



10641 Highway 36
Covington, GA
30014

www.sunbeltbuilders.com

t 770.786.3031
f 770.786.3046

HISTORIC JAIL RENOVATIONS

TechOptics
463 Bankhead Hwy.
Winder, GA 30680
ph: 770-867-1777
Chad Maynard
chad@techoptics.net

28-1000 Access Controls & Cameras O&M

NEWTON COUNTY, GA –HISTORIC JAIL
OPERATIONS & MAINTENANCE MANUAL –
ACCESS CONTROL SYSTEM

Version 1.0

Date 07/29/2026

VERSION HISTORY

Version #	Implemented By	Revision Date	Approved By	Approval Date	Reason
1.0	<i>Chad Maynard</i>	<i>07/29/2026</i>	<i>Chad Maynard</i>	<i>07/29/2026</i>	<i>Original release</i>

PROJECT INFORMATION

Item	
Owner	<i>Newton County, GA</i>
Facility	<i>Newton County Historic Jail</i>
Access Control Software	<i>SALTO Space</i>
ACS Server	<i>Not provided – existing server utilized</i>
Server Location	<i>Unknown</i>
Doors Installed	<i>5</i>
Installation Date	<i>May 2026</i>
Contractor	<i>TechOptics, Inc.</i>

TABLE OF CONTENTS

1 INTRODUCTION	4
2 PROJECT SCOPE	4
3 SYSTEM DESCRIPTION	4
4 INSTALLED EQUIPMENT.....	5
5 OPERATION	5
6 PREVENTIVE MAINTENANCE.....	5
7 WARRANTY	5
8 TROUBLESHOOTING	6
9 INSTALLER INFORMATION.....	6

1 INTRODUCTION

This manual provides operation and maintenance information for the access control work completed at the Newton County Historic Jail. The project consisted of furnishing, licensing, installing, configuring, and commissioning five (5) access control doors to be added to the owner's existing SALTO Space server.

2 PROJECT SCOPE

Work performed by TechOptics included:

- Installation of one Altronix Trove2 unified power enclosure.
- Installation of three SALTO CU4200E IP controllers.
- Installation of five SALTO Design XS wall readers.
- Installation of five HES door strikes.
- Supply and activation of the required Salto licenses.
- Addition of the doors/readers to the existing SALTO Space server.
- Configuration of controller settings.
- Verification of door operation.

Items specifically outside the project scope included:

- Existing SALTO Space server hardware and software licensing.
- Network switches, structured cabling, and fiber infrastructure.

3 SYSTEM DESCRIPTION

The access control installed under this project are connected to the customer's existing network and are managed by the existing SALTO Space server. The controllers and all door related access and configuration is managed through the customer's existing system and can be handled by the Newton County IT Department. If further support is required, see the appropriate section of this document.

4 INSTALLED EQUIPMENT

An Altronix Trove2 PN T2SAK78 was installed in the MDF of the Historic Jail. This unified power enclosure provides power and backup power for the operation of the entire door system as well as houses the SALTO CU42E0 IP control units. Each control unit can operate two (2) readers and two (2) door locks associated with those readers. Additional controller units can be added to this enclosure to achieve up to eight (8) doors with unified power. Currently, three (3) controller units are populated and service the five (5) installed SALTO WRDM0A48 Design XS wall readers and five (5) HES door strikes.

The following doors are controlled:

- Front door room 101
- Conference door room 109
- Side door room 108
- MDF closet door room 114
- Upstairs fire door room 205

5 OPERATION

The SALTO Space server provides facilities to configure users, group, and access to each door and provides reporting capabilities. The configuration, maintenance, and usage of SALTO Space are outside the scope of this project document.

6 PREVENTIVE MAINTENANCE

- The Altronix Trove2 unified power cabinet in the MDF has 2x 12V 10AH batteries installed for backup power. These should be checked annually and replaced if they are more than 4 years old.
- Electric door strikes have a limited number of cycles. If the cycles are exceeded or the strike solenoids fail, the strike will need replacement.
 - HES 9600 Rim Panic Strike – 1,000,000 cycles
 - HES 1600 Mortise / Cylindrical Strike – 1,000,000 cycles

7 WARRANTY

- SALTO readers and controllers covered by the manufacturer's warranty for two (2) years from the date of purchase.
- Altronix power supplies are covered by the manufacturer's limited lifetime warranty.
- HES strikes are covered by the manufacturer's warranty for five (5) years from the date of purchase.
- TechOptics warrants workmanship for one (1) year from the date of installation unless otherwise specified in the contract.
- Damage caused by vandalism, lightning, power surges, network failures, or owner/third party modification is excluded.

8 TROUBLESHOOTING

If a door or reader is offline:

1. Verify power and network connectivity.
2. Confirm the SALTO controller responds on the network.
3. Check SALTO Space for communication errors.
4. Contact TechOptics if hardware replacement or additional support is required.

9 INSTALLER INFORMATION

TechOptics, Inc.

463 Bankhead Hwy.

Winder, GA 30680

<http://www.techoptics.net/>

Phone: 770-867-1777

Fax: 770-868-0111

Service Email: service@techoptics.net

General Email: info@techoptics.net

T2SAK78 (Kit)

Access & Power Integration Solution for Salto

Altronix T2SAK78 kit consists of Trove2 enclosure, TSA2 Salto/Altronix backplane with one (1) 24VDC @ 10A power supply/charger, one (1) fused access power controller, one (1) voltage regulator and one (1) dual input fused power distribution module.

This kit also accommodates up to four (4) Salto CU42E0, CU4200 or CU4EB8 modules for up to eight (8) doors in a single enclosure. Trove simplifies board layout and wire management, reduces installation time and labor costs.

**TROVE™****T2SAK78***Salto boards are not included***Key Features**

- 24VDC power supply/charger
- Accommodates up to four (4) Salto CU42E0, CU4200 or CU4EB8 modules
- Convenient knockout configuration:
 - One (1) single knockout 2.415" (2" Conduit)
 - Sixteen (16) double knockouts 1.362" (1" Conduit) / 1.115" (3/4" Conduit)
- Supervision
 - AC Fail
 - Battery Fail and Battery Presence
- Agency Listings:
 - All Altronix components of this Trove kit are UL Listed sub-assemblies. Please refer to the Sub-Assembly Installation Guides for further information
 - UL: UL294 - Access Control System
 - cUL: CAN/ULC - s319-05 - Electronic Access Control Systems
 - CE European Conformity
- 16 gauge galvanized steel backplane simplifies board layout and wire management
- Enclosure accommodates up to four (4) 12VDC/12AH batteries
- Lifetime Warranty*

**Altronix Power Supply/Chargers and Sub-Assemblies only*

Specifications

Power Supply/Charger (AL1024ULXB2):

Input

Voltage	115VAC 60Hz, 4.2A max.
Input Fuse	5A/250V

Outputs

Voltage	24VDC
Current	10A @ 24VDC continuous max.
Other	Overvoltage protection. Filtered and regulated

Battery Charging

Capacity	12VDC/12AH (4 within enclosure) 40AH/65AH (requires separate enclosure)
Type	Sealed lead acid or gel type
Failover	Upon AC loss, instantaneous
Batteries are sold separately	

Supervision

AC Failure	Form "C" contacts
Battery	Form "C" contacts

Indicators (LED)

Input	115VAC is present
DC Output	Powered
Battery	Discharged or not connected

Dual Input Power Distribution Module (PDS8):

Input

Voltage	24VDC from AL1024ULXB2 and 12VDC from VR6
Input Fuses	10A/32V

Outputs

Voltage	12VDC and/or 24VDC
Any of the eight (8) power outputs are selectable to follow power Input 1 or Input 2	
Individual outputs may be set to OFF position for servicing	
Output Fuses	3A/32V

Indicators (LED)

DC Output	Eight (8) individual output LEDs
Green:	12VDC
Red:	24VDC

Voltage Regulator (VR6):

Input

Voltage	24VDC from AL1024ULXB2
---------	------------------------

Output

Voltage	12VDC
Current	6A continuous
Other	Surge suppression

Indicators (LED)

Input	24VDC is present
Output	Powered

Access Power Controller (ACM8):

Input

Voltage	24VDC from AL1024ULXB2
Input Fuse	10A/250V

Outputs

Voltage	24VDC
Eight (8) independently controlled fused outputs:	
a) Fail-Safe and/or Fail-Secure power outputs	
Form "C" Relays rated 28VAC or VDC @ 2.5A	
b) Auxiliary power outputs (unswitched)	
c) Any combination of the above	

Output Fuses	3.5A/250V
--------------	-----------

Indicators (LED)

Red LEDs	Outputs are triggered (relays energized)
Green LED	FACP disconnect is triggered

T2SAK78 Kit:

Agency Listings

All components of this Trove kit are UL Listed sub-assemblies. Please refer to the corresponding Sub-Assembly Installation Guides for further information.

CE	European Conformity
----	---------------------

Physical and Environmental

Dimensions (H x W x D)

Enclosure:	27.25" x 21.5" x 6.5" (692.2mm x 546.1mm x 165.1mm)
Shipping:	32.5" x 26.5" x 11.125" (826mm x 673mm x 283mm)

Weight (approx.)

Product	54.3 lb. (24.6 kg)
Shipping	59.3 lb. (26.9 kg)

Temperature

Operating	0°C to 49°C (32°F to 120°F)
Storage	- 20°C to 70°C (- 4°F to 158°F)

Relative Humidity

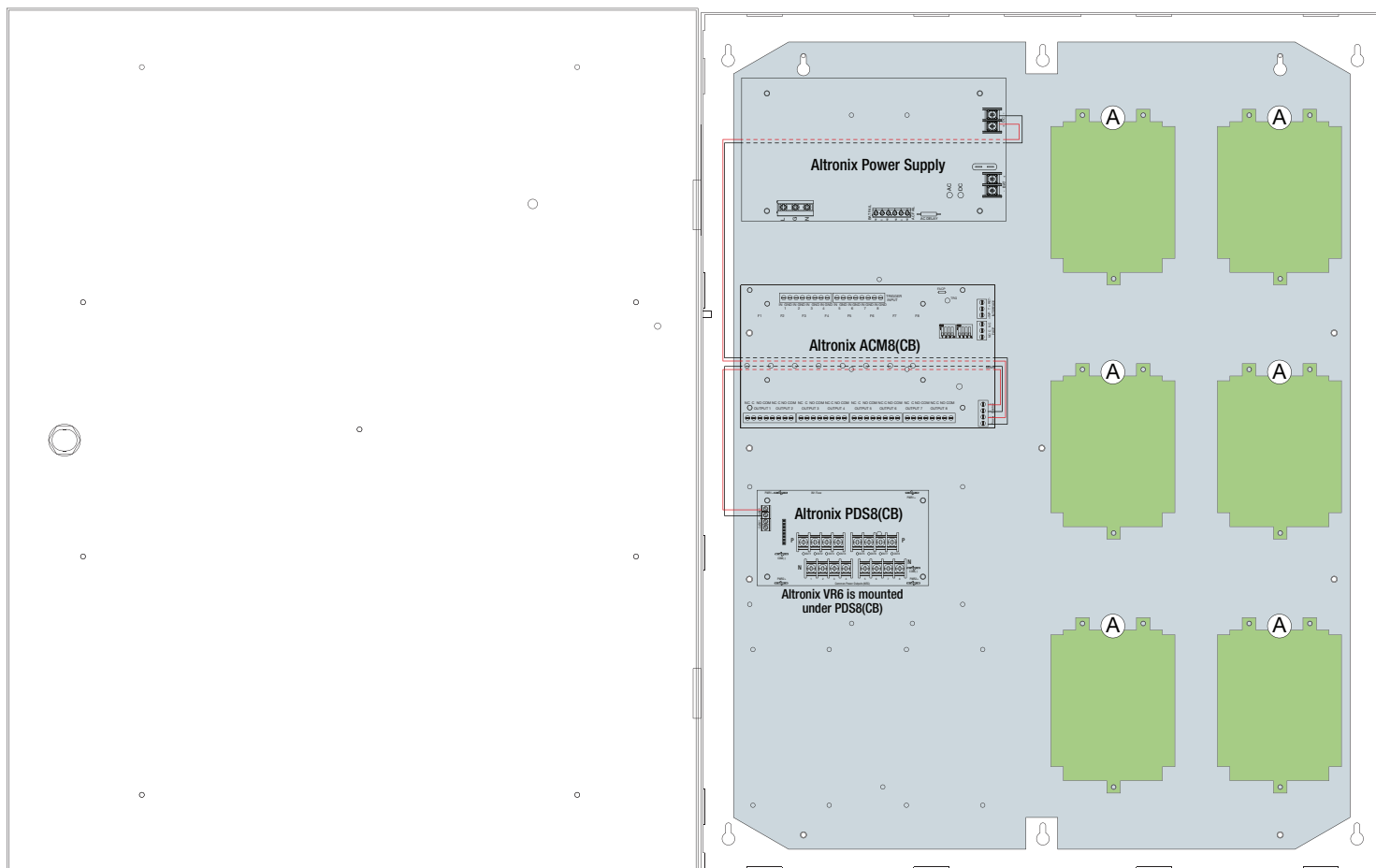
85% +/- 5%

BTU/Hr (approx.):

128 BTU/Hr.

Access Controller Position Chart for the Following Models:

Salto	Pem Mounting
CU4200, CU42E0, CU4EB8	(A)



Accessories (order separately)

WM5

WM5, WM25, WM100 - Magnetic Cable Tie Mounts

Altronix WM5, WM25, and WM100 are packs of 5, 25 or 100 magnetic cable tie mounts respectively. They accommodate standard zip ties or velcro straps. These are ideal for wire management in our Trove series.



Mounting Magnet

MM4, MM8, MM12, MM24 - Magnetic Mounting Solution

Altronix mounting magnets accommodate screws and nylon standoffs to allow for mounting various boards/ accessories in any metal enclosure or backplane.



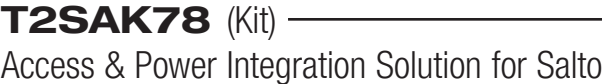
BR1

BR1 - Sub-Assembly Mounting Bracket

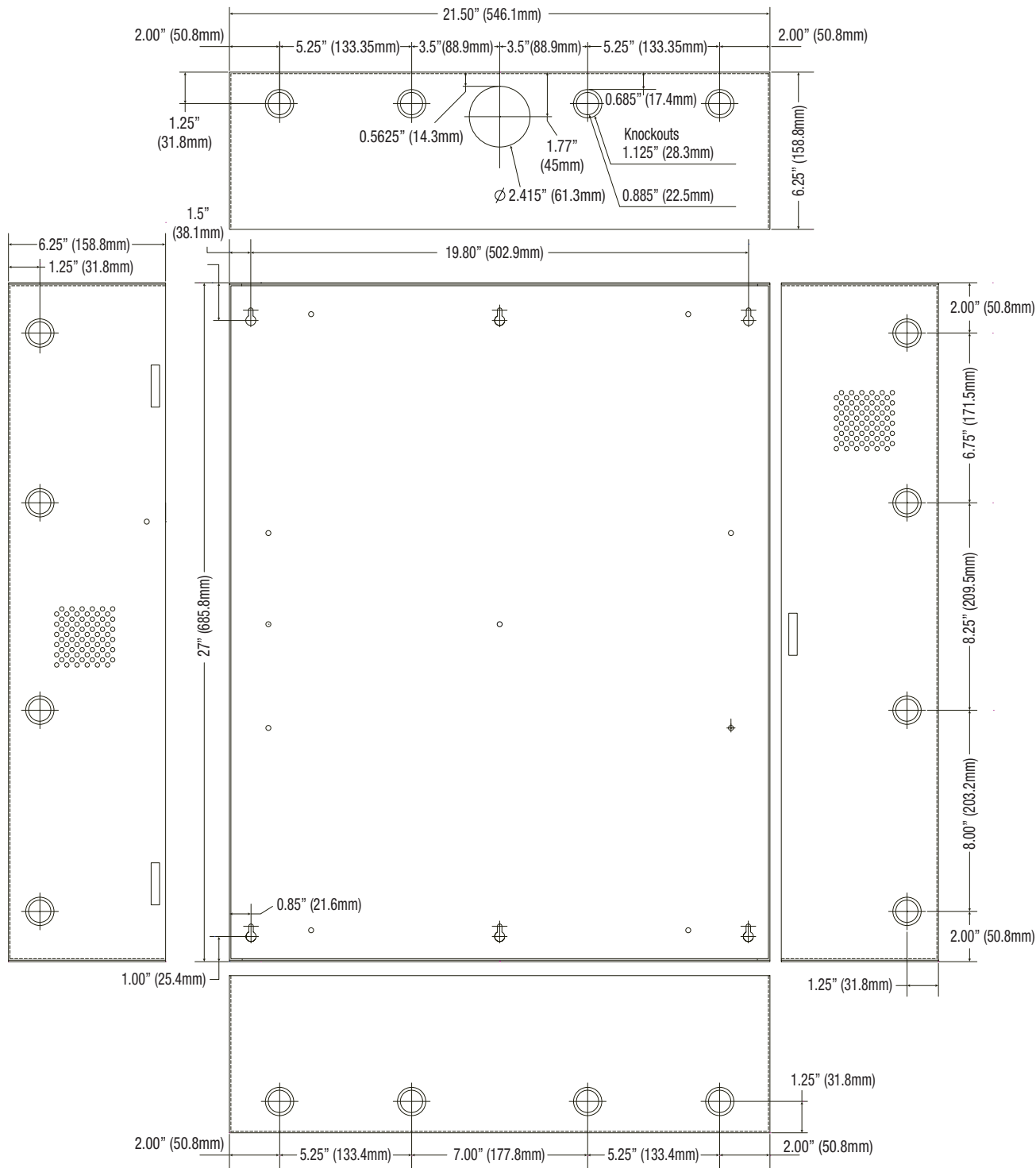
Altronix BR1 mounting bracket is compatible with Altronix Maximal and Trove enclosures. It allows to mount one (1) PD4UL(CB), PD8UL(CB), ACM4(CB), MOM5, VR6, PDS8, NetWay5B or LINQ8PD(CB) sub-assembly on the enclosure's inside wall, saving valuable space.

Trove2BWC
with
batteriesTrove2BWC
with
wires**TROVE2BWC - Battery/Wire Trough Enclosure**

Altronix Trove2BWC is a dual-purpose enclosure that can be used as wiring trough or battery cabinet when mounted above or below of the Trove2 integrated power and access solution. The knockouts on the Trove2BWC have been strategically placed to line up with the Trove2 allowing for easy conduit connections between cabinets. Trove2BWC includes cam locks and 2 tamper switches to ensure access to wiring and batteries is secure.



Dimensions (H x W x D approximate)
27.25" x 21.5" x 6.5" (692.2mm x 546.1mm x 165.1mm)



Installation guide

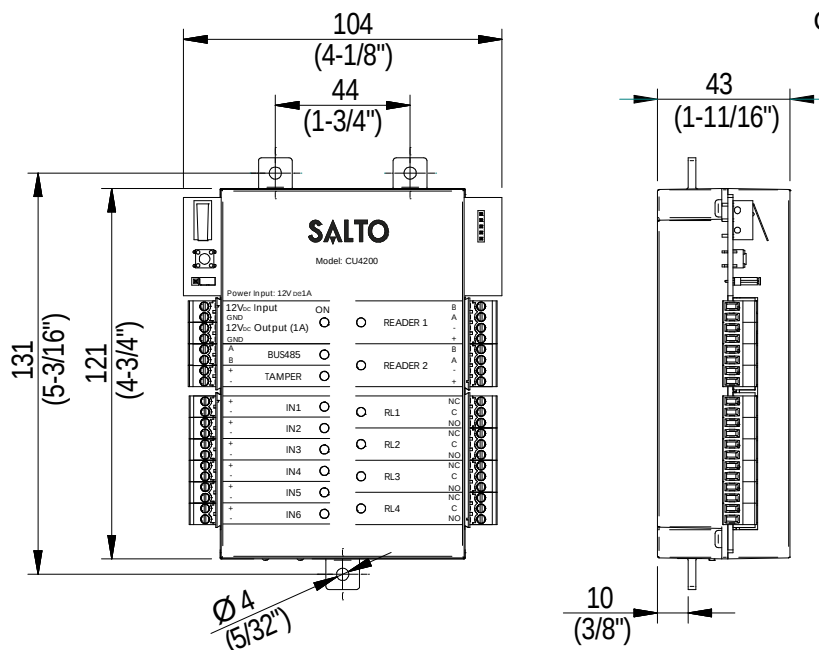
XS4 Controller

- Eng **Installation guide**
E **Guía de instalación**
F **Guide d'installation**

CU42xx.. series

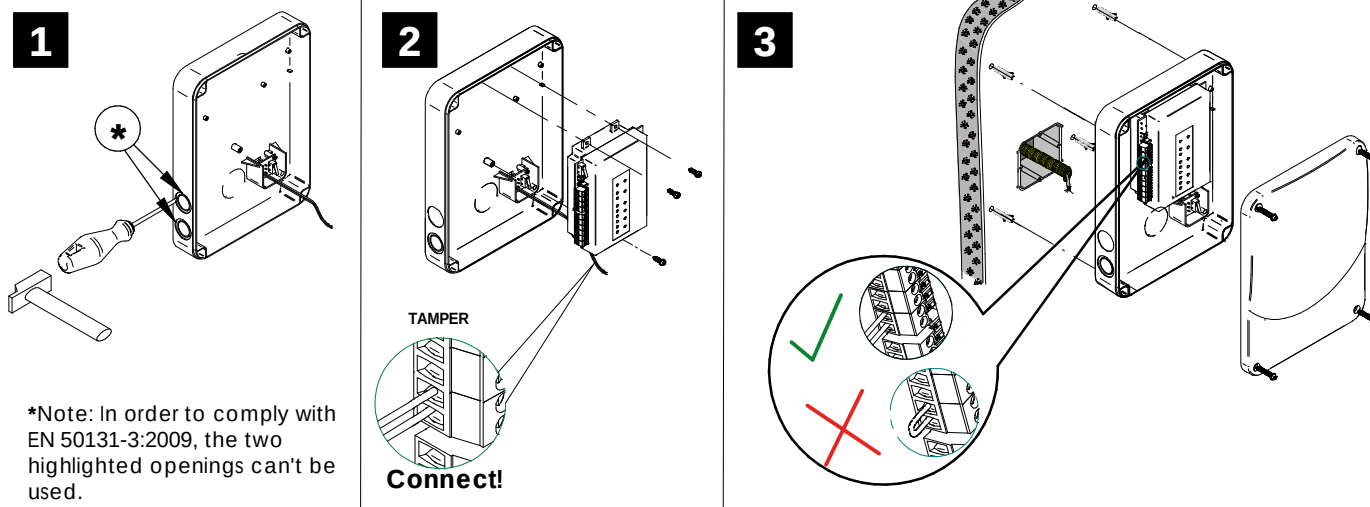
The door controller reads the encrypted data contained on the carrier and allows for updating of the carrier via SALTO Virtual Network technology, making it possible to cancel lost or stolen cards remotely. It is equipped with input connections that permit third party readers integration.

CU42E0	CU42E0T00 CU42E0G00
228g	600g
CU4200	CU4200T00 CU4200G00
190g	570g



Eng **Mechanical Installation** E **Instalación mecánica** F **Installation mécanique**

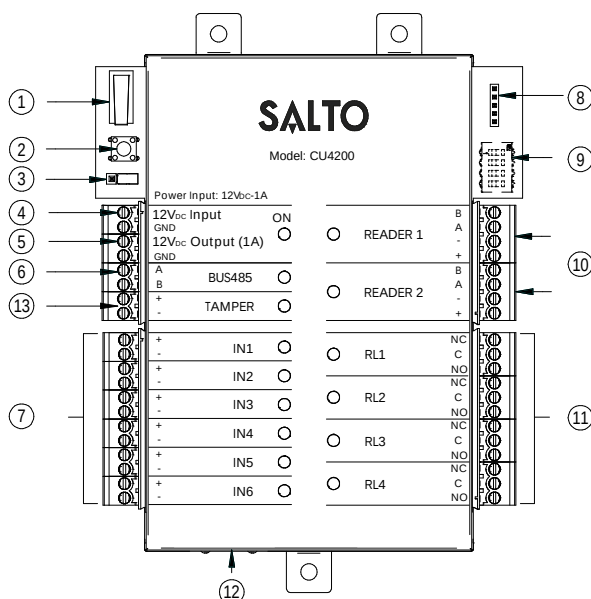
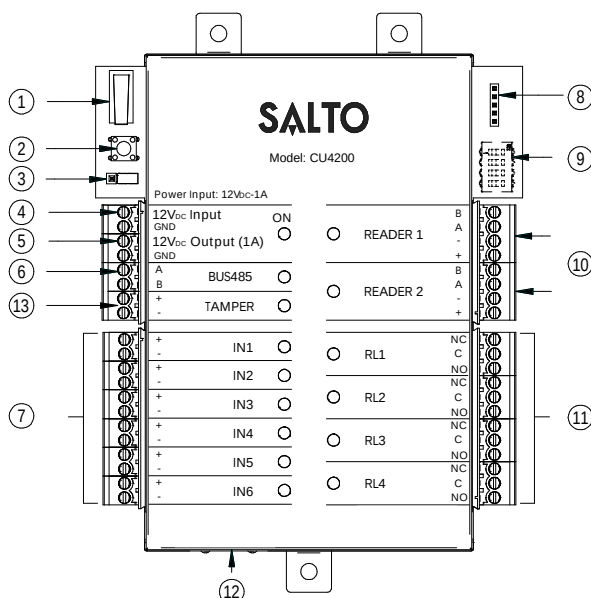
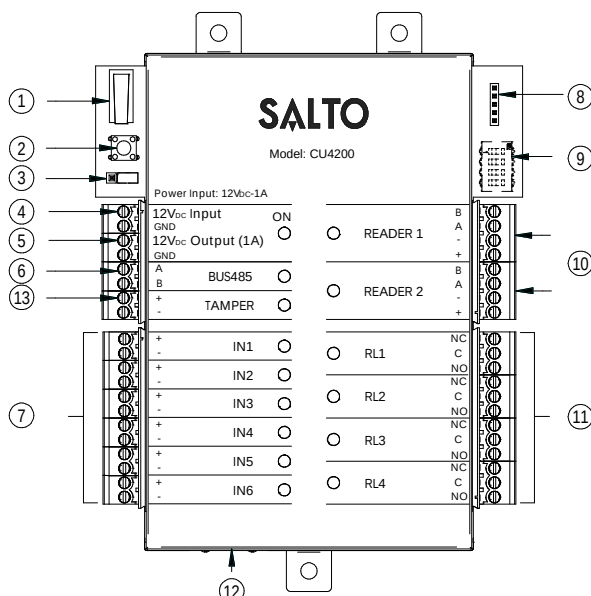
CU42E0T - CU42E0G - CU4200T - CU4200G
CU42E0T00 - CU42E0G00 - CU4200T00 - CU4200G00



Note: Follow the same connection model, using the CU tamper input, when using a third party electric box equipped with a tamper opening detection.

Installation guide

XS4 Controller



(Eng)

- ① **Physical tamper switch** to be operated by external electric box models.
- ② **Clear button** must be pushed (not more than 5 seconds) if the configuration has been changed, (i.e. reader added, connected by Ethernet, device connected by BUS485) and the tamper alarm must be activated by removing the tamper switch connector.
- ③ **BUS RS485 Terminal resistor** must be in the ON position when the CU is connected at the end of the BUS.
- ④ **Power input.**
- ⑤ **Power output:** this output is directly connected to the power input port protected by a 1A fuse.
- ⑥ **BUS485.**
- ⑦ **Inputs:** installer must identify the bridge cable needed depending on the input configuration.
- ⑧ **PPD Connection.**
- ⑨ **Address configure (Only CU4200)** All connected CU addresses must be different from each other.
- ⑩ **Connection to readers:** check reader installation manual to see recommended cable, connections and max. distances.
- ⑪ **Relay connections:** please take into account the max. load restrictions (2A-30VDC). Use the provided varistor if an inductive load is used.
- ⑫ **Ethernet connection (only CU42E0).**
- ⑬ **Tamper input to connect the tamper signal from the SALTO electric box or other compatible devices.**

(E)

- ① **Tamper switch**, conectado en paralelo a la entrada del tamper.
- ② **Clear button** ha de ser pulsado (menos de 5 segundos), si se cambia la configuración: lector añadido, conectado por Ethernet, dispositivo conectado por BUS485 etc. Para ello, la alarma de tamper ha de estar activada (quitar el conector del tamper input).
- ③ **Resistor del terminal BUS RS485** requerido (posición ON) cuando la CU está conectada al final del BUS.
- ④ **Entrada de alimentación.**
- ⑤ **Salida alimentada:** esta salida se conecta directamente a la entrada de alimentación protegida por un fusible de 1 A.
- ⑥ **BUS485.**
- ⑦ **Entradas:** el instalador ha de identificar el cable para el puente dependiendo de la configuración de la entrada.
- ⑧ **Conexión para el PPD.**
- ⑨ **Configurador del direccionador (Solo CU4200)** Todos los direccionamientos de las distintas CUs han de ser diferentes.
- ⑩ **Conexión al lector.** Consultar el manual de instalación del lector para ver el tipo de cable recomendado, conexionado y distancias máximas.
- ⑪ **Conexión al Relé:** Tener en cuenta las restricciones de las cargas máximas (2ª-30VDC). Utilizar el varistor suministrado si la carga es inductiva.

(F)

- ① **Contacteur anti sabotage** monté en parallèle avec l'entrée anti sabotage.
- ② **Bouton Clear** doit être appuyé (pendant au moins 5 secondes) lorsque la configuration est modifiée (ex: ajout d'un lecteur, connexion d'un cordon Ethernet, ajout d'un dispositif sur le BUS485) l'alarme anti sabotage doit être active en enlevant le cavalier du bornier.
- ③ **La résistance de fin de bus RS485** est nécessaire (position ON) lorsque la CU est positionnée à l'extrémité du bus.
- ④ **Puissance d'entrée.**
- ⑤ **Puissance de sortie:** Cette sortie est reliée directement au port d'entrée de l'alimentation protégée par un fusible de 1 A.
- ⑥ **BUS485.**
- ⑦ **Inputs:** L'installateur doit identifier le cable nécessaire en fonction de la configuration d'entrée.
- ⑧ **Connexion pour le PPD.**
- ⑨ **Configuration de l'adresses (Uniquement pour CU4200)** Les adresses des CU connectées au même BUS doivent être toutes différentes.
- ⑩ **Connexion des lecteurs:** Consultez le manuel d'installation du lecteur afin de voir les câbles recommandés, les connexions et les distances maximales.
- ⑪ **Connexion des relais:** S'il vous plaît prendre en compte les restrictions de charge max. (2ª-30VDC). Utilisez les varistances fournis si une charge inductive est utilisée (24v AC/DC Max).
- ⑫ **Connexion Ethernet** (uniquement CU42E0).

