedule' section with an 'Add...' button. At the bottom, there is an 'Apply' button.

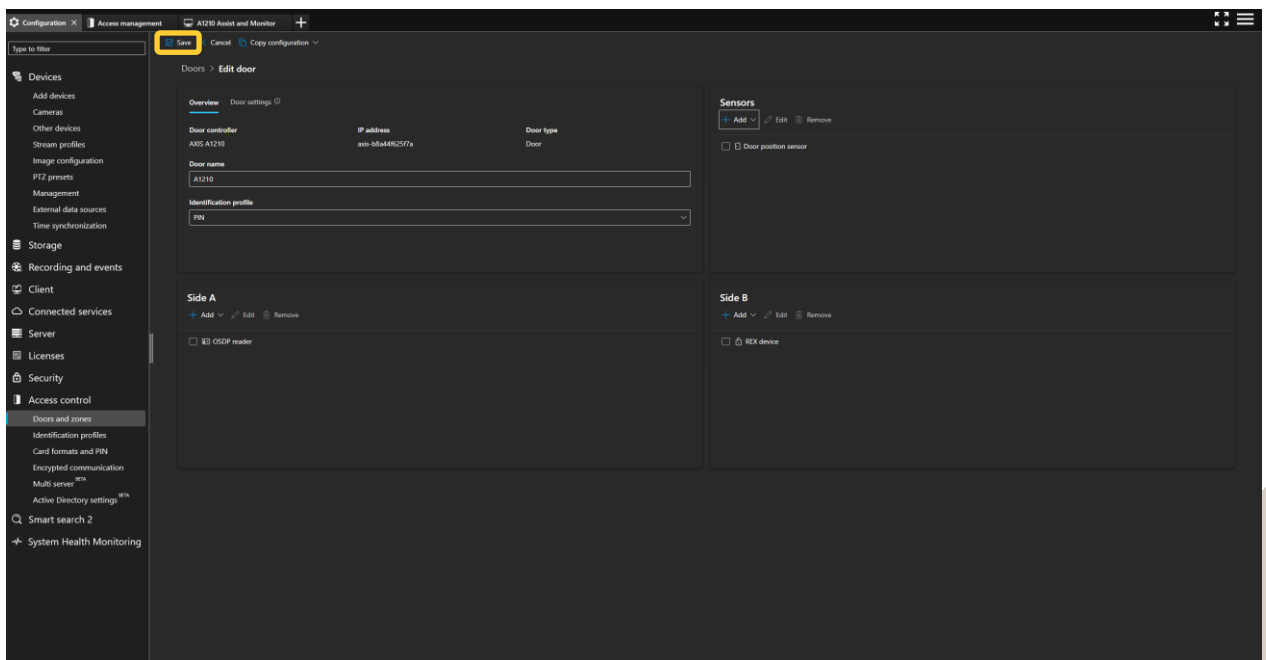
Step 3 - Creating a door

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”.



NOTE

To be able for Anti-passback to be used, a door monitor is required.

