HOW TO.

Setup AXIS Camera Station Secure Entry



December 17, 2020 Rev. 1.00 © Axis Communications AB

Contents

Introduction	4
Basic configuration	4
Add AXIS A1601s to AXIS Camera Station	5
Upgrading firmware of the AXIS A1601	7
Time setup of the AXIS A1601	7
Configuration under access control	9
Identification profiles	9
Adding and editing identification profiles	10
Card formats and PIN	11
PIN length configurations	12
Adding and editing card formats	13
Doors and Zones	15
Add door	15
Door name and controller selection	15
Cloning a configuration	16
Door settings	17
Door monitor settings	18
Emergency input settings	19
Reader settings	20
REX settings	21
Supervised inputs	23
PIN chart	24
Add zone	26
Access Management	28
Access management configuration	29
↑ Import and export of cardholder data	29
Import cardholder data	30
Exporting cardholder data	32
	2

Restoring from last import point	32
Access Management dashboard	33
Adding a cardholder group	33
Adding and editing a cardholder	35
Adding and editing a card credential	36
Adding and editing a PIN credential	38
Adding and editing access rules	38
Edit door in access management	39
Edit zone in access management	40
Sending actions to doors and zones from the access management dashboard	40
ê Access Management reports	41
Unifying Video surveillance and Access Control	41
Connect a split view or camera view to a door	41
Door plugin view	42
Data search (Access Control Event log with video link)	43
Terminology	44
Hardware	44
Access management	44

Introduction

AXIS Camera Station Secure Entry is a video centric access control solution within AXIS Camera Station

Prerequisites

AXIS Camera Station Secure Entry

• AXIS Camera Station version 5.35 or higher

AXIS A1601 Door controllers

• A1601 with firmware from the Secure Entry firmware track

Windows computer (AXIS Camera Station Server/Client)

• Optimized for resolutions of at least 1920x1080, not deviating from 100% in scaling setting

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.

Basic configuration

In this chapter we will cover adding door controllers and doing the basic setup of AXIS Camera Station Secure Entry.

Add AXIS A1601s to AXIS Camera Station

AXIS Camera Station Client

Start the AXIS Camera Station Client if not already started.

			IXA	S Camera Station Clie	nt [master-15986]				? _ [×
Configuration									K 3	
Type to search	×	Add o	devices							
📽 Devices	^ î	Select the de under either	evices in your network that Cameras or Other devices.	you want to add to To multiselect dev	the server. You ca	n find the added de or Shift keys.	vices	Type to search	1	×
Add devices			Name	IP Address	Hostname	MAC address	Status	Manufacturer	Model	
Cameras			AXIS A1601	192.168.1.62		ACCC8EB43500		Axis	AXIS A1601	
Other devices Streaming profiles			AXIS A1601 (2)	<u>192.168.1.63</u>		00408C187873		Axis	AXIS A1601	
Image configuration		0	AXIS COMPANION RECO	<u>192.168.1.4</u>		ACCC8EA85EE7	HTTPS Certificate.	. Axis	AXIS Compar	io
PTZ presets	•									
Management										
External data sources										
Storage	~	1 selected, 1	with OK status				N	lanual coarch	Pofrach Ada	1 (1)
Recording and events	~ .						IV	ianuai seal Ch	Marenesii Mar	1(1)
Connected to AXISNVR-34Q7FPE i AXIS	Camera S	itation update a	vailable						∧ Alarms ar	nd Tasks

From AXIS Camera Station version 5.35 AXIS A1601 Network Door Controllers can be added as a device. Add AXIS A1601s to the system just as you are used to doing with your cameras.

Configuration +							£3 ≡
Type to search	×	Othe	r devices				
🔋 Devices	^	Change the modules. To	e name, addresses, and o multiselect devices, u	ports of devices such a se the CTRL or Shift key	s network speakers, rs.	door controllers a	Edit Aux devices ? X
Add devices			Name	Address	MAC address	Model	Settings
Cameras	_		AXIS A1001	192.168.1.61	ACCC8E25128C	AXIS A1001	Name: AXIS_Main_Door_Contr
Other devices			AXIS A1601 (2)	192.168.1.63	00408C187873	AXIS A1601	Address: 192.168.1.63
Streaming profiles							
Image configuration		11					Credentials
PTZ presets							Username: root
Management							Password:
External data sources							Help OK Cancel
🛢 Storage	\sim						
Recording and ever	nts 🗸 🗸						Edit Remove
Connected to AXISNVR-34Q7FPE	AXIS Camera	Station update	available				 Alarms and Tasks

Setting	gs
Name:	AXIS_Main_Door_Controller
Address:	192.168.1.63
HTTP port:	80
HTTP port:	80 ntials
HTTP port: Crede	80 ntials root

To change the name of your door controller: Go to Configuration \rightarrow Devices \rightarrow Other Devices and edit the system names. Setting a name for your door controller can also be done when adding the device.

Type to search	× N	lanage device	es				
📽 Devices	^ î	201 60) 💮 🔁	S			
Add devices	6	devices, 1 selected					
Cameras		Name	MAC address	Status	Address	Manufacturer	Model
		AXIS A1001	ACCC8E25128C	ОК	10.0.0.61	Axis	AXIS A1001
Other devices		AXIS M3027 (2) - Basem	ACCC8E39DF3E	OK	10.0.0.53	Axis	AXIS M3027
Streaming profiles	· · · ·	AXIS M3027 (4) - Quad	ACCC8E39DF39	OK	10.0.0.50	Axis	AXIS M3027
		AXIS T8508	ACCC8E918035	OK	10.0.0.6	Axis	AXIS T8508
Image configuration		Main Door Controller	ACCC8EB43500	ОК		Axis	AXIS A1601
PTZ presets		Main entrance camera, A	ACCC8E68B550	OK	10.0.0.55	Axis	AXIS A8105-E
Management							
Management							

