HOW TO.

Create action rules to solve specific use cases for access control in AXIS Camera Station Secure Entry

October 4, 2021
Rev. 2.0

Contents

Introduction

Using the steps in this document you will be guided through the possibilities of setting up specific action rules for relevant scenarios when it comes to access control in AXIS Camera Station Secure Entry.

Prerequisites

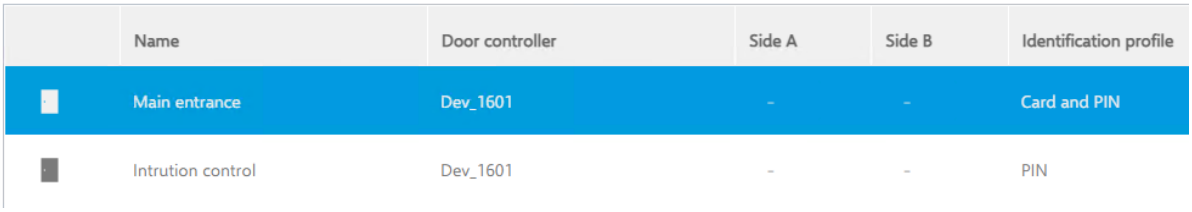
AXIS Camera Station 5.39 or higher

AXIS A1601 10.7.0.2 or higher.

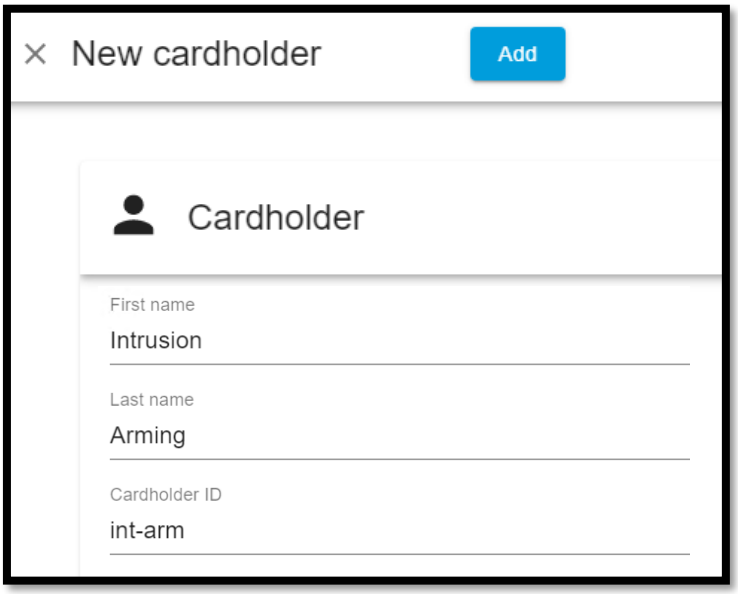
Please note that Axis doesn't take any responsibility for how this configuration may affect your system. If the modification fails or if you get other unexpected results, you may have to restore the settings to default.

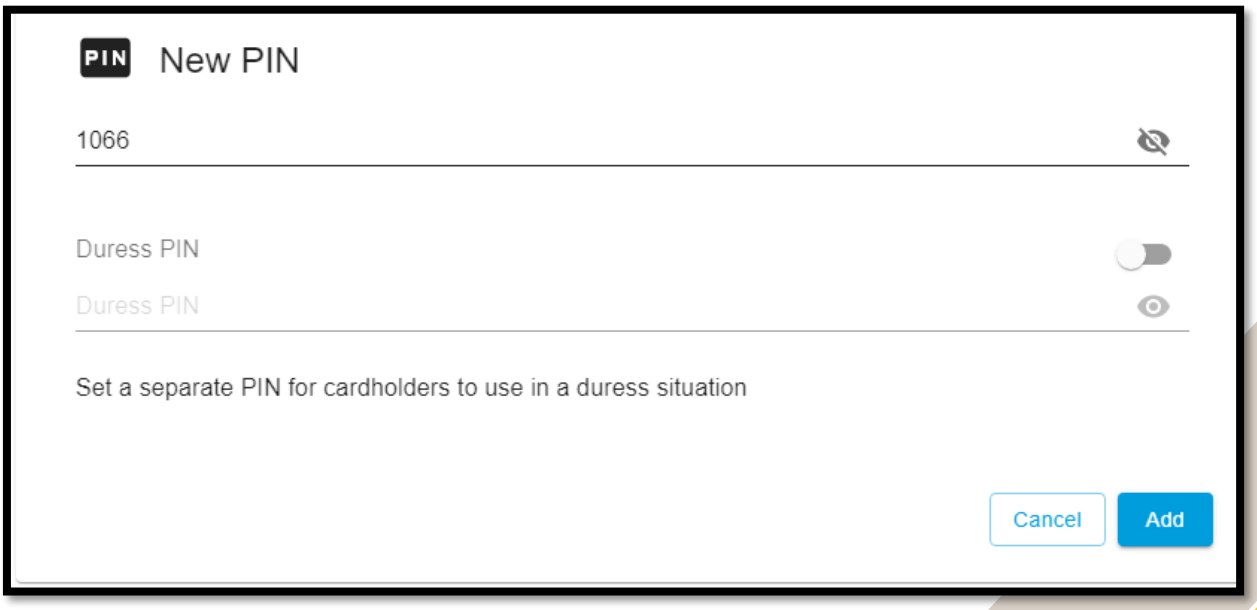
Use Case 1: Arming/Disarming intrusion panel with a specific PIN

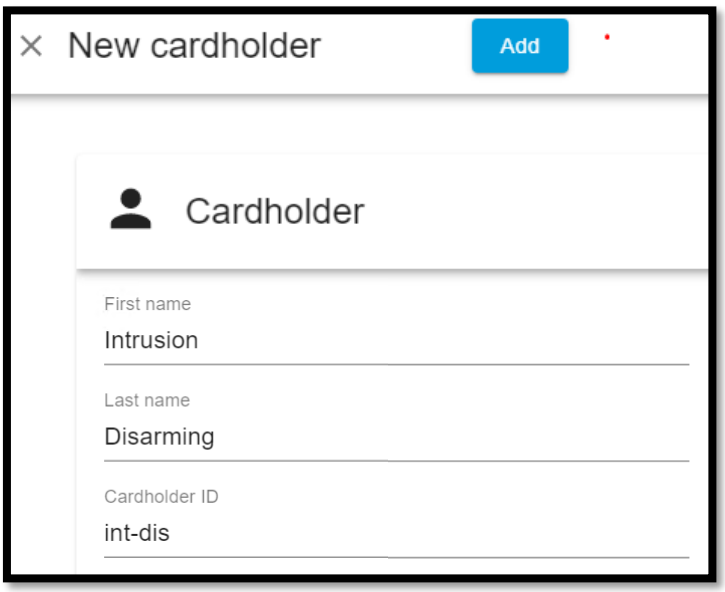
There is a possibility to connect to an intrusion system with for instance the relays of a A91 series with specific PIN-codes for arming and disarming.
For this example, we will have one specific door (Intrusion control) with separate card reader with keypad configured for managing the arming and disarming.

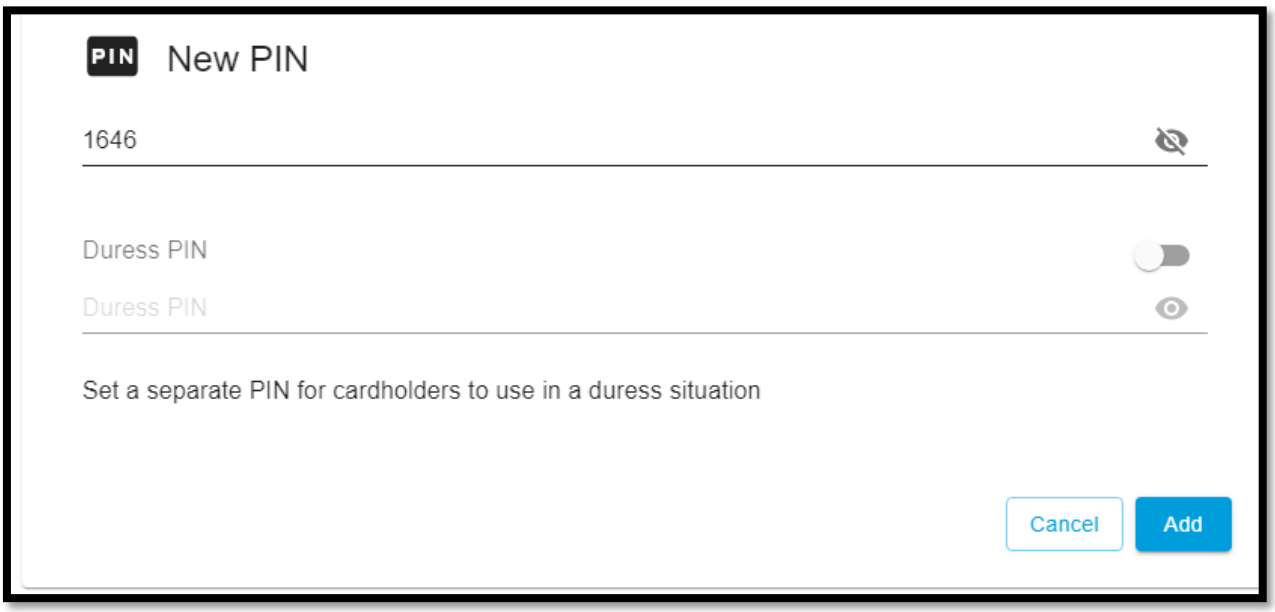


Step 1 – Make arming and disarming cardholders with different PIN Credentials.
Create cardholders with one separate PIN each. One for arming and one for disarming.