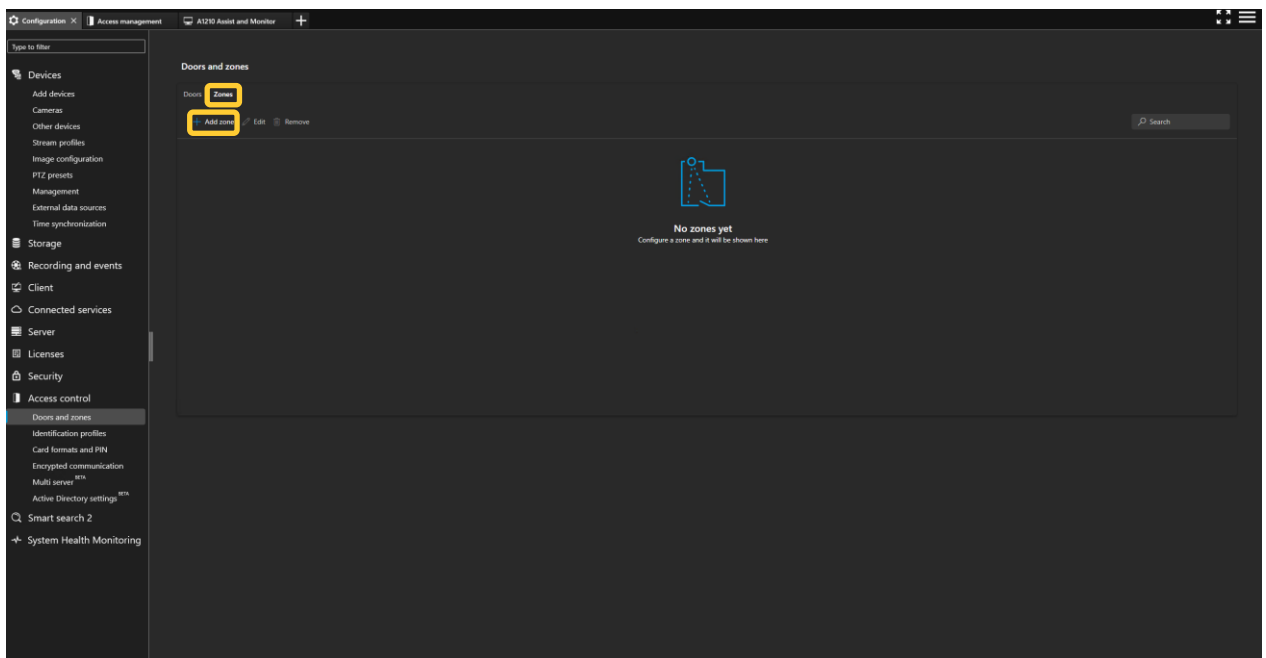
Step 5- Creating a zone and applying Anti-passback

To create a Zone

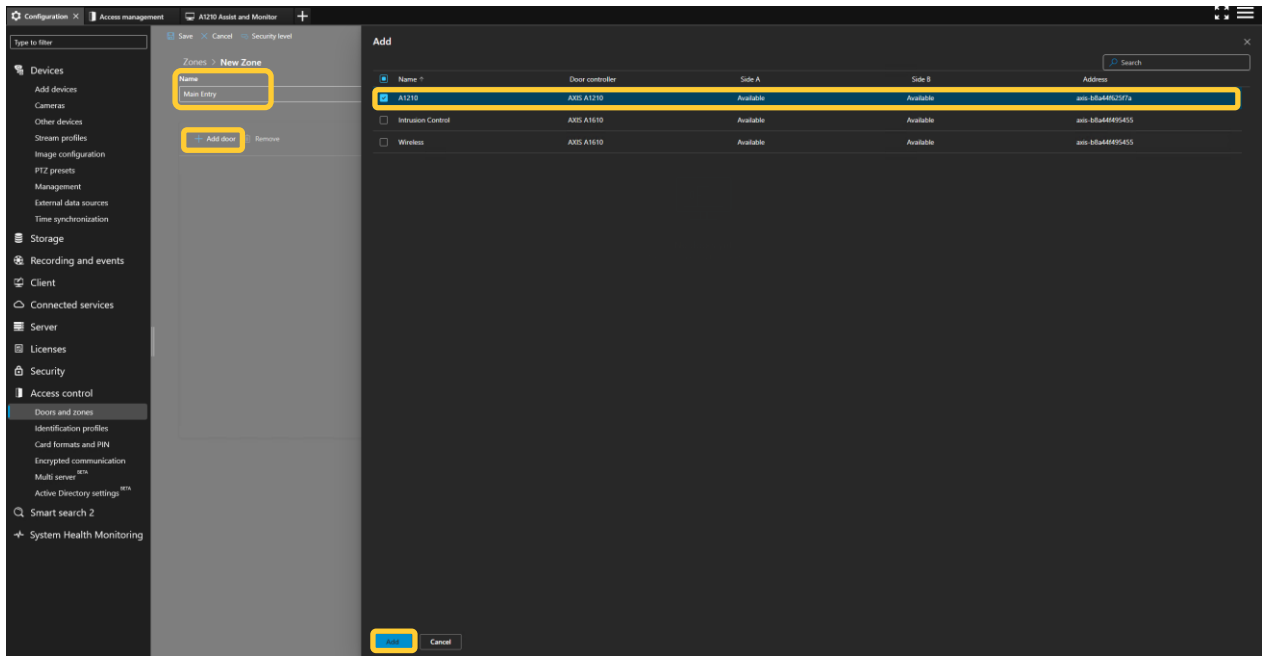
If you already have a Zone in your system that you wish to apply Anti-passback too, please highlight your zone and click edit, then follow from step 5.