Installation guide

XS4 Controller

(Eng)

Factory configuration		
IN1	DOOR state for DOOR1	unsupervised NC
IN2	RTE input for DOOR1	unsupervised NO
IN3	DOOR state for DOOR2	unsupervised NC
IN4	RTE input for DOOR2	unsupervised NO
IN5	Office input for DOOR1	unsupervised NO
IN6	Office input for DOOR2	unsupervised NO
RL1	Lock Relay for DOOR1	
RL2	Tamper Alarm, DLO and intrusion DOOR 1	
RL3	Lock Relay for DOOR2	
RL4	Tamper Alarm, DLO and intrusion DOOR 2	

(E)

Configuración de fábrica		
IN1	Estado de puerta PUERTA 1	unsupervised NC
IN2	Input PULSADOR salida PUERTA 1	unsupervised NO
IN3	Estado de puerta PUERTA 2	unsupervised NC
IN4	Input PULSADOR salida PUERTA 2	unsupervised NO
IN5	Input modo OFFICE PUERTA 1	unsupervised NO
IN6	Input modo OFFICE PUERTA 2	unsupervised NO
RL1	Relé PUERTA 1	
RL2	Alarmas de Tamper, DLO e intrusión de PUERTA 1	
RL3	Relé PUERTA 2	
RL4	Alarmas de Tamper, DLO e intrusión de PUERTA 2	

(F)

Configuration d'usine		
IN1	État de porte pour la PORTE 1	non supervisé NC
IN2	Bouton poussoir pour la PORTE 1	non supervisé NO
IN3	État de porte pour la PORTE 2	non supervisé NC
IN4	Bouton poussoir pour la PORTE 2	non supervisé NO
IN5	Fonction office pour la PORTE 1	non supervisé NO
IN6	Fonction office pour la PORTE 2	non supervisé NO
RL1	Relais de commande pour la PORTE 1	
RL2	Alarme sabotage, intrusion ou porte ouverte PORTE 1	
RL3	Relais de commande pour la PORTE 2	
RL4	Alarme sabotage, intrusion ou porte ouverte PORTE 2	

Note: in order to comply with EN 60839-11:2013, the Enforce password policy must be enabled.

(Eng)

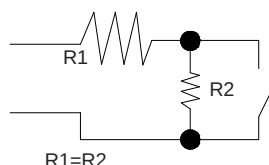
Input connections

(Input supervision has not been evaluated by UL)

CUADAP or third partie readers

	Wiegand	Omron	RS232
IN3	D0 output	Clock output	
IN4	D1 output	Data output	TX output
IN5	D0 output	Clock output	
IN6	D1 output	Data output	TX output

Supervised input connections



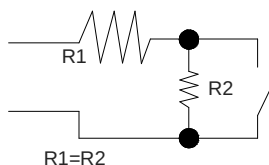
The resistance value R1 and R2 are defined in the software: 1k (recommended), 1k5, 2k2, 3k3, 4k7 6k8, 10k

(E) Conexión de las entradas

CUADAP o lectores de terceros

	Wiegand	Omron	RS232
IN3	Salida D0	Salida reloj	
IN4	Salida D1	Salida Datos	Salida TX
IN5	Salida D0	Salida reloj	
IN6	Salida D1	Salida Datos	Salida TX

Conexión de las entradas supervisadas



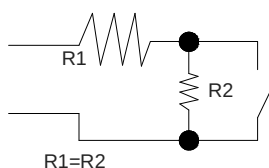
El valor de resistencia R1 y R2 se define en el Software: 1k (recomendado), 1k5, 2k2, 3k3, 4k7, 6k8, 10k

(F) Connexion d'entrée

CUADAPT ou lecteur tiers.

	Wiegand	Omron	RS232
IN3	Sortie D0	Sortie Clock	
IN4	Sortie D1	Sortie Data	Sortie TX
IN5	Sortie D0	Sortie Clock	
IN6	Sortie D1	Sortie Data	Sortie TX

Connexion d'entrée supervisée.



La valeur des résistances R1 et R2 sont définies dans le logiciel : 1k (recommandé), 1k5, 2k2, 3k3, 4k7, 6k8, 10k.

Installation guide

XS4 Controller

Eng Electrical characteristics:

Operation conditions

	Min	Typ	Max	Unit
Temperature	0	25	60	°C
Humidity	35		85	

Power

	Min	Nom.	Max	Unit
Input Voltage		12		V
Current consumption			2 ^{Note1}	A
Output port current ^{Note2}			1	A
Reader Output Voltage		12		V

Input

Electrical characteristics	5V ^{Note3}
Configuration	Via Software ^{Note4}

Cable recommendation

Ethernet ^{Note5}	UTP CAT5e
BUS485	Twisted pair
Inputs	AWG24
Readers	AWG18

Output relays

Rated load (resistive)	2A-30Vdc
------------------------	----------

Note 1: This is consumption of the CU with 2 WR and using the output power port. The CU alone consumes 400mA. Depending on the installation installer must calculate the Power Supply needed.

Note 2: Same voltage as the input.

Note 3: 1K pull-up resistor.

Note 4: See the software User Manual.

Note 5: When Ethernet is available

E Características eléctricas

Condiciones ambientales

	Min	Typ	Max	Unit
Temperatura	0	25	60	°C
Humedad	35		85	

Potencia

	Min	Nom.	Max	Unit
Voltage		12		V
Consumo de la corriente			2 ^{Note 1}	A
Output Corriente ^{Note 2}			1	A

Entrada

Características Eléctricas	5V ^{Note 3}
Configuración	Via Software ^{Note 4}

Cable recomendado

Ethernet ^{Note 5}	UTP CAT5e
BUS485	Pares trenzados
Inputs	AWG24
Lectores	AWG18

Salida relés

Carga (resistiva)	2A-30Vdc
-------------------	----------

Nota 1: consumo de la CU con 2 lectores y utilizando la salida alimentada. La CU consume 400mA. Dependiendo de la instalación, el instalador tiene que calcular la alimentación a utilizar.

Nota 2: mismo voltage que la salida.

Nota 3: resistor de 1K.

Nota 4: consultar el manual de usuario.

Nota 5: cuando ethernet disponible.

F Caractéristique électronique

Condition de fonctionnement

	Min	Typ	Max	Unité
Température	0	25	60	°C
Humidité	35		85	

Puissance

	Min	Nom.	Max	Unité
Tension d'entrée		12		V
Courant de consommation			2 ^{Note1}	A
Courant en sortie du bornier ^{Note2}			1	A

Entrée

Caractéristique électrique	5V ^{Note3}
Configuration	Via Logiciel ^{Note4}

Type de câble

Ethernet ^{Note5}	UTP CAT5e
Bus d'extension	Paire torsadée
Inputs	AWG24
Lecteurs	AWG18

Relais de sortie

Charge nominale (résistive)	2A-30Vdc
-----------------------------	----------

Note 1: Ceci est la consommation de la CU avec 2 lecteurs et utilisant le bornier de puissance de sortie. La CU à elle seule consomme 400mA. Dépendant de l'installataion, l'installateur doit calculer l'alimentation nécessaire.

Note 2: Même tension que l'entrée

Note 3: Résistance de pull-up 1K

Note 4: Consultez le manuel du logiciel utilisateur

Note 5: Si connectique Ethernet

UL Statements

Comply with ULC-S319 Class I:

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

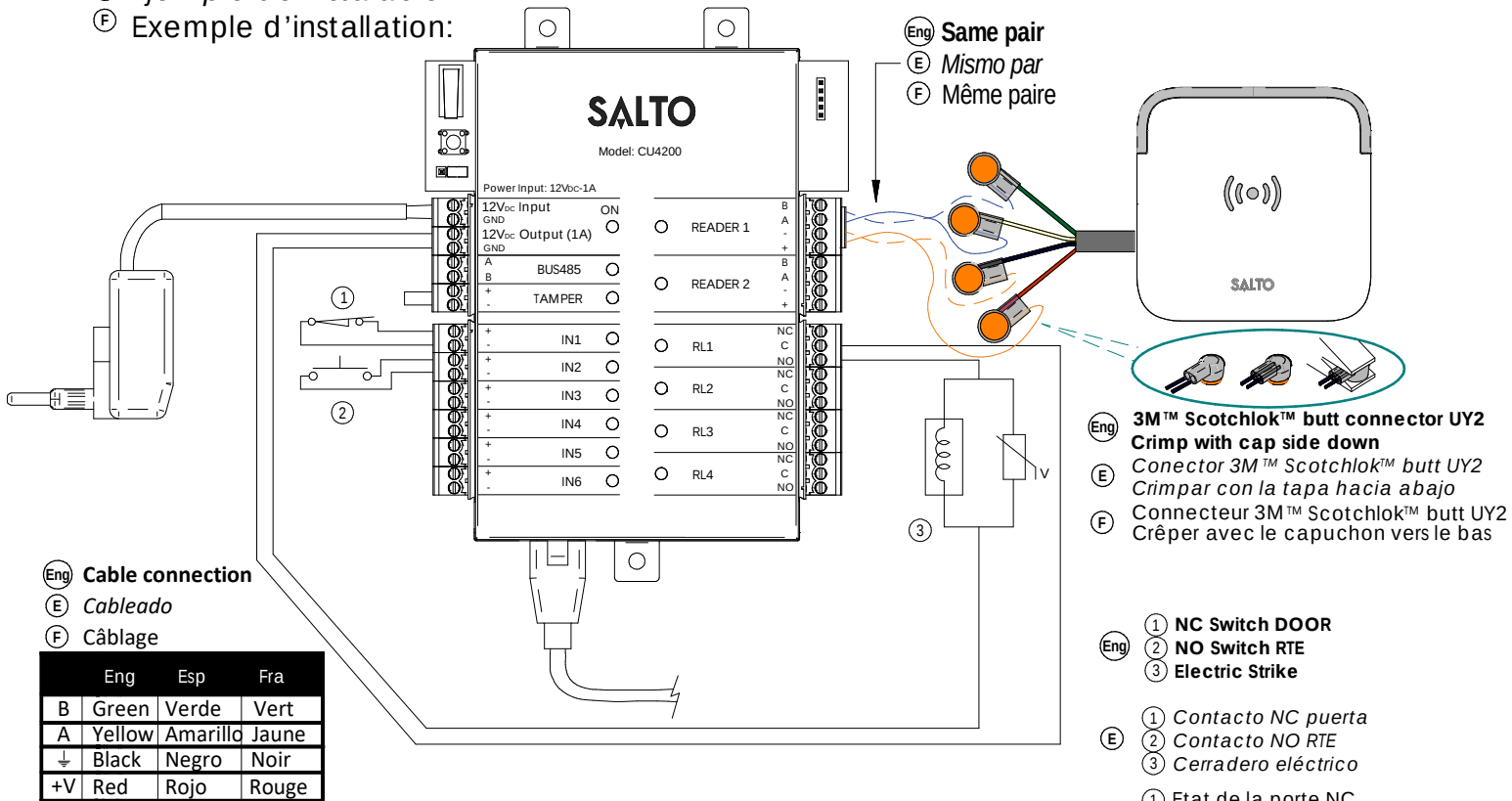
Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes: (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

This device has been tested and found to comply with the limits for a Class B digital device, pursuant to ICES-003.

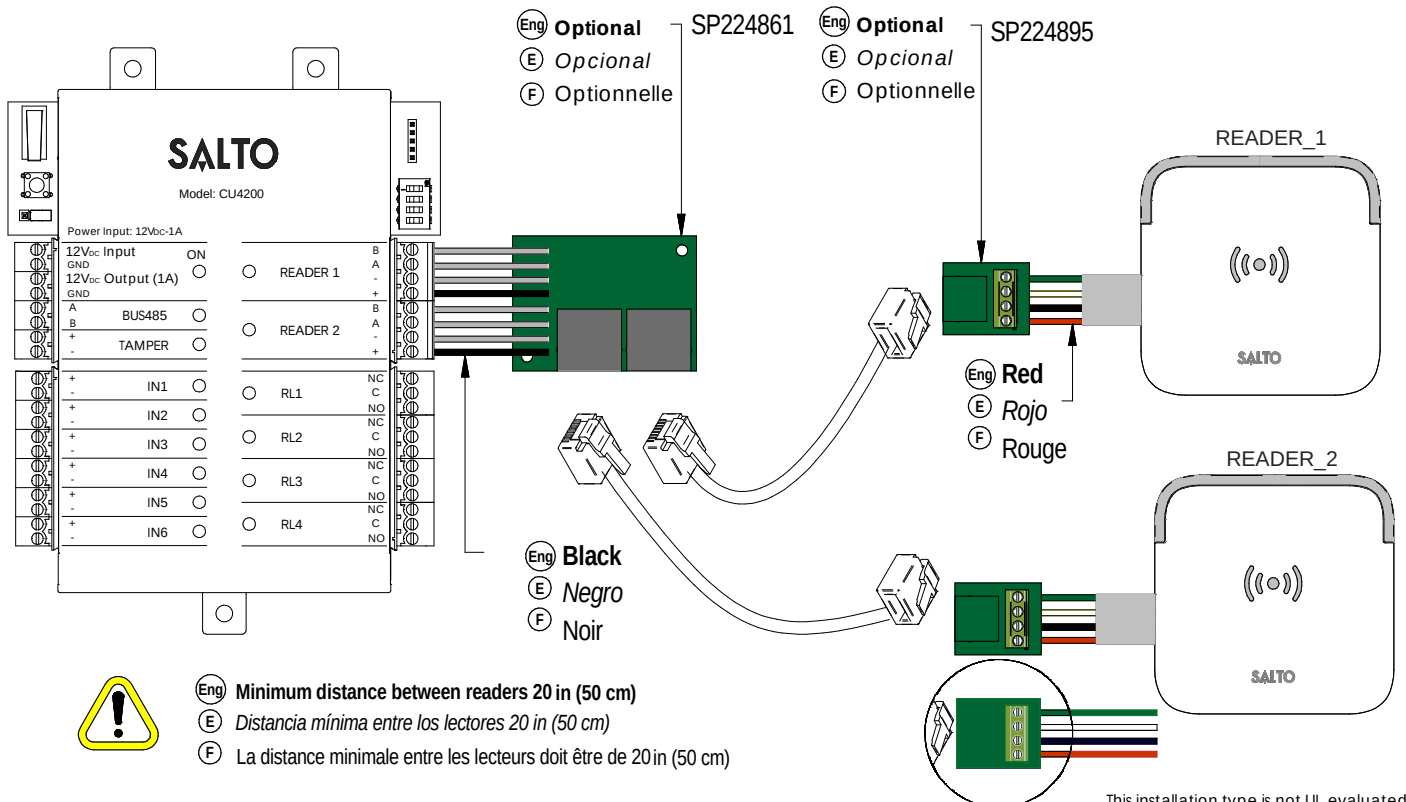
Installation guide

XS4 Controller

- (Eng) **Installation example:**
(E) *Ejemplo de instalación:*
(F) *Exemple d'installation:*



- (Eng) **Installation example with RJ45:**
(E) *Ejemplo de instalación RJ45:*
(F) *Exemple d'installation avec connecteur RJ45 :*



This installation type is not UL evaluated.

Installation guide

XS4 Controller

Eng Configuration:

1. Prepare all the network connections (including Ethernet cable) setting up the dip-switch of each CU4200. Generate a tamper alarm by opening the CU housing or removing the tamper switch cable and then press the CLR button to detect all the connected readers. Check that the readers LEDs are ON (READER 1, READER 2).
2. Perform the set up in the software (Consult SALTO ProAccess SPACE user guide). Set up all the CU4200s with their dip-switches and assign the IP address to the CU42E0.
3. Address the CU42E0:
 - 3.1. Press the CLR BUTTON (CU42E0) to detect the readers and the connected CU4200. Check that the reader's LEDs blink and the BUS485 LEDs are switched ON.
 - 3.2. The CU42E0 is a DHCP ready device. If there's no DHCP server, the user can manually set up a static IP address using a web browser.
 - 3.2.1. Press the CLR button for 5 seconds to access the addressing mode (LED ON will blink orange).
 - 3.2.2. Access the IP address 192.168.0.234 with your web browser. Set up the network parameters and click on "send".
 - 3.2.3. The CU42E0 will leave the addressing mode automatically, but you can also leave the addressing mode manually by pressing the CLR button for 5 seconds.
4. Use SALTO ProAccess software to detect the device (consult SALTO ProAccess Software user manual).

CU42E0 Configuration

SALTO inspiredaccess

CU42E0
Mac Number: 000A830293F1

Address configuration: ☒ Static ☐ Dynamic

Address: 192 . 168 . 110 . 055
Netmask: 255 . 255 . 255 . 000
Gateway: 192 . 168 . 110 . 001

Send

CU42E0 Configuration

SALTO inspiredaccess

CU42E0
Mac Number: 000A830293F1

Address configuration: ☐ Static ☒ Dynamic

Mac Number: 000A830293F1
Network Name: SALTO-CU4K-0293F1

Send

CU42E0 Configuration

SALTO inspiredaccess

Configuration successfully sent.

Installation guide

XS4 Controller

E Configuración:

1. Hacer todas las conexiones físicas de la red (incluido el cable Ethernet), configurando el dip-switch de cada CU4200. Crear una alarma de tamper. Para ello, abrir la caja o desconectar cable nulo de la entrada tamper y pulsar brevemente el botón de CLR para detectar los lectores conectados. Comprobar que los LEDs de los lectores están encendidos (READER 1, READER 2).
2. Crear configuración de la red en el Software (consultar el manual de usuario de usuario de SALTO ProAccess SPACE).
3. Direccional la CU42E0:
 - 3.1. Pulsación corta del CLR (en la CU42E0) para detectar los lectores y CU4200 conectados. Comprobar que los LEDs de los lectores y el BUS485 están encendidos.
 - 3.2. La CU42E0 es un dispositivo DHCP ready. Pero el usuario (si no hay servidor DHCP en su instalación) puede configurar manualmente una IP estática usando un navegador de Internet.
 - 3.2.1. Pulsar durante 5 segundos el botón de CLR para entrar en el modo addressing (LED ON parpadeando en naranja).
 - 3.2.2. Acceder a la dirección IP 192.168.0.234 con un explorador estándar. Configurar los parámetros de red y pulsar el botón 'send' en cualquier momento (sin guardar los cambios) pulsando el botón de CLR durante 5 segundos.
4. Usar el Software de SALTO para detectar el dispositivo consultar el manual de usuario de SALTO ProAccess Software).

CU42E0 Configuration

SALTO inspiredaccess

CU42E0
Mac Number: 000A830293F1

Address configuration: ☐ Static ☐ Dynamic

Address: 192 . 168 . 110 . 055
Netmask: 255 . 255 . 255 . 000
Gateway: 192 . 168 . 110 . 001

Send

CU42E0 Configuration

SALTO inspiredaccess

CU42E0
Mac Number: 000A830293F1

Address configuration: ☐ Static ☒ Dynamic

Mac Number: 000A830293F1
Network Name: SALTO-CU4K-0293F1

Send

CU42E0 Configuration

SALTO inspiredaccess

CU42E0
Mac Number: 000A830293F1

Address configuration: ☐ Static ☒ Dynamic

Mac Number: 000A830293F1
Network Name: SALTO-CU4K-0293F1

Send

Configuration successfully sent.

Installation guide

XS4 Controller

⑥ Configuration:

1. Préparez toutes les connexions réseau (câble ethernet compris), paramétrez les micro-interrupteurs de chaque CU4200. Générez une alarme Tamper en ouvrant le boîtier de la CU ou en déconnectant le cavalier Tamper et appuyez sur le bouton CLR pour détecter tous les lecteurs connectés. Vérifiez que les LEDs des lecteurs sont allumées (READER 1 et READER 2).
2. Définir la configuration dans le logiciel (Consultez le mode d'emploi ProAccess SPACE SALTO). Configurer toutes les CU4200s en fonction des Dipswitchs et attribuer l'adresse IP à la CU42E0.
3. Adresser la CU42E0:
 - 3.1. Appuyer sur la touche CLR (CU42E0) pour détecter les lecteurs et les CU4200 connectées. Vérifier que les voyants des lecteurs clignotent et que les voyants du BUS485 sont allumés.
 - 3.2. Le CU42E0 est un appareil livré en DHCP. Si il n'y a pas de serveur DHCP, l'utilisateur peut configurer manuellement une adresse IP statique à l'aide d'un navigateur Web.
 - 3.2.1. Appuyer sur le bouton CLR pendant 5 seconds pour accéder au mode d'adressage (LED ON clignote en orange).
 - 3.2.2. Accéder à l'adresse IP 192.168.0.234 avec votre navigateur web. Mettre en place les paramètres réseau et cliquer sur 'send'.
 - 3.2.3. Le CU42E0 va quitter le mode d'adressage automatiquement, il est toutefois possible d'arrêter le mode d'adressage sans enregistrer la modification en appuyant sur la touche CLR 5 secondes.
4. Utiliser un logiciel ProAccess SALTO pour détecter les périphériques (consultez du logiciel ProAccess SALTO).

CU42E0 Configuration

SALTO inspiredaccess

CU42E0
Mac Number: 000A830293F1

Address configuration: ☐ Static ☐ Dynamic

Address: 192 . 168 . 110 . 055
Netmask: 255 . 255 . 255 . 000
Gateway: 192 . 168 . 110 . 001

Send

CU42E0 Configuration

SALTO inspiredaccess

CU42E0
Mac Number: 000A830293F1

Address configuration: ☐ Static ☒ Dynamic

Mac Number: 000A830293F1
Network Name: SALTO-CU4K-0293F1

Send

CU42E0 Configuration

SALTO inspiredaccess

Configuration successfully sent.

Installation guide

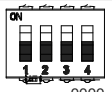
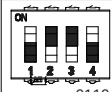
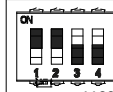
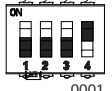
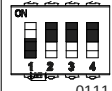
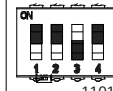
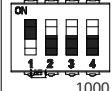
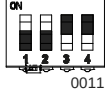
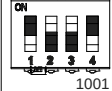
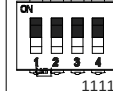
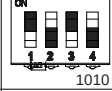
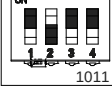
XS4 Controller

Eng Dipswitch set up:

When CU4200 is used offline, the dip-switch setting has to be OFF for all 4 switches (0000). When connected to an online CU42E0 by BUS485, the CU4200 dip-switch setting is used to give each device on the BUS485 a unique address. Ensure that the address in the software is the same as the one you put on the hardware. (See Table). Both ends of the BUS485 must have the RS485 BUS termination resistor in the ON position, intermediate CU4200s need to have the resistor in OFF position.

E Configuración del dip-switch:

Si la CU4200 está en modo offline, la configuración del dip-switch ha de estar en OFF con los 4 switches en off (0000). Cuando la CU4200 está conectada a una CU42E0 ONLINE por BUS485, el dip-switch de la CU4200 se usa para asignarle una dirección dentro del BUS485. Esta dirección ha de ser detallada en el software. Ver tabla adjunta. Ambos extremos del BUS485 han de tener la resistencia del terminal en posición ON, y el resto de CU4200s han de tener este resistor en posición OFF.

	ADDRESS		ADDRESS		ADDRESS
	Offline 0000		Address 6 0110		Address 12 1100
	Address 1 0001		Address 7 0111		Address 13 1101
	Address 2 0010		Address 8 1000		Address 14 1110
	Address 3 0011		Address 9 1001		Address 15 1111
	Address 4 0100		Address 10 1010		
	Address 5 0101		Address 11 1011		

F Configuration du Dipswitch:

Si la CU4200 est en mode déconnectée, les réglages du dipswitch doit être éteint avec le 4 switches en OFF (0000). Lorsque la CU4200 est connectée à une CU42E0 ONLINE par BUS485, le dipswitch de la CU4200 est utilisé pour attribuer une adresse dans le BUS485. Cette adresse doit être détaillé dans le logiciel. Voir tableau ci-joint. les deux extrémités de BUS485 doivent avoir les résistances de fin de ligne en position ON, et le reste des CU4200 doivent avoir cette résistance hors tension.

Eng Set up example:

Same configuration at SALTOS ProAccess SPACE Software

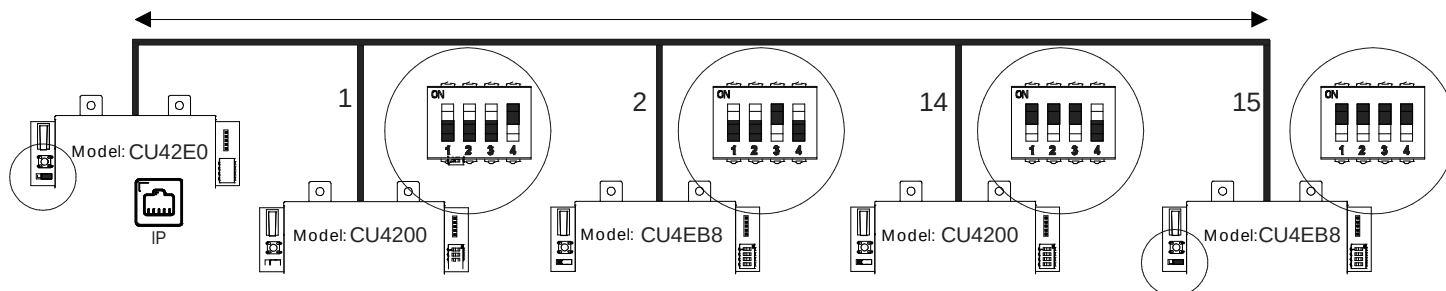
E Ejemplo de configuración:

Misma configuración que en el Software ProAccess SPACE de SALTO

F Exemple de configuration:

Même configuration que le logiciel SALTO ProAccess SPACE

Max 300m - UTP CAT5e



(The interconnection has not been evaluated by UL, the model CU4EB8 has not been evaluated by UL)

Eng **Maximum number of devices on BUS485: 16 units, with a maximum of 4 units CU4200 and 15 units CU4EB8.**

E **Número máximo de dispositivos en BUS485: 16 unidades, con un máximo de 4 unidades CU4200 y 15 unidades CU4EB8.**

F **Nombre maximum d'appareils sur un BUS485: 16 unités, avec un maximum de 4 unités CU4200 et 15 unités CU4EB8.**

Installation guide

XS4 Controller

Eng Signaling:

The LEDs in the top layer of the CU show the state of the system:

LED name	Description
ON	GREEN ON: the unit is powered correctly
	BLINKING RED: the unit is not powered properly (check power supply)
	BLINKING ORANGE: addressing mode
	OFF: not powered
BUS485	ON CU4200: The unit is communicating with the CU42E0
	ON CU42E0: To be defined
	OFF CU4200: The unit is not communicating with the CU42E0 (press the CLR to start detection process)
TAMPER	OFF CU42E0: To be defined
	ON: tamper alarm active
IN1-IN6	OFF: tamper alarm not active
	ON: active input (depends on the input type configured in the software)
READER	OFF: inactive input (depends on the input type configured in the software)
	ON: the reader is communicating with the CU
RL1-RL4	OFF: the reader is not communicating with the CU (press the CLR to start detection process)
	ON: the relay is activated (NO is connected with C).
	OFF: the relay is inactive (NC is connected with C).

E Señalética:

Los LEDs en la parte superior de la CU muestran el estado del sistema:

Nombre del LED	Descripción
ON	VERDE ON: el dispositivo está correctamente alimentado
	ROJO INTERMITENTE: el dispositivo no está correctamente alimentado (comprobar la fuente de alimentación)
	NARANJA INTERMITENTE: modo direccionamiento
	OFF: sin alimentación
BUS485	ON CU4200: El dispositivo se comunica con la CU42E0
	ON CU42E0: Por definir.
	OFF CU4200: el dispositivo no se comunica con la CU42E0 (presione el botón CLR para iniciar la detección)
TAMPER	OFF CU42E0: Por definir.
	ON: alarma tamper activada
IN1-IN6	OFF: alarma tamper desactivada
	ON: input activado (depende del tipo de input configurado a través del software)
READER	OFF: input desactivado (depende del tipo de input configurado a través del software)
	ON: el lector comunica con la CU
RL1-RL4	OFF: el lector no comunica con la CU (presione el botón CLR para iniciar la detección)
	ON: relé activado (NO está conectado con C).
	OFF: relé desactivado (NC está conectado con C).

F Signalisation:

Les LEDS en façade avant de la CU indique l'état du système

Nom LED	Description
ON	VERT : l'appareil est correctement alimenté
	Rouge clignotant : l'appareil est mal alimenté (vérifier la tension d'alimentation)
	Orange clignotant : en mode adressage
	OFF: non alimenté
BUS485	ON CU4200 : L'unité communique correctement avec la CU42E0
	ON CU42E0 : À définir.
	OFF CU4200 : L'unité ne communique pas avec la CU42E0 (appuyez sur le CLR pour lancer le processus de détection)
TAMPER	OFF CU42E0 : À définir.
	ON : alarme active
IN1-IN6	OFF : alarme désactivé
	ON : entrée active (dépend du type d'entrée configuré dans le logiciel)
READER	OFF : entrée inactive (dépend du type d'entrée configuré dans le logiciel)
	ON : le lecteur est en communication avec la CU
RL1-RL4	OFF : le lecteur ne communique pas avec la CU (appuyez sur le CLR pour lancer le processus de détection)
	ON : le relais est actif (NO est connecté avec C)
	OFF : le relais est inactif (NC est relié à C)

UL Statements

UL listed models are CU42E0G00, CU42E0T00, CU4200G00 and CU4200T00. Models CU42E0, CU4200, CU42E0G, CU42E0T, CU4200G, CU4200T and CU4EB8 are not UL listed.

The unit shall be supplied by UL294 and S319 listed external power supply with built-in secondary battery, whose output is Class 2, and rating is 12 VDC, minimum 2 A.

Field wiring leads must be UL listed but the AWG should not be smaller than AWG26 and no bigger than AWG18.

Maximum length of the cable for the readers is 400 m with AWG18 cable.

The interconnection between CU4200 and CU42E0, and between CU42E0 and PC are not UL evaluated.

The LAN connect cable shall locate in the same room, and is not permitted to be greater than 98.5 ft (30 m) long.

Comply with ULC-S319 Class I.

UL294 Performance level:

Feature	Level
Destructive Attack	I
Line Security	I
Endurance	IV
Standby Power	Per rating of external listed P.S.

EN 50131-3:2009 & EN 60839-11-1:2013 Statements

Certification issued by ALTER TECHNOLOGY TÜV NORD S.A.U. for the models: CU42E0T00, CU42E0G00, CU4200T00 and CU4200G00. Stationary ACE, Type B.

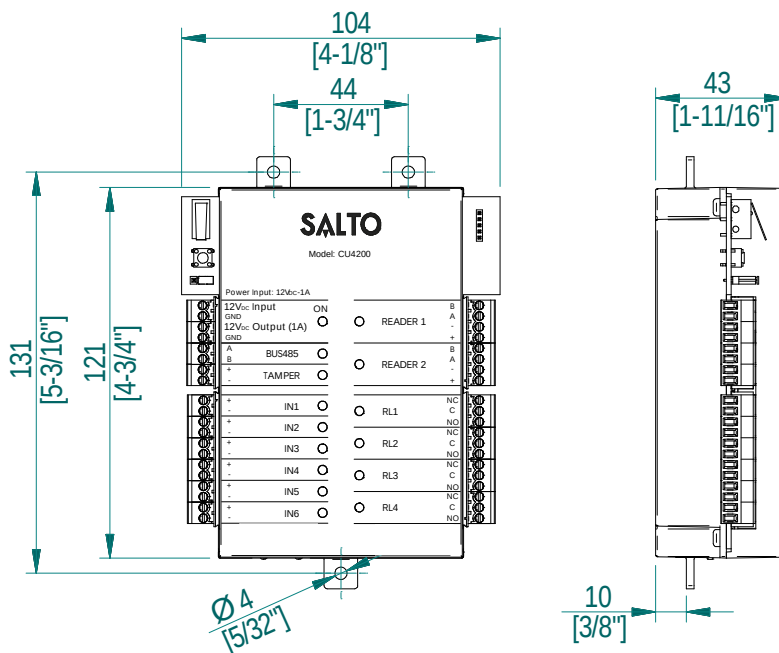
Performance level:

- Security Grade 2 (EN 50131-3:2009), Class II
- Grade 2 (EN60839-11-1:2013), Class II
- IK04
- 2²⁴ variations of supported credentials
- CU42E0 contains 3x EEPROM (512Kbits)/ CU4200 contains 2x EEPROM (512Kbits)
- The unit shall be supplied by a EN 50131-6:2017 certified external power supply or by the power output of another SALTO Control Unit.