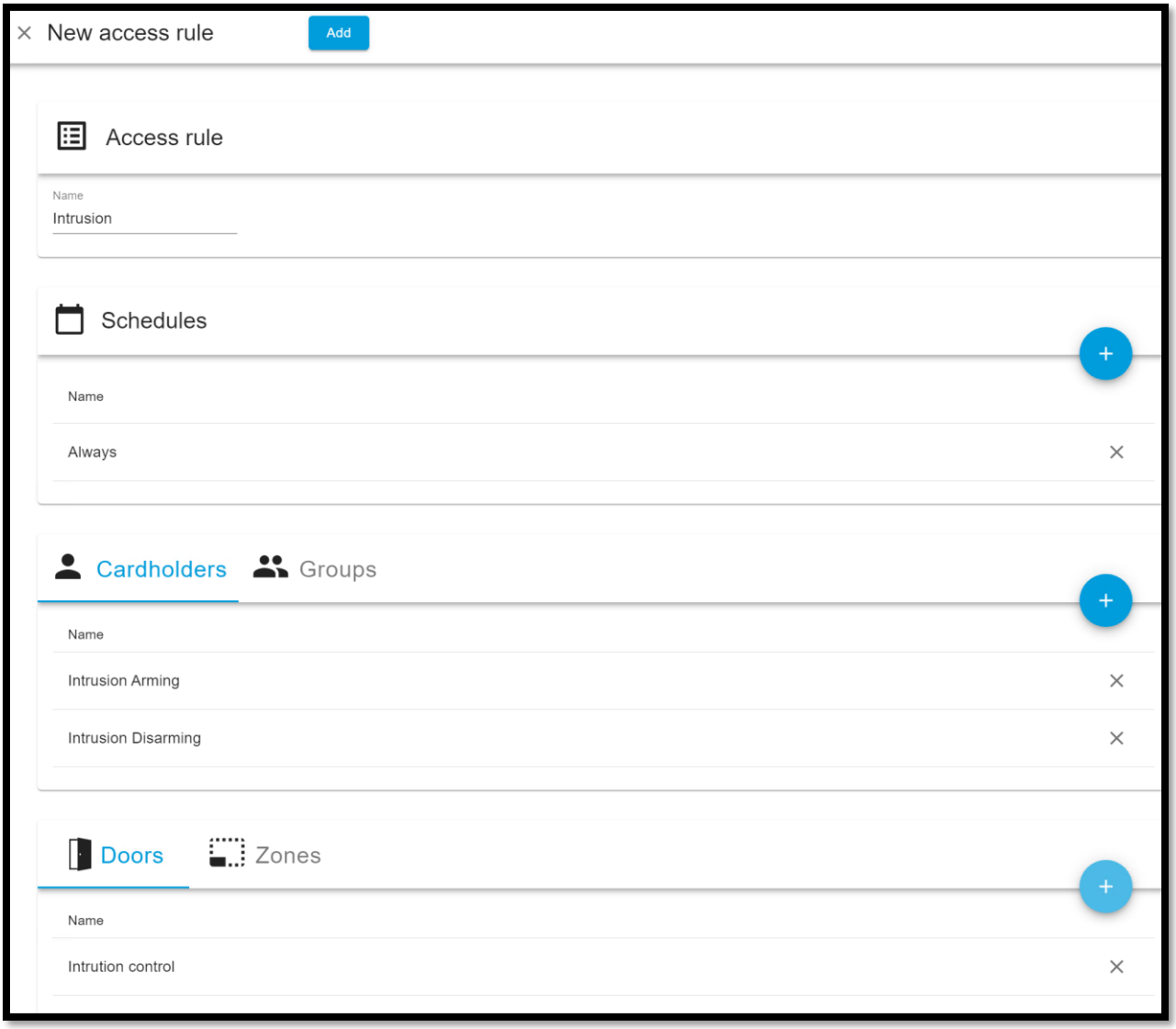





New cardholder
Add
Cardholder
First name
Intrusion
Last name
Disarming
Cardholder ID
int-dis

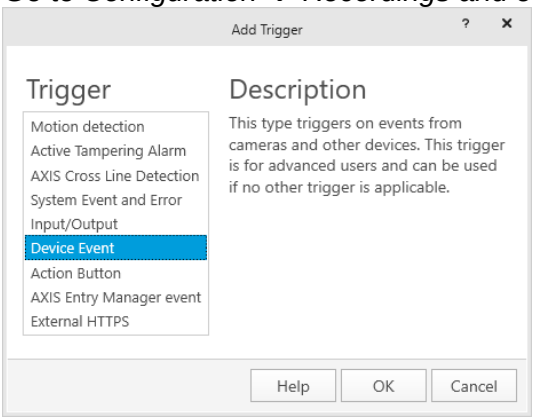

PIN
New PIN
1646
Duress PIN
Duress PIN
Set a separate PIN for cardholders to use in a duress situation
Cancel
Add

Add the Cardholders, the “Intrusion control” door and the schedule “Always” to a new access rule:

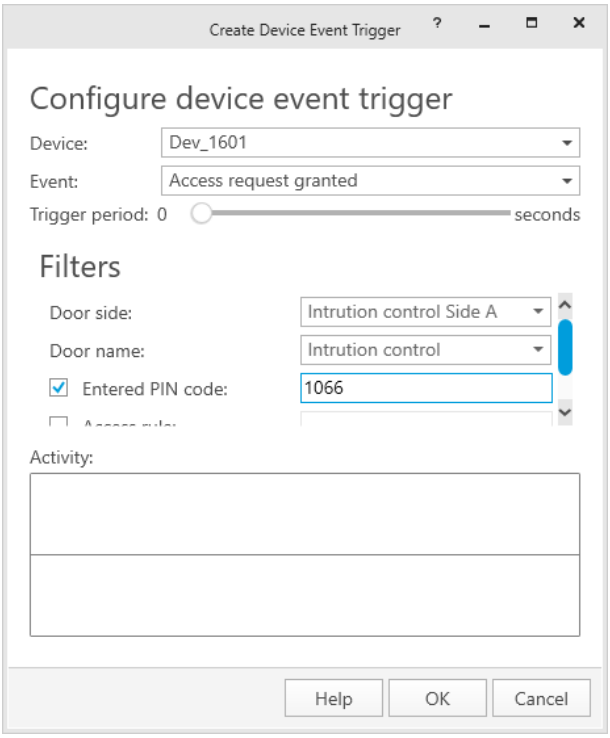


Step 2 – Create an arming rule.

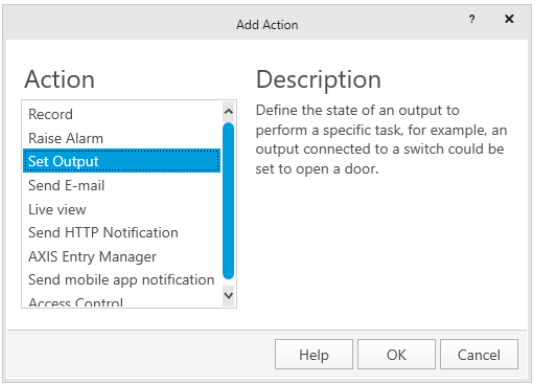
Go to *Configuration* → *Recordings and events* → *Action rules* and create a new rule.



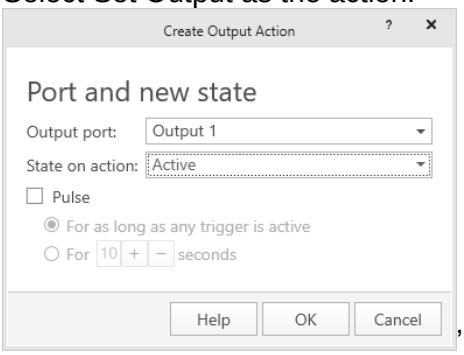
Select device event.



Configure the trigger as an Access request granted with the filter on the specific arming PIN configured earlier.



Select Set Output as the action.

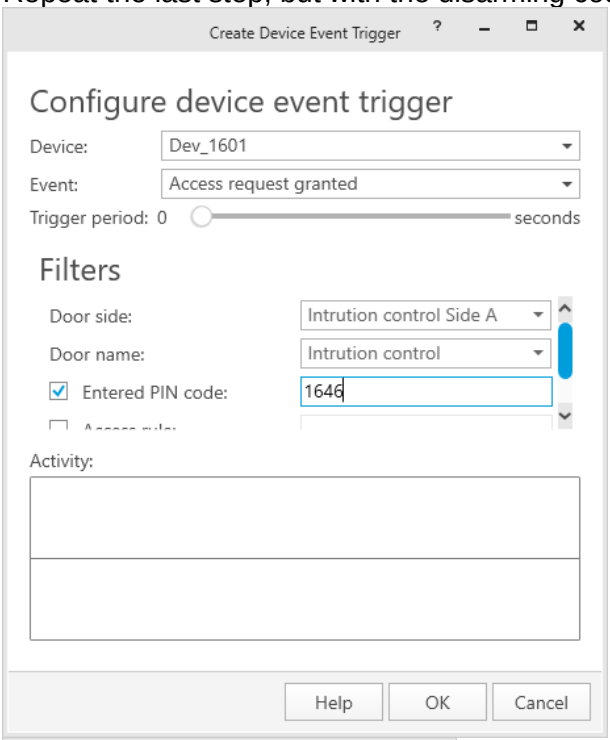


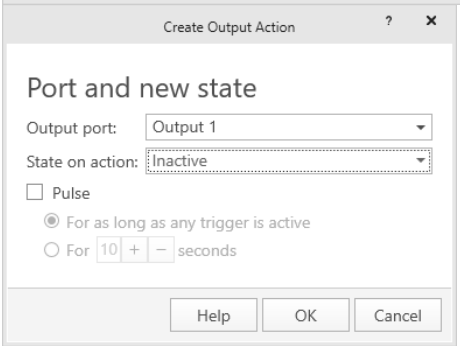
,

This could be a relay of a A91 series device or an output of any Axis camera that is connected to the intrusion system to control it.