Upgrading firmware of the AXIS A1601

Go to Configuration \rightarrow Devices \rightarrow Management and update the Firmware of the added A1601s

NOTE Factory defaulting when doing a firmware upgrade is required when going from the Active firmware track to the Secure Entry firmware track

Time setup of the AXIS A1601

			AXIS Camera Statior	Client [master-1941])]	
Configuration						
Type to search X	Manage device	S				
🔹 Devices 🔥 🖍	2 8 ± 1 % 0	· · · · · · · · · · · · · · · · · · ·	G			
Add devices	6 devices, 1 selected	- •				
Cameras	Name	MAC address	Status	Address	Manufacturer	Model
	AXIS A1001	ACCC8E25128C	ОК	10.0.0.61	Axis	AXIS A1001
Other devices	AXIS M3027 (2) - Basem	ACCC8E39DF3E	ОК	10.0.0.53	Axis	AXIS M3027
itreaming profiles	AXIS M3027 (4) - Quad	ACCC8E39DF39	ОК	10.0.0.50	Axis	AXIS M3027
	📟 AXIS T8508	ACCC8E918035	ОК	10.0.0.6	Axis	AXIS T8508
mage configuration	🔲 Main Door Controller	ACCC8EB43500	ОК	<u>10.0.62</u>	Axis	AXIS A1601
PTZ presets	Main entrance camera, A	ACCC8E68B550	OK	10.0.0.55	Axis	AXIS A8105-E
Management						
External data sources						

Set the correct Date and Time for all your controllers.

Since it is important in an access control setup that all devices and the server is in sync when it comes to time, specifying an NTP_-server for time synchronization or having the AXIS Camera Station Server act as an NTP server is strongly recommended. You can setup the Server to act as an NTP under Configuration→Server→Settings

Configuration	
Type to search X	
📽 Devices 🔨	
Add devices	
Cameras	<u>rest All</u> <u>Add</u> <u>E</u> dit
Other devices	System alarm 💿
Streaming profiles	Send e-mail on system alarm to the following recipients
Image configuration	Recipients:
PTZ presets	To: 👻
Management	
External data sources	
🛢 Storage 🗸	
$igoplus$ Recording and events \checkmark	
🖆 Client 🗸	
△ Connected services ∨	Time synchronization
Server ^	✓ Use this server as the NTP server for connected devices
Scheduled export	Device connection
Incident report	Keep using the hostnames even if they become unreachable
Settings	Advenced
Plugins	Aavancea Change settings only when you are instructed by Avis support

Configuration under access control

Identification profiles

NOTE The solution contains identification profiles by default. If you have no special needs that you know of, you can skip this section and come back to it later if there is a need.

An identification profile is a profile applied to one or many doors that defines how a cardholder's access attempt is validated through the sides of a door. The identification type needs to be associated with a door to have an effect on the system.

₽	Configuration +	
Туре	to search	×
9 10	Devices	~
()))	Storage	~
8	Recording and events	~
Ŷ	Client	~
\bigcirc	Connected services	~
	Server	~
5	Licenses	~
ð	Security	~
	Access control	^
Doc	ors and zones	
Ider	ntification profiles	
Card	d formats and PIN	

Identification profiles are configured under Configuration \rightarrow Access control \rightarrow Identification profiles. There are four system default Identification profiles available as reference that you can edit to achieve the system functionality you need, or you can create your own identification profiles from scratch.

Adding and editing identification profiles

	prome	
Name		
My new Identific	cation profile	
Side A	+ Add	
	Identification profile	Schedule
	Identification profile Card, PIN	Schedule Alway
	Identification profile Card, PIN Card Card	Schedule Alway

When creating an identification profile, you combine the means of identification such as Card and PIN with a schedule as to when the created identification type (for instance card + pin) should be active on the specific side of the door or doors that will later have this identification profile applied to it.

You can combine many identification types on different schedules to configure exactly how your means of identification should be applied on, for instance entrance doors.

Clicking on the small calendar icon is to the far right of the identification profile's respective door side will give you a visual calendar representation of the identification profile applied to that side of the door. Remember, you need to add an identification type for both Side A and B

Card formats and PIN

NOTE The solution contains card formats by default. If you have no special needs that you know of, you can skip this section and come back to it later if there is a need.



Let's say you have a reader (or all readers) in the system providing you with a card number that is not what is expected/printed on the card. A card format can adjust this inside each door controller so that the validation data are matched correctly with the credentials connected to the cardholders in the system.

Configuration	×	Card fo	ormats Inclivate card formats.			
🕵 Devices	~	+ Add card	length: 4, Max PIN length: 4		Type to se	earch
🛢 Storage	~	In use	Name	Bit length		
Recording and events	s 🗸	in use	Hame	bit length		
🖆 Client	~		32-bit raw card data	32		5
→ Connected services	~		56-bit raw card data	56	/	5
E Server	~		Smart Card Alliance 75-bit GSA	75		5
Licenses	~					
Security	~		Standard 26-bit Wiegand (H10301)	26		5
Access control	^		Standard 34-bit Wiegand (H10306)	34		5
Doors and zones			Standard 37-bit Wiegand (H10302)	37	<i>.</i>	5
dentification profiles			Standard 37-bit Wiegand with facility code (H10304)	37		5

Configuring Card formats are done under Configuration \rightarrow Access control \rightarrow Card formats and PIN. What is done here is setting up the translation table between the data that the door controllers in the system receive from their connected card readers and the wanted data that access validations are based on.

The system has a few predefined commonly used card formats that you can use as they are or use as reference when creating custom card formats. Each card format has a different set of data parameters, field maps, for how the information stored on the card is organized. By defining a card format you tell the system how to interpret the information that the controller gets from the reader. For information about which card formats the reader supports, see the manufacturer's instructions. In this view you also have the possibility to adjust your systems PIN code length.