Installation guide

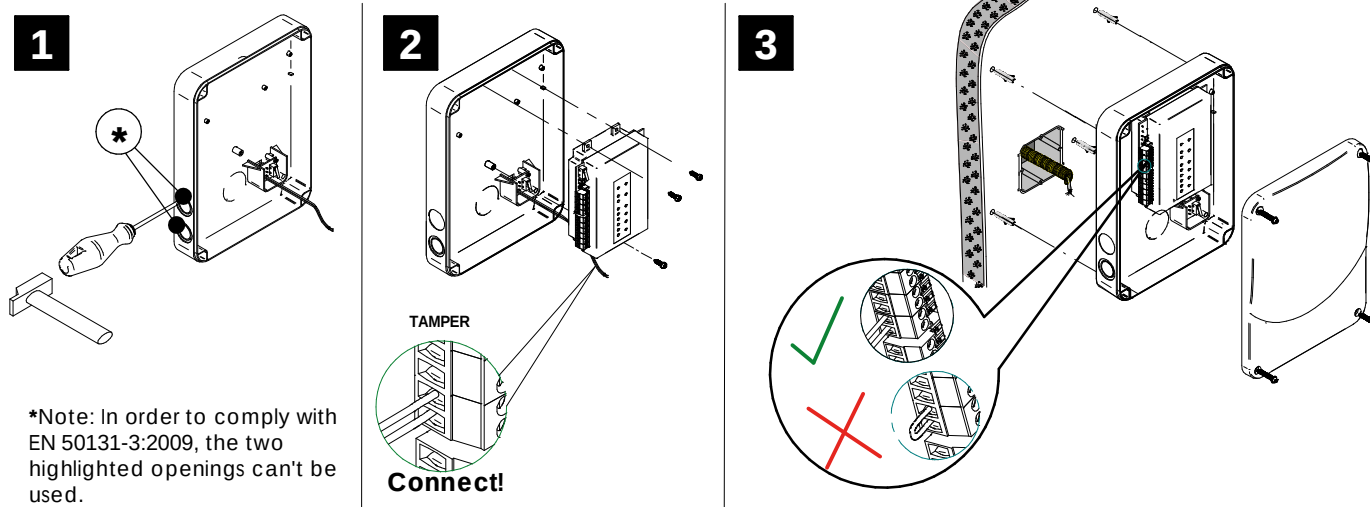
XS4 Controller

- (D) Installationsanleitung
 (NL) Installatiehandleiding
 (SVE) Installationsguide



(D) Mechanische installation (NL) Mechanische installatie (SVE) Mekanisk installation

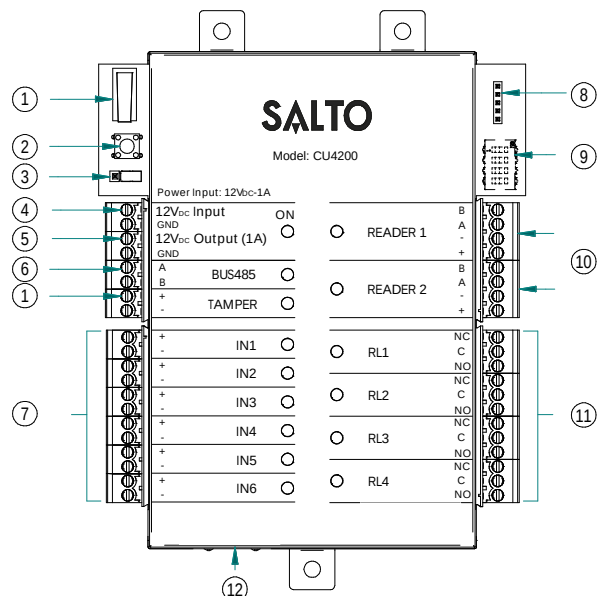
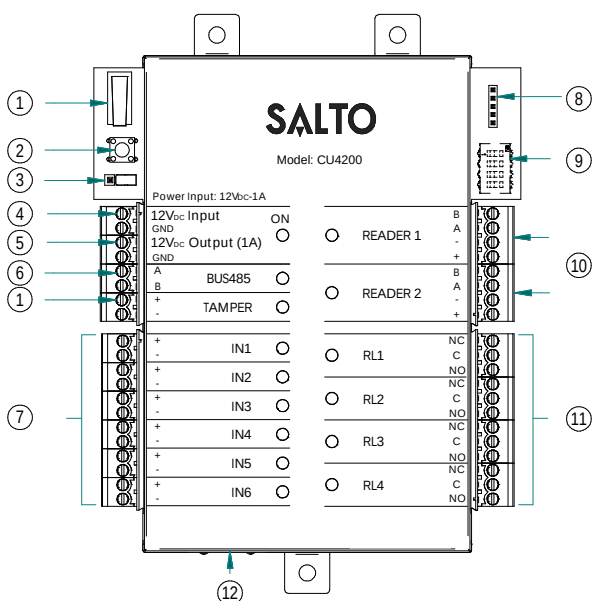
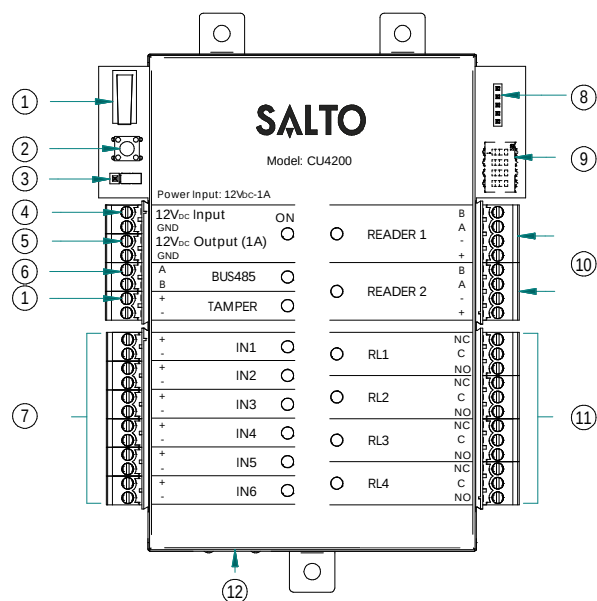
CU42E0T - CU42E0G - CU4200T - CU4200G
 CU42E0T00 - CU42E0G00 - CU4200T00 - CU4200G00



Note: Follow the same connection model, using the CU tamper input, when using a third party electric box equipped with a tamper opening detection.

Installation guide

XS4 Controller



- ① **Sabotageschalter** ist parallel mit dem Sabotage Eingang (Tamper)
- ② Der "CLR" Taster muss einmal weniger als 5 Sekunden gedrückt werden, wenn die Konfiguration verändert wurde (z.B. Leser zugefügt, Netzwerk angeschlossen, Buskomponenten angeschlossen). Vor dem Drücken muss der Sabotagekontakt "Tamper" ausgelöst sein, hierzu einfach die Kabel- brücke abziehen.
- ③ **485 Bus Abschluss Widerstände** notwendig (ON Position) wenn die CU am Anfang oder Ende des Buses sitzt.
- ④ **Spannungseingang**
- ⑤ **Spannungsausgang:** Dieser Spannungsausgang ist direkt mit dem Spannungseingang verbunden, jedoch durch eine 1A Sicherung abgesichert.
- ⑥ **BUS485**
- ⑦ **Eingänge:** Bei der Installation müssen je nach Konfiguration eventuell Eingänge gebrückt werden. Der Steuerung liegen hierzu 3 Kabelbrücken für diesen Zweck bei
- ⑧ **PPD Verbindung**
- ⑨ **Adresskonfiguration (Nur CU4200)** Alle CU4200 im selben Bus, müssen unterschiedliche Adressen haben
- ⑩ **Verbindung für Leser:** Für Anschluß und Entfernungen, bitte die Montag-eanleitung des Lesers beachten.
- ⑪ **Ausgangsrelais:** Bitte beachten Sie die maximale Schaltleistung von 2A-30VDC. Nutzen Sie die beiliegenden Varistoren, für Induktive Verbraucher (24v AC/DC max.)
- ⑫ **Netzwerkverbindung (Nur CU42E0).**

- ① **Sabotage schakelaar** is parallel verbonden met Sabotage ingang.
- ② **Clear button** moet ingedrukt worden (minder dan 5 sec) als configuratie is veranderd. Bijv. Lezer toegevoegd, Ethernet verbonden of een apparaat is toegevoegd aan BUS485, enz. De sabotagemelding (tamper) moet aanstaan om de configuratie te kunnen voltooien.
- ③ **RS485 Bus eindweerstand** is nodig (ON positie) wanneer de CU aan het einde van de bus ligt.
- ④ **Voeding ingang**
- ⑤ **Voeding uitgang:** Deze output is direct verbonden met de power input poort beschermd door een 1A zekering.
- ⑥ **BUS485**
- ⑦ **Ingangen:** Installateur moet vaststellen welke kabel nodig is, afhankelijk van de input configuratie. Indien geen deursensoren of sabotagecontact gebruikt wordt, sluit de meegeleverde 3 kabelbruggen aan op deze ingangen.
- ⑧ **PPD Connectie**
- ⑨ **Adres configuratie (Alleen CU4200)** Alle CU4200 adressen verbonden met de RS485Bus moeten van elkaar verschillen.
- ⑩ **Lezer aansluitingen:** Zie de installatie handleiding van de (wand)lezer voor de aanbevolen kabel, verbindingen en maximale afstanden.
- ⑪ **Relais aansluitingen:** Houd alstublieft rekening met de maximale belasting (2A-30VDC). Gebruik de meegeleverde varistors als er een inductieve lading wordt gebruikt (24vC/DC max.)
- ⑫ **Ethernet aansluiting (alleen bij de CU42E0)**

- ① **Sabotage-kontakt** är ansluten parallellt med sabotageingång.
- ② **Resetknappen** måste tryckas ner (inte mer än 5 sekunder) om hårdvarukonfigurationen har ändrats (t.ex. en läsare är inkopplad, nätverkssladd har anslutits, osv.) samt så måste tamper-larmet aktiveras genom att koppla ur tamper-bygeln/kontakten.
- ③ **RS485 Buss-terminering krävs** (position ON) om detta är den sista enheten i slingan.
- ④ **Power Input**
- ⑤ **Ström utgång:** Denna utgång är direkt kopplad till strömingången,
- ⑥ **BUS485**
- ⑦ **Ingångar:** Installatören måste identifiera vilka kablar som behövs, beroende på konfigurationen. Tre kablar medföljer vid leverans för detta ändamål.
- ⑧ **PPD Anslutning**
- ⑨ **Adress-konfigurering (endast CU4200):** Alla CU4200 anslutna via BUS485 måste ha olika adresser.
- ⑩ **Anslutning till läsare:** Se väggläsarens manual för rekommendation kring kabeltyp, anslutning och avstånd.
- ⑪ **Reläanslutningar:** V.g. notera max. belastningen (2A-30VDC). Använd medföljande Varistor vid behov. (24v AC/DC max.)
- ⑫ **Nätverksanslutning (endast CU42E0)**

Installation guide

XS4 Controller

(D)

Werkskonfiguration		
IN1	Türkontakt Tür 1	unüberwachter NC
IN2	Türöffnungstaster Tür 1	unüberwachter NO
IN3	Türkontakt Tür 2	unüberwachter NC
IN4	Türöffnungstaster Tür 2	unüberwachter NO
IN5	Eingang für Office-Mode Tür 1	unüberwachter NO
IN6	Eingang für Office-Mode Tür 2	unüberwachter NO
RL1	Ausgangsrelais Tür 1	
RL2	Sabotagealarm, Tür zu lange offen und Einbruch Tür 1	
RL3	Ausgangsrelais Tür 2	
RL4	Sabotagealarm, Tür zu lange offen und Einbruch Tür 2	

(NL)

Fabrieksinstellingen		
IN1	Deurstatus voor DEUR1	onbewaakt NC
IN2	Req EXIT input voor DEUR1	onbewaakt NO
IN3	Deurstatus voor DEUR2	onbewaakt NC
IN4	Req EXIT input voor DEUR2	onbewaakt NO
IN5	Loopstand voor DEUR1	onbewaakt NO
IN6	Loopstand voor DEUR2	onbewaakt NO
RL1	Uitgangrelais voor DEUR1	
RL2	Sabotage alarm, Deur open laten staan, inbraak Deur1	
RL3	Uitgangrelais voor DEUR2	
RL4	Sabotage alarm, Deur open laten staan, inbraak Deur2	

(SVE)

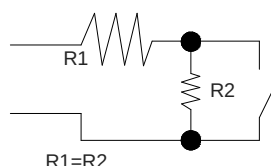
Fabriksinställning		
IN1	DÖRRLÄGE för DOOR1	Ej övervakad NC
IN2	Öppningsknapp för DOOR1	Ej övervakad NO
IN3	DÖRRLÄGE för DOOR2	Ej övervakad NC
IN4	Öppningsknapp för DOOR2	Ej övervakad NO
IN5	KONTORSLÄGE för DOOR1	Ej övervakad NO
IN6	KONTORSLÄGE för DOOR2	Ej övervakad NO
RL1	Låsrelä för DOOR1	
RL2	Sabotagealarm, Dörr lämnad öppen, Inträngsalarms DÖRR 1	
RL3	Låsrelä för DOOR2	
RL4	Sabotagealarm, Dörr lämnad öppen, Inträngsalarms DÖRR 2	

(D) EINGANG Konfiguration

CUADAP oder Fremdleser

	Wiegand	Omron	RS232
IN3	D0 Ausgang	Clock Ausgang	
IN4	D1 Ausgang	Data Ausgang	TX Ausgang
IN5	D0 Ausgang	Clock Ausgang	
IN6	D1 Ausgang	Data Ausgang	TX Ausgang

Überwacher Eingang



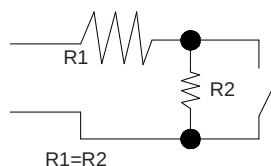
Die Widerstandswerte können via Software definiert werden: 1k5, 2k2, 3k3, 4k7, 6k8, 10k

(NL) Ingangen

CUADAP en lezers van derden

	Wiegand	Omron	RS232
IN3	D0 uitgang	Clock uitgang	
IN4	D1 uitgang	Data uitgang	TX uitgang
IN5	D0 uitgang	Clock uitgang	
IN6	D1 uitgang	Data uitgang	TX uitgang

Ingangen onder toezicht



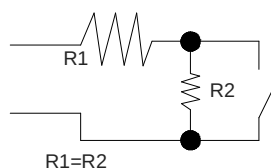
De weerstandswaarden R1 en R2 zijn in te stellen in de software: 1k (aanbevolen), 1k5, 2k2, 3k3, 4k7, 6k8 of 10k

(SVE) Ingång

CUADAP eller 3e partsläsare

	Wiegand	Omron	RS232
IN3	D0 utgång	Clock utgång	
IN4	D1 utgång	Data utgång	TX utgång
IN5	D0 utgång	Clock utgång	
IN6	D1 utgång	Data utgång	TX utgång

Övervakad ingång

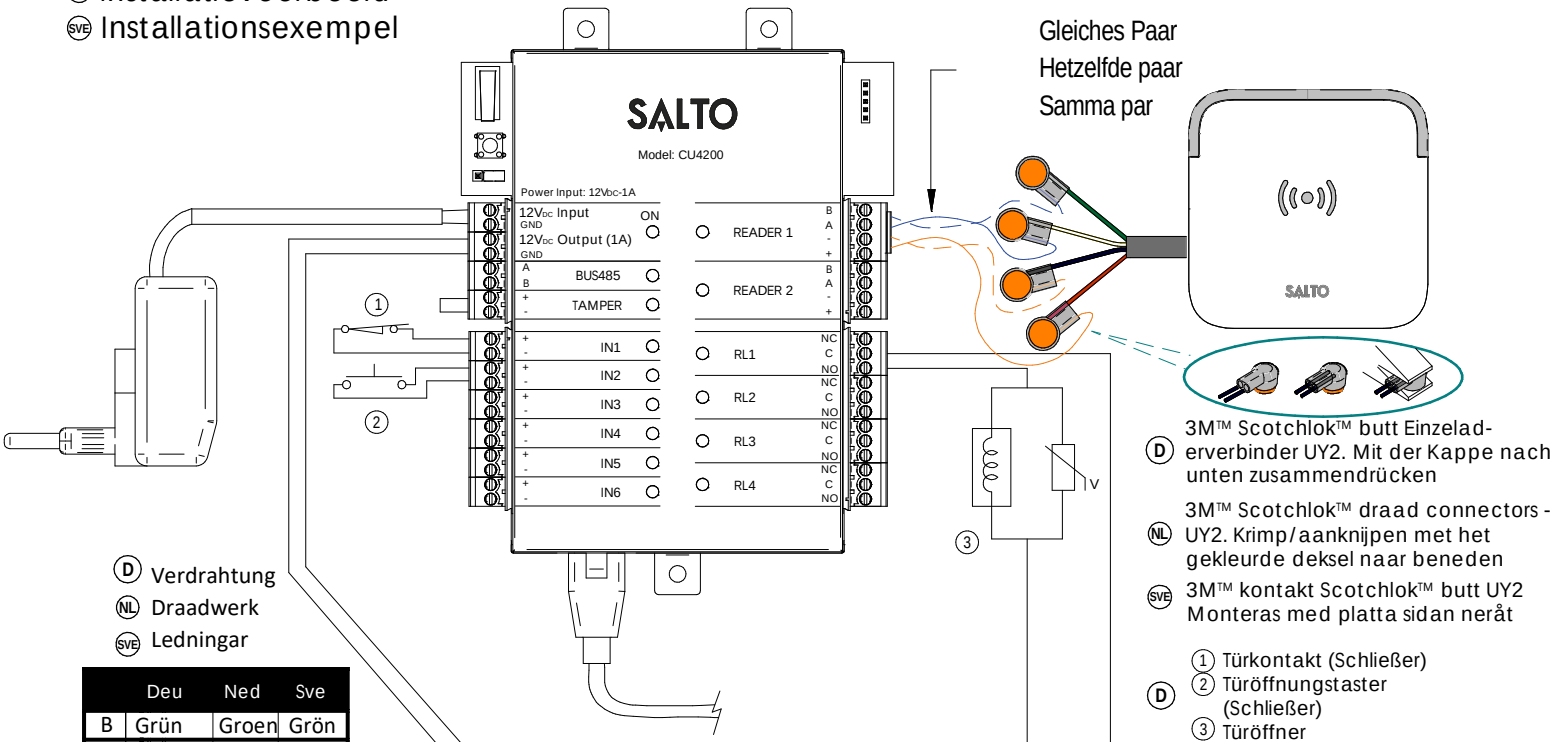


Motståndsvärdet R1 och R2 anges i mjukevaran: 1k (rekommenderas), 1k5, 2k2, 3k3, 4k7 6k8, 10k

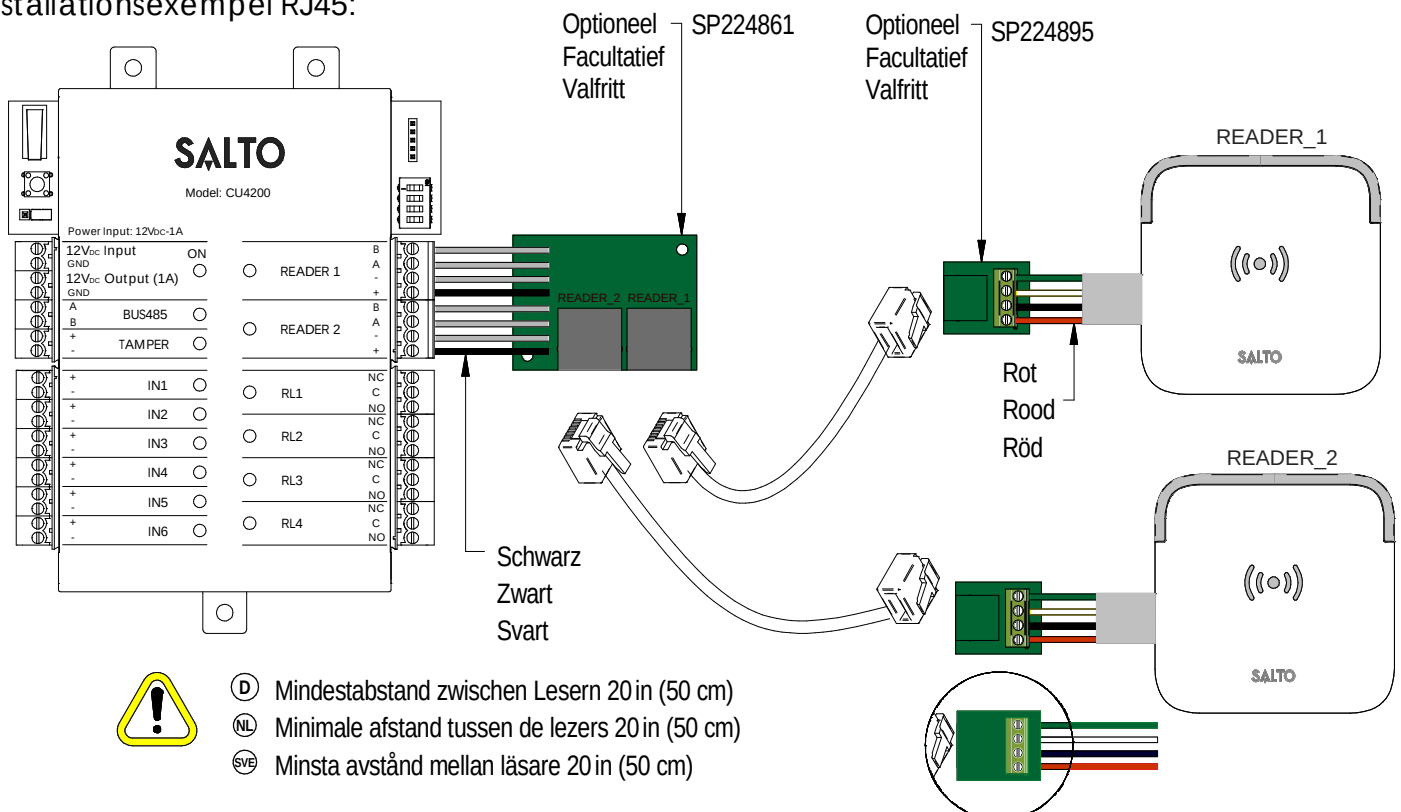
Installation guide

XS4 Controller

- (D) Installationsbeispiel
 (NL) Installatievoorbeeld
 (SVE) Installationsexempel



- (D) Installationsbeispiel RJ45:
 (NL) Installatie voorbeeld RJ45:
 (SVE) Installationsexempel RJ45:



Installation guide

XS4 Controller

④ Elektronische Charakteristik:

Umgebungsbedingungen

	Min	Typ	Max	Einheit
Temperatur	0	25	60	°C
Feuchtigkeit	35		85	

Spannung

	Min	Nom.	Max	Einheit
Eingangsspannung		12		V
Stromverbrauch			2	Note1 A
Steuerung				
Max. Belastung			1	A
Spannungsausgang				Note2

Eingänge

Max. Spannung	5V Note3
Konfiguration	Via Software Note4

Verkabelung

Ethernet	Note5 UTP CAT5e
Erweiterungs Bus	Twisted pair
Inputs	AWG24
Leser	AWG18

Ausgangsrelais

Zulässige Belastung	2A-30Vdc
---------------------	----------

Note 1: Diese Angabe ist bei 2 angeschlossenen Wandlesern und Verwendung des 12V Ausganges. Die Steuerung alleine verbraucht 400mA. Abhängig von den angeschlossenen Komponenten muss der Installateur ein entsprechendes Netzteil berechnen und planen.

Note 2: Gleiche Spannung wie Eingang

Note 3: 1K Pull-Up-Widerstand

Note 4: Bitte im Softwarehandbuch nachschlagen

Note 5: Wenn Netzwerk verfügbar ist

④ Technische gegevens:

Omgeving

	Min	Typ	Max	Eenheid
Temperatuur	0	25	60	°C
Vochtigheid	35		85	

Vermogen

	Min	Nom.	Max	Eenheid
Input Voltage		12		V
Stroomverbruik			2	opm1 A
Stroom uitgaand			1	opm2 A

Input

Electra eigenschappen	5V opm3
Configuratie	Via Software opm4

Kabel aanbeveling

Ethernet	opm5 UTP CAT5e
Uitbreidingsbus	Twisted pair
Inputs	AWG24
Wandlezers	AWG18

Relaisuitgangen

Ratedload (resistive)	2A-30Vdc
-----------------------	----------

Opm 1: Dit verbruik is wanneer er 2 wandlezers aangesloten zijn op een CU en gebruik wordt gemaakt van de 12 V-uitgang. De controller alleen verbruikt 400mA. Afhankelijk van de aangesloten componenten, moet de installateur een geschikte voeding berekenen en plaatsen.

Opm 2: Evenveel vermogen als ingevoerd door voeding.

Opm 3: 1K pull-up weerstand.

Opm 4: Zie de Software gebruikershandleiding

Opm 5: Wanneer Ethernet beschikbaar is

④ Tekniska data:

Arbetsområde

	Min	Typ	Max	Enhet
Temperatur	0	25	60	°C
Fukt	35		85	

Ström

	Min	Nom.	Max	Enhet
Spänning in		12		V
Strömförbrukning			2	Not 1 A
Spänning ut			1	A

Drift

Spänning	5V Not 3
Konfiguration	Via Mjukvara Not 4

Kabel rekommendation

Nätverk	Not 5
Expansionsbuss	
Ingångar	
Läsare	

Reläutgångar

Märkström (resistiv)	2A-30Vdc
----------------------	----------

Not. 1: Detta är strömförbrukningen för Kontrollboxen med 2 aktiva läsare samt den externa utgången aktiv. Kontrollboxen själv drar 400mA. Beroende på vad som ingår i installationen måste installatören beräkna hur mycket strömförsörjningen måste kunna leverera.

Not. 2: Samma voltal som kopplas in i kontrollenheten

Not. 3: 1K PU motstånd.

Not. 4: Se mjukvarumaterial

Not. 5: När nätverk skall användas

Installation guide

XS4 Controller

④ Konfiguration:

1. Bereiten Sie alle Netzwerkverbindungen vor (inkl. Patchkabel) und stellen alle DIP Schalter der CU4200 korrekt ein. Lösen Sie den Sabotage (Tamper) Alarm aus, so dass die LED rot leuchtet. Drücken Sie die CLR Taste einmal um alle angeschlossenen BUS Komponenten und Leser einzulernen. Prüfen Sie ob die LED's für Leser 1 und 2 leuchten.
2. Programmieren Sie alle Komponenten in der Software ProAccess SPACE, hierzu können Sie das Handbuch der Software zu rate ziehen.
3. Adressierung CU42E0:
 - 3.1. Drücken Sie den "CLR" Taster einmal kurz, wenn der Sabotagekontakt offen ist. Die LED's müssen einmal kurz aufleuchten.
 - 3.2. CU42E0 ist DHCP Vorbereitet. In Werksauslieferung ist der DHCP Modus aktiviert. Wenn der Kunde keinen DHCP Server verwendet, dann muss eine manuelle IP-Adresse konfiguriert werden.
 - 3.2.1. Drücken Sie den "CLR" Button so lange, bis die Steuerung im Adressiermodus ist (ON LED blinkt orange). Wichtig vor dem Drücken des "CLR" Tasters muss der Sabotagekontakt offen sein.
 - 3.2.2. Greifen Sie per Web-Browser auf die Standard IP-Adresse 192.168.0.234 der Steuerung zu. Konfigurieren Sie in dem Menu die notwendigen Parameter für das Netzwerk des Kunden. Ein Klick auf den Button "Send" speichert die Konfiguration.
 - 3.2.3. Die CU42E0 verlässt den Programmiermodus automatisch, Sie können ihn manuell abbrechen, wenn Sie die "CLR"-Taste länger als 5 Sekunden gedrückt halten.
- 4.- Prüfen Sie in der ProAccess SPACE Software ob alle Komponenten korrekt erkannt wurden. Hierzu bei Bedarf das Handbuch zu rate ziehen.

CU42E0 Configuration

SALTO inspiredaccess

CU42E0
Mac Number: 000A830293F1

Address configuration: ☒ Static ☐ Dynamic

Address: 192 . 168 . 110 . 055
Netmask: 255 . 255 . 255 . 000
Gateway: 192 . 168 . 110 . 001

Send

CU42E0 Configuration

SALTO inspiredaccess

CU42E0
Mac Number: 000A830293F1

Address configuration: ☐ Static ☒ Dynamic

Mac Number: 000A830293F1
Network Name: SALTO-CU4K-0293F1

Send

CU42E0 Configuration

SALTO inspiredaccess

CU42E0
Mac Number: 000A830293F1

Address configuration: ☐ Static ☒ Dynamic

Mac Number: 000A830293F1
Network Name: SALTO-CU4K-0293F1

Send

Configuration successfully sent.

Installation guide

XS4 Controller

Configuratie:

1. Bereid alle netwerkverbindingen voor (inclusief ethernet-kabel) en stel de dip-switch in van elke CU4200. Genereer een sabotage-alarm d.m.v. het openen van of het verwijderen van de sabotageschakelaar kabel en druk op de CLR toets om alle nieuwe aangesloten lezers te detecteren. Controleer of de LED bij lezers op 'ON' staan (READER1, Reader2).
2. Creëer de CU4200 reeks in de software (raadpleeg hierbij de SALTO ProAccess SPACE gebruikershandleiding. Configureer alle CU4200 met de juiste DIP-Switch instellingen en ken het IP adres toe aan de CU42E0 in de software.
3. Adresseer de CU42E0:
 - 3.1. Klik de CLR knop kort in om de aangesloten lezers te detecteren, controleer of de oranje led op de lezers geknipperd hebben en dat de LED van de 485BUS aanstaat.
 - 3.2. CU42E0 is voorbereid op DHCP. Wanneer er geen DHCP server in het lokale ethernet netwerk is kan de gebruiker handmatig een vast IP adres configureren door verschillende parameters te veranderen d.m.v. een webbrowser.
 - 3.2.1. CLR knop 5 seconden indrukken, CU42E0 gaat in adresseringmodus (LED gaat oranje knipperen).
 - 3.2.2. Ga naar 192.168.0.234 IP adres in een webbrowser. Configureer netwerk parameters zoals benodigd en klik op 'send'.
 - 3.2.3. De CU42E0 zal de adresseringmodus automatisch verlaten na opslaan. Het is ook mogelijk de adresseringmodus zonder opslaan de verlaten door nogmaals 5 seconden op de CLR knop te drukken.
4. Gebruik de SALTO ProAccess SPACE Software om het apparaat op te zoeken (zie SALTO Software gebruikershandleiding).

CU42E0 Configuration P: X

← → ↻ 🏠 192.168.0.234

SALTO
inspiredaccess

CU42E0
Mac Number: 000A830293F1

Address configuration: ☐ Static ☐ Dynamic

Address:	192	.	168	.	110	.	055
Netmask:	255	.	255	.	255	.	000
Gateway:	192	.	168	.	110	.	001

Send

CU42E0 Configuration P: X

← → ↻ 🏠 192.168.0.234

SALTO
inspiredaccess

CU42E0
Mac Number: 000A830293F1

Address configuration: ☐ Static ☒ Dynamic

Mac Number:	000A830293F1
Network Name:	SALTO-CU4K-0293F1

Send

CU42E0 Configuration P: X

← → ↻ 🏠 192.168.0.234/?mode=0&staticos=1&dhcp=0&new=192&new=168&new=110&new=055&new=255&new=255&new=000&new=192&new=16

SALTO
inspiredaccess

Configuration successfully sent.