Follow these steps to create a door:

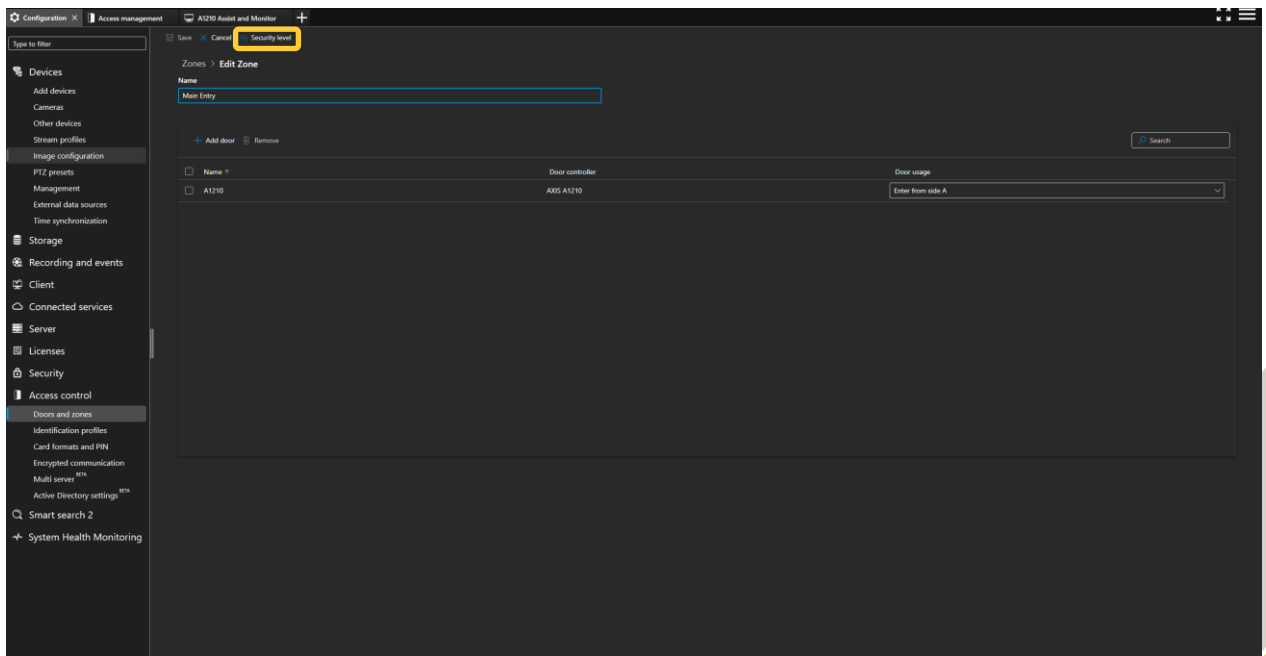
1. In Axis Camera Station open the configuration tab via the “+” symbol found at the top of the screen.
2. From the left menu select “Access control” and under this drop-down select “Doors and zones”
3. On this page Press on “Zones” then press “Add zone”