Settings done in this section are applied generally on all readers in the system unless they have been changed to local settings with deviations from the general settings.

PIN length configurations



Press the PIN length button to adjust the wanted PIN lengths in the system.

	garación	
Min PIN length	Max PIN length	End of PIN
4	4	#

Here you can adjust your systems minimum pin length as well as maximum pin length. If you have a difference between the minimum and maximum values, you need to set an end of pin character for the system's door controllers to know that a cardholder with a shorter PIN is finished inputting the PIN at the card reader.

Adding and editing card formats

New card format	
Name	
My new card format	

Give your new card format a name.

Bit length			
32	Invert bit order	Invert byte order	

Define the bit length of the format enabling the systems door controllers to use this format when card data with 32 bits are received from the card reader. Check the boxes if you want to invert bit or byte order of the entire data received.

NOTE	Inverting bit order	١
	Inverting the bit order of the incoming data is basically switching the reading of the bits (ones or zeroes from reading from left to right to reading from right to left)	
	19 275 = 0100 1011 0100 1011 → 1101 0010 1101 0010 = 53 970 → Read from left Read from right←	1
	Inverting byte order	I
	Firstly, we must establish that one byte equals eight bits (ones or zeroes). Same as for inverting the bit order we switch the reading of bytes from left to right to from right to left. $64\ 332 = 1111\ 1011\ 0100\ 1100\ = FB4C \rightarrow 4CFB = 0100\ 1100\ 1111\ 1011 = 19\ 707$ F B 4 C	

Name	Range	2	
CardNr	11	-	32
FacilityCode	1	-	10

Choose if card number and/or facility code should be data fields that are active in your card format and set the bit ranges for the respective fields to get the field representation out from the binary card data.

Format
Int 🔻
Hexadecimal lowercase 🔻

Choose what output format you want from the respective field for your system's credential validation. If it should be decimal (Int) or hexadecimal output.

Bit order
Little-endian 🝷
Big-endian 🝷

Choose the bit order of the data field.

Doors and Zones

To configure the doors and zones in the system you need to go to Configuration \rightarrow Access control \rightarrow Doors and zones

Configuration					
pe to search	×	Doors and zones			
Devices	~	Add or edit doors and zones. You can set an identification profile on mu + Add door + Add zone	ultiple doors. To select multiple doors, us	e the CTRL or Shift keys.	
Storage	~	Doors Zones			
Recording and events	~	Name	Door controller	Side A in	Side B in
🖞 Client	~				
Connected services	~				
Server	~				
Licenses	~				
Security	~				
Access control	~				
oors and zones					
dentification profiles					
Card formats and PIN					

Add door

Add a door by pressing the "+ Add door"-button.

Door name and controller selection

New door	
	Name
	Main Entrance
	Connect to a door controller
	The configuration requires a door controller.
	Main controller
	Main Door Controller

Give the door a name and connect it to a door controller you have configured in the system. Click "Next".

Doors and zones Add or edit doors and zones.		Copy configuration	
Door		Type to search *	
Door	Name Main entrance Connected to Main entrance controller Locks Relay port 1 Not connected Sensor input + Add door monitor + Add emergency input	Type to search •	Door settings General Advanced Long access time (s) 30 Long open-too-long time (s) 60 Relock time after opening (ms) © Relock time after closing (ms) 0
	Side A Side B + Add reader + Add REX device + Add REX device		Delete door Cancel Ok

Cloning a configuration

Doors and zones Add or edit doors and zones.		Copy configuration	
Door		Type to search	•
	Name Main entrance Connected to Main entrance controller Locks Relay port 1 * Sensor input + Add door Monitor Side A Side A + Add reader + Add REX device		Door settings Advanced General Advanced Long access time (s) 30 Boot 0 Relock time after opening (ms) 0 O 0 Relock time after closing (ms) 0
	/		Delete door Cancel Ok
Copy configuration	on •		

If you want to copy a door configuration from a previously configured door you can select doors in this list to copy the configuration from.