Installation guide

XS4 Controller

ⓈⓋⓔ Configuration:

1. Förbered alla kabelanslutningar (inkl. ethernet kabel) och sätt dip-switcharna i rätt läge på resp. CU4200.
Aktivera TAMPER-larmet genom att bryta TAMPER-ingången och tryck på CLR knappen en gång, då kommer all ansluten hårdvara att detekteras. Kontrollera att de inkopplade läsarnas LED är ON (READER1, READER2)
2. Konfigurera mjukvaran (se manualen för detaljer). Ställ in dip-switcharna för alla CU4200 och tilldela IP-adress till CU42E0.
3. Adressera CU42E0:
 - 3.1. Tryck på CLR-knappen (CU42E0) för att detektera läsarna och den anslutna CU4200. Kontrollera att läsarnas LED blinkar och BUS485 LED är ON.
 - 3.2. CU42E0 är en DHCP kompatibel enhet, om ingen DHCP server finns kan du manuellt sätta en statisk IP-adress med hjälp av en webbläsare.
 - 3.2.1. Tryck på CLR knappen i 5 sekunder för att komma till adresseringsläge, (ON LED börjar blinka orange).
 - 3.2.2. Surfa in på ipadress 192.168.0.234 med en webbläsare, konfigurera nätverket och tryck på Send.
 - 3.2.3. CU42E0 kommer lämna adresseringsläget automatiskt, men det är möjligt att avsluta adresseringen utan att spara genom att trycka på CLR-knappen i 5 sekunder.
4. Använd SALTO ProAccess mjukvaran för att detektera enheten (Se manualen för instruktioner).

CU42E0 Configuration P: X

← → ↻ 🏠 192.168.0.234

SALTO
inspiredaccess

CU42E0
Mac Number: 000A830293F1

Address configuration: ☒ Static ☐ Dynamic

Address: 192 . 168 . 110 . 055
Netmask: 255 . 255 . 255 . 000
Gateway: 192 . 168 . 110 . 001

Send

CU42E0 Configuration P: X

← → ↻ 🏠 192.168.0.234

SALTO
inspiredaccess

CU42E0
Mac Number: 000A830293F1

Address configuration: ☐ Static ☒ Dynamic

Mac Number: 000A830293F1
Network Name: SALTO-CU4K-0293F1

Send

CU42E0 Configuration P: X

← → ↻ 🏠 192.168.0.234/?mode=0&staticos=1&dhcp=0&new=192&new=168&new=110&new=055&new=255&new=255&new=000&new=192&new=16

SALTO
inspiredaccess

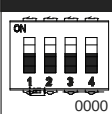
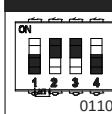
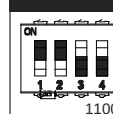
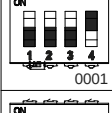
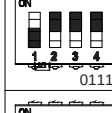
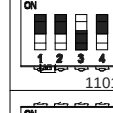
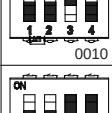
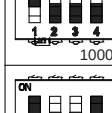
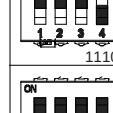
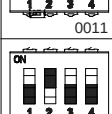
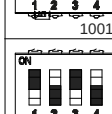
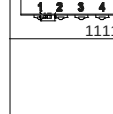
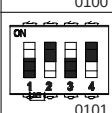
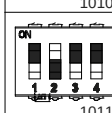
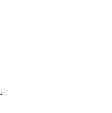
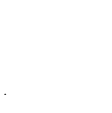
Configuration successfully sent.

Installation guide

XS4 Controller

D DIP-Schalter Einstellungen:

Wenn die CU4200 im Offline Modus verwendet wird, müssen alle DIP Schalter auf "OFF" stehen. Bei der Nutzung der CU4200 in Kombination mit einer CU42E0, muss jede CU4200 eine eindeutige ID haben. Die ID wird über die DIP-Schalter eingestellt und muss mit der Konfiguration in der Software übereinstimmen. Für die Auswahl der korrekten Adresseinstellungen bitte die Abbildung nebenan beachten. Bei der ersten und letzten Komponente im Bus muss jeweils der Abschlusswiderstand auf "ON" gesteckt werden.

	ADDRESS		ADDRESS		ADDRESS
	Offline		Address 6		Address 12
	Address 1		Address 7		Address 13
	Address 2		Address 8		Address 14
	Address 3		Address 9		Address 15
	Address 4		Address 10		
	Address 5		Address 11		

NL Dipswitch setup:

Indien de CU4200 offline gebruikt word, moeten de dipswitch instellingen voor alle 4 knopjes 'UIT' staan (0000). Wanneer deze verbonden is via een online CU42E0 d.m.v. een 485BUS, moet elke CU4200 een uniek adres d.m.v. dipswitch instelling hebben. Deze instelling moet gelijk zijn zoals in de software is aangegeven. Zie tabel hiernaast. Bij begin en eind van de 485BUS moeten de eindweerstand op de 'ON' positie staan. Een CU4200 of CU42E0 die tussen begin en eind van de bus zijn geplaatst, moet de eindweerstand op 'OFF' staan.

SVE Dipswitch set up:

När CU4200 används Offline måste alla 4 Dipswitcharna stå i läge OFF (0000). När du är ansluter CU4200 till en online CU42E0 med BUS485, används dipswitch inställningen i CU4200 för att ge varje enhet på BUS485 anslutningen en unik adress. Denna adress används i programvaran för att identifiera CUn i programvaran. (Se tabellen bredvid.) Båda ändarna av BUS485 anslutningen skall ha RS485 termineringen i läge ON, mellanliggande CU4200 skall ha termineringen i läge OFF.

D Konfigurationsbeispiel:

Gleichen Einstellungen in der Software SALTO Pro Access SPACE

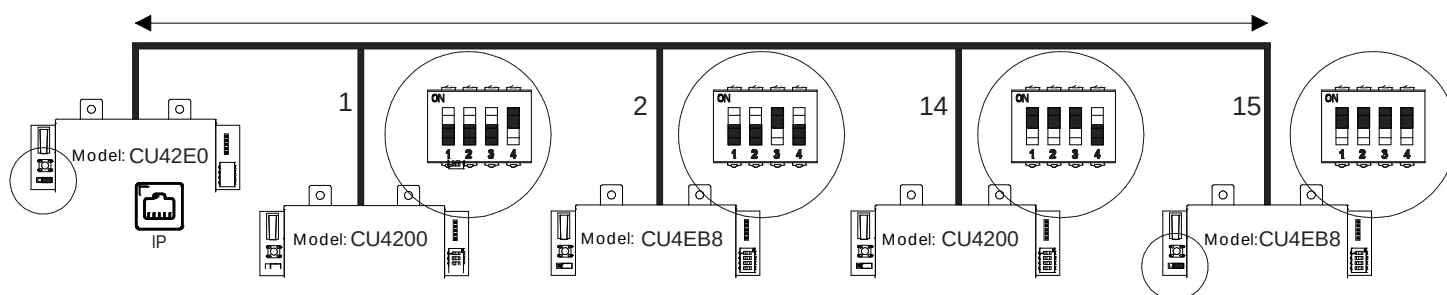
NL Configuratie voorbeeld:

Dezelfde instellingen in de Software SALTO Pro Access SPACE

SVE Konfiguration exempel:

Samma inställningar i programvaran SALTO Pro Tillgång SPACE

Max 300m - UTP CAT5e



D **Maximale Anzahl der Geräte auf dem BUS485: 16 Geräte, davon maximal 4 CU4200 und 15 CU4EB8.**

NL **Maximaal aantal apparaten op 485BUS: 16 eenheden in totaal, met een maximum van 4x CU4200 en 7 of 15x CU4EB8.**

SVE **Max antal enheter på BUS485 Är 16st totalt, varav max 4st CU4200 och 15st CU4EB8.**

Installation guide

XS4 Controller

④ Signale:

Die LED's auf der Steuerung zeigen den Zustand des Systems an:

LED name	Beschreibung
ON	GRÜN ON: Die Eingangsspannung ist ok und aktiv
	ROT BLINKEND: Das Netzteil ist nicht korrekt, bitte die Eingangsspannung kontrollieren
	ORANGE BLINKEND: Steuerung im Adressiermodus (IP 192.168.0.234 aktiv)
	AUS: Keine Spannung vorhanden.
BUS485	EIN CU4200: Die Einheit kommuniziert mit einer CU42E0
	EIN CU42E0: Definiert werden.
	AUS CU4200: Die Einheit kommuniziert nicht mit einer CU42E0 (Drücken Sie den CLR um den Erkennungsmodus zu starten)
TAMPER	AUS CU42E0: Definiert werden.
	EIN: Sabotagekontakt aktiv
IN1-IN6	AUS: Sabotagekontakt nicht aktiv
	EIN: Aktiviert (Hängt von Programmierung in der Software ab)
READER	AUS: Nicht aktiviert (Hängt von Programmierung in der Software ab)
	EIN: Ein Leser ist angeschlossen und kommuniziert mit der Steuerung
RL1-RL4	AUS: Der Leser kommuniziert nicht mit der Steuerung. (Wenn ein Leser angeschlossen ist, bitte den CLR Button einmal kurz drücken um die Erkennung zu starten)
	EIN: Das Relais ist aktiv (NO und C verbunden).
	AUS: Das Relais ist nicht aktiv (NC und C verbunden).

Ⓝ Signalering:

De LEDs op de bovenkant van de CU laat de status van het systeem zien:

LED-naam	Beschrijving
ON	GROEN AAN: De controller is juist gevoed
	KNIPPEREND ROOD: De controller is niet juist gevoed (controleer de voeding)
	KNIPPEREND ORANJE: adressering modus
	UIT: Geen voeding
BUS485	AAN op CU4200: De controller communiceert met de CU42E0
	AAN op CU42E0: Worden gedefinieerd
	UIT op CU4200: De controller communiceert niet met de CU42E0 (CLR indrukken om (zoek) proces te starten)
TAMPER	UIT op CU42E0: Worden gedefinieerd
	AAN: Sabotage alarm actief
IN1-IN6	UIT: Sabotage alarm niet actief
	AAN: actieve input (afhankelijk van type input dat in de software is geconfigureerd)
READER	UIT: inactieve input (afhankelijk van type input dat in de software is geconfigureerd)
	AAN: De lezer communiceert met de CU
RL1-RL4	UIT: De lezer communiceert niet met de CU (CLR indrukken om (zoek) proces te starten)
	AAN: Relais is geactiveerd (NO is verbonden met C).
	UIT: Relais is gedeactiveerd (NC is verbonden met C).

Ⓢ Signaler:

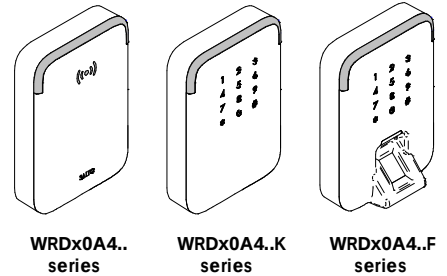
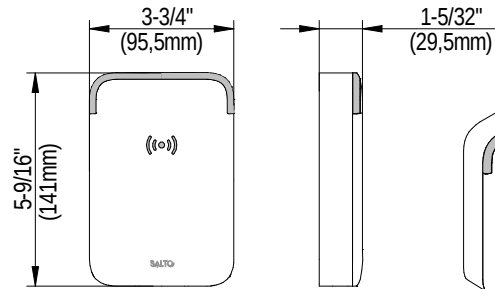
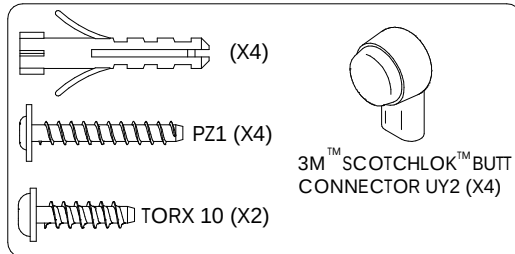
LED lamporna på kontrollboxen visar systemstatus enl. nedan:

LED namn	Förklaring
ON	GRÖN PÅ: Spänning till enheten är korrekt inkopplat
	BLINKANDE RÖTT: Spänning till enheten är inte korrekt inkopplat, v.g. kontrollera strömkällan.
	BLINKANDE ORANGE: adresseringsläge
	AV: Ingen spänning ansluten
BUS485	PÅ CU4200: Enheten kommunicerar med CU42E0
	PÅ CU42E0: Att definieras
	AV CU4200: Enheten kommunicerar inte med CU42E0 (tryck på CLR för att starta sökläge)
TAMPER	AV CU42E0: Att definieras
	PÅ: sabotage larm aktivt
IN1-IN6	AV: sabotage larm inaktivt
	PÅ: aktiv ingång (beror på konfigurationen i mjukvaran)
READER	AV: inaktiv ingång (beror på konfigurationen i mjukvaran)
	PÅ: Läsaren kommunicerar med kontrollenheten
RL1-RL4	AV: Läsaren kommunicerar inte med kontrollenheten (tryck på CLR för att starta sökläge)
	PÅ: Reläutgången är aktiv (NO är ansluten mot C).
	AV: Reläutgången är inaktiv (NC är ansluten mot C).

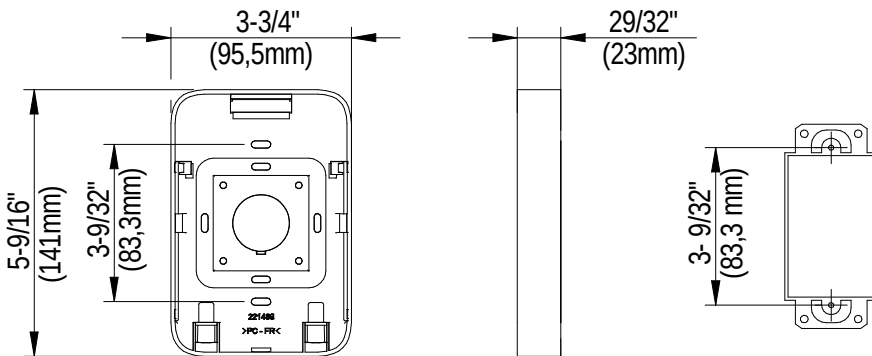
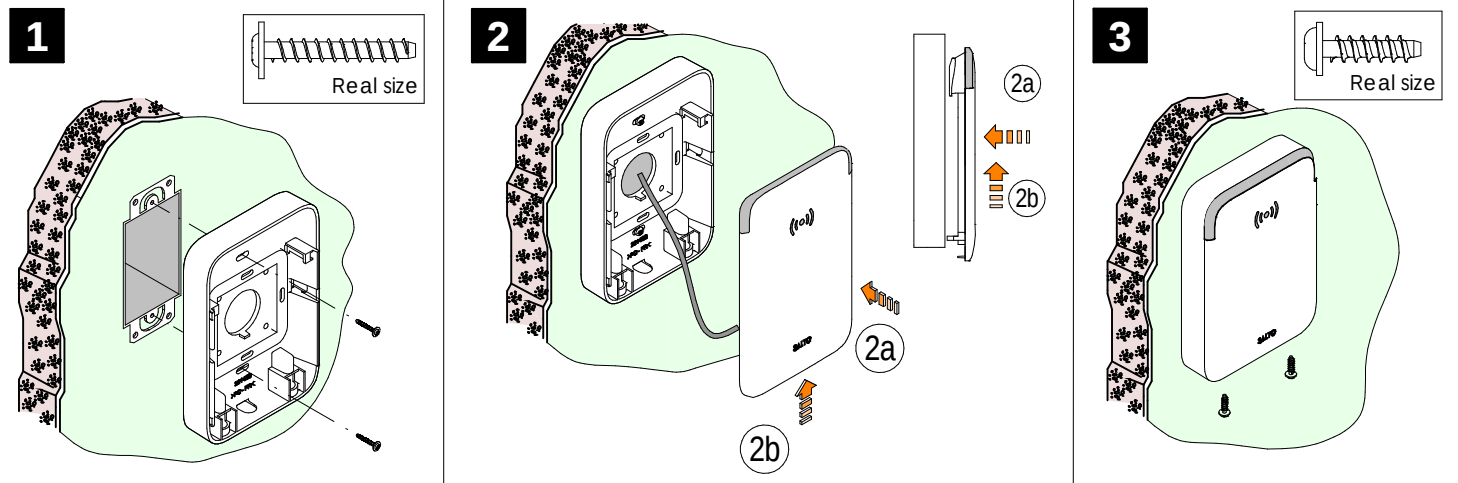
WRDx0A4.. series
WRDx0A4..K series
WRDx0A4..F series

Eng Card reader installation guide

- E** Guía de instalación lector de tarjetas
D Kartenleser installationsanleitung
F Guide d'installation lecteur de cartes
NL Kaartlezer Installatiehandleiding
SVE Kortläsare installationsguide



Eng Installation **E** Instalación **D** Installation **F** Installation **NL** Installatie **SVE** Installation



Eng GANG ELECTRICAL STANDARD BOX
E MÓDULO CAJA ELÉCTRICA ESTÁNDAR
D STANDARD SCHALTERDOSE
F PLOTS D'ENCASTREMENT STANDARD
NL STANDAARD ELEKTRISCHE INBOUWDOOS
SVE STANDARD APPARATLADA

Eng Maintenance **E** Mantenimiento **D** Instandhaltung **F** Entretien **NL** Onderhoud **SVE** Underhåll

Eng Dampen a lint-free cloth or cotton swap with alcohol. Gently rub the cloth back and forth across the sensor. Repeat the process once or twice as needed. Visually observe that no residual solution remains on the sensor, especially the edges.
Caution: Harsh and abrasive materials are not recommended for cleaning sensors.

E Humedezca un paño sin pelusa o un algodón con alcohol. Frótelo suavemente de un lado a otro del sensor. Repita el proceso una o dos veces según sea necesario. Comprobar que no queden residuos, especialmente en los bordes.
Precaución: No se recomiendan materiales ásperos y abrasivos para limpiar el sensor.

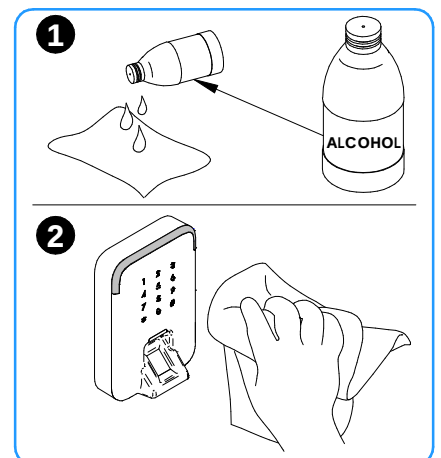
D Befeuchten Sie ein fusselfreies Tuch oder einen Wattestäbchen mit Alkohol. Reiben Sie das Tuch vorsichtig über den Sensor hin und her. Wiederholen Sie den Vorgang bei Bedarf ein- bis zweimal. Beobachten Sie optisch, dass keine Restlösung auf dem Sensor verbleibt, insbesondere in den Ecken.
Vorsicht: Harte und abrasive Materialien werden nicht zur Reinigung des Sensors empfohlen.

F Humidifiez un chiffon non pelucheux ou un coton-tige avec de l'alcool. Frottez doucement le chiffon d'avant en arrière sur le capteur. Répétez le processus une ou deux fois au besoin. Observez visuellement qu'aucune solution résiduelle ne reste sur le capteur, en particulier les bords.
Attention: Les matériaux durs et abrasifs ne sont pas recommandés pour le nettoyage des capteurs.

NL Bevochtig een pluivrije / katoendoek met alcohol. Wrijf de doek voorzichtig heen en weer over de sensor. Controleer visueel of er geen resterende vloeistof op de sensor achterblijft, vooral niet langs de randen van de sensor.
Waarschuwing: Harde en schurende materialen worden niet aanbevolen voor het reinigen van de sensoren.

SVE Fukta en luddfri trasa eller bomullsbyte med alkohol. Gnid försiktigt trasan fram och tillbaka över sensorn. Upprepa hela processen fler gånger efter behov, säkerställ att ingen restlösning finns kvar på sensorn, särskilt vid kanterna.
Varning: Hårt och slipande material rekommenderas inte för rengöringssensorer.

European view



Eng Electrical characteristics

Operation conditions

	Min.	Max.	Unit
Temperature WRDOB - WRDOS - WRDOBK	-35	+66	°C
Temperature WRDOJ - WRDOGK - WRDOJK	-25	+66	°C
Temperature WRDOBF - WRDOJF	-20	+66	°C
Humidity	35	85	%

RF characteristics

	Min	Cen.	Max	Unit
RFID frequency		13.56		Mhz
Bluetooth Smart frequency	2.4	2.445	2.4835	Ghz

E Características eléctricas

Condiciones ambientales

	Min.	Max.	Unidad
Temperatura WRDOB - WRDOS - WRDOBK	-35	+66	°C
Temperatura WRDOJ - WRDOGK - WRDOJK	-25	+66	°C
Temperatura WRDOBF - WRDOJF	-20	+66	°C
Humedad	35	85	%

Características RF

	Min	Cen.	Max	Unit
Frecuencia RFID		13.56		Mhz
Frecuencia Bluetooth Smart	2.4	2.445	2.4835	Ghz

D Elektronische Eigenschaften:

Umgebungsbedingungen

	Min.	Max.	Einheit
Temperatur WRDOB - WRDOS - WRDOBK	-35	+66	°C
Temperatur WRDOJ - WRDOGK - WRDOJK	-25	+66	°C
Temperatur WRDOBF - WRDOJF	-20	+66	°C
Feuchtigkeit	35	85	%

RF Frequenzen

	Min	Mitte	Max	Einheit
RFID Frequenz		13.56		Mhz
Bluetooth Smart Frequenz	2.4	2.445	2.4835	Ghz

F Caractéristique électronique

Condition de fonctionnement

	Min.	Max.	Unité
Température WRDOB - WRDOS - WRDOBK	-35	+66	°C
Température WRDOJ - WRDOGK - WRDOJK	-25	+66	°C
Température WRDOBF - WRDOJF	-20	+66	°C
Humidité	35	85	%

Caractéristiques RF

	Min	Cen.	Max	Unité
Fréquence RFID		13.56		Mhz
Fréquence Bluetooth Smart	2.4	2.445	2.4835	Ghz

NL Technische gegevens:

Omgeving

	Min.	Max.	Unit
Temperatuur WRDOB - WRDOS - WRDOBK	-35	+66	°C
Temperatuur WRDOJ - WRDOGK - WRDOJK	-25	+66	°C
Temperatuur WRDOBF - WRDOJF	-20	+66	°C
Vochtigheid	35	85	%

RF karakteristieken

	Min	Cen.	Max	Unit
RFID frequency		13.56		Mhz
Bluetooth Smart frequency	2.4	2.445	2.4835	Ghz

SVE Teknisk data:

Arbetsområde

	Min.	Max.	Enhet
Temperatur WRDOB - WRDOS - WRDOBK	-35	+66	°C
Temperatur WRDOJ - WRDOGK - WRDOJK	-25	+66	°C
Temperatur WRDOBF - WRDOJF	-20	+66	°C
Fukt	35	85	%

RF data

	Min	Cen.	Max	Enhet
RFID Frekvens		13.56		Mhz
Bluetooth Smart Frekvens	2.4	2.445	2.4835	Ghz

Power Consumption Note 1

	Min	Max	Unit
Reader		150	mA
Reader+Keyboard		250	mA
Reader+Keyboard+Fingerprint		300	mA

Note 1: Installer must take this data into account to dimension the CU42xx power supply. Readers only for use with the SALTO Control Units.

Note 2: Not use with Scotchlok butt connector UY2. SALTO recommends to use one cable per wall reader.

Consumo Nota 1

	Min	Max	Unit
Lector		150	mA
Lector + teclado		250	mA
Lector+teclado+Fingerprint		300	mA

Note 1: El instalador ha de tener en cuenta la dimensión del alimentador de la CU42xx

Note 2: No usar el conector Scotchlok butt UY2 con este tipo de cable. SALTO recomienda utilizar un cable por cada lector mural.

Stromaufnahme Note 1

	Min	Max	Einheit
Leser		150	mA
Leser+Keypad		250	mA
Leser+Keypad+Fingerprint		300	mA

Note 1: Bitte beachten Sie die Stromaufnahme bei der Planung des Netzteils für die CU42XX

Note 2: Nicht verwenden mit den Scotchlok Einzeladerverbinder UY2. SALTO empfiehlt die Verwendung einer separaten Leitung je Wandleser.

Consommation Note 1

	Min	Max	Unité
Lecteur		150	mA
Lecteur + Clavier		250	mA
Lecteur + Clavier+Fingerprint		300	mA

Note 1: l'installateur doit calculer l'alimentation nécessaire pour alimenter la CU42xx.

Note 2: Ne pas utiliser le connecteur Scotchlok UY2 avec ce type de câble. SALTO recommande d'utiliser un câble pour chaque lecteur mural.

Voeding in opm 1

	Min	Max	Unit
Wandlezer		150	mA
Wandlezer+Keyboard		250	mA
Wandlezer+Keyboard+Fingerprint		300	mA

Opm. 1: Installateur moet deze info meenemen voor de berekening van de voeding voor de CU42xx
Opm. 2: 3M Scotchlok 2-voudig draad connectors NIET GEBRUIKEN !!!
SALTO adviseert enkel één kabel per wandlezer te gebruiken.

Strömkonsumtion Not 1

	Min	Max	Enhet
Läsare		150	mA
Läsare+Knappsats		250	mA
Läsare+Knappsats+Fingerprint		300	mA

Not. 1: Installatör måste ta med denna information för att beräkna strömförbrukning

Not. 2: Ej med Scotchlock butt UY2 kontakt

SALTO rekommenderar att en kabel per väggläsare används.

Cable type and max. Distances

Cable type	Reader	Reader Keypad	Reader Keypad Fingerprint
UTP Cat5e	328ft	196ft	164ft
2 pairs AWG24	100m	60m	50m
UTP Cat5e	820ft	492ft	328ft
4 pairs AWG24 SP224861/SP224895	250m	150m	100m
Twisted pairs AWG18 Note2	1312ft	918ft	756ft
	400m	280m	200m

Note: UL tested at 24 AWG at 100m.

Tipo de cable y distancias max.

Tipo cable	Lector	Lector Teclado	Lector Teclado Fingerprint
UTP Cat5e			
2 pares AWG24	100m	60m	50m
UTP Cat5e			
4 pares AWG24 SP224861/SP224895	250m	150m	100m
Pares trenzados AWG18 Nota2	400m	280m	200m

Verkabelung und max. Entfernungen

Kabletyp	Leser	Leser Keypad	Leser Keypad Fingerprint
UTP Cat5e			
2 paar AWG24	100m	60m	50m
UTP Cat5e			
4 paar AWG24 SP224861/SP224895	250m	150m	100m
Twisted pair AWG18 Note2	400m	280m	200m

Type de câble

Type de câble	Lecteur	Lecteur Clavier	Lecteur Clavier Fingerprint
UTP Cat5e			
2 paires AWG24	100m	60m	50m
UTP Cat5e			
4 paires AWG24 SP224861/SP224895	250m	150m	100m
Paires torsadées AWG18 Note2	400m	280m	200m

Vermogen en max. Afstand

Kable type	Wandlezer	Wandlezer Keypad	Wandlezer Keypad Fingerprint
UTP Cat5e			
2 pairs AWG24	100m	60m	50m
UTP Cat5e			
4 pairs AWG24 SP224861/SP224895	250m	150m	100m
Twisted pair AWG18 Opm2	400m	280m	200m

Kabletyper och max avstånd

Kabel	Läsare	Läsare Knappsats	Läsare Knappsats Fingerprint
UTP Cat5e			
2 pairs AWG24	100m	60m	50m
UTP Cat5e			
4 pairs AWG24 SP224861/SP224895	250m	150m	100m
Twisted pair AWG18 Not 2	400m	280m	200m

Eng Installation example:

E Ejemplo de instalación:

D Installationsbeispiel:

F Exemple d'installation:

NL Installatievoorbeeld:

SVE Installationsexempel:

Eng Only connect to CU42xx

E Solo conectar a CU42xx

D Nur für Steuereinheit CU42xx

F Connecter uniquement CU42xx

NL Alleen aansluiten aan CU42xx

SVE Ansluts endast till CU42xx

Eng Cable connection

F Câblage

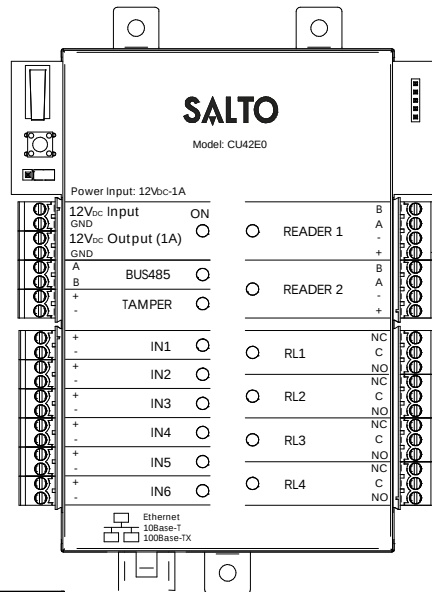
E Cableado

NL Draadwerk

D Verdrahtung

SVE Ledningar

	Eng	Esp	Fra	Deu	Ned	Sve
B	Green	Verde	Vert	Grün	Groen	Grön
A	Yellow	Amarillo	Jaune	Gelb	Geel	Gul
↓	Black	Negro	Noir	Schwarz	Zwart	Svart
+V	Red	Rojo	Rouge	Rot	Rood	Röd



Eng Same pair

E Même paire

D Mismo par

F Gleiches Paar

NL Hetzelfde paar

SVE Samma par

Eng 3M™ Scotchlok™ butt connector UY2. Crimp with cap side down.

E Conector 3M™ Scotchlok™ butt UY2.

D Crimpar con la tapa hacia abajo.

F 3M™ Scotchlok™ butt Einzeladerverbinder UY2.

NL Mit der Kappe nach unten zusammendrücken.

SVE Connecteur 3M™ Scotchlok™ butt UY2.

F Crêper avec le capuchon vers le bas.

NL 3M™ Scotchlok™ draad connectors - UY2.

SVE Krimp/aanknippen met het gekleurde deksel naar beneden.

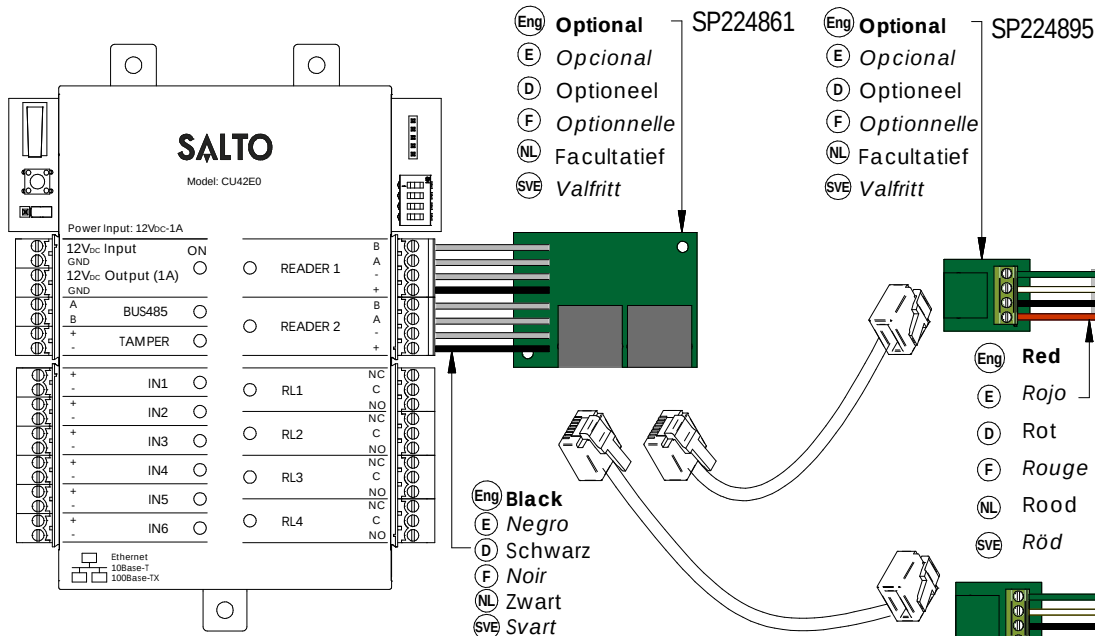
Eng 3M™ kontakt Scotchlok™ butt UY2.