Step 3 – Create an disarming rule.

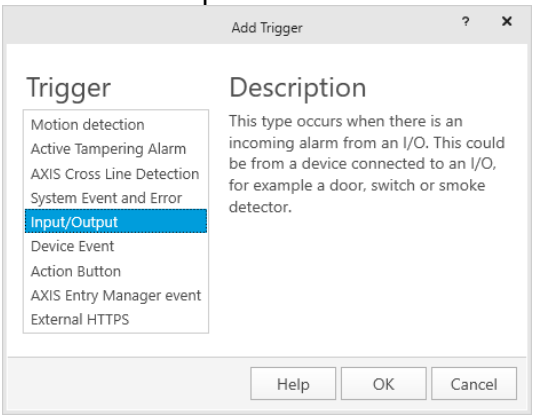
Repeat the last step, but with the disarming code and deactivating the output.



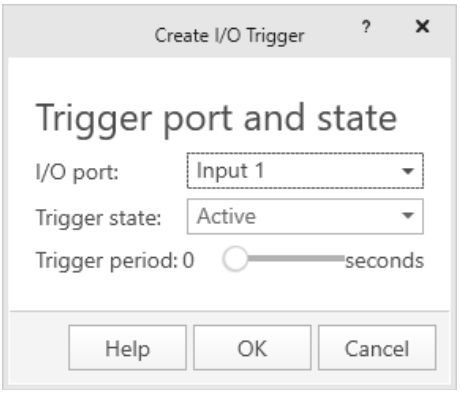


Bonus step – Create rule to lock down doors when intrusion system is armed.

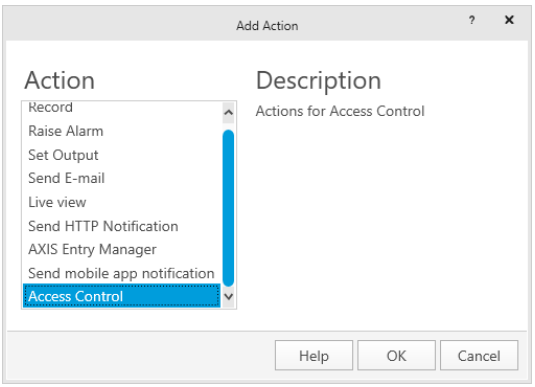
You can also create a rule that locks down the main entrance when the intrusion system is armed. This requires a wire connected to an input on a Axis device, like the A91 series.



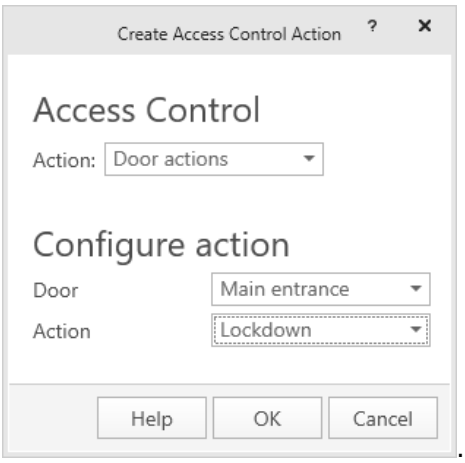
Select the Input/Output trigger



Trigger on when input 1 is active.

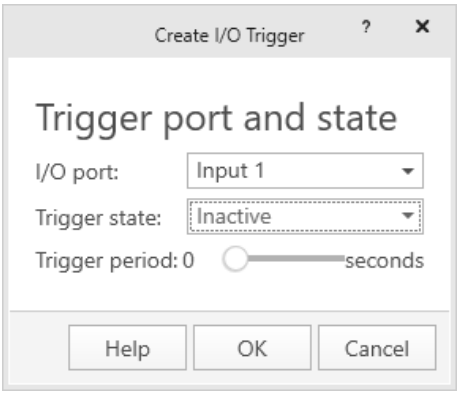


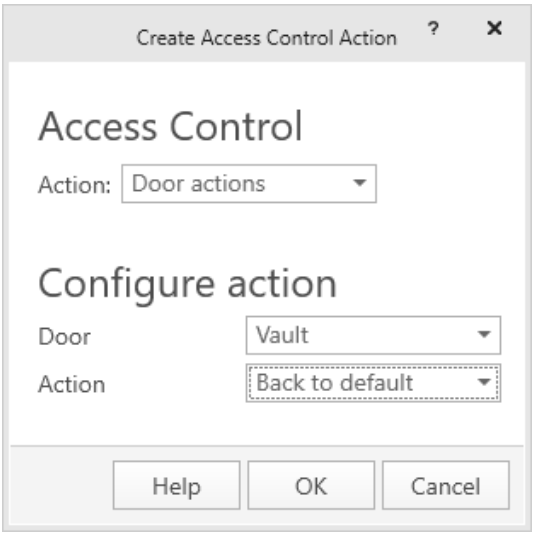
Create an action for Access Control



.

You also need to create the inverted rule for when the intrusion system is not armed.



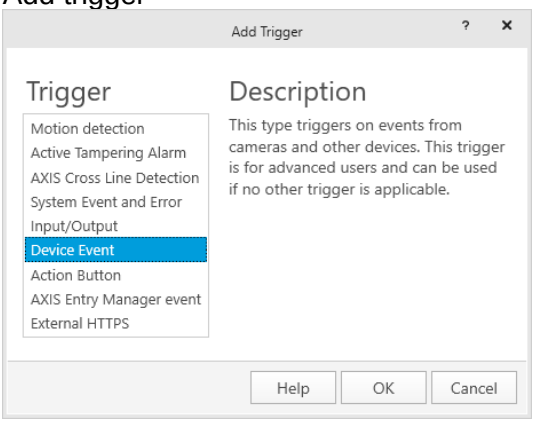

Create Access Control Action
Access Control
Action:
Door actions
Configure action
Door
Vault
Action
Back to default
Help
OK
Cancel

Use Case 2: Security staff mobile notification on door alarm

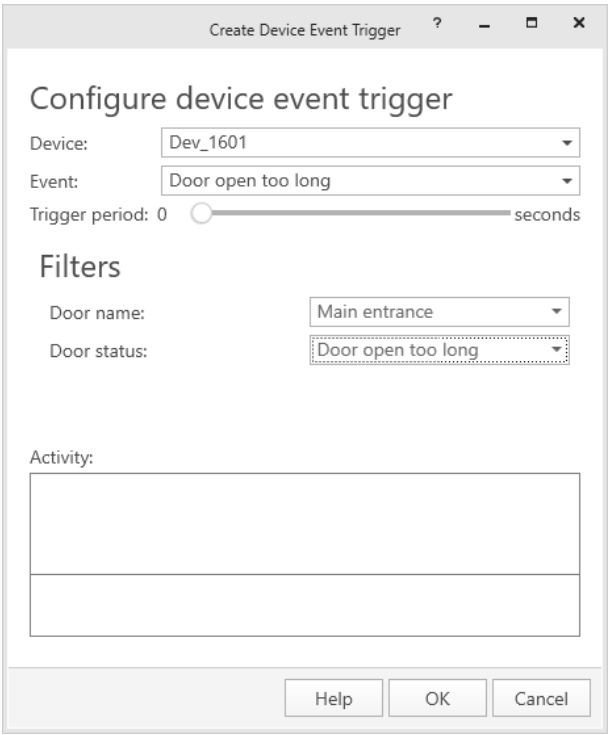
This rule is to setup a rule that sends a notification to the AXIS Camera Station mobile app if there is a door alarm like door forced open in the system.

Creating the rule.

Add trigger

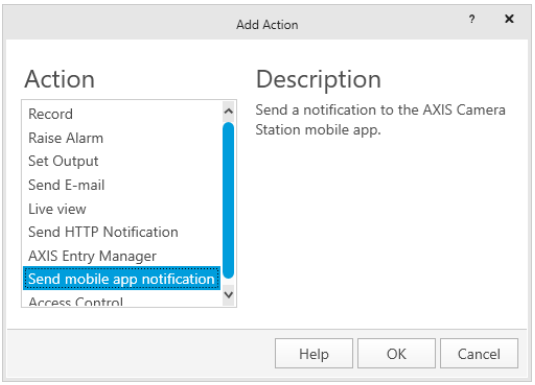


Select Device Event

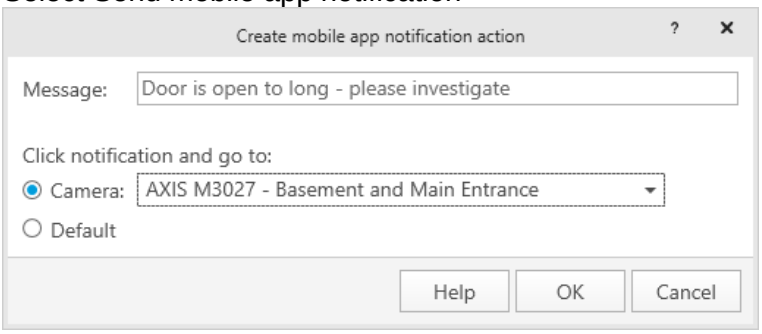


Select the AXIS A1601, the Event you want to trigger on, filter on the door name and the status.