Door settings

Door settings General Advanced Identification profile () Card and PIN Access time (s) () 7 Open-too-long time (s) () 30	Doors and zones dd or edit doors and zones.		Copy configuration			
Image: settings Image: settings <th>loor</th> <th></th> <th>Type to search</th> <th></th> <th></th> <th></th>	loor		Type to search			
Image: Second state				Door settings		
Image: settings Image: settings <th></th> <th>Name</th> <th></th> <th>General Advanced</th> <th></th> <th></th>		Name		General Advanced		
Image: Second secon		Main entrance		Long access time (s) 30		
Image: settings Image: settings Ceneral Advanced Identification profile Identification profile Identification profile Icard and PIN Access time (s) Image: setting sett		Connected to Main entrance controller		Long open-too-long time (s)		
Image: Second state Image: Second state Identification profile (i) Card and PIN Access time (s) (i) 7 Open-too-long time (s) (i) 7 Open-too-long time (s) (i) 7 0		Locks Relay port 1 * Not connected *				
Image: Constraint of the second o		Sensor input		Relock time after opening (ms)		
Image: service of the ser		+ Add door monitor + Add emergency input		Relock time after closing (ms)		
Image: Image		Side A Side B]			
Image: Control of the second seco		+ Add reader + Add reader				
Door settings General Advanced Long access time (s) 30 Long open-too-long time (s) 60 60 Relock time after opening (ms) 7 Open-too-long time (s) 1 0		+ Add REX device + Add REX device				
Door settings General Advanced Identification profile (i) Card and PIN Access time (s) (i) 7 Open-too-long time (s) (i) 7 0 8 0 8 10 10 10 10 10 10 10 10 10 10 10 10 10 10						
Door settings General Advanced Long access time (s) 30 Long open-too-long time (s) 60 Relock time after opening (ms) 7 Open-too-long time (s) 30				Delete door Cancel Ok		
Door settings General Advanced Long access time (s) 30 Long open-too-long time (s) 60 60 Relock time after opening (ms) 7 Open-too-long time (s) 30						
Door settings General Advanced Identification profile (i) Card and PIN Access time (s) (i) 7 Open-too-long time (s) (i) 30 8 0 Relock time after opening (ms) 0 8 0 0						
Door settings General Advanced Long access time (s) 30 Long open-too-long time (s) 60 Card and PIN Access time (s) 7 Open-too-long time (s) 30 8 0 Relock time after opening (ms) 0 Relock time after closing (ms) 0						
Ceneral Advanced Long access time (s) 30 Card and PIN Access time (s) 7 Open-too-long time (s) 7 Open-too-long time (s) 30				D	oor settings	^
Door settings General Advanced Identification profile (i) Card and PIN Access time (s) (i) 7 Open-too-long time (s) (i) 30 General Advanced Long access time (s) 30 Card and PIN Relock time after opening (ms) 0 Relock time after closing (ms) 0						
Door settings General Advanced General Advanced Long access time (s) 30 Long open-too-long time (s) 60 60 Relock time after opening (ms) 7 Open-too-long time (s) 30 Access time (s) 7 0 8 8 9 9 10						
Door settings General Advanced Identification profile (i) Card and PIN Access time (s) (i) 7 Open-too-long time (s) (i) 30 Belock time after opening (ms) 0 Relock time after closing (ms) 0				General	1	Advanced
Door settings Long access time (s) General Advanced Identification profile (i) Identification profile (i) Card and PIN 60 Access time (s) (i) Relock time after opening (ms) 7 0 Open-too-long time (s) (i) 0 30 0						
Door settings Long access time (s) General Advanced Identification profile (i) Identification profile (i) Card and PIN Identification profile (i) Access time (s) (i) Identification profile (i) 7 Identification profile (i) 0 Relock time after opening (ms) 7 Identification profile (i) 30 Identification profile (i)						
General Advanced Identification profile (i) Card and PIN Access time (s) (i) 7 Open-too-long time (s) (i) 30 Belock time after opening (ms) 0 Relock time after closing (ms) 0		Door settings		Long access	time (s)	
General Advanced Identification profile (i) Card and PIN Access time (s) (i) 7 Open-too-long time (s) 30 30		Door settings	^	Long access	cirric (5)	
General Advanced Identification profile (i) Card and PIN Access time (s) (i) 7 Open-too-long time (s) (i) 30 80 Card and PIN Card and PIN <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>						
General Advanced Long open-too-long time (s) Identification profile (i) Card and PIN Access time (s) (i) 7 Open-too-long time (s) (i) 30 Advanced Long open-too-long time (s) 60 60 Belock time after opening (ms) 0 Relock time after closing (ms) 30				30		
Identification profile (i) Card and PIN Access time (s) (i) 7 Open-too-long time (s) (i) 30 Long open-too-long time (s) 60 7 60 60 7 60 60 7 60 60 60 60 7 60 <tr< td=""><td>Gener</td><td>ral Advanced</td><td>ł</td><td></td><td></td><td></td></tr<>	Gener	ral Advanced	ł			
Identification profile (i) Card and PIN Access time (s) (i) 7 Open-too-long time (s) (i) 30					oo long timo (c)
Identification profile (i) Card and PIN Access time (s) (i) 7 Open-too-long time (s) (i) 30 60 Relock time after opening (ms) 0 Relock time after closing (ms) 0				Long open-to	bo-long time (5)
Card and PIN Access time (s) 7 Open-too-long time (s) 30	Identificat	ion profile (i)				
Card and PIN Access time (s) 7 Open-too-long time (s) 30				60		
Access time (s) (i) 7 Open-too-long time (s) (i) 30 Relock time after opening (ms) 0 Relock time after closing (ms) 0 0	Card and	I PIN 🔻				
Access time (s) (i) 7 Open-too-long time (s) (i) 30 Relock time after opening (ms) 0 Relock time after closing (ms) 0 0						
7 0 8 0 8 0 8 0 8 0 8 0 8 0 8 0 9 0 10 0 10 0 10 0	Access tim	ne (s)				
7 Image: Construction of the second seco	Access (III			Relock time a	after opening (ms)
Open-too-long time (s) Relock time after closing (ms) 0 0 0 0 0 0 0 0 0 0<	7					
Open-too-long time (s) (i) 30 O O	/			0		
30 Relock time after closing (ms)	<u> </u>					
	Open-too	-iong time (s) (i)		Relock time	after closing (n	ns)
30 0				Reforment en	arter closing (ii	
	30					
				0		

The door settings is where overall configuration of the door is done. This segment is always visible when in an edit view for a door. Here you apply the correct identification profile for the door as well as set timings for the door to function properly.

Under the Advanced tab you also have the possibility to configure extended access times if you have individuals needing longer times to get through a door or specific relocking options. Some timers are not editable if you don't have a door monitor configured since these timings are reliant of the system knowing that the door changes physical states.

Door monitor settings

+ Add door monitor

Add a door monitor by pressing this button.

		Door settings
		Door monitor
vame		I/O 5
Main entrance		0 1/0 6
onnected to		0 1/0 11
lain entrance controller		0 1/0 12
ocks		O Not connected
Relay port 1	 Not connected 	
ensor input		Open door = Open circuit
Door monitor	× + Add emergency input	Open door = Closed circuit
		Debounce time (ms)
		0 ()
ide A	Side B	Supervised inputs
+ Add reader	+ Add reader	
+ Add REX device	+ Add REX device	

Door monitor 🛛 🔨
 I/O 5
0 1/0 6
I/O 12 Not connected
 Open door = Open circuit Open door = Closed circuit
Debounce time (ms)
0 ()
Supervised inputs

Once the door monitor has been added the settings for the door monitor is available in the panel on the right-hand side of the screen in the "Selected Peripheral"-part visible under the Door settings.