E Monteras med platta sidan neråt.

F Exemple d'installation avec connecteur RJ45 :

NL Installatie voorbeeld RJ45:

SVE Installationsexempel RJ45:



Eng Minimum distance between readers 20in (50cm).

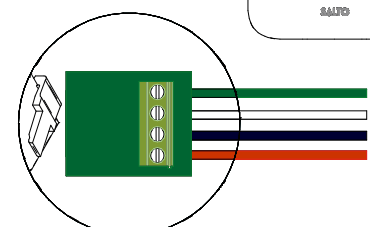
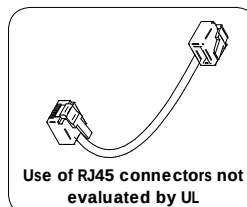
E Distancia mínima entre los lectores 20in (50cm).

D Mindestabstand zwischen Lesern 20in (50cm).

F Distance minimale entre les lecteurs doit être de 20in (50cm).

NL Minimale afstand tussen de lezers 20in (50cm).

SVE Minsta avstånd mellan läsare 20in (50cm).



SIGNAL	LIGHT	TIME	BUZZER	TIME
Card / finger rejection	Red	1sec	High pitched 50/50	1sec
Privacy or emergency status	Red 5x(50/50x3 + off 300)	3sec	High pitched 5x(50/50x3 + off 300)	3sec
Standard opening	Green	1sec	Low pitched	0,3sec
Standard locking	Red	0,5sec	Low pitched	0,2sec
Open plus office	Green 400/200	2,4sec	High pitched/Low pitched 400/200	2,4sec
CLR Button	Orange	Cont.	High pitched	Cont.
Reset	Orange 50/100	450msc	Low pitched 50/100	450msc
Waiting for card / finger	Blinking green 500/500	Cont.	Low pitched 500/500	Cont.
Card / finger processing	Blinking yellow 50/50	100msc	Low pitched 50/50	100 msec
Successfully processed card / finger	Green	1sec	Low pitched	1 sec
SEÑAL	LUZ	TIEMPO	BUZZER	TIEMPO
Rechazo de tarjeta / huella	Rojo	1seg	Agudo 50/50	1seg
Rechazo por privacidad o emergencia	Rojo 5x(50/50x3 + apagado 300)	3seg	Agudo 5x(50/50x3 + apagado 300)	3seg
Apertura normal	Verde	1seg	Medio	0,3seg
Cierre normal	Rojo	0,5seg	Grave	0,2seg
Abrir y paso	Verde 400/200	2,4seg	Agudo/Grave400/200	2,4seg
Botón CLR (3)	Naranja	Cont.	Agudo	Cont.
Reset	Naranja 50/100	450mseg	Medio 50/100	450mseg
Espera de tarjeta / huella	Verde intermitente 500/500	Cont.	Grave intermitente 500/500	Cont.
Procesado de tarjeta / huella	Amarillo intermitente 50/50	100 msec	Grave intermitente 50/50	100 msec
Tarjeta / huella procesada con éxito	Verde	1 seg	Medio	1 seg
SIGNAL	LED	ZEIT	BUZZER	ZEIT
Medium / Finger abgelehnt	Rot	1sek	Hoher Ton 50/50	1sek
Bitte-nicht-stören oder Notschließung	Rot 5x(50/50x3 + aus 300)	3sek	Hoher Ton 5x(50/50x3 + aus 300)	3sek
Normale Türöffnung	Grün	1sek	Tiefer Ton	0,3sek
Verschluss de Tür	Rot	0,5sek	Tiefer Ton	0,2sek
Office-Mode aktiviert	Grün 400/200	2,4sek	Hoher Ton/Grave400/200	2,4sek
CLR Taste gedrückt	Orange	Kont.	Hoher Ton	Cont.
Reset	Orange 50/100	450msk	Tiefer Ton 50/100	450msk
Warte auf Medium / Finger	Grün blinken 500/500	Konst.	Tiefer Ton 500/500	Konst.
Medium / Fingerverarbeitung	Gelb blinken 50/50	100msk	Tiefer Ton 50/50	100msk
Medium / Finger erfolgreich verarbeitet	Grün	1sek	Tiefer Ton	1sek
SIGNAL	VOYANT	TEMP	BUZZER	TEMP
Carte / Empreinte rejeté	Rouge	1sec	Aigur 50/50	1sec
Privacité ou état d'urgence	Rouge 5x(50/50x3 + off 300)	3sec	Aigu 5x(50/50x3 + off 300)	3sec
Ouverture standard	Vert	1sec	Grave	0,3sec
Verrouillage standard	Rouge	0,5sec	Grave	0,2sec
Ouverture passage libre	Vert 400/200	2,4sec	Aigu/Grave400/200	2,4sec
Bouton CLR	Orange	Cont.	Aigu	Cont.
Reset	Orange 50/100	450msc	Grave 50/100	450msc
En attente de a carte / du doigt	Vert clignotant 500/500	Cont.	Aigur 500/500	Cont.
Traitement de la carte / du doigt	Jaune clignotant	100ms	Aigu 50/50	100ms
Carte / doigt validée avec succès	Vert	1sec	Grave	1sec
SIGNAAL	LED INDICATE	TIME	GELUID	TIME
Kaart/vinger weigering	Rood	1sec	Hoge tonen 50/50	1sec
Privacy-of boodsluiting	Rood 5x(50/50x3 + off 300)	3sec	Hoge tonen 5x(50/50x3 + off 300)	3sec
Standaard opening	Groen	1sec	Lage tonen	0,3sec
Standaard sluiting	Rood	0,5sec	Lage tonen	0,2sec
Open plus loopstand	Groen 400/200	2,4sec	Hoge tonen/Grave400/200	2,4sec
CLR knop	Oranje	Cont.	Hoge tonen	Cont.
Reset	Oansje 50/100	450msc	Lage tonen 50/100	450msc
Wachten op kaart/vinger	Blinkar grön 500/500	Konst.	Låg ton 500/500	Konst.
Kaart/vinger in behandeling	Blinkar gult 50/50	100ms	Låg ton 50/50	100ms
Opening kaart/vinger	Grön	1sek	Låg ton	1sek
HÄNDELSE	LJUSSIGNAL	TID	SUMMER	TID
Kort / Fingeravtryck nekat	Röd	1 sek	Hög ton 50/50	1sek
Stör ej eller Nödläge	Röd 5x(50/50x3 + av 300)	3sek	Hög ton 5x(50/50x3 + av 300)	3sek
Standard öppning	Grön	1sek	Låg ton	0,3sek
Standard stänging	Röd	0,5sek	Låg ton	0,2sek
Öppning med kontorsfunktion	Grön 400/200	2,4sek	Hög ton/Låg tone 400/200	2,4sek
CLR Knapp	Orange	Konst.	Hög ton	Konst.
Nollställning	Orange 50/100	450ms	Låg ton 50/100	450msk
Väntar på kort / finger	Blinkar grön 500/500	Konst.	Låg ton 500/500	Konst.
Kort / Finger processas	Blinkar gult 50/50	100ms	Låg ton 50 /50	100ms

UL Statements

Tested by UL with Mifare (DESFIRE, ULTRALIGHT C) and HID iCLASS RFID communication, and with Mobile APP (JustIN Mobile version 2.x) through Bluetooth version 4.2. Minimum Operating System version for Android: 4.3 or later and for iOS: 10.0 or later. A means of verification shall be employed by the user to enable access to the wireless electronic device such as a PIN or biometric feature. The wireless electronic device is not capable of command, control, programming, or any other system manipulation and it is only to be used in the same manner as a physical credential. Wiring methods that shall be in accordance with the National Electrical Code, ANSI/NFPA 70 or CSA C22.1-02 - *Canadian Electrical Code, Part 1, Safety Standard for Electrical Installations*

- UL294 performance level:

FEATURE	LEVEL
Destructive attack	I
Line Security	I
Endurance	IV
Standby power	Per rating of the power supply

- Comply with ULC-S319 Class I

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes: (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

This device has been tested and found to comply with the limits for a Class B digital device, pursuant to ICES-003.

European view  

(*) Note: WRD0GK, WRD0S, WRD0BFand WRD0JF models, not UL listed.

1500 Series® | 1600 Series® Electric Strike



ASSA ABLOY

Experience a safer
and more open world

Installation & Operating Instructions

Product Components

- A 1500 Series® or 1600 Series® Electric Strike Body
- B Trim Enhancer with #6-32 x 3/16" Screws
- C 5/64" Hex Wrench
- D 12 & 24 Volt Plug In Connectors
- E #12-24 x 1/2" Mounting Screws

Electrical Specifications

Electrical Ratings for Solenoid	Continuous Duty		Intermittent Duty*	
	12 VDC	24 VDC	12-16 VAC	24 VAC
Voltage	12 VDC	24 VDC	12-16 VAC	24 VAC
Resistance in Ohms	50	200	50	200
Amps	.24	.12	.24-.32	.12

Solenoids are rated at +/- 10% indicated value.
* 10% max duty cycle (2 min. max on time)

For inductive kickback protection, consider using with the HES 2005M3 SMART Pac® III or 2001M Plug-in Bridge Rectifier with built-in MOV.

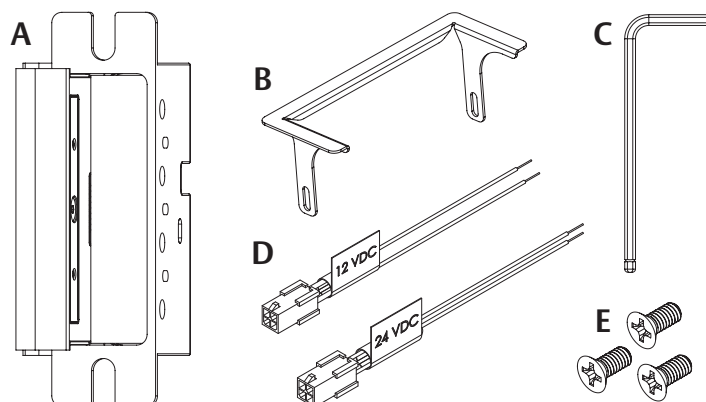
Minimum Wire Gauge Requirements			
Voltage	12 VDC	24 VDC	
200 feet or less	18 gauge	20 gauge	
200-300 feet	16 gauge	18 gauge	
300-400 feet	14 gauge	16 gauge	

The above table applies to Models 1500, 1500E, 1600, and 1600E.
Lengths based on round trip.

1500 1600 Series UL1034 Rating	
Static Strength	1,500 lbs
Dynamic Impact	70 ft-lbs
Endurance	250,000 cycles

UL294 Performance Levels*	
Destructive Attack	Level I (No attack test)
Line Security	Level I (No line security)
Endurance	Level IV (100,000 cycles)
Standby Power	Level I (No secondary power source)

* Monitor options were not evaluated by UL294/UL1034/ULC60839-11-1



Faceplate Options		Description
1J	For Use With	Cylindrical locksets with up to 3/4" throw and all locksets with center-lined bolts.
	Compatible With	All brands of cylindrical latchbolts.
1K	For Use With	Mortise locksets with up to 3/4" throw latchbolt.
	Compatible With	Baldwin, Marks and PDQ.
1KM	For Use With	Mortise locksets with up to 3/4" throw latchbolt.
	Compatible With	Accurate, Arrow, Best, Corbin Russin, Falcon, Sargent (7800, 8200, 9200), ASSA ABLOY ACCENTRA™ 8800 (formerly Yale Commercial).
1KD	For Use With	Mortise locksets with up to 3/4" throw latchbolt.
	Compatible With	Dorma (9500), Jackson, Sargent (7700, 8100), Schlage, ASSA ABLOY ACCENTRA™ 8700 (formerly Yale Commercial).
1N	For Use With	Mortise locksets with deadbolt for night latch function only.
	Compatible With	Accurate, Baldwin, Marks, Omnia, PDQ, Schlage.
1NM	For Use With	Mortise locksets with deadbolt for night latch function only.
	Compatible With	Accurate, Arrow, Baldwin, Corbin Russin, Falcon (45H, 47H, 34H, 37H), Marks, PDQ, Sargent (7800, 8200, 9200), ASSA ABLOY ACCENTRA™ 8800 (formerly Yale Commercial).
1ND	For Use With	Mortise locksets with deadbolt for night latch function only.
	Compatible With	Sargent (7700, 8100), Schlage, ASSA ABLOY ACCENTRA™ 8700 (formerly Yale Commercial).
1NTD	For Use With	Mortise locksets with a normally extended 1" deadbolt and center-lined deadlatch.
	Compatible With	Accurate, Arrow, Baldwin, Marks, Omnia, PDQ, Schlage.

Installation



WARNING: Before connecting any device at the installation site, verify input voltage using a multimeter. Many power supplies and low voltage transformers operate at higher levels than listed. Any input voltage exceeding 10% of the solenoid rating may cause severe damage to the unit. Installation wiring for the product and wiring methods shall be in accordance with the National Electrical Code, ANSI/NFPA 70.

Connecting the Power

For 12 VAC, 12 VDC, or 16 VAC, the Plug In Connector (pigtail) marked "12 VDC" should be used; for 24VAC or 24 VDC, the pigtail marked "24 VDC" should be used.

NOTE: BLACK wire of pigtail is NEGATIVE (-).

- 1 SELECT the appropriate plug in connector that matches system power and electrically CONNECT as shown in **Diagram 1**, "12 VDC to 24 VDC Conversion."

WARNING: Before electrically connecting the device, the input voltage must be verified using a multimeter. Many power supplies and low voltage transformers operate at higher levels than listed. Any input voltage exceeding 10% of the electrical specification (see Page 1) may cause severe damage to the unit and will void the warranty.

Diagram 1:
12 VDC to 24 VDC
Conversion

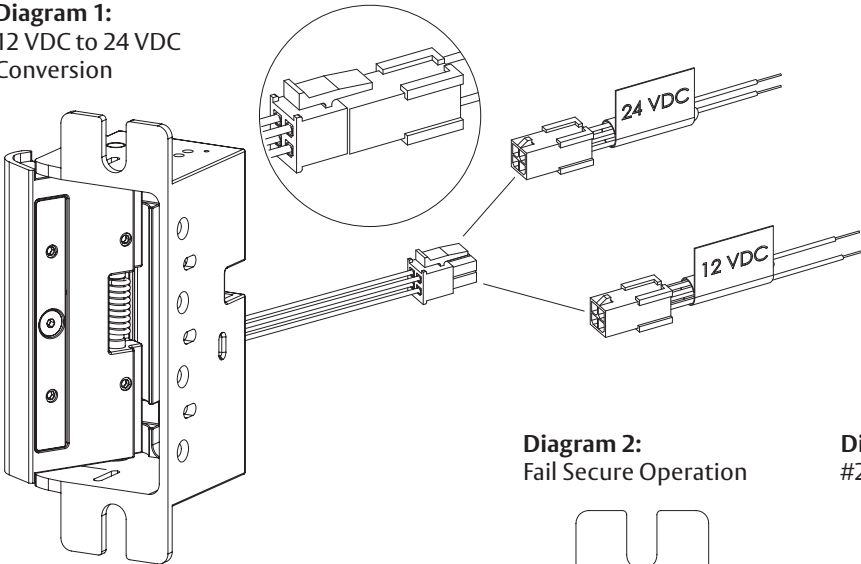


Diagram 2:
Fail Secure Operation

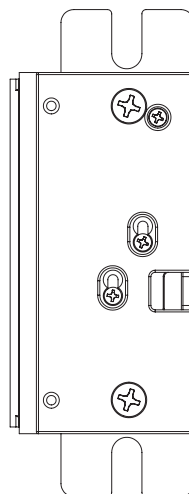


Diagram 3:
#2-56 screws

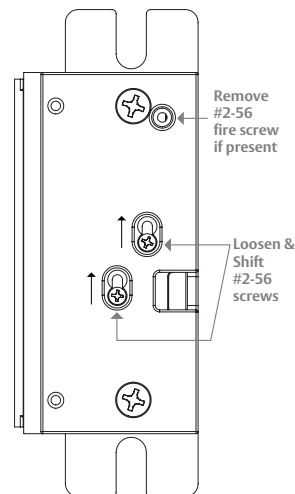
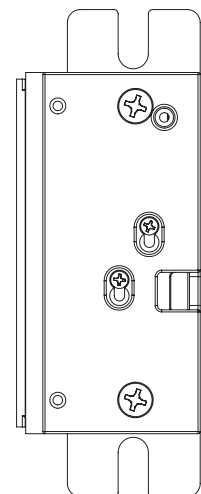


Diagram 4:
Fail Safe Operation



Converting the Operation Mode

The 1500 Series® and 1600 Series® Electric Strikes ship configured for FAIL SECURE OPERATION. The steps below are provided to convert to FAIL SAFE OPERATION, if desired.

The suitability of the strikes in the FAIL SECURE OPERATION mode is up to the local Authority Having Jurisdiction (AHJ) and emergency exit hardware may be required in such installations.

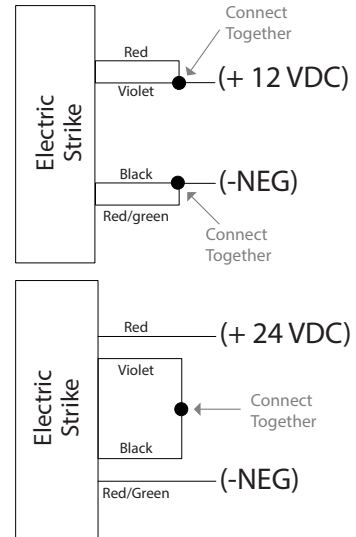
- 1 IF PRESENT, remove #2-56 fire screw. **Diagram 3.**
- 2 LOOSEN, but do not remove the #2-56 screws on the back of the strike.
- 3 SHIFT the #2-56 screws up, as shown in **Diagram 3.**
- 4 TIGHTEN the #2-56 screws on the back of the strike.

Optional Lock and Strike Monitor Wiring

Lock Monitor (LM)	
Contact Rating	500mA @ 30V
White	Open when door is open
Tan	Open when door is open
Strike Monitor (LMS)	
Contact Rating	500mA @ 30V
Brown	Common
Yellow	Normally Open
Blue	Normally Closed

NOTE: Strike in unpowered condition.

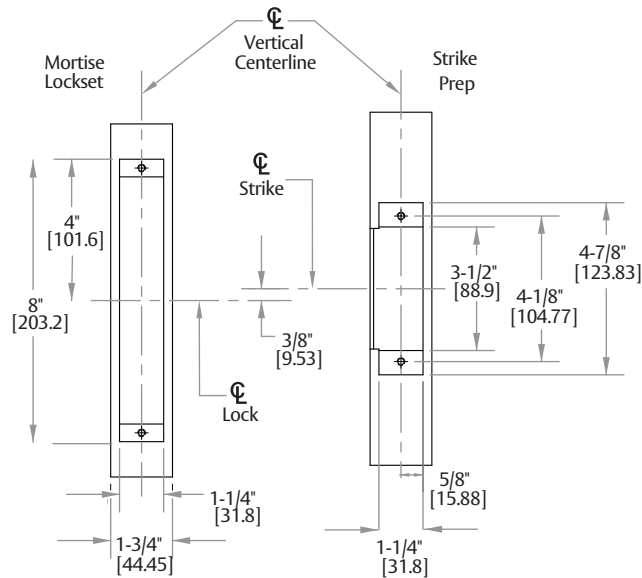
Diagram 1a: If Connector is Missing



Preparing the Frame

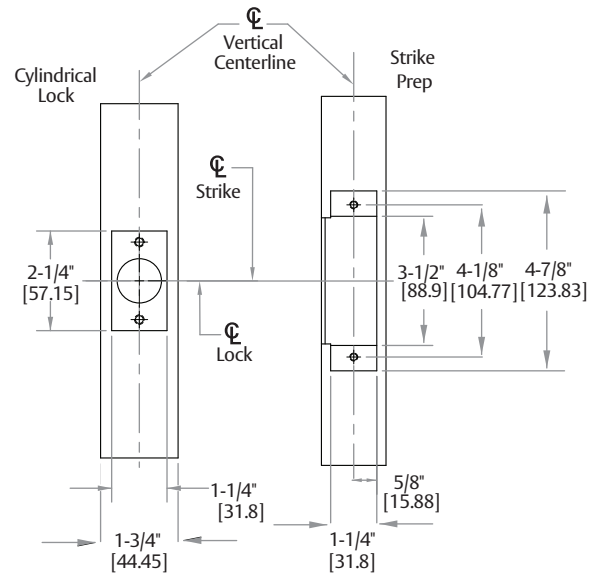
Mortise Locksets

Please note the horizontal centerline of the electric strike in relation to the centerline of the mortise lockset.



Cylindrical Locksets

Please note the horizontal centerline of the electric strike in relation to the centerline of the cylindrical lockset.



Metal Jamb Prep: 1J | 1KM | 1NM

Normally used with Mortise Locks **WITHOUT** Deadbolt.

NOTE: CANNOT be used with Schlage L9000 or ASSA ABLOY ACCENTRA™ 8700 (formerly Yale Commercial).

Metal Jamb Prep: 1KD | 1ND | 1NTD

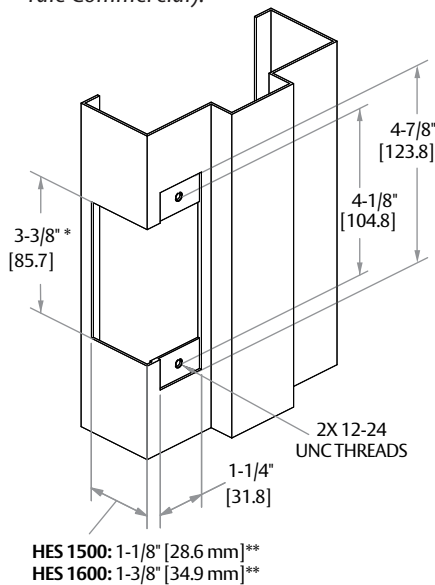
Normally used with Mortise Locks **WITH** Deadbolt.

NOTES: CAN be used with Schlage L9000 or ASSA ABLOY ACCENTRA™ 8700 (formerly Yale Commercial).

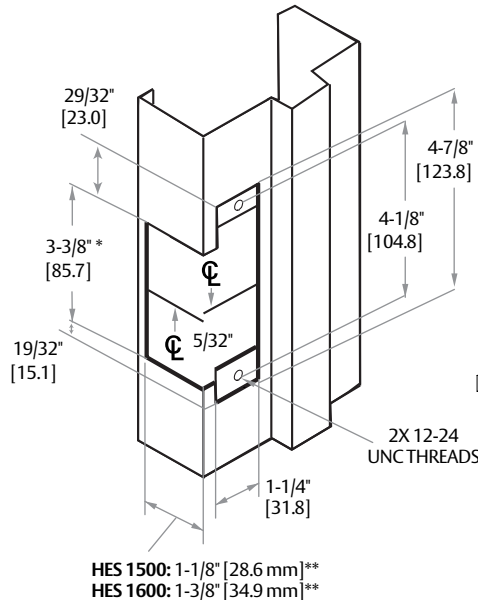
Wood Jamb Prep: 1DB-2 | 1LB-2

1DB-2: Used with Mortise Locks **WITH** Deadbolt.

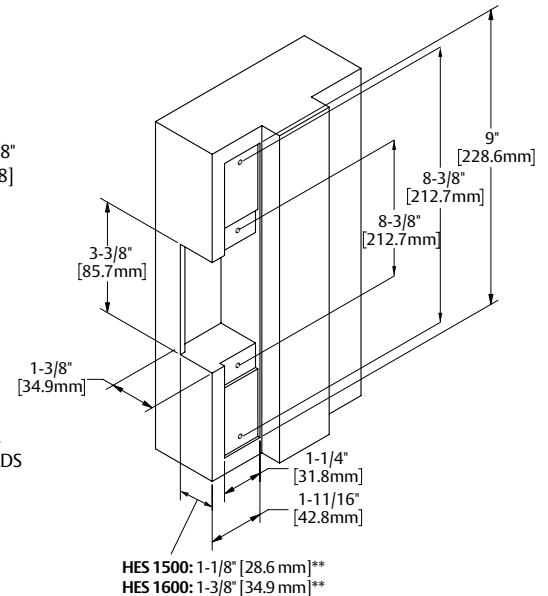
1LB-2: Used with Mortise or Cylindrical Locks **WITHOUT** Deadbolt.



HES 1500: 1-1/8" [28.6 mm]**
HES 1600: 1-3/8" [34.9 mm]**



HES 1500: 1-1/8" [28.6 mm]**
HES 1600: 1-3/8" [34.9 mm]**



HES 1500: 1-1/8" [28.6 mm]**
HES 1600: 1-3/8" [34.9 mm]**

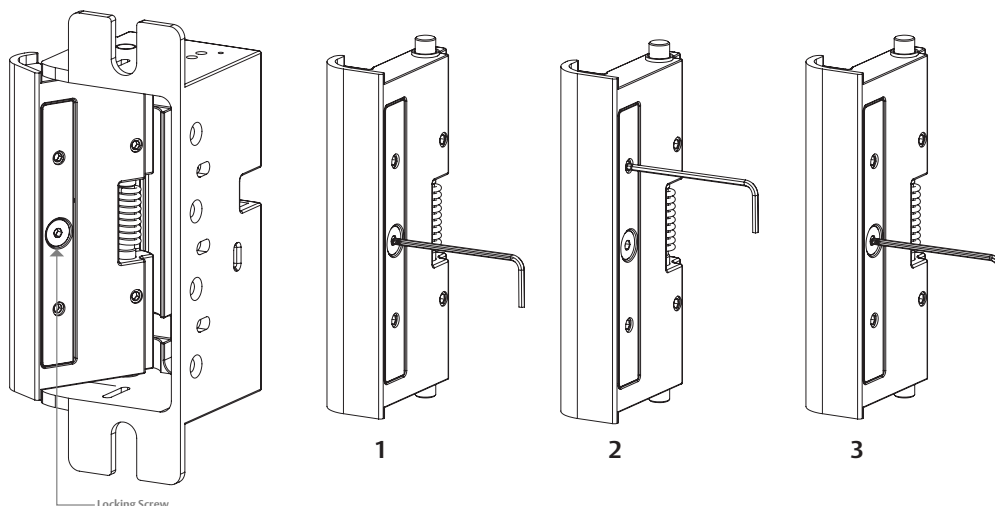
*Add 1/4" [6 mm] to this dimension when using a lip extension. **Add 3/8" [9.5 mm] to this dimension when using a lip extension.

Installation (continued)

Adjusting the Horizontal

To adjust the shim height, it is necessary to power the electric strike to open keeper.

- 1 LOOSEN the locking screw with the 5/64" Hex Wrench.
- 2 ADJUST the shim height to the desired level by turning the upper and lower set screws (clockwise to raise and counterclockwise to lower).
- 3 TIGHTEN the locking screw to lock position.



Faceplate Options

Inches [Millimeters] 4-7/8" x 1-1/4" Square Corners CL = Center Line of faceplate (2nd line = Center Line of faceplate opening)

1J Cylindrical Locksets with up to 3/4" throw and all locksets with center-lined bolts ✓ 1500 ✓ 1600	1K Mortise locksets with up to 3/4" throw latchbolt ✓ 1500 ✓ 1600	1KD Mortise locksets with up to 3/4" throw latchbolt ✓ 1500 ✓ 1600	1KM Mortise locksets with up to 3/4" throw latchbolt ✓ 1500 ✓ 1600
1N Mortise locksets with deadbolt for night latch function only ✓ 1600	1ND Mortise locksets with deadbolt for night latch function only ✓ 1600	1NM Mortise locksets with deadbolt for night latch function only ✓ 1600	1NTD Mortise locksets with a normally extended 1" deadbolt and center-lined deadlatch ✓ 1600

Warranty For information on warranty coverage and replacement options, please visit hesinnovations.com/warranty



techsupport.hes@assaabloy.com
hesinnovations.com | 800 626 7590

Printed in the U.S.A.
Patent pending and/or patent www.assaabloydss.com/patents
Copyright © 2026, Hanchett Entry Systems, Inc., an ASSA ABLOY Group company.
All rights reserved. Reproduction in whole or in part without the express written permission of Hanchett Entry Systems, Inc. is prohibited. 3086006.001_7

9400 | 9500 | 9600 | 9700 | 9800

Electric Strike



ASSA ABLOY

Experience a safer
and more open world

Installation Instructions & Frame Preparation

Product Components

- A** 9400 | 9500 | 9600 | 9700 | 9800
Electric Strike Body
- B** 9400 | 9500 | 9600 | 9700 | 9800
Cover
- C** 1/4"-20 x 1" Mounting Screws
- D** #10-32 & 10-24 Lockdown
Screws (optional)
- E** #6-32 x 1/4" Cover Screws
- F** 5/64" Hex Key
- G** 12 & 24 Volt Plug In Connectors

Electrical Specifications

Electrical Ratings for Solenoid	Continuous Duty	
Voltage	12 VDC	24 VDC
Resistance in Ohms	24	96
mA Continuous Duty	500	250

Solenoids are rated at +/- 10% indicated value.

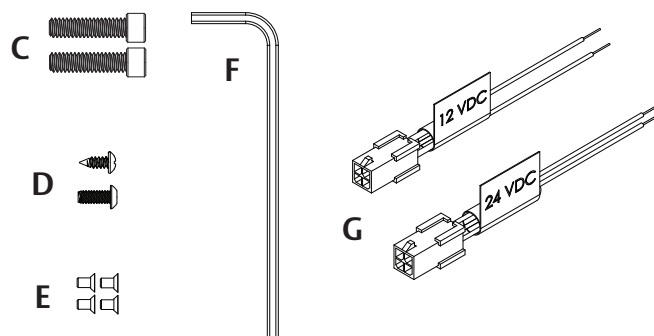
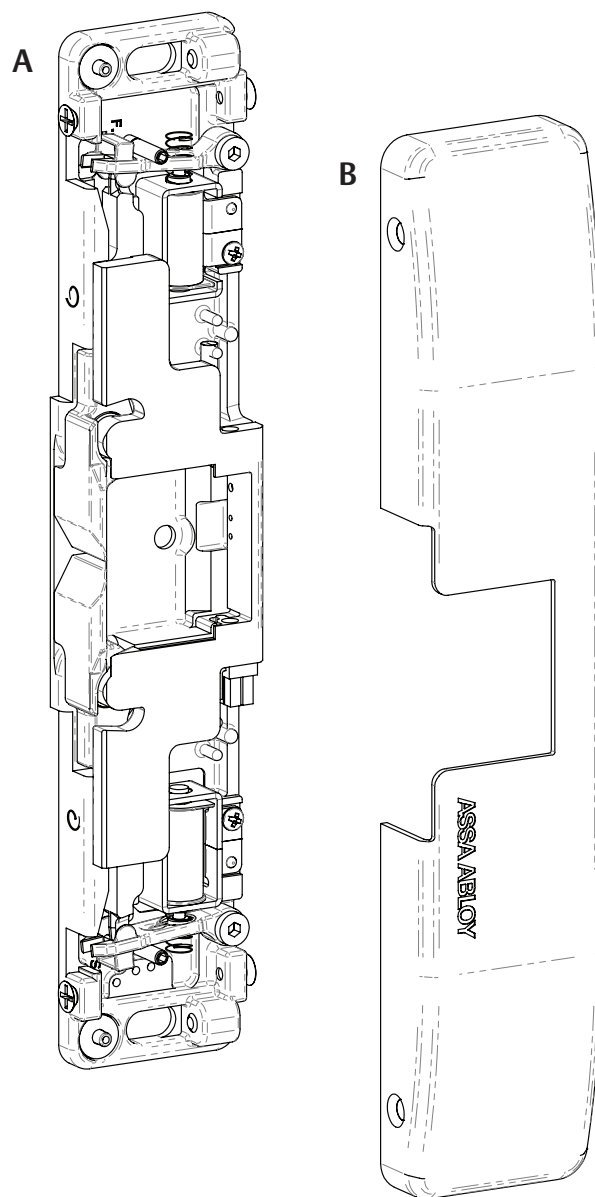
Minimum Wire Gauge Requirements	Continuous Duty	
Voltage	12 VDC	24 VDC
200 feet or less	18 guage	22 guage
200-300 feet	16 guage	22 guage
300-400 feet	16 guage	20 guage

Lengths based on round trip.