Add an action



Select Send mobile app notification



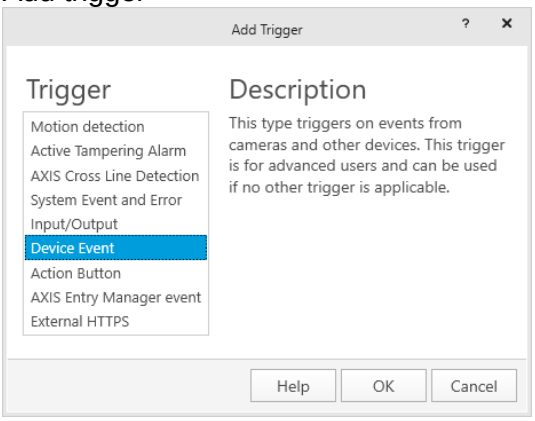
Fill out the message and the camera that the notification should highlight for the security staff.

Use Case 3: Changing PTZ camera view and start recording on door forced open

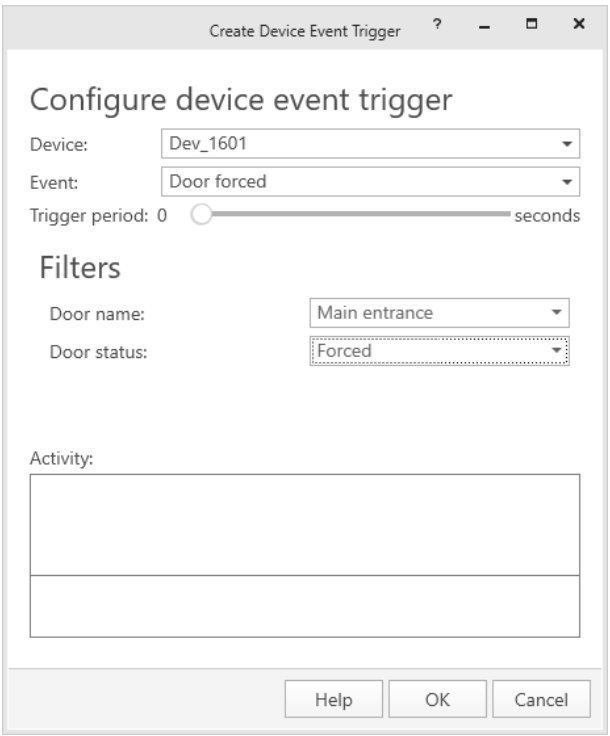
Similar to the last scenario this guides you to create e rule to trigger on door forced open and set a PTZ to go to a preset position and open a live view window.

Creating the rule.

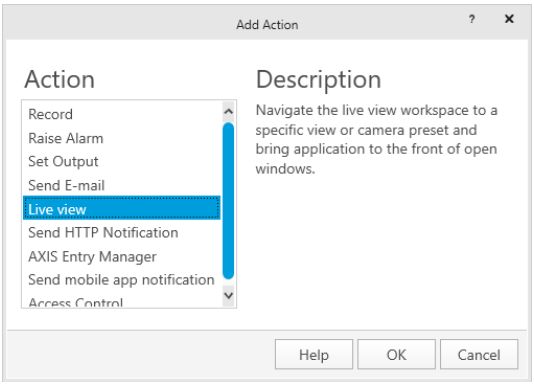
Add trigger



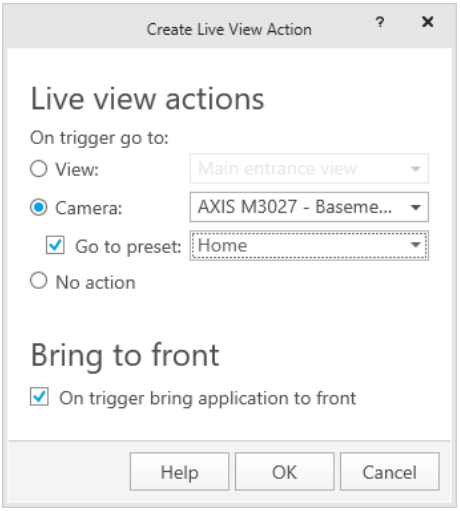
Select Device Event



Select the controller and Door forced, filter the event on door name and status.



Add a Live view action

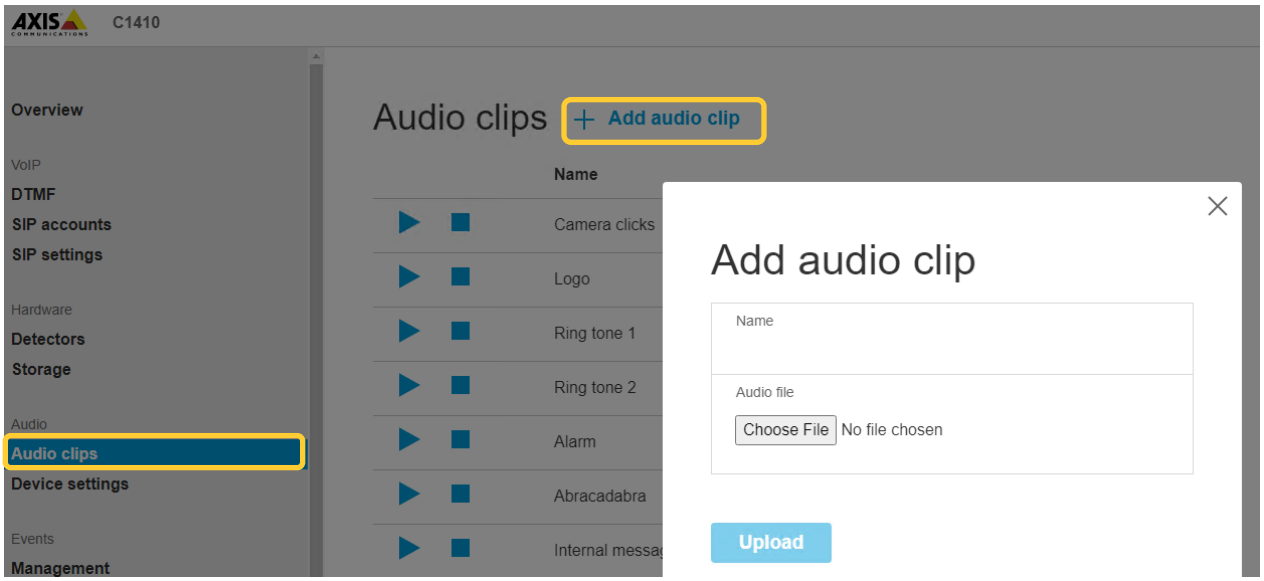


Select the PTZ (Or virtual PTZ) camera and check the preset checkbox and select the preset relevant area, bringing the live view to the top of the application.

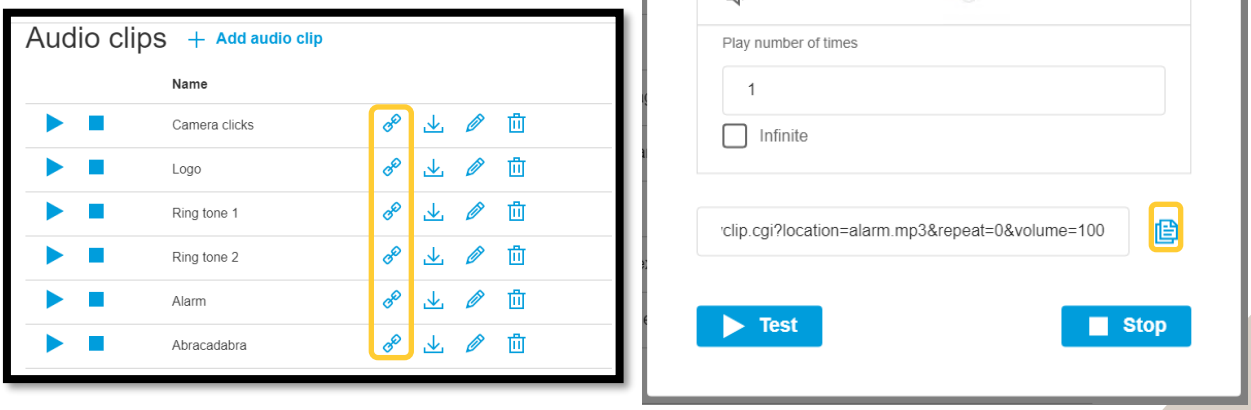
Use Case 4: VIP or VIP group welcome message

Using this setup, a rule can be created to send a personalized message to greet a VIP entering the premises, given that you have a network speaker or intercom by the door.