You may select which specific IO that you want the Door monitor configured on as well as what the system shall interpret as an open door.

If you are experiencing jittering signals you can also set a debounce time on the input signal to stabilize it.

Emergency input settings

You can configure the door to act on the A1601s emergency input, putting the door logical state to either be unlocked or locked if the input is activated.

+	∆dd	emer	denc	/ input	•
	Auu	enter	gene	, inpu	

Add emergency input to the door by clicking this button.

lame			
Main entrance			
onnected to			
fain entrance controller			
ocks			
Relay port 1	-	Not connected	-
ansor input			
chool in par	_		
Door monitor		Emergency input	×



When the emergency input is selected, the "Selected peripheral"-panel presents the settings for the emergency input.

Here you can configure when the controller should interpret the input on the controller is in an emergency state.

You can configure a debounce time to compensate for jitters in the signal and you can select what this door should do in the event of an emergency. – Either lock or unlock the door.

Reader settings



Add a reader by pressing this button either on the door Side A or Side B or both.

Name		Reader ~
Main entrance		Havancea
Connected to Main entrance controller		 Reader port 1 on device card Reader port 2 on device card
Delay and 1		OSDP RS485
Not connected		O Wiegand
Sensor input Door monitor Emerger	ncy input	
Side A Side B		
Reader × + Add	d reader	
+ Add REX device + Add F	REX device	
		selected the
Reader ^ General Advanced	General Advanced Reader port 1 on device card Reader port 2 on device card OSDP RS485 Wiegand LED control	selected the "Selected periphera panel presents the settings for the individual reader. Here you can configure what read port you want to use and if you are using OSDP or Wiegand.
Reader ^ General Advanced O Reader port 1 on device card	General Advanced Reader port 1 on device card Reader port 2 on device card OSDP RS485 Wiegand LED control Single wire Tampera Open sirguit 	Selected the "Selected periphera panel presents the settings for the individual reader. Here you can configure what read port you want to use and if you are using OSDP or Wiegand.
Reader General Advanced Reader port 1 on device card Reader port 2 on device card	General Advanced Reader port 1 on device card Reader port 2 on device card OSDP RS485 Wiegand LED control Single wire Tamper= Open circuit Tamper= Closed circuit	Selected the "Selected periphera panel presents the settings for the individual reader. Here you can configure what reac port you want to use and if you are using OSDP or Wiegand. If selecting Wiegand the specific configurations need
Reader General Advanced O Reader port 1 on device card O Reader port 2 on device card	General Advanced Reader port 1 on device card Reader port 2 on device card OSDP RS485 Viegand LED control Single wire Tamper= Open circuit Tamper= Closed circuit Tamper debounce time (ms) i)	Selected the "Selected periphera panel presents the settings for the individual reader. Here you can configure what read port you want to us and if you are using OSDP or Wiegand. If selecting Wiegand the specific configurations need for Wiegand are displayed. These
Reader General Advanced Image: Constraint of the second secon	General Advanced Reader port 1 on device card Reader port 2 on device card OSDP RS485 Viegand LED control Single wire Tamper = Open circuit Tamper = Closed circuit Tamper debounce time (ms) j 0 O	Selected the "Selected periphera panel presents the settings for the individual reader. Here you can configure what read port you want to us and if you are using OSDP or Wiegand. If selecting Wiegand the specific configurations need for Wiegand are displayed. These include if you have

controlling red and the reader. You can also configure if the reader is in tampered state when the circuit is open or closed on the as well as configuring a debounce time to compensate for signal jitters.

How To. Setup AXIS Camera Station Secure Entry

Advanced General Custom PIN length (j) **(i)** Custom card formats Reader Standard formats General Advanced 32-bit raw card data **(**) Custom PIN length 🗸 56-bit raw card data Min PIN length ✓ Smart Card Alliance 75-bit 4 GSA Standard 26-bit Wiegand Max PIN length (H10301) ✓ Standard 34-bit Wiegand 4 (H10306) End of PIN character Standard 37-bit Wiegand (i) (H10302) 🗸 Standard 37-bit Wiegand with facility code Custom card formats 🔘 🛈 Added formats

Under the Advanced tab you can also make unique settings for card formats and pin lengths to solve specific needs on this individual reader or compensate for an individual reader's need to have an adjusted card format to get the credential interpreted correctly everywhere in the system.



REX settings



Add a REX device by pressing this button either on the door Side A or Side B or both.

Name		
Main entrance		0 1/0 5
		I/O 6
Connected to		0 1/0 11
Main entrance controller		0 1/0 12
locks		O Not connected
Relay port 1 🔹	Not connected 💌	
Sensor input		Action = Unlock door
Door monitor	Emergency input	O Action = None
		REX activate = Open circuit
Side A	Side B	O REX activate = Closed circuit
Reader	+ Add reader	Debounce time (ms)
+ Add REX device	REX device X	0
		Surrenting liquids

 I/O 5 I/O 6 I/O 11 I/O 12 Not connected Action = Unlock door Action = None
 I/O 6 I/O 11 I/O 12 Not connected Action = Unlock door Action = None
 I/O 12 Not connected Action = Unlock door Action = None
 Action = Unlock door Action = None
 REX activate = Open circuit REX activate = Closed circuit
0

Once the REX Device has been added the settings for the REX is available in the panel on the right-hand side of the screen in the "Selected Peripheral"-part visible under the settings.

You may select which specific IO that you want the REX configured on as well as choose whether the REX input really is a request to exit or if it is a mechanical override to the door, meaning it is more of a notification that someone has exited rather than an unlocking action being needed.

You also configure how the system shall interpret as the REX being activated. If you are experiencing jittering signals you can also set a debounce time on the input signal to stabilize the signal

Supervised inputs

	1kΩ	ic
Supervised inputs	2.2kΩ	
Parallel-first connection with a 22kΩ parallel resistor and a 4.7kΩ	4.7kΩ	h
Serial first connection	10kΩ	
Resistor values	1kΩ	
1kΩ •		

Under **Door monitor**, **Emergency input**, **Wiegand tamper** and **REX** there is a possibility to configure a input supervision, meaning the possibility to detect tampering attempts on the cable by measuring a specific connection with end of line resistors mounted as close to the peripheral device as possible.