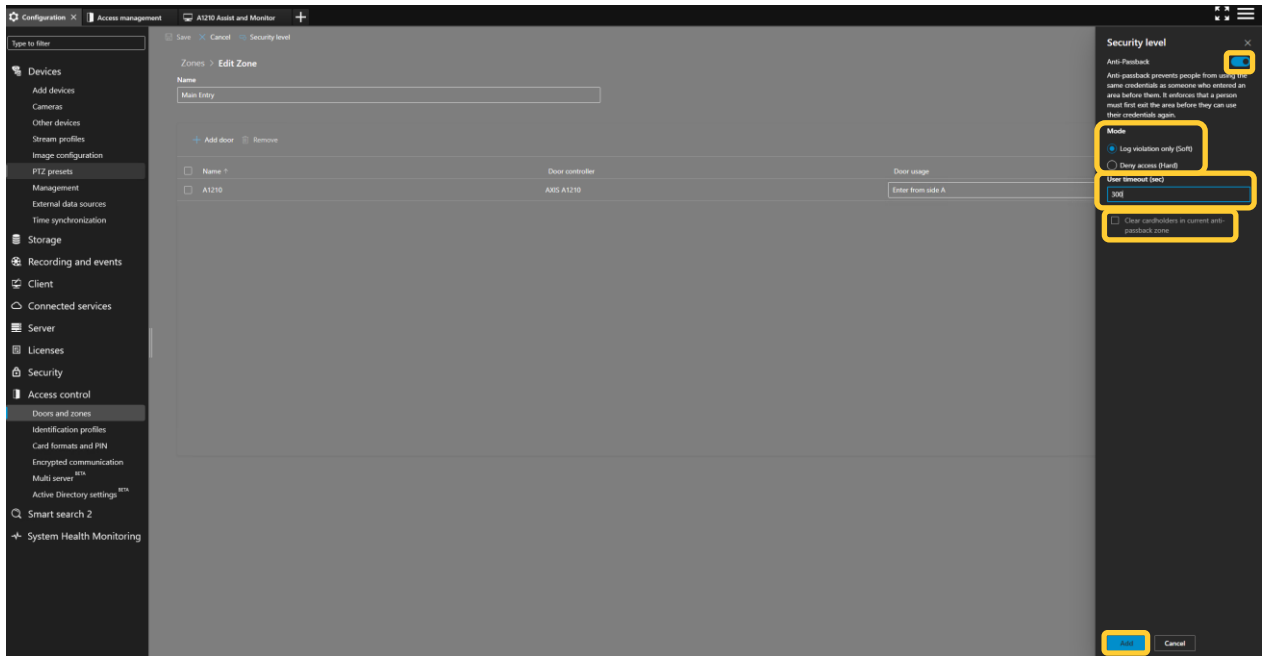
4. Provide the zone a name and click the “+ add door” button, in the new popup select the doors you would like to have in the zone, then click add.



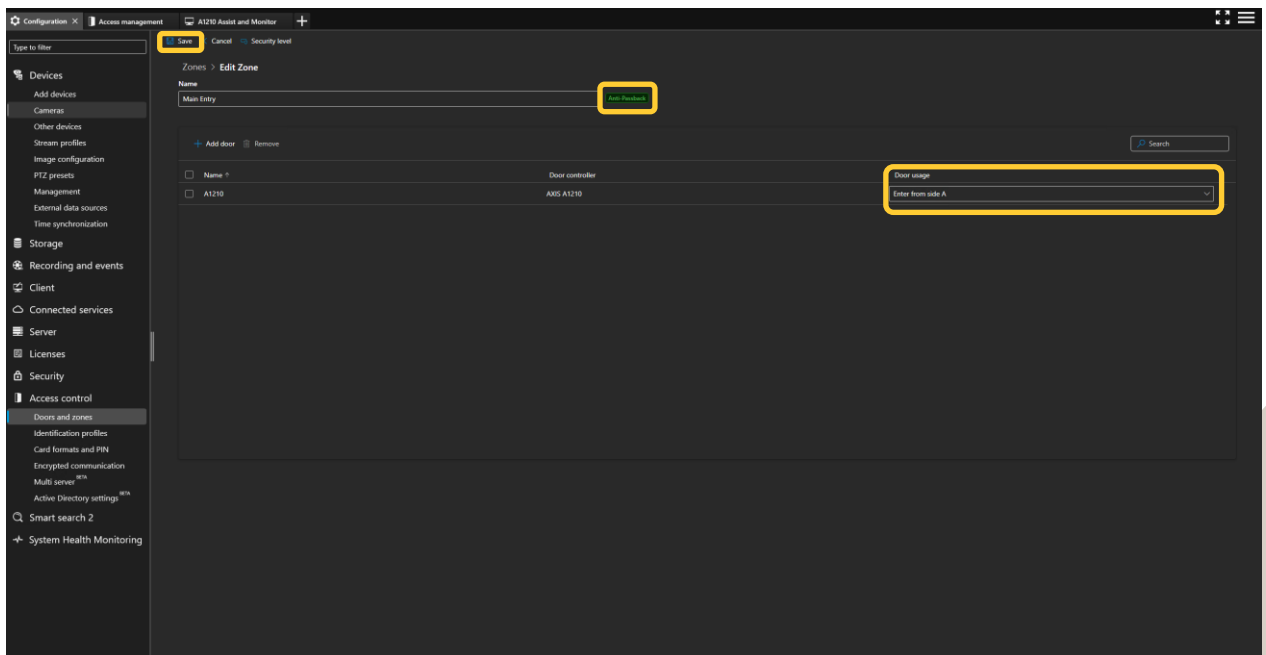
5. Next from the Edit Zone page click on the “security level” button at the top of the screen.