Step 1 – Upload audio clip and retrieve PlayClip-URL

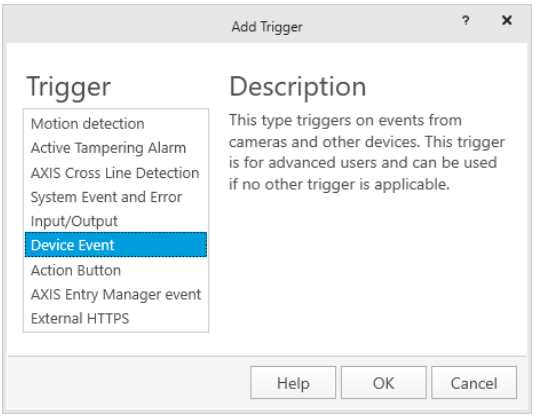


In the web interface of the Axis speakers you can navigate to the Audio clips page and upload a custom audio clip.

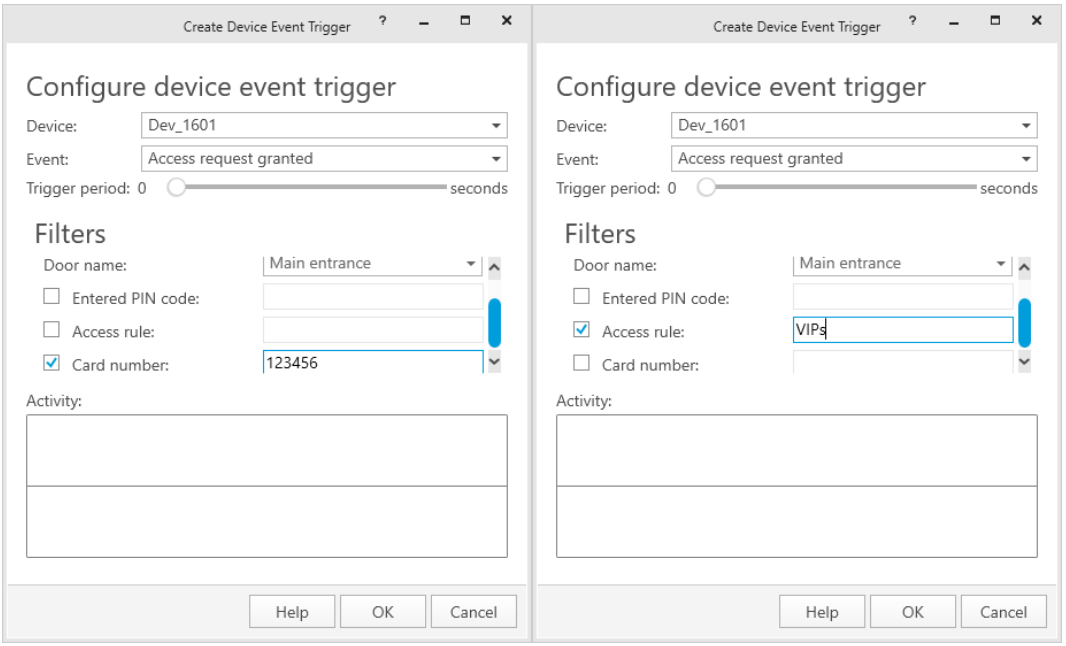


Once that is done, you can easily copy the correct link to play that clip to your windows clipboard from the web interface.

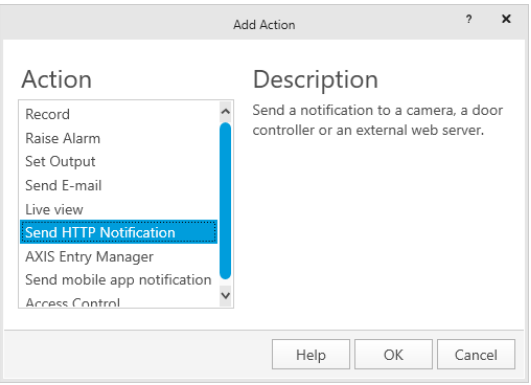
Step 2 – Create the rule.



Add the Device Event trigger



Here you can either setup a rule to give a personalized greeting message to a specific person when he or she uses their card, knowing their card number from the system. Or a Generic VIP greeting when someone enters that is part of a specific access rule in the system.



As action you select to Send HTTP Notification and paste the link you copied from the previous state.

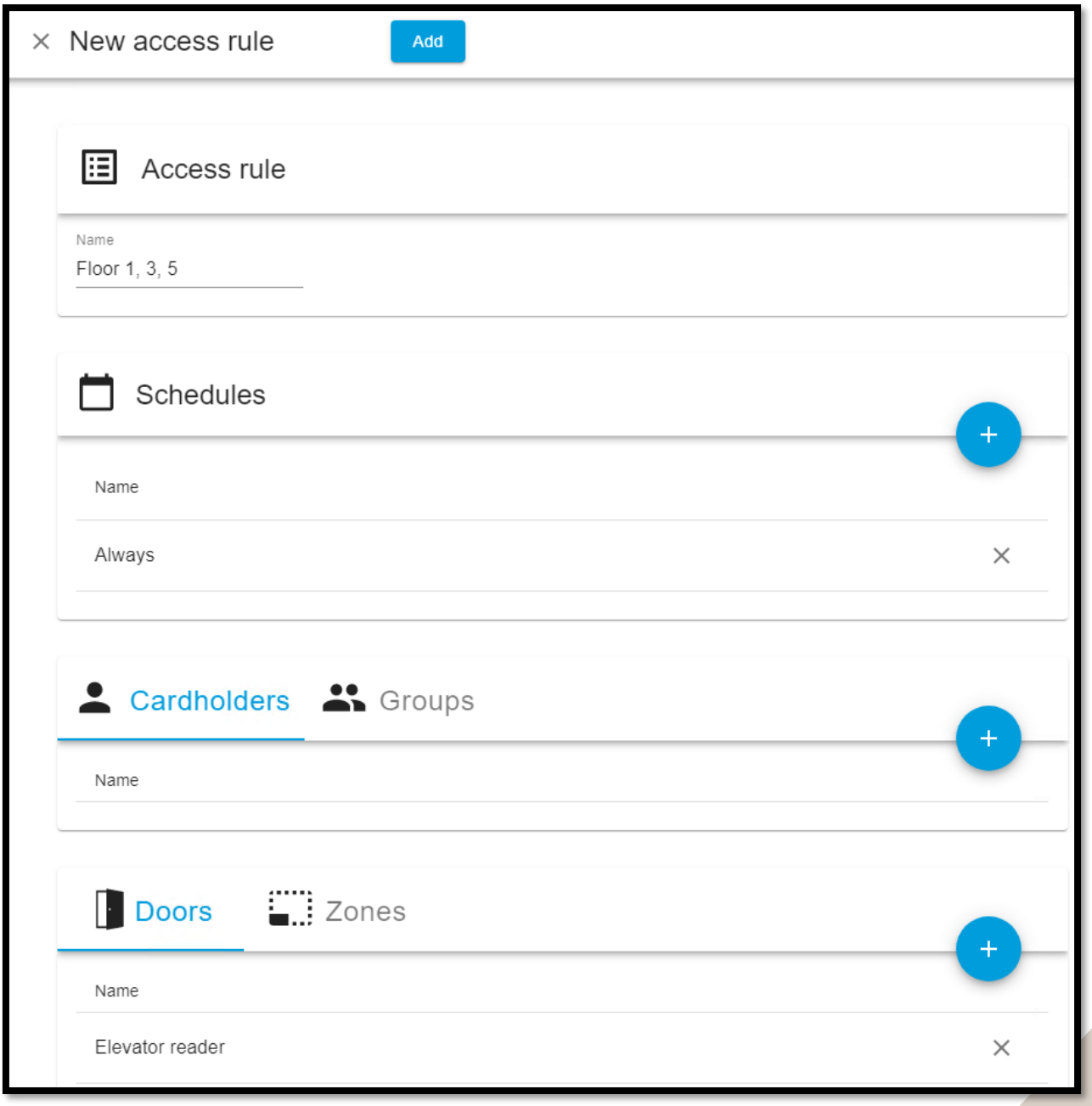
NOTE

A current limitation in the Device interface tab from within AXIS Camera Station is that the copied link retrieved from the speaker interface will not have the correct IP address to the speaker. This needs to be updated to the correct IP address for the HTTP notification to work.