Here you can see examples of the Parallel-first connection as well as the serial first connection with the specified resistor values that are supported in the setups.

PIN chart

oors and zones				
dd or edit doors and zones.				
+ Add door + Add zone				View zones Type to search
Name	Connected to	Side A in	Side B in	
Main entrance	AXIS_Main_Door_Controller	-	-	/ 1
				Pin chart Set identification pro
				Pin chart Set identification pro
				Pin chart Set identification pro
				Pin chart Set identification pro
				Pin chart Set identification pro
Pin chart	Set identification pro	ofile		Pin chart Set identification pro

Once all configurations on a door has been made and it's saved the door is visible in the main Doors and Zones view. From here you can select multiple doors in the system to set identification profiles on multiple doors in unison or select to view the controller pin chart associated with the selected door.

Doors and zones
Add or edit doors and zones.
You can set an identification profile on multiple doors. To select multiple doors, use the CTRL or Shift keys.
Print
Print

When viewing the pin chart, it is also possible to print it out.

NOTE In the first release there is no way to leave the pin chart view in a good way. You must go to another menu and back to Doors and zones again to get back to the door overview.

Add zone

Г	+	Add	zone
		7 1101104	20110

To add a zone, click this button.

New zone
Zone name
My zone
Name
My zone Name

Give the zone a name.

Zones Add or edit doors and zones,				
Zone				
Name				
My zone				
Door name	Door location		Use side A to	
Available doors				Type to search
Name	Door controller	Side A in	Side B in	
Main Entrance	Main Door Controller	-		Add
			/	
				Cancel Ok
-		/		
Add				

When the zone has been added to the system a door can be added to the Zone by clicking on the "Add"-button.

Door location Use side A to	
Perimeter door Enter zone	
Use side A to	
Enter zone 🔺	
Enter zone	
	Door location Use side A to Perimeter door Enter zone

When the door is in the zone it is possible to configure it as a perimeter door, meaning that cardholders enter or exit the zone with the door, or as a door internally within the zone. These settings are done with inline drop downs. Remove the door from the zone by pressing the X furthest to the right.

Doors Add or edit do You can set an	an oors an ident	nd zones. tification profile on multiple doo
+ Add do	or	+ Add zone
Doors		Zones
	Na	ame
Ø	My	/ zone

When a zone is configured it is accessible as a tab on top of the system door list.

Access Management



Clicking the "+" in the top bar of AXIS Camera Station brings up this menu. This section will cover the Access Management tab that can be opened from here.



In the Access management tab, there are four sub-views where things can be done.

- Access management dashboard 🖳
- Access management reporting 🖹
- Access management configuration
- Access management import and export ¹

Access management configuration

n e	Lardholder	Facility code Enable or disable the usage of facility code in the system
•	First name Last name	Apply
îĻ	Cardholder ID	
	Add custom field	
	Cancel Apply	

In this view it is possible to add custom fields to the cardholder template in the access management dashboard. Here is also where facility codes in cardholders' credentials are enabled and disabled in the system.

†Import and export of cardholder data

🛸 Access ma	anagement BETA
n	↑ Import and export
Q	Action Import T

The action dropdown is where the action that will be done is selected.

- Import
- Export
- Restore

Import cardholder data

Import		-
Import cardholders, cardho	older groups, and credentials from a	a comma-
New	<i>.</i>	
Column delimiter		
, Maximum image size		
0	KB	
Unique identifier		
Cardholder ID	*	
Card number format		

This function imports cardholders, cardholder groups and credentials from a CSV-file.

Select "New" if the imported data should be imported as a new database, wiping all stored data currently in the system.

Check the box "First row is header" if the imported file contains column headers. Input the delimiter that the imported file is formatted with.

Select the maximum allowed image size for cardholder photos.

Select what will be the Unique identifier linking cardholders between stored and imported data. Choose if card numbers in the file will remain as they are in the import process or if conversion to decimal or hexadecimal values is needed.

Click "Browse" to select a file.

Browse	csvexample_3000.csv	
		Lord
		Load

When a file has been selected, Click "Load".

Column mapp	ing					× Assign field	
Unassigned 🖍	Undefined 🖍	Undefined 🖍	Undefined 🖍	Undefined 🖍	Undefin	Unassigned	+
Firstname1	Lastname1	4194	1	BD37482E	0BAC084	Cardholder	
Firstname2	Lastname2	9255	2	6AA0426E	890A9AF	Cardholder First name Cardholder Last name	+ +
Firstname3	Lastname3	6620	3	2D5E3059	6A651633	Cardholder Cardholder ID	+
Firstname4	Lastname4	2472	4	5A3A706E	FD3FDA1	Cardholder Email address	+
Firstname5	Lastname5	1635	5	C5078CC8	517CF9C	Cardholder Active	+
Firstname6	Lastname6	4181	6	01192339	64125977	Cardholder Suspended	+
Firstname7	Lastname7	3432	7	E2BA9290	7CA3EF6	Cardholder Long access time	+
Firstname8	Lastname8	9124	8	A40D5DF8	0C18FF6:	Cardholder Custom field 1	+
Firstname9	Lastname9	6495	9	37B435F2	99DA2E7	Cardholder Custom field 3	+
Firstname10	Lastname10	90	10	261585CB	ED4BA55	Cardholder Custom field 4	+
						Cardholder Custom field 6	+
					-	Card 1	
						Card 2	
						Card 3	

An import preview is shown and here the columns need to be linked to the system fields.