9400 9500 9600 9700 9800 Series UL1034 Rating	
Static Strength	1,500 lbs
Dynamic Impact	70 ft-lbs
Endurance	250,000 cycles

UL294 Performance Levels*	
Destructive Attack	Level I (No attack test)
Line Security	Level I (No line security)
Endurance	Level IV (100,000 cycles)
Standby Power	Level I (No secondary power source)

** Monitor options were not evaluated by UL294/UL1034/ULC60839-11-1*



Installation



WARNING: Before connecting any device at the installation site, verify input voltage using a multimeter. Many power supplies and low voltage transformers operate at higher levels than listed. Any input voltage exceeding 10% of the solenoid rating may cause severe damage to the unit. Installation wiring for the product and wiring methods shall be in accordance with the National Electrical Code, ANSI/NFPA 70.

Preparing the Strike

For 12 VDC, the Plug In Connector (pigtail) marked "12 VDC" should be used; for 24 VDC, the pigtail marked "24 VDC" should be used.

- 1 SELECT the appropriate plug in connector that matches system power and electrically CONNECT as shown in Diagram 1.
- 2 IF no connector is present, THEN CONFIGURE the wires as shown in Diagram 2.
- 3 IF using a Latchbolt Monitor (LBM) or Latchbolt Strike Monitor (LBSM), THEN REFER to Diagrams 6 and 7 (see page 3).



WARNING: This unit ships in Fail Secure mode. Converting the 9400 | 9500 | 9600 | 9700 Series Strike to Fail Safe Mode negates the unit's fire rating.

- 4 VERIFY that both keepers are in FAIL SECURE OPERATION as shown in Diagram 3.
- 5 IF the Electric Strike must be converted to Fail Safe mode, THEN CONVERT in accordance with Diagram 4.

Diagram 1:
12 VDC to 24 VDC Conversion

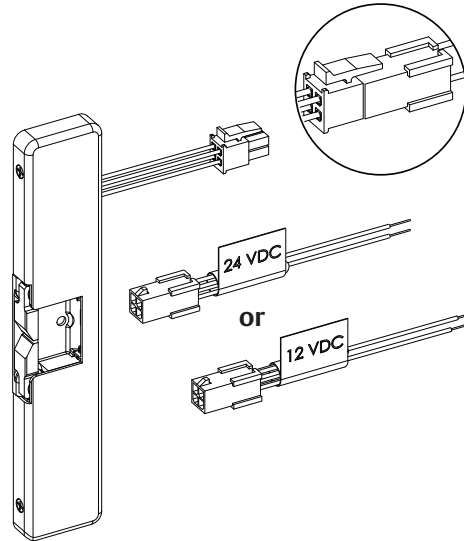


Diagram 2:
If Connector Is Missing

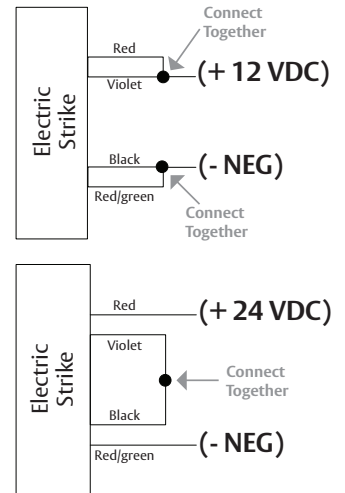


Diagram 3: Fail Secure Operation

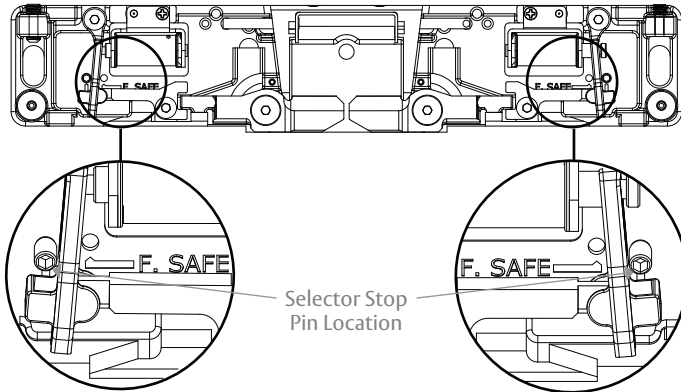
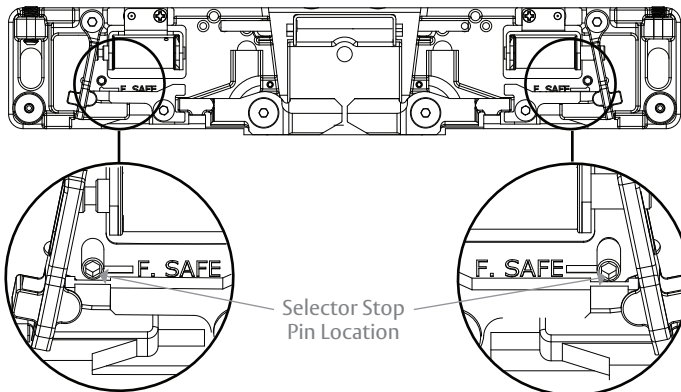


Diagram 4: Fail Safe Operation



Converting the Operation Mode

There are two Selector Stop Pins, one on the left side and one on the right side. Both Selector Stop Pins must be repositioned to convert the strike to FAIL SAFE OPERATION as shown in Diagram 4.

IN FAIL SAFE OPERATION: Both keepers should be unlocked without power and locked when power is applied.

- 1 To convert to FAIL SAFE OPERATION, REMOVE the Selector Stop Pins on each side of the strike body using the provided 5/64" hex key.
- 2 MOVE the Selector Stop Pins to the FAIL SAFE OPERATION position (towards the center of the strike) as shown in Diagram 4.
- 3 TIGHTEN both Selector Stop Pins after they have been moved to the FAIL SAFE OPERATION position using the 5/64" hex key. When converting LBSM from fail secure to fail safe, be sure to move the monitoring switch position shown in Diagram 5.



WARNING: FAIL SAFE OPERATION mode should not be used in fire rated or windstorm resistant applications.

Preparing the Frame

NOTE: When using a Corbin Russwin 5000 Series or ASSA ABLOY ACCENTRA™ 7000 Series (formerly Yale Commercial) equipped with an offset deadlatch, the deadlatch is located just above the vertical alignment line as shown in the dimensions (see page 4).

- 1 IDENTIFY and MARK the latchbolt centerline on the frame.
- 2 USING the dimensions provided (see page 4), MARK all appropriate holes. If using a HES 9000-ASB*, reference the installation instructions provided with that product.

NOTE: In retrofit applications this may require the exit device to shift horizontally towards the hinge side of the door to compensate for the HES 9000-ASB.

- 3 PUNCH, DRILL and TAP the marked holes as required.

NOTE: When mounting on an aluminum frame, with a blade stop, an HES 9000-ASB (sold separately) is necessary to provide a secure installation. The HES 9000-ASB is shown installed in Diagram 10 (see page 4).

Wiring

Diagram 6: Latchbolt Monitor (LBM)

White	Common
Orange	Normally Open
Green	Normally Closed

Diagram 7: Latchbolt Strike Monitor (LBSM)

Brown	Common
Blue	Normally Open
Yellow	Normally Closed

NOTE: The state of switch is listed for an unpowered strike and LBM in unactuated (door open) position.

Finishing the Installation

- 1 ELECTRICALLY CONNECT the HES 9400/9500/9600/9700/9800 to the Plug In Connector, and ATTACH the electric strike to the jamb using the 1/4"-20 x 1" mounting screws provided.
- 2 CHECK the latchbolt interaction with the keepers to ensure proper engagement and clearance. If horizontal adjustment is needed, ADJUST the strike and LOCKDOWN the horizontal adjustment using the 10-32 set screws as show in Diagram 8.
- 3 TIGHTEN the two 1/4"-20 x 1" mounting screws.
- 4 OPTIONAL LOCKDOWN FEATURE: INSTALL the #10-24 UNC or 10-32 UNF lockdown screw if additional security is required; however, REMOVE the strike before drilling hole. If using a HES 9000-ASB it will require drilling and tapping of the lockdown hole.
- 5 INSTALL the cover plate, and SECURE in place using the #6-32 x 1/4" Cover Screws.



WARNING: If no LOCKDOWN SCREW is used, the electric strike WILL NOT be windstorm rated and windstorm label should be removed. This pertains ONLY to the 9600 and 9700.

Diagram 5:
Monitoring Switch Position

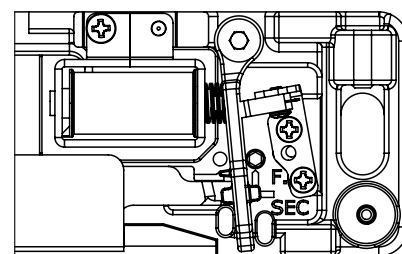


Diagram 6:
Latchbolt Monitor

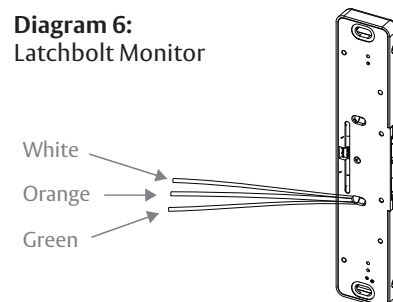


Diagram 7:
Latchbolt Strike Monitor

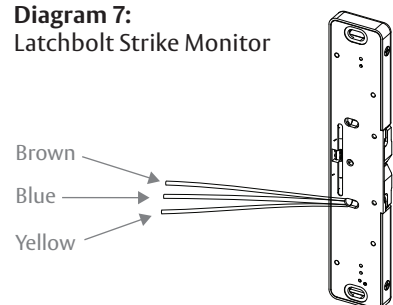
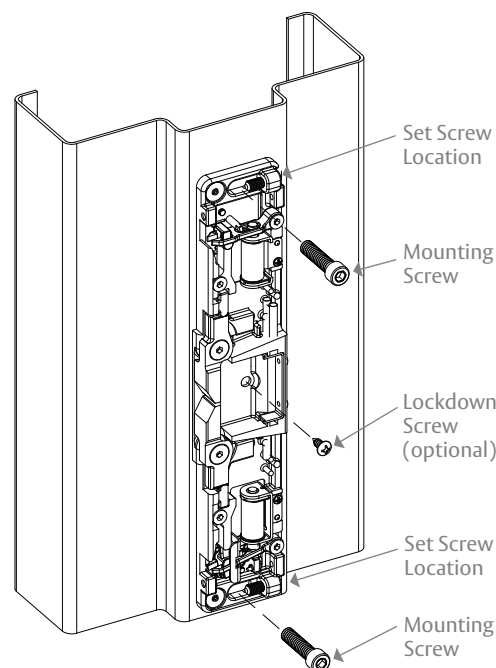


Diagram 8:
Adjusting the Horizontal



Installation *(continued)*

Diagram 9:
9400 Mounted on Hollow Metal Frame

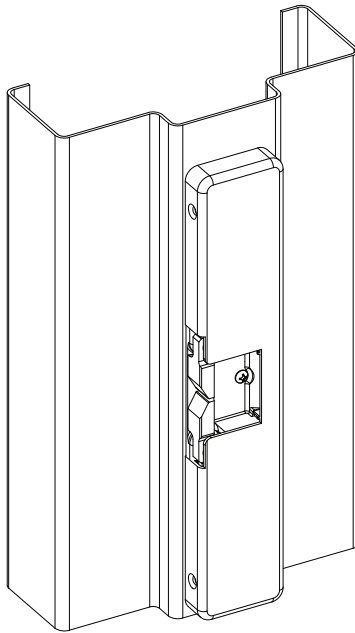
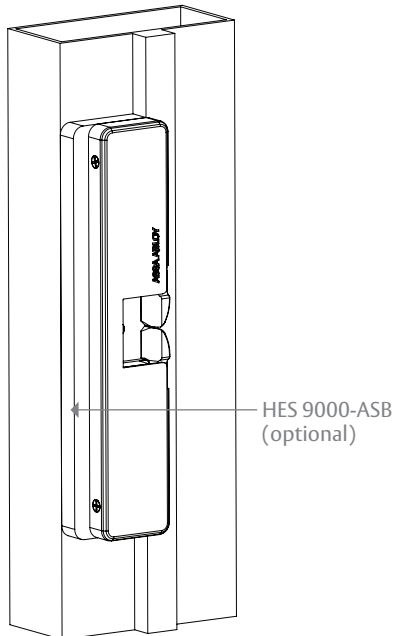
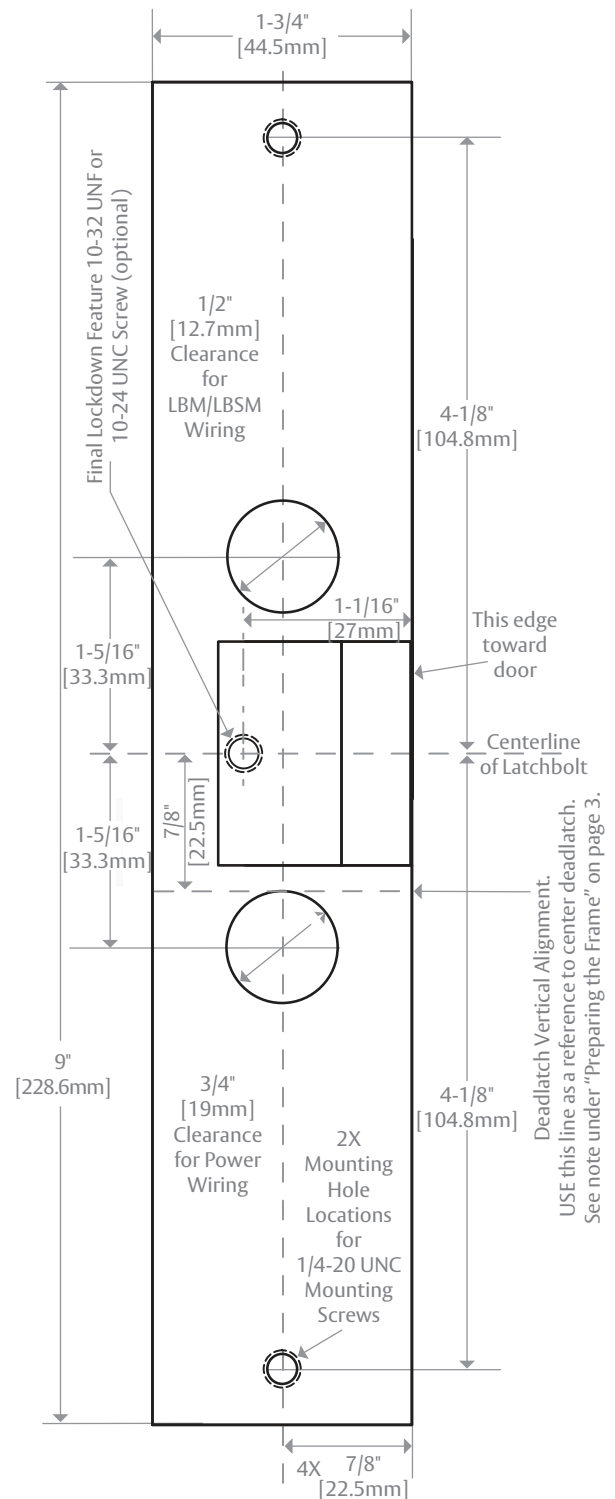


Diagram 10:
9400 Mounted on Aluminum Frame with Blade Stop



Dimensions

NOTE: Not to scale. For easy installation, the HES 9000-MTK should be ordered.



Warranty For information on warranty coverage and replacement options, please visit hesinnovations.com/warranty



techsupport.hes@assaabloy.com
hesinnovations.com | 800 626 7590

Printed in the U.S.A.
Patent pending and/or patent www.assaabloydss.com/patents
Copyright © 2024, Hanchett Entry Systems, Inc., an ASSA ABLOY Group company.
All rights reserved. Reproduction in whole or in part without the express written permission of Hanchett Entry Systems, Inc. is prohibited. 3026006.004_3

NEWTON COUNTY, GA –HISTORIC JAIL
OPERATIONS & MAINTENANCE MANUAL –
SURVEILLANCE CAMERA SYSTEM

Version 1.0
Date 07/29/2026

VERSION HISTORY

Version #	Implemented By	Revision Date	Approved By	Approval Date	Reason
1.0	Chad Maynard	07/29/2026	Chad Maynard	07/29/2026	Original release

PROJECT INFORMATION

Item	
Owner	Newton County, GA
Facility	Newton County Historic Jail
Recording Software	AXIS Camera Station
Recording Server	Not provided – existing AXIS-STORAGE server utilized
Server Location	Newton County Storage Building
Cameras Installed	8
Installation Date	May 2026
Contractor	TechOptics, Inc.

TABLE OF CONTENTS

1 INTRODUCTION	4
2 PROJECT SCOPE	4
3 SYSTEM DESCRIPTION	4
4 INSTALLED EQUIPMENT.....	5
5 OPERATION	5
6 PREVENTIVE MAINTENANCE.....	5
7 WARRANTY	6
8 TROUBLESHOOTING	6
9 INSTALLER INFORMATION.....	6

1 INTRODUCTION

This manual provides operation and maintenance information for the surveillance camera work completed at the Newton County Historic Jail. The project consisted of furnishing, licensing, installing, configuring, and commissioning eight (8) AXIS IP cameras on the owner's existing AXIS Camera Station recording server.

2 PROJECT SCOPE

Work performed by TechOptics included:

- Installation of eight AXIS IP cameras.
- Supply and activation of the required AXIS Camera Station camera licenses.
- Addition of the cameras to the existing AXIS Camera Station server.
- Configuration of camera settings and administrative password.
- Camera aiming and focus adjustment.
- Verification of live video and recording operation.

Items specifically outside the project scope included:

- Existing AXIS Camera Station server hardware.
- Network switches, structured cabling, and fiber infrastructure.
- Recording storage hardware.
- Existing surveillance cameras and system components

3 SYSTEM DESCRIPTION

The surveillance cameras installed under this project are connected to the customer's existing network and are managed by the existing AXIS Camera Station server. The recording server is physically located in the Storage Building adjacent to the Historic Jail. The cameras continuously stream video to the server where recording, playback, user authentication, and camera management are performed.

4 INSTALLED EQUIPMENT

8 AXIS Camera Station 5.0 Core Device licenses (P/N 0879-010) were applied to the existing server at the storage building.

License Key: TPNS-PMQN-WQCN-PNWT

The cameras were commissioned using the following administrative credentials. It is recommended that the Owner change these credentials after acceptance of the project and maintain them in accordance with their cybersecurity policies.

Username: root

Password: N3wt0n26!

<u>Camera</u>	<u>Location</u>	<u>IP Address</u>	<u>Manufacturer</u>	<u>Model</u>
Historic Jail 1	Side door	169.254.119.73	AXIS	M3066-V
Historic Jail 2	Upstairs stairwell	169.254.214.25	AXIS	M3066-V
Historic Jail 3	Downstairs lobby	169.254.71.16	AXIS	M3066-V
Historic Jail 4	Parking	169.254.40.108	AXIS	M3216-LVE
Historic Jail 5	Front door	169.254.156.209	AXIS	M3216-LVE
Historic Jail 6	Elevator upstairs	169.254.123.227	AXIS	M3216-LVE
Historic Jail 7	Fire escape upper	169.254.10.77	AXIS	M3216-LVE
Historic Jail 8	Fire escape lower	169.254.47.160	AXIS	M3216-LVE

5 OPERATION

The AXIS Camera Station server provides live viewing, recording, playback, export, and user management.

Camera configuration changes should be performed through AXIS Camera Station or the individual camera web interface by authorized personnel only.

6 PREVENTIVE MAINTENANCE

Inspect camera images monthly for focus and field of view.

- Clean camera domes/lenses as required.
- Verify all cameras are recording successfully.
- Review storage utilization and retention periodically.
- Install firmware updates during scheduled maintenance windows.
- Re-aim cameras if physical movement is observed.
- TechOptics recommends that the AXIS Camera Station database and server configuration be included in the owner's regular server backup procedures.

7 WARRANTY

- AXIS cameras are covered by the manufacturer's warranty for 5 years from the date of purchase.
- TechOptics warrants workmanship for (1) one year from the date of installation unless otherwise specified in the contract.
- Damage cause by vandalism, lightning, power surges, network failures, or owner/third party modification is excluded.

8 TROUBLESHOOTING

If a camera is offline:

1. Verify PoE power and network connectivity.
2. Confirm the camera responds on the network.
3. Check AXIS Camera Station for communication errors.
4. Verify credentials if authentication fails.
5. Contact TechOptics if hardware replacement or additional support is required.

9 INSTALLER INFORMATION

TechOptics, Inc.
463 Bankhead Hwy.
Winder, GA 30680
<http://www.techoptics.net/>
Phone: 770-867-1777
Fax: 770-868-0111
Service Email: service@techoptics.net
General Email: info@techoptics.net

AXIS M30 Network Camera Series

AXIS M3064-V Network Camera

AXIS M3065-V Network Camera

AXIS M3066-V Network Camera

AXIS M3075-V Network Camera

AXIS M30 Network Camera Series

Table of Contents

About this manual	3
Installation	4
Get started	5
Find the device on the network	5
Open the device's webpage	5
Webpage overview	6
Configure your device	7
Adjust the image	7
View and record video	11
Set up rules for events	12
Audio	14
The device interface	16
Status	16
Video	17
Audio	25
Recordings	26
Apps	27
System	28
Maintenance	45
Learn more	46
View area	46
Capture modes	46
Privacy masks	46
Overlays	47
Streaming and storage	47
Applications	49
Cleaning recommendations	52
Troubleshooting	53
Reset to factory default settings	53
Firmware options	53
Check the current firmware version	53
Upgrade the firmware	53
Technical issues, clues, and solutions	54
Performance considerations	56
Contact support	56
Specifications	57
Product overview	57
LED indicators	57
SD card slot	57
Buttons	58
Connectors	58

AXIS M30 Network Camera Series

About this manual

About this manual

This user manual describes several products. This means you may find instructions that aren't applicable to your product.

AXIS M30 Network Camera Series

Installation

Installation



To watch this video, go to the web version of this document.

help.axis.com/?&pid=49386§ion=about-this-manual

Installation video for the product.

AXIS M30 Network Camera Series

Get started

Get started

Find the device on the network

To find Axis devices on the network and assign them IP addresses in Windows®, use AXIS IP Utility or AXIS Device Manager. Both applications are free and can be downloaded from axis.com/support.

For more information about how to find and assign IP addresses, go to *How to assign an IP address and access your device*.

Browser support

You can use the device with the following browsers:

	Chrome™	Firefox®	Edge™	Safari®
Windows®	recommended	recommended	✓	
macOS®	recommended	recommended	✓	✓
Linux®	recommended	recommended	✓	
Other operating systems	✓	✓	✓	✓*

To use AXIS OS web interface with iOS 15 or iPadOS 15, go to **Settings > Safari > Advanced > Experimental Features and disable **NSURLSession Websocket**.*

If you need more information about recommended browsers, go to *AXIS OS Portal*.

Open the device's webpage

1. Open a browser and type the IP address or host name of the Axis device.
If you do not know the IP address, use AXIS IP Utility or AXIS Device Manager to find the device on the network.
2. Type the username and password. If you access the device for the first time, you must set the root password. See *Set a new password for the root account on page 5*.

Set a new password for the root account

The default administrator username is `root`. There's no default password for the root account. You set a password the first time you log in to the device.

1. Type a password. Follow the instructions about secure passwords. See *Secure passwords on page 5*.
2. Retype the password to confirm the spelling.
3. Click **Add user**.

Important

If you lose the password for the root account, go to *Reset to factory default settings on page 53* and follow the instructions.

Secure passwords

Important

Axis devices send the initially set password in clear text over the network. To protect your device after the first login, set up a secure and encrypted HTTPS connection and then change the password.

The device password is the primary protection for your data and services. Axis devices do not impose a password policy as they may be used in various types of installations.

AXIS M30 Network Camera Series

Get started

To protect your data we strongly recommend that you:

- Use a password with at least 8 characters, preferably created by a password generator.
- Don't expose the password.
- Change the password at a recurring interval, at least once a year.

Webpage overview

This video gives you an overview of the device interface.



To watch this video, go to the web version of this document.

help.axis.com/?&pid=49386&tsection=webpage-overview

Axis device web interface

AXIS M30 Network Camera Series

Configure your device

Configure your device

Adjust the image

This section includes instructions about configuring your device. If you want to learn more about how certain features work, go to *Learn more on page 46*.

Select exposure mode

To improve image quality for specific surveillance scenes, use exposure modes. Exposure modes lets you control aperture, shutter speed, and gain. Go to **Video > Image > Exposure** and select between the following exposure modes:

- For most use cases, select **Automatic** exposure.
- For environments with certain artificial lighting, for example fluorescent lighting, select **Flicker-free**.
Select the same frequency as the power line frequency.
- For environments with certain artificial light and bright light, for example outdoors with fluorescent lighting at night and sun during daytime, select **Flicker-reduced**.
Select the same frequency as the power line frequency.
- To lock the current exposure settings, select **Hold current**.

Benefit from IR light in low-light conditions by using night mode

Your camera uses visible light to deliver color images during the day. But as the visible light diminishes, color images become less bright and clear. If you switch to night mode when this happens, the camera uses both visible and near-infrared light to deliver bright and detailed black-and-white images instead. You can set the camera to switch to night mode automatically.

1. Go to **Video > Image > Day-night mode**, and make sure that the **IR-cut filter** is set to **Auto**.
2. To set at what light level you want the camera to switch to night mode, move the **Threshold** slider toward **Bright** or **Dark**.

Note

If you set the switch to night mode to occur when it's brighter, the image remains sharper as there is less low-light noise. If you set the switch to occur when it's darker, the image colors are maintained for longer, but there is more image blur due to low-light noise.

Reduce noise in low-light conditions

To reduce noise in low-light conditions, you can adjust one or more of the following settings:

- Adjust the trade-off between noise and motion blur. Go to **Video > Image > Exposure** and move the **Blur-noise trade-off** slider toward **Low noise**.
- Set the exposure mode to automatic.

Note

A high max shutter value can result in motion blur.

- To slow down the shutter speed, set max shutter to the highest possible value.

Note

When you reduce the max gain, the image can become darker.

- Set the max gain to a lower value.

AXIS M30 Network Camera Series

Configure your device

- If possible, open the aperture.
- Reduce sharpness in the image, under **Appearance**.

Reduce motion blur in low-light conditions

To reduce motion blur in low-light conditions, adjust one or more of the following settings in **Video > Image > Exposure**:

- Move the **Blur-noise trade-off** slider toward **Low motion blur**.

Note

When you increase the gain, image noise also increases.

- Set **Max shutter** to a shorter time, and **Max gain** to a higher value.

If you still have problems with motion blur:

- Increase the light level in the scene.
- Mount the camera so that objects move toward it or away from it rather than sideways.

Maximize the details in an image

Important

If you maximize the details in an image, the bitrate will probably increase and you might get a reduced frame rate.

- Make sure to select the capture mode that has the highest resolution.
- Go to **Video > Stream > General** and set the compression as low as possible.
- Below the live view image, click  and in **Video format**, select **MJPEG**.
- Go to **Video > Stream > H.264 and H.265 encoding > Zipstream** and select **Off**.

Handle scenes with strong backlight

Dynamic range is the difference in light levels in an image. In some cases the difference between the darkest and the brightest areas can be significant. The result is often an image where either the dark or the bright areas are visible. Wide dynamic range (WDR) makes both dark and bright areas of the image visible.



Image without WDR.

AXIS M30 Network Camera Series

Configure your device



Image with WDR.

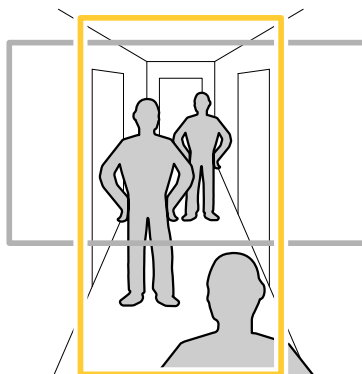
Note

- WDR can cause artifacts in the image.
 - WDR may not be available for all capture modes.
1. Go to **Video > Image > Wide dynamic range**.
 2. Turn on WDR.
 3. Use the **Local contrast** slider to adjust the amount of WDR.
 4. If you still have problems, go to **Exposure** and adjust the **Exposure zone** to cover the area of interest.

Find out more about WDR and how to use it at axis.com/web-articles/wdr.

Monitor long and narrow areas

Use corridor format to better utilize the full field of view in a long and narrow area, for example a staircase, hallway, road, or tunnel.



1. Depending on your device, turn the camera or the 3-axis lens in the camera 90° or 270°.
2. If the device doesn't have automatic rotation of the view, go to **Video > Installation**.
3. Rotate the view 90° or 270°.

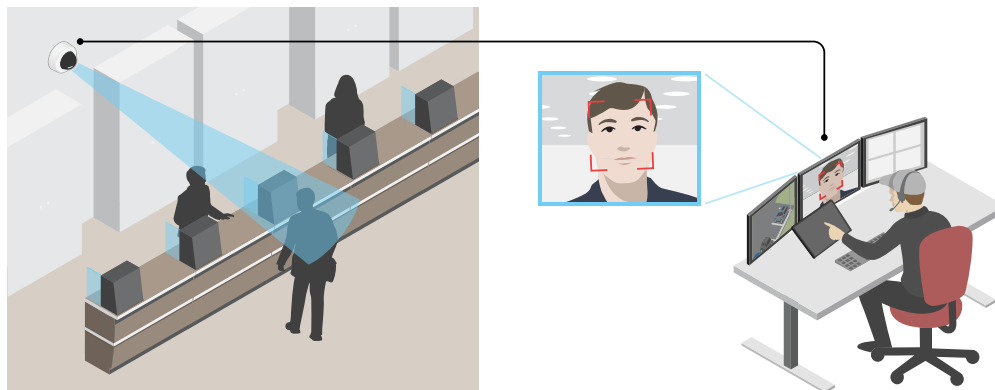
Find out more at axis.com/axis-corridor-format.

Verify the pixel resolution

To verify that a defined part of the image contains enough pixels to, for example, recognize the face of a person, you can use the pixel counter.