Use Case 5: Elevator access control (workaround)

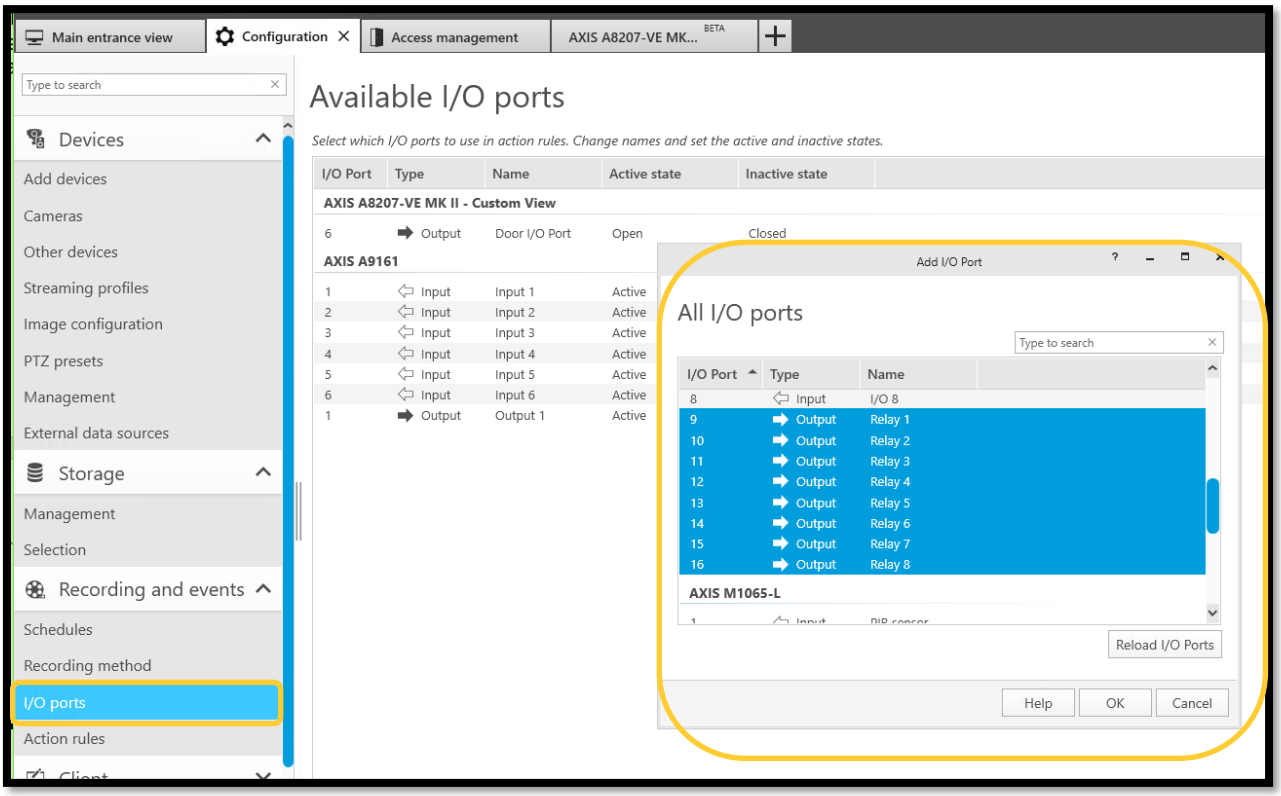
This describes a workaround that you can apply to configure elevator access control to floors based on Access rules before the feature is available.

Step 1 – Create relevant access rules for each floor combination



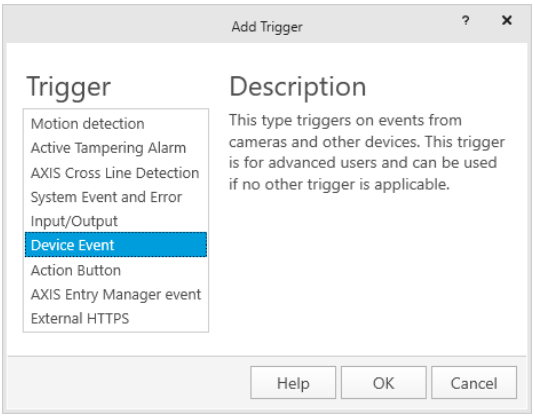
Firstly you need to have a door named something like “Elevator reader” that is installed inside the elevator. Then Access rules needs to be created for each relevant floor combination that is needed for access management, in this example we create an access rule for floors 1, 3 and 5. Add the “Elevator reader”-door to the rule with a relevant schedule.

Step 2 – Add the A9188 Relay's to the system

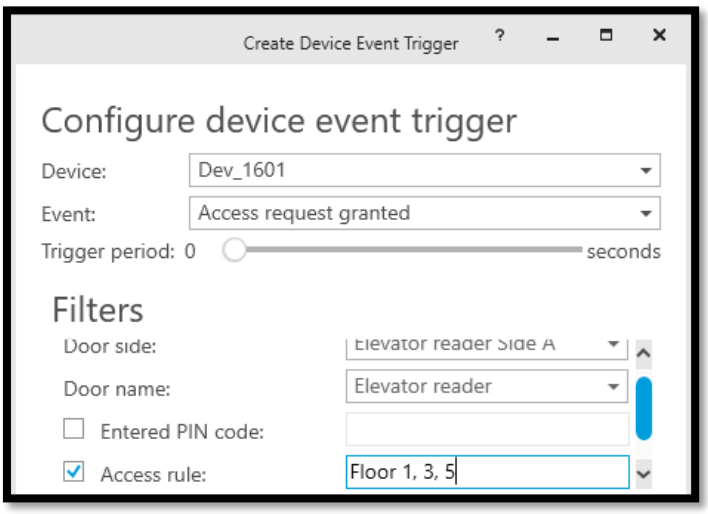


Under Configuration → Recording and events →I/O Ports, add the A9188's relay's to the system.

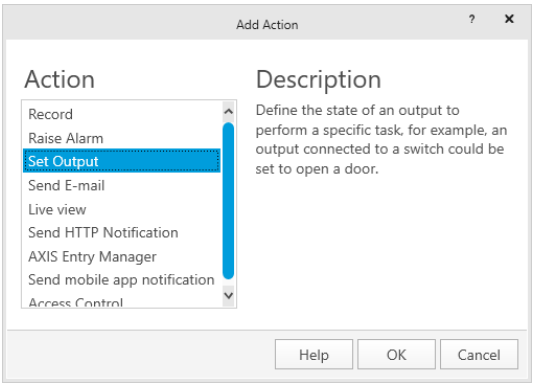
Step 2 – Create rules to trigger IOs based on access rule access.



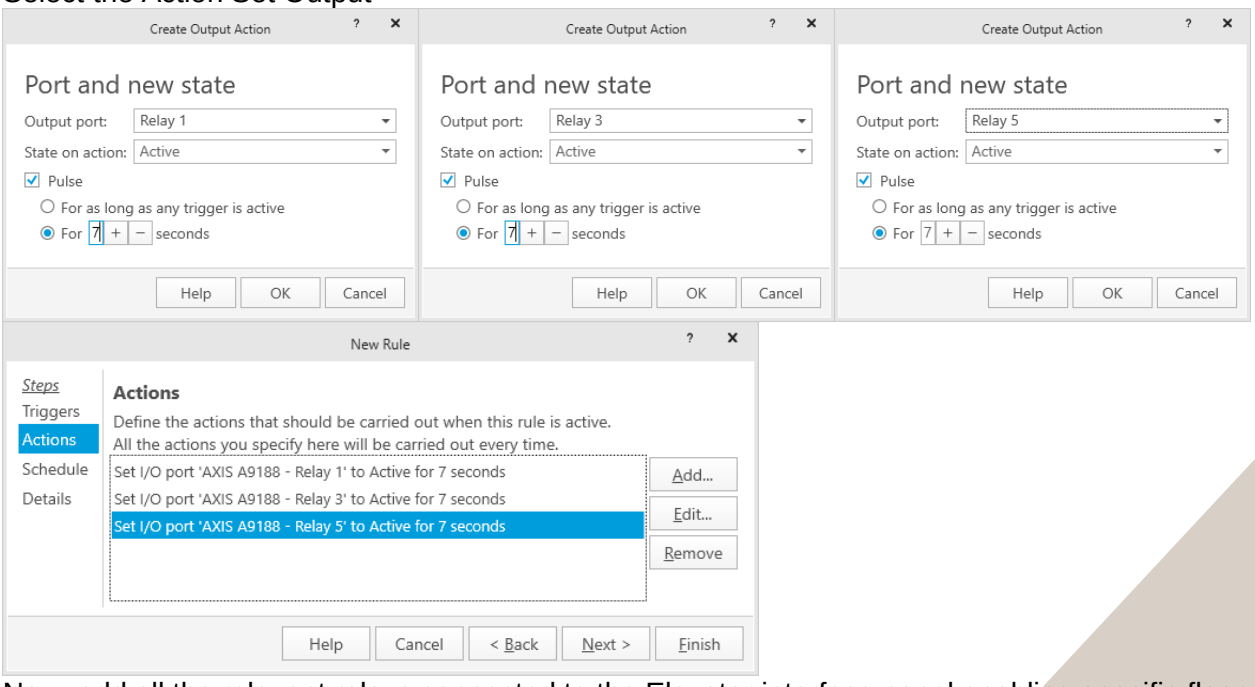
Add the Device Event trigger



Input the correct name of the relevant access rule as trigger.