First name 🎤	Last name 🖌	PIN pin 🖍	Cardholder ID 🧪	Card 1 Cardnumber 🖍	Card 2 Cardnumber 🖍	Card 3 Cardnumber
irstname1	Lastname1	4194	1	BD37482E	0BAC084B	599E3500
firstname2	Lastname2	9255	2	6AA0426E	890A9AF0	055F10C3
irstname3	Lastname3	6620	3	2D5E3059	6A651633	F590F2BA
irstname4	Lastname4	2472	4	5A3A706E	FD3FDA1E	CD4F9F02
irstname5	Lastname5	1635	5	C5078CC8	517CF9CE	0B4F30AB
irstname6	Lastname6	4181	6	01192339	64125977	9B9522B8
irstname7	Lastname7	3432	7	E2BA9290	7CA3EF63	A93CCCFC
irstname8	Lastname8	9124	8	A40D5DF8	0C18FF62	F944E72C
firstname9	Lastname9	6495	9	37B435F2	99DA2E73	45EBB1DD
irstname10	Lastname10	90	10	261585CB	ED4BA550	8DC4B4ED

When all column headers have been assigned the import is started by Clicking on the "Import" button.

Column mapping	S Import successful
----------------	---------------------

A notification will be shown when all the data has been imported.

NOTE The user won't get an error if they try to import a file with wrong card number (eg. have a strange character). The user can't import the file, but don't know why.

Exporting cardholder data



There are no settings in the export action. To export the cardholders, cardholder groups and credentials from the system click on the "Export" button.

Restoring from last import point

Astiss		
Posot		
Reset		
Reset cardi	nolder data to last saved state. You can	only reset once
because the	e system saves only one state automati	cally.

The system saves its state prior the last import action. If the import has been unsatisfactory, it is possible to roll back the database to the version that was in place before the last executed import. This action can only be done once and if multiple import actions have been done in a short period of time the reset will only take the database one step backwards in time.

Cardholders Groups	Q Type to search			Access rules	Q Type to search
Derek Wang		Les In a group	:	Tule rule	(3 cardholder(s) (1 door
Gustaf Scheja			:	Employee access	2 group(s)
Martin Gren		Lin a group	:		
Matthew Meade			:		
Tamara Abdulrazak			:		
				Doors Zones	Q Type to search
				Main entrance	Belongs to Outdoors, Office zone

Access Management dashboard

From the access management dashboard, it is possible to:

- add cardholders with credentials to the system.
- add cardholder groups to group cardholders together for easy management.
- create access rules to set levels of access on designated doors or zones, combining with a schedule.
- configure unlock schedules for doors and zones.
- send commands to doors and zones to for instance lock or unlock.

Adding a cardholder group

Access m	anagement 🕂			
n	Cardholders	Groups	Q Type to search	
Ê				Gibups

To add a cardholder group, click on the '+'-sign, and then select groups.

×	New group
	🛎 Group
	Name My group

Edit group Appty Delete		× Cardholders
Sroup		Q Type to search
Name		Matthew Meade
Employees		Tamara Abdulrazak
Lardholders		Gustaf Scheja
Martin Gren	×	
Derek Wang	×	

The group needs a name. It is also possible to add existing cardholders in the group from the system.

Adding and editing a cardholder

				AXIS Camera Station Client
Access n	nanagement 🕂			
	Cardholders Grou	ps	Q Type to search	Cardholders
Ê				

To add a cardholder, click the '+'-sign and then select the cardholder icon.

	+
ist name	No credentials
ast name	
ardholder ID	
mail address	
Groups v	
] Suspend cardholder	
Extended access time	

First name			
Last name			
Cardholder ID		-	
Email address			
Groups	~		
^			
Suspend cardholder			

the arrow below the group's selection.

To add a cardholder photo to the system, click on the Add Photo-icon.

Here is where the cardholder data is put into the system.

The Cardholder ID is a mandatory and system unique field to always be able to identify a specific cardholder. This is due to all other data for the cardholder may change over time.

It is possible to expand the cardholder form with additional features by pressing

Lardholders	Credentia	
First name	No credentials	
Last name		
Cardholder ID		
Groups		
^		
Suspend cardholder		

It is also possible to add the cardholder to an already created group from here.

Adding and editing a card credential

Lardholders			Credentials	C
First name Gustaf			No credentiais	
Last name Scheia				
10666 Email address gustaf.scheja@axis.com		6		
Groups	^	Source Image pro		
My group	×			

Credentials	
No credentials	

To add a card credential, click on the '+'-sign on the credentials form. Click on the card-icon.

Card name			
Select reader to get data from			
None	*	Get last swiped	
Card number		card data from the selected	
		leader	
Bit length O			
Bit length O			
Expiration date			
Bit length 0 Expiration date			
Bit length O Expiration date Valid from			
Bit length O Expiration date Valid from 2020/10/28	<u></u>		
Bit length 0 Expiration date Valid from 2020/10/28 Valid to			

Give the card a name and input the card number (Facility code will also be visible here if enabled under Access management configuration). It is also possible to select a reader in the system to retrieve the card data of the last swiped card from there.

Under expiration date it is possible to set different expiration settings.

- No end date Credential will never expire
- Date Set a date of expiration
- From first use Select this option if you want to give access for a specific time after the credential is first used.
- From last use Select this option if you want to access to end if the credential is inactive for a specific time.

Adding and editing a PIN credential

Credentials	
Card credential Access Card	=

To add a PIN Credential, click on the '+'-sign and then the PIN-icon.

PIN		
1234		
Duress PIN		
Duress PIN		
1235		

A PIN Credential has no expiration. However, it is possible to configure a separate duress PIN that still opens the door in normal operations but triggers a silent alarm in the system to alert security staff if used.

NOTE For duress PIN to work, authentication with card + PIN is required for the validation to be non-anonymous.	
--	--

Adding and editing access rules

From the access management dashboard access rules can be created. Create an access rule by pressing the '+'-sign.