AXIS M30 Network Camera Series

Configure your device



1. Go to **Video > Image** and click .
2. Click  for **Pixel counter**.
3. In the camera's live view, adjust the size and position of the rectangle around the area of interest, for example where you expect faces to appear.

You can see the number of pixels for each of the rectangle's sides, and decide if the values are enough for your needs.

Hide parts of the image with privacy masks

You can create one or several privacy masks to hide parts of the image.

1. Go to **Video > Privacy masks**.
2. Click .
3. Click the new mask and type a name.
4. Adjust the size and placement of the privacy mask according to your needs.
5. To change the color for all privacy masks, click **Privacy masks** and select a color.

See also *Privacy masks on page 46*

Show a text overlay in the video stream when the device detects an object

This example explains how to display the text "Motion detected" when the device detects an object.

1. Start the application if it is not already running.
2. Make sure you have set up the application according to your needs.

Add the overlay text:

1. Go to **Video > Overlays**.
2. Under **Overlays**, select **Text** and click .
3. Enter #D in the text field.

AXIS M30 Network Camera Series

Configure your device

4. Choose text size and appearance.
5. To position the text overlay, click  and select an option.

Create a rule:

1. Go to **System > Events** and add a rule.
2. Type a name for the rule.
3. In the list of actions, under **Overlay text**, select **Use overlay text**.
4. Select a video channel.
5. In **Text**, type "Motion detected".
6. Set the duration.
7. Click **Save**.

View and record video

This section includes instructions about configuring your device. To learn more about how streaming and storage works, go to *Streaming and storage on page 47*.

Reduce bandwidth and storage

Important

Reducing the bandwidth can result in loss of details in the image.

1. Go to **Video > Stream**.
2. Click  in the live view.
3. Select **Video format H.264**.
4. Go to **Video > Stream > General** and increase **Compression**.
5. Go to **Video > Stream > H.264 and H.265 encoding** and do one or more of the following:
 - Select the **Zipstream** level that you want to use.

Note

The **Zipstream** settings are used for both H.264 and H.265.

- Turn on **Dynamic FPS**.
- Turn on **Dynamic GOP** and set a high **Upper limit GOP length** value.

Note

Most web browsers don't support H.265 decoding and because of this the device doesn't support it in its web interface. Instead you can use a video management system or application that supports H.265 decoding.

View a live video stream on a monitor

Your camera can transmit a live video stream to an HDMI monitor even without a network connection. Use the monitor for surveillance purposes or for public viewing, for example in a store.

1. Connect an external monitor using the HDMI connector.

AXIS M30 Network Camera Series

Configure your device

2. Go to **System > Video out** and turn on HDMI.
3. Select a **Source**. Rotate the image if needed.

Set up network storage

To store recordings on the network, you need to set up your network storage.

1. Go to **System > Storage**.
2. Click  **Add network storage** under **Network storage**.
3. Type the IP address of the host server.
4. Type the name of the shared location on the host server under **Network share**.
5. Type the username and password.
6. Select the SMB version or leave it on **Auto**.
7. Select **Add share even if connection fails** if you experience temporary connection issues, or if the share is not yet configured.
8. Click **Add**.

Record and watch video

Record video directly from the camera

1. Go to **Video > Image**.
2. To start a recording, click .

If you haven't set up any storage, click  and . For instructions on how to set up network storage, see *Set up network storage on page 12*

3. To stop recording, click  again.

Watch video

1. Go to **Recordings**.
2. Click  for your recording in the list.

Set up rules for events

You can create rules to make your device perform an action when certain events occur. A rule consists of conditions and actions. The conditions can be used to trigger the actions. For example, the device can start a recording or send an email when it detects motion, or show an overlay text while the device is recording.

To learn more, check out our guide *Get started with rules for events*.

Trigger an action

1. Go to **System > Events** and add a rule. The rule defines when the device will perform certain actions. You can set up rules as scheduled, recurring, or manually triggered.

AXIS M30 Network Camera Series

Configure your device

2. Enter a **Name**.
3. Select the **Condition** that must be met to trigger the action. If you specify more than one condition for the rule, all of the conditions must be met to trigger the action.
4. Select which **Action** the device should perform when the conditions are met.

Note

If you make changes to an active rule, the rule must be turned on again for the changes to take effect.

Note

If you change the definition of a stream profile that is used in a rule, then you need to restart all the rules that use that stream profile.

Record video when the camera detects an object

This example explains how to set up the camera to start recording to the SD card when the camera detects an object. The recording will include five seconds before detection and one minute after detection ends.

Before you start:

- Make sure you have an SD card installed.
1. Start the application if it is not already running.
 2. Make sure you have set up the application according to your needs.

Create a rule:

1. Go to **System > Events** and add a rule.
2. Type a name for the rule.
3. In the list of actions, under **Recordings**, select **Record video while the rule is active**.
4. In the list of storage options, select **SD_DISK**.
5. Select a camera and a stream profile.
6. Set the prebuffer time to 5 seconds.
7. Set the postbuffer time to 1 minute.
8. Click **Save**.

Send an email automatically if someone spray paints the lens

Activate the tampering detection:

1. Go to **System > Detectors > Camera tampering**.
2. Set a duration for **Trigger after**. The value indicates the time that must pass before an email is sent.
3. Turn on **Trigger on dark images** to detect if the lens is sprayed, covered, or rendered severely out of focus.

Add an email recipient:

4. Go to **System > Events > Recipients** and add a recipient.
5. Type a name for the recipient.
6. Select **Email**.
7. Type an email address to send the email to.

AXIS M30 Network Camera Series

Configure your device

8. The camera doesn't have its own email server, so it has to log into another email server to send mails. Fill in the rest of the information according to your email provider.
9. To send a test email, click **Test**.
10. Click **Save**.

Create a rule:

11. Go to **System > Events > Rules** and add a rule.
12. Type a name for the rule.
13. In the list of conditions, under **Video**, select **Tampering**.
14. In the list of actions, under **Notifications**, select **Send notification to email** and then select the recipient from the list.
15. Type a subject and a message for the email.
16. Click **Save**.

Audio

Add audio to your recording

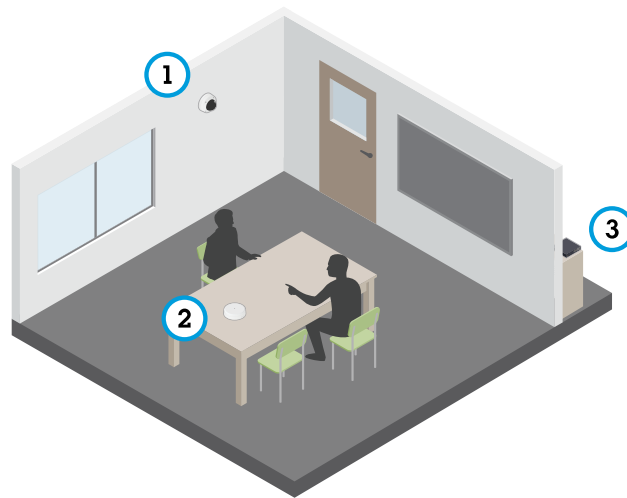
1. Go to **Video > Stream > Audio** and include audio.
2. If the device has more than one input source, select the correct one in **Source**.
3. Go to **Audio > Device settings** and turn on the correct input source.
4. If you make any changes to the input source, click **Apply changes**.
5. Edit the stream profile that is used for the recording:
 - 5.1 Go to **System > Stream profiles** and select the stream profile.
 - 5.2 Select **Include audio** and turn it on.
 - 5.3 Click **Save**.

Add audio capability to your product

With the AXIS T61 Audio and I/O Interface products, you can add audio capability to your product. Use the setup in, for example, interview rooms. You can place the Axis network video product on the wall or ceiling to give good visual coverage, and the AXIS T61 Audio and I/O Interface on or above the interview table.

AXIS M30 Network Camera Series

Configure your device



Interview room with AXIS T61 Series setup.

- 1 Axis network video device
- 2 AXIS T61 Audio and I/O Interface
- 3 PoE switch

To add audio capability to your Axis network video device, connect the AXIS T61 Audio and I/O Interface between your device and the PoE switch which provides power.

1. Connect the Axis network video device (1) and the AXIS T61 Audio and I/O Interface (2) with a PoE cable.
2. Connect the AXIS T61 Audio and I/O Interface (2) and the PoE switch (3) with a PoE cable.



Once the devices are connected, an audio tab becomes visible in the settings for your Axis network video device. Go to the audio tab and turn on **Allow audio**.

See T61 user manual for further instructions.

AXIS M30 Network Camera Series

The device interface

The device interface

To reach the device interface, type the device's IP address in a web browser.

Note

Support for the features and settings described in this section varies between devices.



Show or hide the main menu.



Access the product help.



Change the language.



Set light theme or dark theme.



The user menu contains:

- Information about the user who is logged in.
- Change user** : Log out the current user and log in a new user.
- Log out** : Log out the current user.



The context menu contains:

- Analytics data**: Accept to share non-personal browser data.
- Feedback**: Share any feedback to help us improve your user experience.
- Legal**: View information about cookies and licenses.
- About**: View device information, including firmware version and serial number.
- Legacy device interface**: Change the device interface to the legacy device interface.

Status

NTP sync

Shows NTP synchronization information, including if the device is in sync with an NTP server and the time remaining until the next sync.

NTP settings: Click to go to the Date and time page where you can change the NTP settings.

Device info

Shows device information, including firmware version and serial number.

Upgrade firmware: Click to go to the Maintenance page where you can do a firmware upgrade.

AXIS M30 Network Camera Series

The device interface

Video



Click to play the live video stream.



Click to freeze the live video stream.



Click to take a snapshot of the live video stream. The file is saved in the 'Downloads' folder on your computer. The image file name is [snapshot_YYYY_MM_DD_HH_MM_SS.jpg]. The size of the snapshot depends on the compression that is applied from the specific web-browser engine where the snapshot is received, therefore, the snapshot size may vary from the actual compression setting that is configured in the device.



Click to show I/O output ports. Use the switch to open or close the circuit of a port, for example to test external devices.



Click to manually turn on or turn off the IR illumination.



Click to access onscreen controls:

- **Predefined controls:** Turn on to use the available onscreen controls.



- **Custom controls:** Click  Add custom control to add an onscreen control.



Click to manually turn on the heater for a selected period of time.



Click to start a continuous recording of the live video stream. Click again to stop the recording. If a recording is ongoing, it will resume automatically after a reboot.



Click to show the storage that is configured for the device. To configure the storage you need to be logged in as an administrator.



Click to access more settings:

- **Video format:** Select the encoding format to use in the live view.
- **Client stream information:** Turn on to show dynamic information about the video stream used by the browser that shows the live video stream. The bitrate information differs from the information shown in a text overlay, because of different information sources. The bitrate in the client stream information is the bitrate of the last second, and it comes from the encoding driver of the device. The bitrate in the overlay is the average bitrate of the last 5 seconds, and it comes from the browser. Both values cover only the raw video stream and not the additional bandwidth generated when it's transported over the network through UDP/TCP/HTTP.
- **Adaptive stream:** Turn on to adapt the image resolution to the viewing client's actual display resolution, to improve the user experience and help prevent a possible overload of the client's hardware. The adaptive stream is only applied when you view the live video stream in the web interface in a browser. When adaptive stream is turned on, the maximum frame rate is 30 fps. If you take a snapshot while adaptive stream is turned on, it will use the image resolution selected by the adaptive stream.
- **Level grid:** Click  to show the level grid. The grid helps you decide if the image is horizontally aligned. Click  to hide it.
- **Pixel counter:** Click  to show the pixel counter. Drag and resize the box to contain your area of interest. You can also define the pixel size of the box in the **Width** and **Height** fields.

AXIS M30 Network Camera Series

The device interface

- Refresh: Click  to refresh the still image in the live view.

1:1

Click to show the live view at full resolution. If the full resolution is larger than your screen size, use the smaller image to navigate in the image.



Click to show the live video stream in full screen. Press ESC to exit full screen mode.

Installation

Capture mode  : A capture mode is a preset configuration that defines how the camera captures images. When you change the capture mode, it can affect many other settings, such as view areas and privacy masks.

Mounting position  : The orientation of the image can change depending on how the camera is mounted.

Power line frequency: Select the frequency that is used in your region to minimize image flicker. The American regions usually use 60 Hz. The rest of the world mostly uses 50 Hz. If you're not sure of your region's power line frequency, check with the local authorities.

Rotate: Select the preferred image orientation.

Image

Appearance

Scene profile  : Select a scene profile that suits your surveillance scenario. A scene profile optimizes image settings, including color level, brightness, sharpness, contrast, and local contrast, for a specific environment or purpose.

- Forensic: Suitable for surveillance purposes.
- Indoor  : Suitable for indoor environments.
- Outdoor  : Suitable for outdoor environments.
- Vivid: Useful for demonstration purposes.
- Traffic overview: Suitable for vehicle traffic monitoring.

Saturation: Use the slider to adjust the color intensity. You can for example get a grayscale image.



Contrast: Use the slider to adjust the difference between light and dark.

AXIS M30 Network Camera Series

The device interface



Brightness: Use the slider to adjust the light intensity. This can make objects easier to see. Brightness is applied after image capture, and doesn't affect the information in the image. To get more details from a dark area, it's usually better to increase gain or exposure time.



Sharpness: Use the slider to make objects in the image appear sharper by adjusting the edge contrast. If you increase the sharpness, it may increase the bitrate and the amount of storage space needed as well.



Wide dynamic range

WDR: Turn on to make both bright and dark areas of the image visible.

Local contrast ⓘ : Use the slider to adjust the contrast of the image. A higher value makes the contrast higher between dark and light areas.

Tone mapping ⓘ : Use the slider to adjust the amount of tone mapping that is applied to the image. If the value is set to zero only the standard gamma correction is applied, while a higher value increases the visibility of the darkest and brightest parts in the image.

White balance

AXIS M30 Network Camera Series

The device interface

When the camera detects the color temperature of the incoming light, it can adjust the image to make the colors look more natural. If this is not sufficient, you can select a suitable light source from the list.

The automatic white balance setting reduces the risk of color flicker by adapting to changes gradually. If the lighting changes, or when the camera is first started, it can take up to 30 seconds to adapt to the new light source. If there is more than one type of light source in a scene, that is they differ in color temperature, the dominating light source acts as a reference for the automatic white balance algorithm. This behavior can be overridden by choosing a fixed white balance setting that matches the light source you want to use as a reference.

Light environment:

- **Automatic:** Automatic identification and compensation for the light source color. This is the recommended setting which can be used in most situations.
- **Automatic – outdoors**  : Automatic identification and compensation for the light source color. This is the recommended setting which can be used in most outdoor situations.
- **Custom – indoors**  : Fixed color adjustment for a room with some artificial light other than fluorescent lighting and good for a normal color temperature around 2800 K.
- **Custom – outdoors**  : Fixed color adjustment for sunny weather conditions with a color temperature around 5500 K.
- **Fixed – fluorescent 1:** Fixed color adjustment for fluorescent lighting with a color temperature around 4000 K.
- **Fixed – fluorescent 2:** Fixed color adjustment for fluorescent lighting with a color temperature around 3000 K.
- **Fixed – indoors:** Fixed color adjustment for a room with some artificial light other than fluorescent lighting and good for a normal color temperature around 2800 K.
- **Fixed – outdoors 1:** Fixed color adjustment for sunny weather conditions with a color temperature around 5500 K.
- **Fixed – outdoors 2:** Fixed color adjustment for cloudy weather condition with a color temperature around 6500 K.
- **Street light – mercury**  : Fixed color adjustment for ultraviolet emission in mercury vapor lights common in street lighting.
- **Street light – sodium**  : Fixed color adjustment that compensates for the yellow orange color of sodium vapor lights common in street lighting.
- **Hold current:** Keep the current settings and do not compensate for light changes.
- **Manual**  : Fix the white balance with the help of a white object. Drag the circle to an object that you want the camera to interpret as white in the live view image. Use the **Red balance** and **Blue balance** sliders to adjust the white balance manually.

Day-night mode

IR-cut filter:

- **Auto:** Select to automatically turn on and off the IR-cut filter. When the camera is in day mode, the IR-cut filter is turned on and blocks incoming infrared light, and when in night mode, the IR-cut filter is turned off and the camera's light sensitivity increases.
- **On:** Select to turn on the IR-cut filter. The image is in color, but with reduced light sensitivity.
- **Off:** Select to turn off the IR-cut filter. The image is in black and white for increased light sensitivity.

Threshold: Use the slider to adjust the light threshold where the camera changes from day mode to night mode.

- Move the slider towards **Bright** to decrease the threshold for the IR-cut filter. The camera changes to night mode earlier.
- Move the slider towards **Dark** to increase the threshold for the IR-cut filter. The camera changes to night mode later.

IR light

If your device doesn't have built-in illumination, these controls are only available when you have connected a supporting Axis accessory.

Allow illumination: Turn on to let the camera use the built-in light in night mode.

AXIS M30 Network Camera Series

The device interface

Synchronize illumination: Turn on to automatically synchronize the illumination with the surrounding light. The synchronization between day and night only works if the IR-cut filter is set to **Auto** or **Off**.

Automatic illumination angle ⓘ : Turn on to use the automatic illumination angle.

Illumination angle ⓘ : Use the slider to manually set the illumination angle, for example if the angle needs to be different from the camera's angle of view. If the camera has a wide angle of view, you can set the illumination angle to a narrower angle, which equals a greater tele position. This will result in dark corners in the image.

IR wavelength ⓘ : Select the desired wavelength for the IR light.

White light ⓘ

Allow illumination ⓘ : Turn on to let the camera use white light in night mode.

Synchronize illumination ⓘ : Turn on to automatically synchronize the white light with the surrounding light.

Exposure

Exposure mode: Select an exposure mode to reduce rapidly changing irregular effects in the image, for example flicker produced by different types of light sources. We recommend you to use the automatic exposure mode, or the same frequency as your power network.

- **Automatic:** The camera adjusts the aperture, gain and shutter automatically.
- **Automatic aperture** ⓘ : The camera adjusts the aperture and gain automatically. The shutter is fixed.
- **Automatic shutter** ⓘ : The camera adjusts the shutter and gain automatically. The aperture is fixed.
- **Hold current:** Locks the current exposure settings.
- **Flicker-free** ⓘ : The camera adjusts the aperture and gain automatically, and uses only the following shutter speeds: 1/50 s (50 Hz) and 1/60 s (60 Hz).
- **Flicker-free 50 Hz** ⓘ : The camera adjusts the aperture and gain automatically, and uses the shutter speed 1/50 s.
- **Flicker-free 60 Hz** ⓘ : The camera adjusts the aperture and gain automatically, and uses the shutter speed 1/60 s.
- **Flicker-reduced** ⓘ : This is the same as flicker-free, but the camera might use shutter speeds faster than 1/100 s (50 Hz) and 1/120 s (60 Hz) for brighter scenes.
- **Flicker-reduced 50 Hz** ⓘ : This is the same as flicker-free, but the camera might use shutter speeds faster than 1/100 s for brighter scenes.
- **Flicker-reduced 60 Hz** ⓘ : This is the same as flicker-free, but the camera might use shutter speeds faster than 1/120 s for brighter scenes.
- **Manual** ⓘ : The aperture, gain and shutter are fixed.

Exposure zone: Use exposure zones to optimize the exposure in a selected part of the scene, for example, the area in front of an entrance door.

AXIS M30 Network Camera Series

The device interface

Note

The exposure zones are related to the original image (unrotated), and the names of the zones apply to the original image. This means, for example, that if the video stream is rotated 90°, then the **Upper** zone becomes the **Right** zone in the stream, and **Left** becomes **Lower**.

- **Automatic:** Suitable for most situations.
- **Center:** Uses a fixed area in the center of the image to calculate the exposure. The area has a fixed size and position in the live view.
- **Full** ⓘ : Uses the entire live view to calculate the exposure.
- **Upper** ⓘ : Uses an area with a fixed size and position in the upper part of the image to calculate the exposure.
- **Lower** ⓘ : Uses an area with a fixed size and position in the lower part of the image to calculate the exposure.
- **Left** ⓘ : Uses an area with a fixed size and position in the left part of the image to calculate the exposure.
- **Right** ⓘ : Uses an area with a fixed size and position in the right part of the image to calculate the exposure.
- **Spot:** Uses an area with a fixed size and position in the live view to calculate the exposure.
- **Custom:** Uses an area in the live view to calculate the exposure. You can adjust the size and position of the area.

Max shutter: Select the shutter speed to provide the best image. Low shutter speeds (longer exposure) might cause motion blur when there is movement, and a too high shutter speed might affect the image quality. Max shutter works with max gain to improve the image.

Max gain: Select the suitable max gain. If you increase the max gain, it improves the visible level of detail in dark images, but also increases the noise level. More noise can also result in increased use of bandwidth and storage. If you set the max gain to a high value, images can differ a lot if the light conditions are very different from day to night. Max gain works with max shutter to improve the image.

Motion-adaptive exposure ⓘ : Select to reduce motion blur in low-light conditions.

Blur-noise trade-off: Use the slider to adjust the priority between motion blur and noise. If you want to prioritize low bandwidth and have less noise at the expense of details in moving objects, move the slider towards **Low noise**. If you want to prioritize the preservation of details in moving objects at the expense of noise and bandwidth, move the slider towards **Low motion blur**.

Note

You can change the exposure either by adjusting the exposure time or by adjusting the gain. If you increase the exposure time, it results in more motion blur, and if you increase the gain it results in more noise. If you adjust the **Blur-noise trade-off** towards **Low noise**, the automatic exposure will prioritize longer exposure times over increasing gain, and the opposite if you adjust the trade-off towards **Low motion blur**. Both the gain and exposure time will eventually reach their maximum values in low-light conditions, regardless of the priority set.

Lock aperture ⓘ : Turn on to keep the aperture size set by the **Aperture** slider. Turn off to allow the camera to automatically adjust the aperture size. You can, for example, lock the aperture for scenes with permanent light conditions.

Aperture ⓘ : Use the slider to adjust the aperture size, that is, how much light passes through the lens. To allow more light to enter the sensor and thereby produce a brighter image in low-light conditions, move the slider towards **Open**. An open aperture also reduces the depth of field, which means that objects close to or far from the camera can appear unfocused. To allow more of the image to be in focus, move the slider towards **Closed**.

Exposure level: Use the slider to adjust the image exposure.

Defog ⓘ : Turn on to detect the effects of foggy weather and automatically remove them for a clearer image.

AXIS M30 Network Camera Series

The device interface

Note

We recommend you not to turn on **Defog** in scenes with low contrast, large light level variations, or when the autofocus is slightly off. This can affect the image quality, for example, by increasing the contrast. Furthermore, too much light can negatively impact the image quality when defog is active.

Stream

General

Resolution: Select the image resolution suitable for the surveillance scene. A higher resolution increases bandwidth and storage.

Frame rate: To avoid bandwidth problems on the network or reduce storage size, you can limit the frame rate to a fixed amount. If you leave the frame rate at zero, the frame rate is kept at the highest possible rate under the current conditions. A higher frame rate requires more bandwidth and storage capacity.

Compression: Use the slider to adjust the image compression. High compression results in a lower bitrate and lower image quality. Low compression improves the image quality, but uses more bandwidth and storage when you record.

Signed video  : Turn on to add the signed video feature to the video. Signed video protects the video from tampering by adding cryptographic signatures to the video.

H.26x encoding

Zipstream: A bitrate reduction technology, optimized for video surveillance, that reduces the average bitrate in an H.264 or H.265 stream in real time. Axis Zipstream applies a high bitrate in scenes where there are multiple regions of interest, for example in scenes with moving objects. When the scene is more static, Zipstream applies a lower bitrate, and thereby reduces the required storage. To learn more, see *Reducing the bit rate with Axis Zipstream*

Select the desired level of bitrate reduction:

- **Off:** No bitrate reduction.
- **Low:** No visible quality degradation in most scenes. This is the default option and it can be used in all types of scenes to reduce the bitrate.
- **Medium:** Visible effects in some scenes through less noise and a slightly lower level of detail in regions of lower interest, for example where there's no movement.
- **High:** Visible effects in some scenes through less noise and a lower level of detail in regions of lower interest, for example where there's no movement. We recommend this level for cloud-connected devices and devices that use local storage.
- **Higher:** Visible effects in some scenes through less noise and a lower level of detail in regions of lower interest, for example where there's no movement.
- **Extreme:** Visible effects in most scenes. The bitrate is optimized for smallest possible storage.

Dynamic FPS (frames per second): Turn on to allow the bandwidth to vary based on the level of activity in the scene. More activity requires more bandwidth.

Lower limit  : Enter a value to adjust the frame rate between minimal fps and the stream default fps based on scene motion. We recommend you to use lower limit in scenes with very little motion, where the fps could drop to 1 or lower.

Dynamic GOP (Group of Pictures): Turn on to dynamically adjust the interval between I-frames based on the level of activity in the scene.

Upper limit  : Enter a maximum GOP length, that is, the maximum number of P-frames between two I-frames. An I-frame is a self-contained image frame that has no dependency on other frames.

P-frames: A P-frame is a predicted image that shows only the changes in the image from the previous frame. Enter the desired number of P-frames. The higher the number, the less bandwidth is required. However, if there are network congestion, there could be a noticeable deterioration in the video quality.

AXIS M30 Network Camera Series

The device interface

Bitrate control:

- **Average:** Select to automatically adjust the bitrate over a longer time period and provide the best possible image quality based on the available storage.
 -  Click to calculate the target bitrate based on available storage, retention time, and bitrate limit.
 - **Target bitrate:** Enter desired target bitrate.
 - **Retention time:** Enter the number of days to keep the recordings.
 - **Storage:** Shows the estimated storage that can be used for the stream.
 - **Maximum bitrate:** Turn on to set a bitrate limit.
 - **Bitrate limit**  : Enter a bitrate limit that is higher than the target bitrate.
- **Maximum:** Select to set a maximum instant bitrate of the stream based on your network bandwidth.
 - **Maximum:** Enter the maximum bitrate.
- **Variable:** Select to allow the bitrate to vary based on the level of activity in the scene. More activity requires more bandwidth. We recommend this option for most situations.

Orientation

Rotate  : Rotate the image to match your requirements.

Mirror: Turn on to mirror the image.

Audio

Include: Turn on to use audio in the video stream.

Source  : Select what audio source to use.

Stereo  : Turn on to include built-in audio as well as audio from an external microphone.

Overlays

+ : Click to add an overlay. Select the type of overlay from the dropdown list:

- **Text:** Select to show a text that is integrated in the live view image and visible in all views, recordings and snapshots. You can enter your own text, and you can also include pre-configured modifiers to automatically show for example time, date, frame rate.
 -  : Click to add the date modifier %F to show yyyy-mm-dd.
 -  : Click to add the time modifier %X to show hh:mm:ss (24-hour clock).
 - **Modifiers:** Click to select any of the modifiers shown in the list to add them to the text box. For example, %a shows the day of the week.
 - **Size:** Select the desired font size.
 - **Appearance:** Select the text color and background color, for example, white text on a black background (default).
 -  : Select the position of the overlay in the image.
- **Image:** Select to show a static image superimposed over the video stream. You can use .bmp, .png, .jpeg, or .svg files. To upload an image, click **Images**. Before you upload an image, you can choose to:
 - **Scale with resolution:** Select to automatically scale the overlay image to fit the video resolution.

AXIS M30 Network Camera Series

The device interface

- **Use transparency:** Select and enter the RGB hexadecimal value for that color. Use the format RRGGBB. Examples of hexadecimal values: FFFFFFFF for white, 000000 for black, FF0000 for red, 6633FF for blue, and 669900 for green. Only for .bmp images.
- **Streaming indicator**  : Select to show an animation superimposed over the video stream. The animation indicates that the video stream is live, even if the scene doesn't contain any motion.
 - **Appearance:** Select the animation color and background color, for example, red animation on a transparent background (default).
 - **Size:** Select the desired font size.
 - : Select the position of the overlay in the image.

View areas



: Click to create a view area.



Click the view area to access settings.

Name: Enter a name for the view area. The maximum length is 64 characters.

Aspect ratio: Select desired aspect ratio. The resolution adjusts automatically.

PTZ: Turn on to use pan, tilt, and zoom functionality in the view area.

Privacy masks



: Click to create a new privacy mask. The maximum number of masks depend on the complexity of all masks combined. Each mask can have maximum 10 anchor points.

Privacy masks: Click to change the color of all privacy masks, or to delete all privacy masks permanently.



Mask x: Click to rename, disable, or permanently delete the mask.

Audio

Device settings

Input: Turn on or off audio input. Shows the type of input.

Allow stream extraction



: Turn on to allow stream extraction.

Input type



: Select the type of input, for instance if it's internal microphone or line-in.

Power type



: Select power type for your input.

Apply changes



: Click to apply your selection.

Separate gain controls



: Turn on to adjust the gain separately for the different input types.

AXIS M30 Network Camera Series

The device interface

Automatic gain control  : Turn on to dynamically adapt the gain to changes in the sound.

Gain: Use the slider to change the gain. Click the microphone icon to mute or unmute.

Output  : Shows the type of output.

Gain: Use the slider to change the gain. Click the speaker icon to mute or unmute.

Stream

Encoding: Select the encoding to use for the input source streaming. You can only choose encoding if audio input is turned on. If audio input is turned off, click **Enable audio input** to turn it on.

Audio clips

 **Add clip:** Click to add a new audio clip. You can use .au, .mp3, .opus, .vorbis, .wav files.

 **Click to play the audio clip.**

 **Click to stop playing the audio clip.**

 **The context menu contains:**

- **Rename:** Change the name of the audio clip.
- **Create link:** Create a URL which, when used, plays the audio clip on the device. Specify the volume and number of times to play the clip.
- **Download:** Download the audio clip to your computer.
- **Delete:** Delete the audio clip from the device.

Recordings

 **Click to filter the recordings.**

From: Show recordings done after a certain point in time.

To: Show recordings up until a certain point in time.

Source  : Show recordings based on source.

Event: Show recordings based on events.

Storage: Show recordings based on storage type.

AXIS M30 Network Camera Series

The device interface

Ongoing recordings: Show all ongoing recordings on the camera.

Select to start a recording on the camera.

Choose which storage device to save to.



Select to stop a recording on the camera.

Triggered recordings will end both when manually stopped and when the camera is shut down.

Continuous recordings will continue until manually stopped. Even if the camera is shut down, the recording will continue when the camera starts up again.



Click to play the recording.

Click to stop playing the recording.

Click to show more information and options about the recording.

Set export range: If you only want to export part of the recording, enter from when to when.



Click to delete the recording.

Export: Click to export (part of) the recording.

Apps

Add app: Click to install a new app.

Find more apps: Click to go to an overview page of Axis apps.



The context menu contains:

- **App log:** Click to view a log of the app events. The log is helpful when you contact support.
- **Activate license with a key:** If the app requires a license, you need to activate it. Use this option if your device doesn't have internet access.
If you don't have a license key, go to axis.com/applications. You need a license code and the Axis product serial number to generate a license key.
- **Activate license automatically:** If the app requires a license, you need to activate it. Use this option if your device has internet access. You need a license code to activate the license.
- **Deactivate the license:** Deactivate the license to use it in another device. If you deactivate the license, you also remove it from the device. To deactivate the license requires internet access.
- **Settings**  : Configure the parameters.
- **Delete:** Delete the app permanently from the device. If you don't deactivate the license first, it remains active.

Note

The device's performance might be affected if you run several apps at the same time.

Start: Start or stop the app.

Open: Click to access the app's settings. The available settings depend on the application. Some applications don't have any settings.

AXIS M30 Network Camera Series

The device interface

System

Date and time

The time format depends on the web browser's language settings.