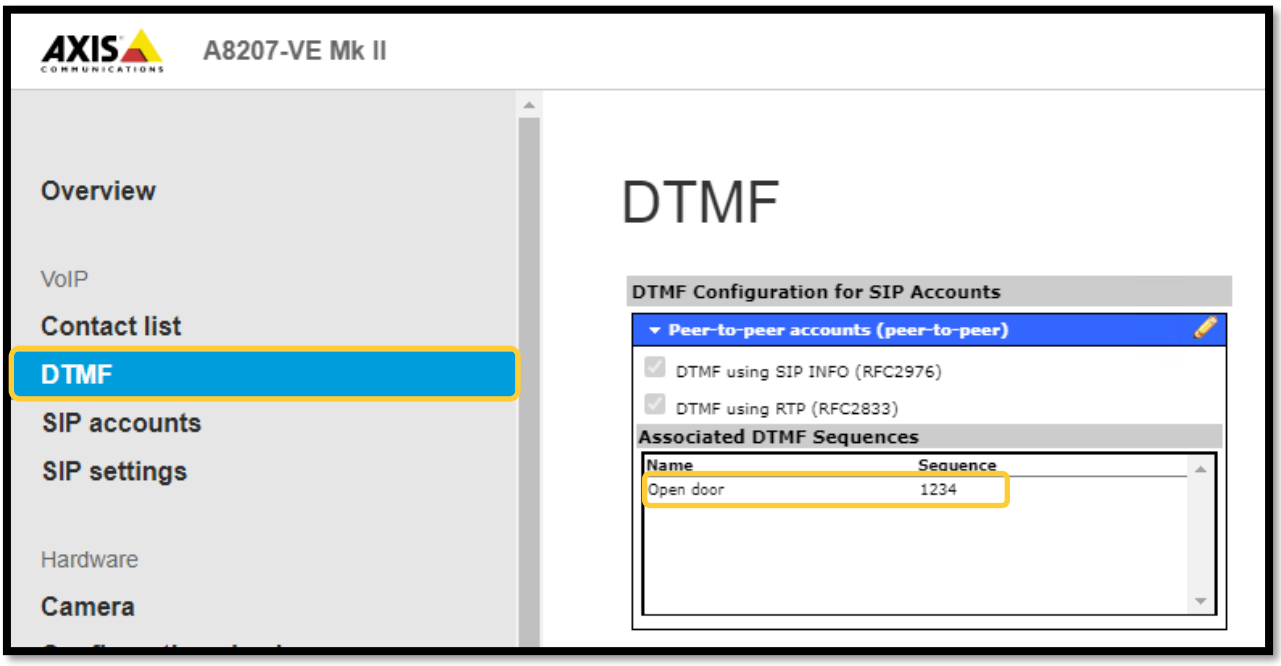
Select the Action Set Output



Now, add all the relevant relays connected to the Elevator interface panel enabling specific floor buttons

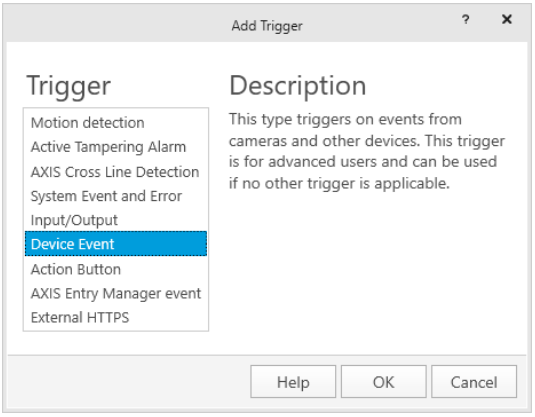
Use Case 6: Using a DTMF sequence to access a door

Step 1 – Create the DTMF sequence on your Axis Intercom

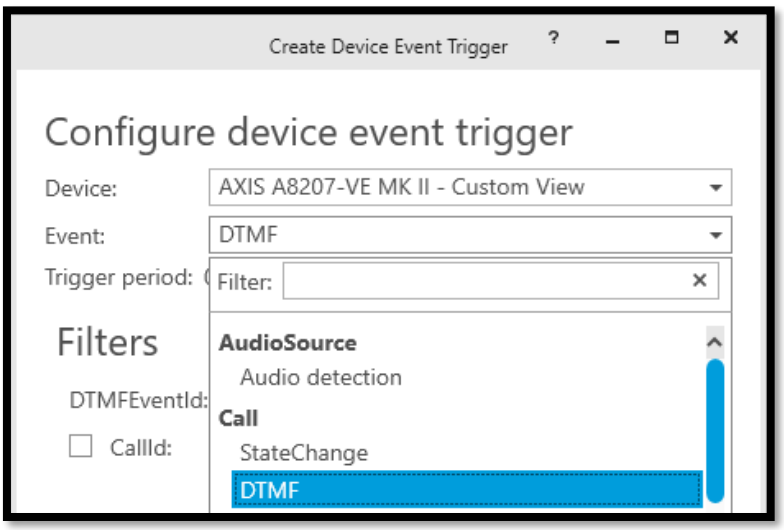


In the web interface of the Axis Intercom, you create a DTMF Sequence for the correct SIP account where the VoIP call is being initiated.

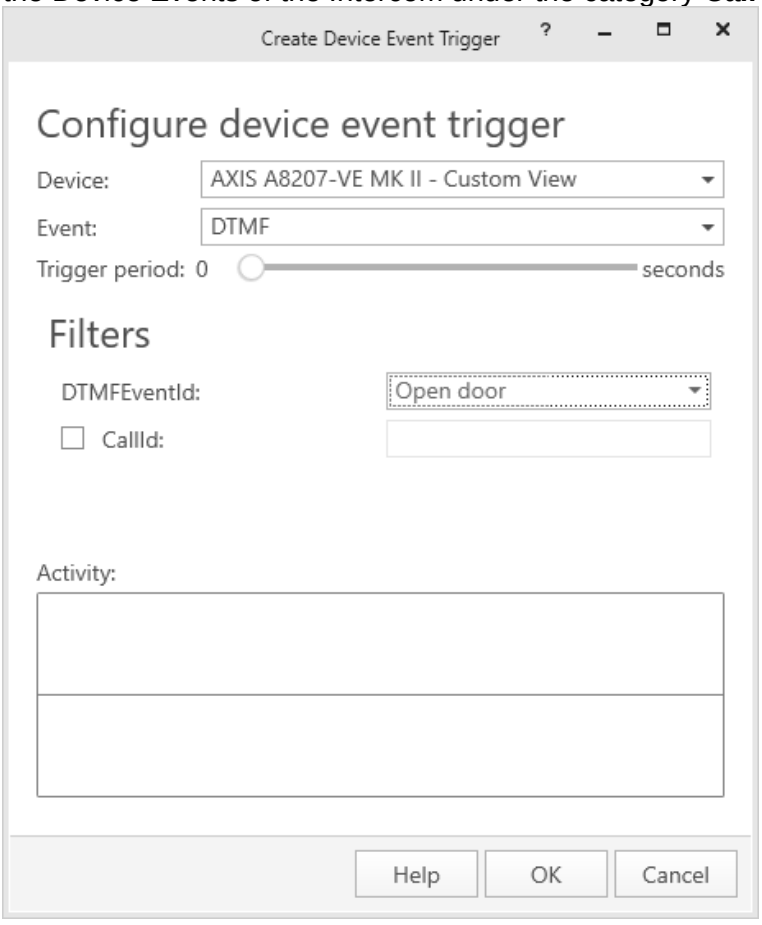
Step 2 – Create the rule that triggers on the DTMF sequence and accesses the door.



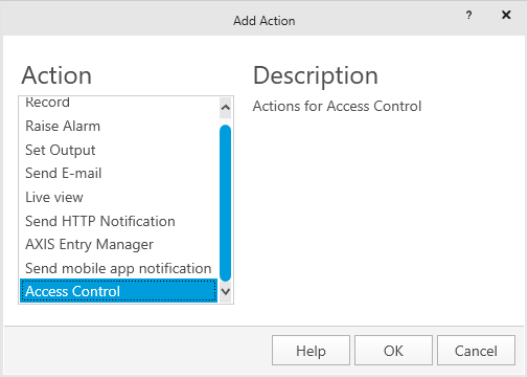
Add the Device Event trigger



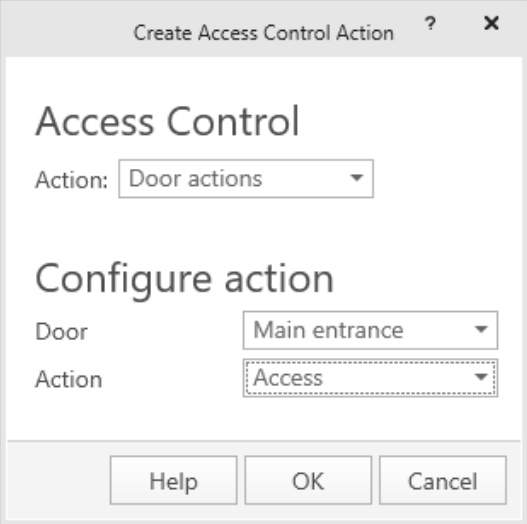
If SIP is enabled on the Axis Intercom and you have a DTMF trigger created this is visible under the Device Events of the Intercom under the category ***Call***



You can then also select to filter on the specific sequence if you have the need of triggering multiple things depending on different input.



Select the Action for Access Control

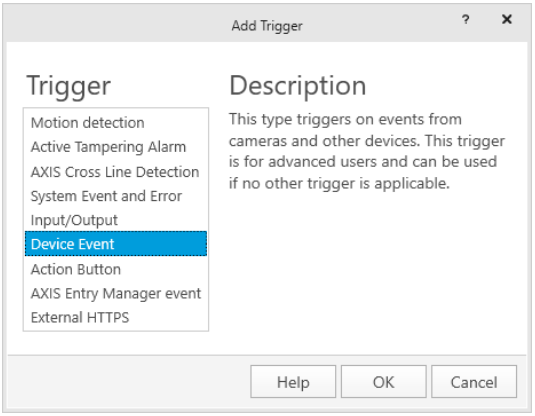


Now you can select to access a specific door based on the DTMF sequence.