× New access rule Add	
E Access rule	
Name	
Schedules	
Name	
Lardholders Groups	
Name	-
Doors Zones	•
Name	

An access rule is comprised of a name, schedules when the rule should be active, cardholders, cardholder groups, doors and/or zones. It is possible to add all components of the rule from here when adding or editing the access rule. Adding cardholders, cardholder groups, doors and zones can also be done with multi-select drag-and-drop on the access management dashboard.

Edit door in access management

Doors Zones	Q Type to search
Main entrance	Belongs to Outdoors, Office zone

To edit a door in the access management dashboard, click on the edit-pen next to the door you want to edit.



- see what zone the door is included in (A)
- set an unlock schedule (B)
- enable first person in rule for the unlock schedules (C)

Edit zone in access management

Doors Zones	Q Type to search
Outdoors	
Office zone	

To edit a zone in the access management dashboard, click on the edit-pen next zone you want to edit.

× Edit zone Apply	
Zone	Summation schedules
Name Outdoors	
Doors included Main entrance A	
Unlock schedules	
Name Valid for	

In this edit view it is possible to

- see the doors in the zone (A)
- set an unlock schedule (B)
 - Note that it is not possible to apply a first person in rule on the zone.

Sending actions to doors and zones from the access management dashboard

Doors Zones	Access	Unlock	∂ Lock	O Lockdown	Schedule
Main entrance	_	(Belongs t	o Outdoors, Office	zone

Select one door or hold down the Ctrl-key and multiple select a number of doors or zones to send door commands using the — icon.

Access Management reports

Here it is possible to save some pre-defied reports from the system in a .csv-format.



Unifying Video surveillance and Access Control



Connect a split view or camera view to a door

Go to Configuration \rightarrow Devices \rightarrow External data sources to find a list of the configured doors in the system. By clicking "Edit..." it is possible to connect the door to a designated camera view.

Door plugin view



Open a new View tab by clicking on the "+"-sign and then choose Live view in the AXIS Camera Station Client.

Right click on a view you want to include the assist and monitor in and select "Edit..."



Selecting the door views will list the configured doors. Drag and drop the view into the split screen view. Save the view.

Main entrance



Now it is possible to provide assistance to a cardholder as well as monitor the door's current transactions and status.

::≡ 🖵 Main view 🚯 Main view 🗘 Configuration 📿 Data search X 🖵 Main view Live view Start 🖼 2020-12-13 16:06 End 🖼 2020-12-14 16:06 Search Time Source Recording C Sn Φ 日日 Logs 2020-12-14 ▼ ■ 日 er et AXIS A8105-E - La AXIS M3027 (2) - Terrace 9 + â + to DESKTOP-7GMHVUI

Data search (Access Control Event log with video link)

Opening a tab for Data search will show the access control specific event log together with the associated view and recordings that are triggered on door events. Apply the dates and times you want to investigate and press search.

NOTE The filtering in the External Data Search is case sensitive.

Terminology

Hardware

Door monitor	A door position switch that sense physical state of the door (open or closed) usually providing a closed circuit when the door is closed.
Emergency input	An input on the AXIS A1601 that can be configured through AXIS Camera Station Secure Entry to initiate an unlocking or locking action locally in the device. Normally these inputs are configured to be active on an open circuit to accommodate for a scenario that the wire has been cut.
OSDP	SIAs Open Supervised Device Protocol – Communication standard between Access Control Units (Door controllers) and Peripheral Devices (Readers)
Reader	A device that reads a cardholder's different credentials.
REX	A Request to Exit device usually a button or a PIR-sensor indicating that someone wants to exit the door. A REX can also be configured that it does not unlock the door if it is only a notification that a mechanical override, such as a panic bar or mechanical opening handle has been used, to not send door forced open events.
Wiegand	One of the oldest standardized ways to get card data from a reader. Supported for legacy and compatibility purposes.

Access management

Card format	A card format is what defines how data is stored in a card. All data is in binary so the card format in the system is a translation table between the data stream the door controller is receiving from the card reader to the data structure the door controller does access validation on. Therefore, the card format in the solution has the possibility to define different fields (bit ranges), encodings and bit and byte order swapping. All to get the card number and / or the facility code we want to validate
Card number	A facility code is a subset of the incoming data stream from the reader and / or data stored on a card that is meant to identify the specific card and / or cardholder
Cardholder	An access control user with a card or other credential whose main purpose in the access control system is to get access through doors where they need to go and not get through doors where they don't need to go.
Cardholder ID	A unique identifier for a specific cardholder, since names can change and therefore also email addresses an attribute is needed for identifying the specific cardholder in a system. The cardholder ID is system unique and mandatory and can be alphanumerical.

Facility code	A facility code is a subset of the incoming data stream from the reader and / or data stored on a card that can be encoded to be identical for a specific end customer / site. Legacy access control systems used this means to avoid any card duplicates when the id numbers started running out.
Identification profile	An identification profile is a combination of one or more identification types and one or more schedules. Administrators of the system can apply an identification profile to one one or many doors to determine how and when a cardholder gets access to that or those doors.
Identification type	Identification types are carriers of the credential information that cardholders need to get access to a door. A means of identification. Common identification types are tokens, such as cards (card raw, card number) or key fobs, personal identification numbers (PINs), fingerprints, facial maps, and request to exit (REX) devices. And depending on the identification type, it can carry one or more types of information.
Internal Door	Internal doors can only be part of one zone and is defined as inside the physical zone.
Perimeter Door	Perimeter door in a zone moves cardholders between, into or out of zones.
Zone	A zone is a group of doors designated to a specific physical zone. In the future the zones can be applied in anti-passback-regulations as well as people tracking. There are two types of doors in a zone. A Perimeter door that moves cardholders between zones and internal doors. Internal doors can only be part of one zone, but perimeter doors can be part of two zones if they are physically adjacent and this moving cardholders from one zone to another.