- 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”.



- 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”.



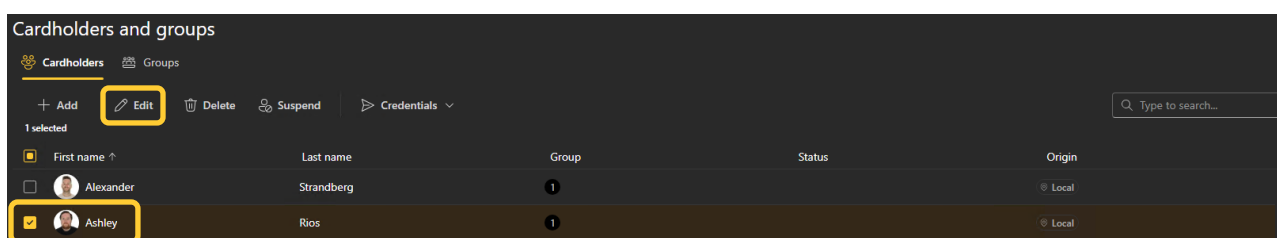
Bonus Step –Exempt from Anti-passback

To configure exempt from anti-passback

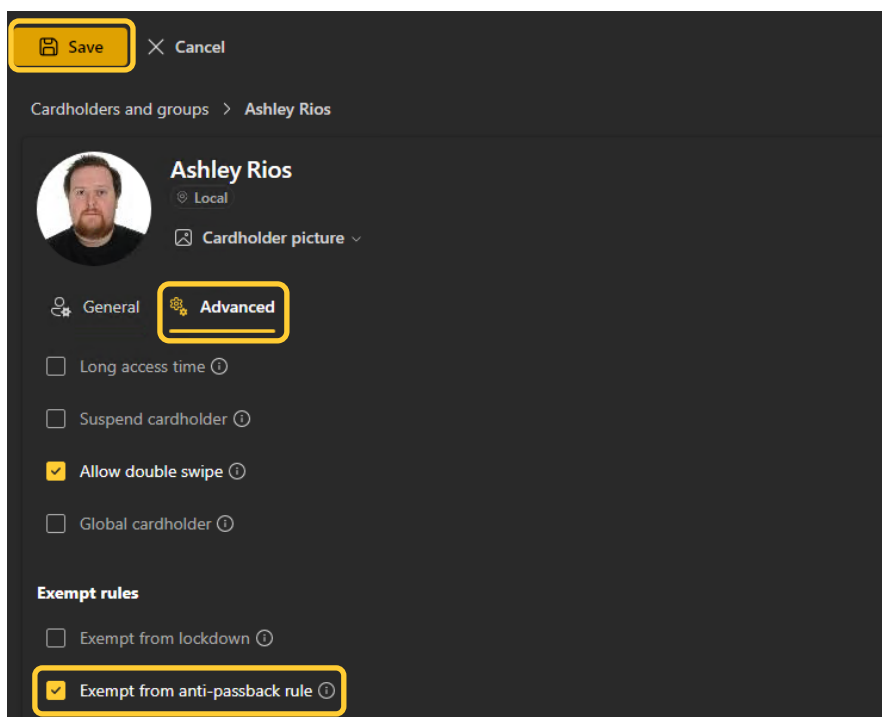
If you have a cardholder who should not trigger this rule, please follow to allow them to be exempt.

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.



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.