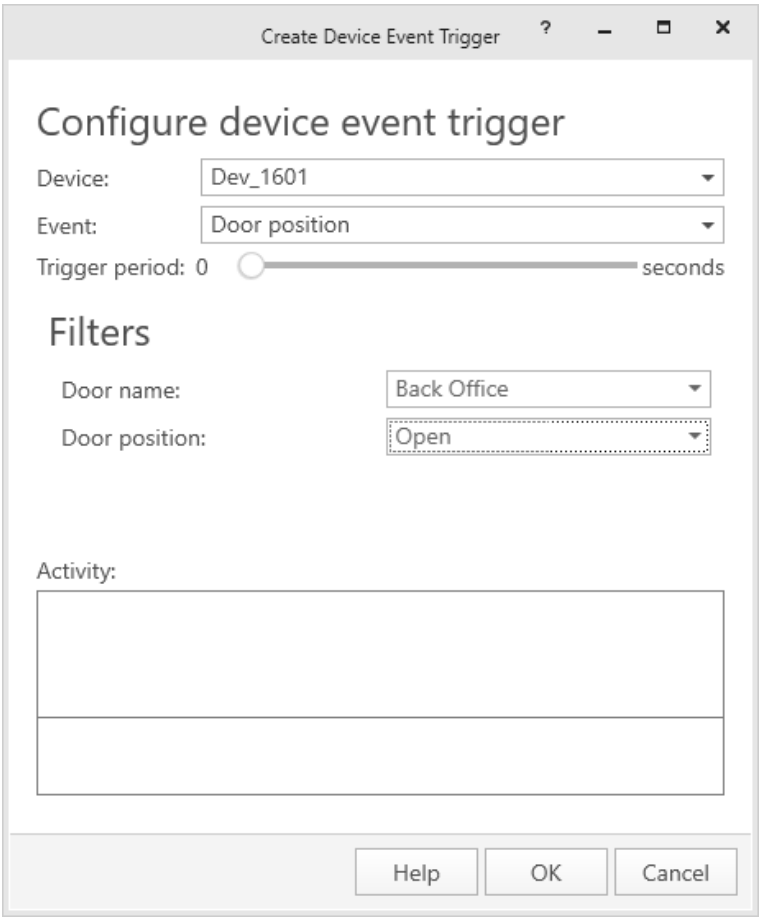
Use Case 7: Interlock between two doors

In some instances, you want to be able to block access attempts to a door based on the door status of a second door. For instance, like an airlock-function.

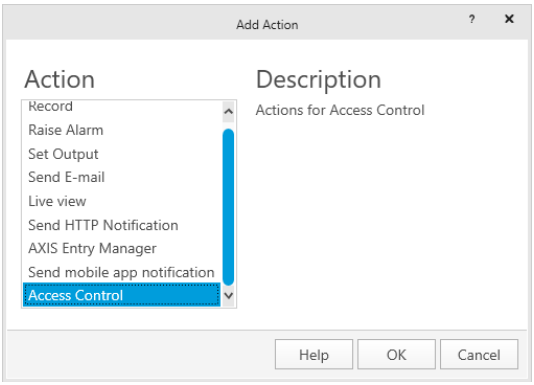
Step 1 – Create a rule locking down the 'vault' based on 'back office' door position



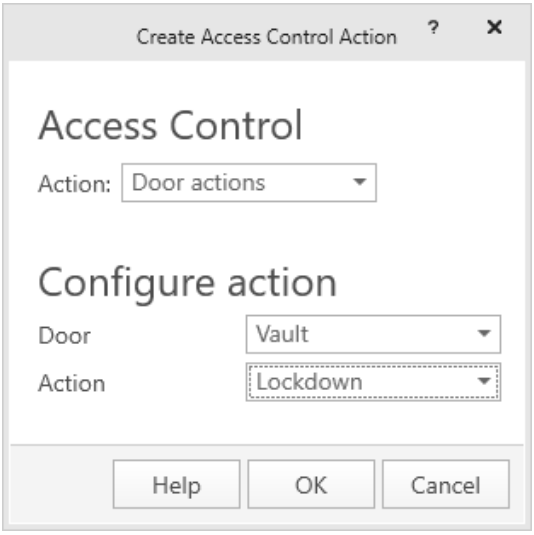
Create a rule trigger on Device Event



Select the AXIS A1601 Network Door Controller, choose the Door position event and filter on the door in question and that the door is opened.



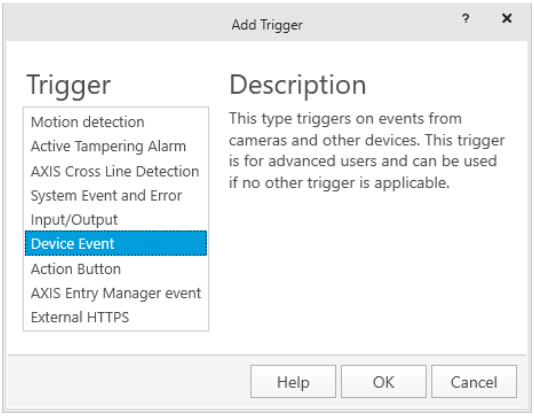
Add an Access Control action in the rule.



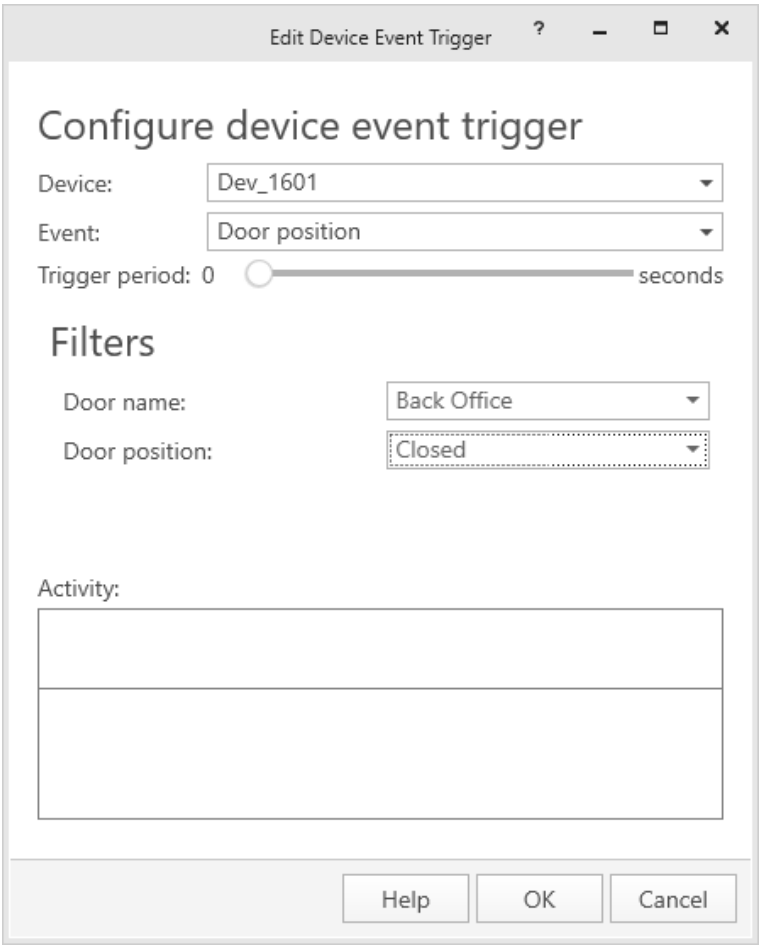
Select Door actions, the door to be locked down and select the action “Lockdown”.

Step 2 – Create rule to return the ‘vault’ to default status when the ‘back office’ door is closed.

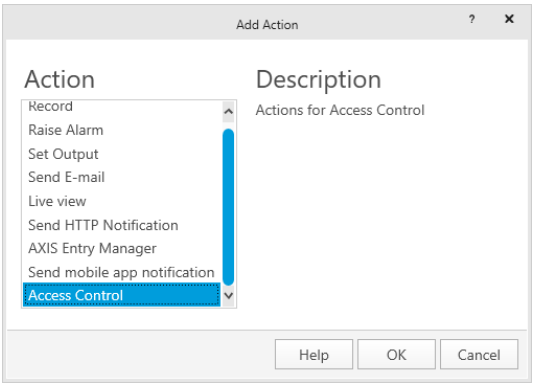
Basically, this is the inverse of Step 1



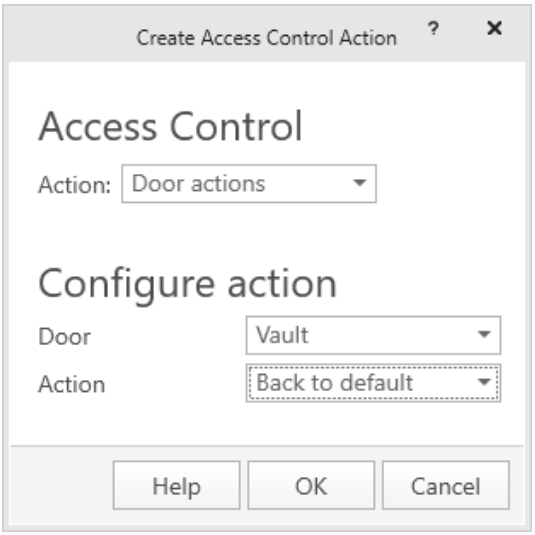
Create a rule trigger on Device Event



Select the AXIS A1601 Network Door Controller, choose the Door position event and filter on the door in question and that the door is closed.



Add an Access Control action in the rule.



Select Door actions, the door to release from lockdown and select the action “Back to default”.