Note

We recommend you to synchronize the device's date and time with an NTP server.

Synchronization: Select an option for synchronizing the device's date and time.

- **Automatic date and time (manual NTS KE servers):** Synchronize with the secure NTP key establishment servers connected to the DHCP server.
 - **Manual NTS KE servers:** Enter the IP address of one or two NTP servers. When you use two NTP servers, the device synchronizes and adapts its time based on input from both.
- **Automatic date and time (NTP servers using DHCP):** Synchronize with the NTP servers connected to the DHCP server.
 - **Fallback NTP servers:** Enter the IP address of one or two fallback servers.
- **Automatic date and time (manual NTP servers):** Synchronize with NTP servers of your choice.
 - **Manual NTP servers:** Enter the IP address of one or two NTP servers. When you use two NTP servers, the device synchronizes and adapts its time based on input from both.
- **Custom date and time:** Manually set the date and time. Click **Get from system** to fetch the date and time settings once from your computer or mobile device.

Time zone: Select which time zone to use. Time will be automatically adjusted for daylight saving time and standard time.

Note

The system uses the date and time settings in all recordings, logs and system settings.

Network

IPv4

Assign IPv4 automatically: Select to let the network router assign an IP address to the device automatically. We recommend automatic IP (DHCP) for most networks.

IP address: Enter a unique IP address for the device. Static IP addresses can be assigned at random within isolated networks, provided that each address is unique. To avoid conflicts, we recommend you to contact your network administrator before you assign a static IP address.

Subnet mask: Enter the subnet mask to define what addresses are inside the local area network. Any address outside the local area network goes through the router.

Router: Enter the IP address of the default router (gateway) used to connect devices that are attached to different networks and network segments.

IPv6

Assign IPv6 automatically: Select to turn on IPv6 and to let the network router assign an IP address to the device automatically.

Hostname

Assign hostname automatically: Select to let the network router assign a hostname to the device automatically.

Hostname: Enter the hostname manually to use as an alternative way of accessing the device. The Hostname is used in the server report and in the system log. Allowed characters are A-Z, a-z, 0-9 and -.

DNS servers

AXIS M30 Network Camera Series

The device interface

Assign DNS automatically: Select to let the network router assign search domains and DNS server addresses to the device automatically. We recommend automatic DNS (DHCP) for most networks.

Search domains: When you use a hostname that is not fully qualified, click **Add search domain** and enter a domain in which to search for the hostname used by the device.

DNS servers: Click **Add DNS server** and enter the IP address of the DNS server. This provides the translation of hostnames to IP addresses on your network.

HTTP and HTTPS

Allow access through: Select if a user is allowed to connect to the device through the HTTP, HTTPS, or both HTTP and HTTPS protocols.

HTTPS is a protocol that provides encryption for page requests from users and for the pages returned by the web server. The encrypted exchange of information is governed by the use of an HTTPS certificate, which guarantees the authenticity of the server.

To use HTTPS on the device, you must install an HTTPS certificate. Go to **System > Security** to create and install certificates.

Note

If you view encrypted web pages through HTTPS, you might experience a drop in performance, especially when you request a page for the first time.

HTTP port: Enter the HTTP port to use. Port 80 or any port in the range 1024–65535 are allowed. If you are logged in as an administrator, you can also enter any port in the range 1–1023. If you use a port in this range, you get a warning.

HTTPS port: Enter the HTTPS port to use. Port 443 or any port in the range 1024–65535 are allowed. If you are logged in as an administrator, you can also enter any port in the range 1–1023. If you use a port in this range, you get a warning.

Certificate: Select a certificate to enable HTTPS for the device.

Network discovery protocols

Bonjour®: Turn on to allow automatic discovery on the network.

Bonjour name: Enter a friendly name to be visible on the network. The default name is the device name and MAC address.

UPnP®: Turn on to allow automatic discovery on the network.

UPnP name: Enter a friendly name to be visible on the network. The default name is the device name and MAC address.

WS-Discovery: Turn on to allow automatic discovery on the network.

One-click cloud connection

One-click cloud connection (O3C) together with an O3C service provides easy and secure internet access to live and recorded video from any location. For more information, see axis.com/end-to-end-solutions/hosted-services.

Allow O3C:

- **One-click:** The default setting. Press and hold the control button on the device to connect to an O3C service over the internet. You need to register the device with the O3C service within 24 hours after you press the control button. Otherwise, the device disconnects from the O3C service. Once you have registered the device, **Always** is enabled and the device stays connected to the O3C service.
- **Always:** The device constantly attempts to connect to an O3C service over the internet. Once you have registered the device, it stays connected to the O3C service. Use this option if the control button on the device is out of reach.
- **No:** Disables the O3C service.

Proxy settings: If needed, enter the proxy settings to connect to the proxy server.

Host: Enter the proxy server's address.

AXIS M30 Network Camera Series

The device interface

Port: Enter the port number used for access.

Login and Password: If needed, enter username and password for the proxy server.

Authentication method:

- **Basic:** This method is the most compatible authentication scheme for HTTP. It's less secure than the **Digest** method because it sends the username and password unencrypted to the server.
- **Digest:** This method is more secure because it always transfers the password encrypted across the network.
- **Auto:** This option lets the device select the authentication method depending on the supported methods. It prioritizes the **Digest** method over the **Basic** method.

Owner authentication key (OAK): Click **Get key** to fetch the owner authentication key. This is only possible if the device is connected to the internet without a firewall or proxy.

SNMP

The Simple Network Management Protocol (SNMP) allows remote management of network devices.

SNMP: Select the version of SNMP to use.

- **v1 and v2c:**
 - **Read community:** Enter the community name that has read-only access to all supported SNMP objects. The default value is **public**.
 - **Write community:** Enter the community name that has read/write access to all supported SNMP objects (except read-only objects). The default value is **write**.
 - **Activate traps:** Turn on to activate trap reporting. The device uses traps to send messages for important events or status changes to a management system. In the device interface, you can set up traps for SNMP v1 and v2c. Traps are automatically turned off if you change to SNMP v3 or turn off SNMP. If you use SNMP v3, you can set up traps through the SNMP v3 management application.
 - **Trap address:** Enter the IP address or host name of the management server.
 - **Trap community:** Enter the community to use when the device sends a trap message to the management system.
 - **Traps:**
 - **Cold start:** Sends a trap message when the device starts.
 - **Warm start:** Sends a trap message when you change an SNMP setting.
 - **Link up:** Sends a trap message when a link changes from down to up.
 - **Authentication failed:** Sends a trap message when an authentication attempt fails.

Note

All Axis Video MIB traps are enabled when you turn on SNMP v1 and v2c traps. For more information, see *AXIS OS Portal > SNMP*.

- **v3:** SNMP v3 is a more secure version, which provides encryption and secure passwords. To use SNMP v3, we recommend you to activate HTTPS, as the password is then sent through HTTPS. This also prevents unauthorized parties to access unencrypted SNMP v1 and v2c traps. If you use SNMP v3, you can set up traps through the SNMP v3 management application.
 - **Password for the account "initial":** Enter the SNMP password for the account named "initial". Although the password can be sent without activating HTTPS, we don't recommend it. The SNMP v3 password can only be set once, and preferably only when HTTPS is enabled. Once the password is set, the password field is no longer displayed. To set the password again, you must reset the device to factory default settings.

Connected clients

The list shows all clients that are connected to the device.

Update: Click to refresh the list.

Security

Certificates

AXIS M30 Network Camera Series

The device interface

Certificates are used to authenticate devices on a network. The device supports two types of certificates:

- **Client/server certificates**
A client/server certificate validates the device's identity, and can be self-signed or issued by a Certificate Authority (CA). A self-signed certificate offers limited protection and can be used before a CA-issued certificate has been obtained.
- **CA certificates**
You can use a CA certificate to authenticate a peer certificate, for example to validate the identity of an authentication server when the device connects to a network protected by IEEE 802.1X. The device has several pre-installed CA certificates.

These formats are supported:

- Certificate formats: .PEM, .CER, and .PFX
- Private key formats: PKCS#1 and PKCS#12

Important

If you reset the device to factory default, all certificates are deleted. Any pre-installed CA certificates are reinstalled.



Filter the certificates in the list.



Add certificate : Click to add a certificate.



The context menu contains:

- **Certificate information:** View an installed certificate's properties.
- **Delete certificate:** Delete the certificate.
- **Create certificate signing request:** Create a certificate signing request to send to a registration authority to apply for a digital identity certificate.

IEEE 802.1x

IEEE 802.1x is an IEEE standard for port-based network admission control providing secure authentication of wired and wireless network devices. IEEE 802.1x is based on EAP (Extensible Authentication Protocol).

To access a network protected by IEEE 802.1x, network devices must authenticate themselves. The authentication is performed by an authentication server, typically a RADIUS server (for example FreeRADIUS and Microsoft Internet Authentication Server).

Certificates

When configured without a CA certificate, server certificate validation is disabled and the device tries to authenticate itself regardless of what network it is connected to.

When using a certificate, in Axis' implementation, the device and the authentication server authenticate themselves with digital certificates using EAP-TLS (Extensible Authentication Protocol - Transport Layer Security).

To allow the device to access a network protected through certificates, a signed client certificate must be installed on the device.

Client certificate: Select a client certificate to use IEEE 802.1x. The authentication server uses the certificate to validate the client's identity.

CA certificate: Select a CA certificate to validate the authentication server's identity. When no certificate is selected, the device tries to authenticate itself regardless of what network it is connected to.

EAP identity: Enter the user identity associated with the client certificate.

EAPOL version: Select the EAPOL version that is used in the network switch.

Use IEEE 802.1x: Select to use the IEEE 802.1x protocol.

Prevent brute-force attacks

AXIS M30 Network Camera Series

The device interface

Blocking: Turn on to block brute-force attacks. A brute-force attack uses trial-and-error to guess login info or encryption keys.

Blocking period: Enter the number of seconds to block a brute-force attack.

Blocking conditions: Enter the number of authentication failures allowed per second before the block starts. You can set the number of failures allowed both on page level and device level.

IP address filter

Use filter: Select to filter which IP addresses that are allowed to access the device.

Policy: Choose whether to **Allow** access or **Deny** access for certain IP addresses.

Addresses: Enter the IP numbers that are either allowed or denied access to the device. You can also use the CIDR format.

Custom-signed firmware certificate

To install test firmware or other custom firmware from Axis on the device, you need a custom-signed firmware certificate. The certificate verifies that the firmware is approved by both the device owner and Axis. The firmware can only run on a specific device which is identified by its unique serial number and chip ID. Custom-signed firmware certificates can only be created by Axis, since Axis holds the key to sign them.

Click **Install** to install the certificate. You need to install the certificate before you install the firmware.

Users



Add user: Click to add a new user. You can add up to 100 users.

Username: Enter a unique username.

New password: Enter a password for the user. Passwords must be 1 to 64 characters long. Only ASCII printable characters (code 32 to 126) are allowed in the password, for example letters, numbers, punctuation, and some symbols.

Repeat password: Enter the same password again.

Role:

- **Administrator:** Has full access to all settings. Administrators can also add, update, and remove other users.
- **Operator:** Has access to all settings except:
 - All **System** settings.
 - Adding apps.
- **Viewer:** Has access to:
 - Watch and take snapshots of a video stream.
 - Watch and export recordings.
 - With PTZ user access: pan, tilt, and zoom.



The context menu contains:

Update user: Edit the user's properties.

Delete user: Delete the user. You can't delete the root user.

Anonymous users

Allow anonymous viewers: Turn on to allow anyone to access the device as a viewer without having to log in with a user account.

Allow anonymous PTZ operators: Turn on to allow anonymous users to pan, tilt, and zoom the image.

AXIS M30 Network Camera Series

The device interface

Events

Rules

A rule defines the conditions that must be met for the product to perform an action. The list shows all the currently configured rules in the product.

Note

You can create up to 256 action rules.



Add a rule: Click to create a rule.

Name: Enter a name for the rule.

Wait between actions: Enter the minimum time (hh:mm:ss) that must pass between rule activations. It is useful if the rule is activated by for example day-night mode conditions, to avoid that small light changes during sunrise and sunset activate the rule repeatedly.

Condition: Select a condition from the list. A condition must be met for the device to perform an action. If multiple conditions are defined, all of them must be met to trigger the action. For information about specific conditions, see *Get started with rules for events*.

Use this condition as a trigger: Select to make this first condition function only as a starting trigger. It means that once the rule is activated it remains active for as long as all the other conditions are met, no matter the state of the first condition. If you don't select this option, the rule will simply be active whenever all the conditions are met.

Invert this condition: Select if you want the condition to be the opposite of your selection.



Add a condition: Click to add an additional condition.

Action: Select an action from the list and enter its required information. For information about specific actions, see *Get started with rules for events*.

Recipients

You can set up your device to notify recipients about events or send files. The list shows all the recipients currently configured in the product, along with information about their configuration.

Note

You can create up to 20 recipients.



Add a recipient: Click to add a recipient.

Name: Enter a name for the recipient.

Type: Select from the list:

- **FTP**
 - **Host:** Enter the server's IP address or hostname. If you enter a hostname, make sure that a DNS server is specified under **System > Network > IPv4 and IPv6**.
 - **Port:** Enter the port number used by the FTP server. The default is 21.
 - **Folder:** Enter the path to the directory where you want to store files. If this directory doesn't already exist on the FTP server, you will get an error message when uploading files.
 - **Username:** Enter the username for the login.
 - **Password:** Enter the password for the login.

AXIS M30 Network Camera Series

The device interface

- **Use temporary file name:** Select to upload files with temporary, automatically generated filenames. The files get renamed to the desired names when the upload completes. If the upload is aborted/interrupted, you don't get any corrupt files. However, you probably still get the temporary files. This way you know that all files that have the desired name, are correct.
- **Use passive FTP:** Under normal circumstances the product simply requests the target FTP server to open the data connection. The device actively initiates both the FTP control and data connections to the target server. This is normally needed if there is a firewall between the device and the target FTP server.
- **HTTP**
 - **URL:** Enter the network address to the HTTP server and the script that will handle the request. For example: `http://192.168.254.10/cgi-bin/notify.cgi`.
 - **Username:** Enter the username for the login.
 - **Password:** Enter the password for the login.
 - **Proxy:** Turn on and enter the required information if a proxy server must be passed to connect to the HTTP server.
- **HTTPS**
 - **URL:** Enter the network address to the HTTPS server and the script that will handle the request. For example: `https://192.168.254.10/cgi-bin/notify.cgi`.
 - **Validate server certificate:** Select to validate the certificate that was created by HTTPS server.
 - **Username:** Enter the username for the login.
 - **Password:** Enter the password for the login.
 - **Proxy:** Turn on and enter the required information if a proxy server must be passed to connect to the HTTPS server.
- **Network storage**

You can add network storage such as a NAS (Network Attached Storage) and use it as a recipient to store files. The files are stored in the Matroska (MKV) file format.

 - **Host:** Enter the IP address or hostname for the network storage.
 - **Share:** Enter the name of the share on the host.
 - **Folder:** Enter the path to the directory where you want to store files.
 - **Username:** Enter the username for the login.
 - **Password:** Enter the password for the login.
- **SFTP**
 - **Host:** Enter the server's IP address or hostname. If you enter a hostname, make sure that a DNS server is specified under **System > Network > IPv4 and IPv6**.
 - **Port:** Enter the port number used by the SFTP server. The default is 22.
 - **Folder:** Enter the path to the directory where you want to store files. If this directory doesn't already exist on the SFTP server, you will get an error message when uploading files.
 - **Username:** Enter the username for the login.
 - **Password:** Enter the password for the login.
 - **SSH host public key type (MD5):** Enter the fingerprint of the remote host's public key (a 32-digit hexadecimal string). The SFTP client supports SFTP servers using SSH-2 with RSA, DSA, ECDSA, and ED25519 host key types. RSA is the preferred method during negotiation, followed by ECDSA, ED25519, and DSA. Make sure to enter the right MD5 host key that is used by your SFTP server. While the Axis device supports both MD5 and SHA-256 hash keys, we recommend using SHA-256 due to stronger security over MD5. For more information on how to configure an SFTP server with an Axis device, go to the *AXIS OS Portal*.
 - **SSH host public key type (SHA256):** Enter the fingerprint of the remote host's public key (a 43-digit Base64 encoded string). The SFTP client supports SFTP servers using SSH-2 with RSA, DSA, ECDSA, and ED25519 host key types. RSA is the preferred method during negotiation, followed by ECDSA, ED25519, and DSA. Make sure to enter the right MD5 host key that is used by your SFTP server. While the Axis device supports both MD5 and SHA-256 hash keys, we recommend using SHA-256 due to stronger security over MD5. For more information on how to configure an SFTP server with an Axis device, go to the *AXIS OS Portal*.
 - **Use temporary file name:** Select to upload files with temporary, automatically generated filenames. The files get renamed to the desired names when the upload completes. If the upload is aborted/interrupted, you don't get any corrupt files. However, you probably still get the temporary files. This way you know that all files that have the desired name, are correct.
- **SIP**  :
 - **From SIP account:** Select from the list.
 - **To SIP address:** Enter the SIP address.
- **Email**
 - **Send email to:** Enter the email address to send emails to. To enter multiple addresses, use commas to separate them.
 - **Send email from:** Enter the email address of the sending server.

AXIS M30 Network Camera Series

The device interface

- **Username:** Enter the username for the mail server. Leave this field empty if the mail server does not require authentication.
- **Password:** Enter the password for the mail server. Leave this field empty if the mail server does not require authentication.
- **Email server (SMTP):** Enter the name of the SMTP server, for example smtp.gmail.com, smtp.mail.yahoo.com.
- **Port:** Enter the port number for the SMTP server, using values in the range 0–65535. The default value is 587.
- **Encryption:** To use encryption, select either SSL or TLS.
- **Validate server certificate:** If you use encryption, select to validate the identity of the device. The certificate can be self-signed or issued by a Certificate Authority (CA).
- **POP authentication:** Turn on to enter the name of the POP server, for example pop.gmail.com.

Note

Some email providers have security filters that prevent users from receiving or viewing large amount of attachments, from receiving scheduled emails and similar. Check the email provider's security policy to avoid your email account being locked or missing out on your expected emails.

- **TCP**

- **Host:** Enter the server's IP address or hostname. If you enter a hostname, make sure that a DNS server is specified under **System > Network > IPv4 and IPv6**.
- **Port:** Enter the port number used to access the server.

Test: Click to test the setup.



The context menu contains:

View recipient: Click to view all the recipient details.

Copy recipient: Click to copy a recipient. When you copy, you can make changes to the new recipient.

Delete recipient: Click to delete the recipient permanently.

Schedules

Schedules and pulses can be used as conditions in rules. The list shows all the schedules and pulses currently configured in the product, along with information about their configuration.



Add schedule: Click to create a schedule or pulse.

Manual trigger

The manual trigger is used to manually trigger a rule. The manual trigger can for example be used to validate actions during product installation and configuration.

MQTT

MQTT (Message Queuing Telemetry Transport) is a standard messaging protocol for the Internet of Things (IoT). It was designed for simplified IoT integration and is used in a wide variety of industries to connect remote devices with a small code footprint and minimal network bandwidth. The MQTT client in Axis device firmware can simplify integration of data and events produced in the device to systems which are not video management systems (VMS).

Set up the device as an MQTT client. MQTT communication is based on two entities, the clients and the broker. The clients can send and receive messages. The broker is responsible for routing messages between clients.

You can learn more about MQTT in *AXIS OS Portal*.

MQTT client

AXIS M30 Network Camera Series

The device interface

Connect: Turn on or off the MQTT client.

Status: Shows the current status of the MQTT client.

Broker

Host: Enter the hostname or IP address of the MQTT server.

Protocol: Select which protocol to use.

Port: Enter the port number.

- 1883 is the default value for **MQTT over TCP**
- 8883 is the default value for **MQTT over SSL**
- 80 is the default value for **MQTT over WebSocket**
- 443 is the default value for **MQTT over WebSocket Secure**

Username: Enter the username that the client will use to access the server.

Password: Enter a password for the username.

Client ID: Enter a client ID. The client identifier is sent to the server when the client connects to it.

Clean session: Controls the behavior at connection and disconnection time. When selected, the state information is discarded at connect and disconnect.

Keep alive interval: The keep alive interval enables the client to detect when the server is no longer available without having to wait for the long TCP/IP timeout.

Timeout: The time interval in seconds to allow a connect to complete. Default value: 60

Device topic prefix: Used in the default values for the topic in the connect message and LWT message on the **MQTT client** tab, and in the publication conditions on the **MQTT publication** tab.

Reconnect automatically: Specifies whether the client should reconnect automatically after a disconnect.

Connect message

Specifies if a message should be sent out when a connection is established.

Send message: Turn on to send messages.

Use default: Turn off to enter your own default message.

Topic: Enter the topic for the default message.

Payload: Enter the content for the default message.

Retain: Select to keep the state of client on this Topic

QoS: Change the QoS layer for the packet flow.

Last Will and Testament message

The Last Will Testament (LWT) lets a client provide a testament along with its credentials when connecting to the broker. If the client disconnects ungracefully at some point later (maybe because his power source died), it can let the broker deliver a message to other clients. This LWT message has the same form as an ordinary message and gets routed via the same mechanics.

Send message: Turn on to send messages.

Use default: Turn off to enter your own default message.

Topic: Enter the topic for the default message.

Payload: Enter the content for the default message.

Retain: Select to keep the state of client on this Topic

AXIS M30 Network Camera Series

The device interface

QoS: Change the QoS layer for the packet flow.

MQTT publication

Use default topic prefix: Select to use the default topic prefix, that is defined in the device topic prefix in the **MQTT client** tab.

Include topic name: Select to include the topic that describes the condition in the MQTT topic.

Include topic namespaces: Select to include ONVIF topic namespaces in the MQTT topic.

Include serial number: Select to include the device's serial number in the MQTT payload.



Add condition: Click to add a condition.

Retain: Defines which MQTT messages are sent as retained.

- **None:** Send all messages as non-retained.
- **Property:** Send only stateful messages as retained.
- **All:** Send both stateful and stateless messages as retained.

QoS: Select the desired level for the MQTT publication.

MQTT subscriptions



Add subscription: Click to add a new MQTT subscription.

Subscription filter: Enter the MQTT topic that you want to subscribe to.

Use device topic prefix: Add the subscription filter as prefix to the MQTT topic.

Subscription type:

- **Stateless:** Select to convert MQTT messages into a stateless message.
- **Stateful:** Select to convert MQTT messages into a condition. The payload is used as the state.

QoS: Select the desired level for the MQTT subscription.

SIP

SIP settings

Session Initiation Protocol (SIP) is used for interactive communication sessions between users. The sessions can include audio and video.

Enable SIP: Check this option to make it possible to initiate and receive SIP calls.

Allow incoming calls: Check this option to allow incoming calls from other SIP devices.

Call handling

- **Call timeout:** Set the maximum time a call can last before it ends if there is no answer (max 10 min).
- **Incoming call duration:** Set the maximum time an incoming call can last (max 10 min).
- **End calls after:** Set the maximum time that a call can last (max 60 min). Select **Infinite call duration** if you don't want to limit the length of a call.

Ports

A port number must be between 1024 and 65535.

- **SIP port:** The network port used for SIP communication. The signaling traffic through this port is non-encrypted. The default port number is 5060. Enter a different port number if required.

AXIS M30 Network Camera Series

The device interface

- **TLS port:** The network port used for encrypted SIP communication. The signaling traffic through this port is encrypted with Transport Layer Security (TLS). The default port number is 5061. Enter a different port number if required.
- **RTP start port:** The network port used for the first RTP media stream in a SIP call. The default start port number is 4000. Some firewalls block RTP traffic on certain port numbers.

NAT traversal

Use NAT (Network Address Translation) traversal when the device is located on an private network (LAN) and you want to make it available from outside of that network.

Note

For NAT traversal to work, the router must support it. The router must also support UPnP®.

Each NAT traversal protocol can be used separately or in different combinations depending on the network environment.

- **ICE:** The ICE (Interactive Connectivity Establishment) protocol increases the chances of finding the most efficient path to successful communication between peer devices. If you also enable STUN and TURN, you improve the ICE protocol's chances.
- **STUN:** STUN (Session Traversal Utilities for NAT) is a client-server network protocol that lets the device determine if it is located behind a NAT or firewall, and if so obtain the mapped public IP address and port number allocated for connections to remote hosts. Enter the STUN server address, for example, an IP address.
- **TURN:** TURN (Traversal Using Relays around NAT) is a protocol that lets a device behind a NAT router or firewall receive incoming data from other hosts over TCP or UDP. Enter the TURN server address and the login information.

Audio and video

- **Audio codec priority:** Select at least one audio codec with the desired audio quality for SIP calls. Drag-and-drop to change the priority.

Note

The selected codecs must match the call recipient codec, since the recipient codec is decisive when a call is made.

- **Audio direction:** Select allowed audio directions.
- **H.264 packetization mode:** Select which packetization mode to use.
 - **Auto:** (Recommended) The device decides which packetization mode to use.
 - **None:** No packetization mode is set. This mode is often interpreted as mode 0.
 - **0:** Non-interleaved mode.
 - **1:** Single NAL unit mode.
- **Video direction:** Select allowed video directions.

Additional

- **UDP-to-TCP switching:** Select to allow calls to switch transport protocols from UDP (User Datagram Protocol) to TCP (Transmission Control Protocol) temporarily. The reason for switching is to avoid fragmentation, and the switch can take place if a request is within 200 bytes of the maximum transmission unit (MTU) or larger than 1300 bytes.
- **Allow via rewrite:** Select to send the local IP address instead of the router's public IP address.
- **Allow contact rewrite:** Select to send the local IP address instead of the router's public IP address.
- **Register with server every:** Set how often you want the device to register with the SIP server for the existing SIP accounts.
- **DTMF payload type:** Changes the default payload type for DTMF.

SIP accounts

AXIS M30 Network Camera Series

The device interface

All current SIP accounts are listed under **SIP accounts**. For registered accounts, the colored circle lets you know the status.

- The account is successfully registered with the SIP server.
- There is a problem with the account. Possible reasons can be authorization failure, that the account credentials are wrong, or that the SIP server can't find the account.

The **peer to peer (default)** account is an automatically created account. You can delete it if you create at least one other account and set that account as default. The default account is always used when a VAPIX® Application Programming Interface (API) call is made without specifying which SIP account to call from.



Account: Click to create a new SIP account.

- **Active:** Select to be able to use the account.
- **Make default:** Select to make this the default account. There must be a default account, and there can only be one default account.
- **Name:** Enter a descriptive name. This can, for example, be a first and last name, a role, or a location. The name is not unique.
- **User ID:** Enter the unique extension or phone number assigned to the device.
- **Peer-to-peer:** Use for direct calls to another SIP device on the local network.
- **Registered:** Use for calls to SIP devices outside the local network, through a SIP server.
- **Domain:** If available, enter the public domain name. It will be shown as part of the SIP address when calling other accounts.
- **Password:** Enter the password associated with the SIP account for authenticating against the SIP server.
- **Authentication ID:** Enter the authentication ID used for authenticating against the SIP server. If it is the same as the user ID, you don't need to enter the authentication ID.
- **Caller ID:** The name which is presented to the recipient of calls from the device.
- **Registrar:** Enter the IP address for the registrar.
- **Transport mode:** Select the SIP transport mode for the account: UDP, TCP, or TLS. When you select TLS, you get the option to use media encryption.
- **Media encryption (only with transport mode TLS):** Select the type of encryption for media (audio and video) in SIP calls.
- **Certificate (only with transport mode TLS):** Select a certificate.
- **Verify server certificate (only with transport mode TLS):** Check to verify the server certificate.
- **Secondary SIP server:** Turn on if you want the device to try to register on a secondary SIP server if registration on the primary SIP server fails.
- **Answer automatically:** Select to automatically answer an incoming call.
- **SIP secure:** Select to use Secure Session Initiation Protocol (SIPS). SIPS uses the TLS transport mode to encrypt traffic.
- **Proxies**



- **Proxy:** Click to add a proxy.
- **Prioritize:** If you have added two or more proxies, click to prioritize them.
- **Server address:** Enter the IP address of the SIP proxy server.
- **Username:** If required, enter the username for the SIP proxy server.
- **Password:** If required, enter the password for the SIP proxy server.
- **Video** ⓘ
 - **View area:** Select the view area to use for video calls. If you select none, the native view is used.
 - **Resolution:** Select the resolution to use for video calls. The resolution affects the required bandwidth.
 - **Frame rate:** Select the number of frames per second for video calls. The frame rate affects the required bandwidth.
 - **H.264 profile:** Select the profile to use for video calls.
- **DTMF**
 - **Use RTP (RFC2833):** Select to allow dual-tone multifrequency (DTMF) signaling, other tone signals and telephony events in RTP packets.
 - **Use SIP INFO (RFC2976):** Select to include the INFO method to the SIP protocol. The INFO method adds optional application layer information, generally related to the session.
 - **DTMF sequence:** Click to add an action rule triggered by touch-tone. You must activate the action rule in the **Events** tab.
 - **Sequence:** Enter the characters to trigger the action rule. Allowed characters: 0-9, A-D, #, and *.
 - **Description:** Enter a description of the action to be triggered.

AXIS M30 Network Camera Series

The device interface

SIP test call

SIP account: Select which account to make the test call from.

SIP address: Enter a SIP address and click  to make a test call and verify that the account works.

Storage

Network storage

Add network storage: Click to add a network share where you can save recordings.

- **Address:** Enter the IP address or host name of the host server, typically a NAS (Network Attached Storage). We recommend you to configure the host to use a fixed IP address (not DHCP since a dynamic IP address can change) or that you use DNS. Windows SMB/CIFS names are not supported.
- **Network share:** Enter the name of the shared location on the host server. Several Axis devices can use the same network share, since each device gets its own folder.
- **User:** If the server requires a login, enter the username. To log in to a specific domain server, type DOMAIN\username.
- **Password:** If the server requires a login, enter the password.
- **SMB version:** Select the SMB storage protocol version to connect to the NAS. If you select **Auto**, the device tries to negotiate one of the secure versions SMB: 3.02, 3.0, or 2.1. Select 1.0 or 2.0 to connect to older NAS that don't support higher versions. You can read more about SMB support in Axis devices [here](#).
- **Add share even if connection test fails:** Select to add the network share even if an error is discovered during the connection test. The error can be, for example, that you didn't enter a password even though the server requires one.

Remove network storage: Click to remove the connection to the network share. This removes all settings for the network share.

Write protect: Turn on to stop writing to the network share and protect recordings from being removed. You can't format a write-protected network share.

Ignore: Turn on to stop storing recordings on the network share.

Retention time: Select how long to keep recordings, to limit the amount of old recordings or to comply with regulations regarding data storage. If the network storage becomes full, old recordings are removed before the selected time period has passed.

Tools

- **Test connection:** Test the connection to the network share.
- **Format:** Format the network share, for example when you need to quickly erase all data. cifs is the available file system option.

Click **Use** tool to activate the selected tool.

Onboard storage

Important

Risk of data loss and corrupted recordings. Do not remove the SD card while the device is running. Unmount the SD card before you remove it.

Unmount: Click to safely remove the SD card.

Write protect: Turn on to stop writing to the SD card and protect recordings from being removed. You can't format a write-protected SD card.

Autoformat: Turn on to automatically format a newly inserted SD card. It formats the file system into ext4.

Ignore: Turn on to stop storing recordings on the SD card. When you ignore the SD card, the device no longer recognizes that the card exists. The setting is only available for administrators.

Retention time: Select how long to keep recordings, to limit the amount of old recordings or to comply with regulations regarding data storage. If the SD card becomes full, old recordings are removed before the selected time period has passed.

AXIS M30 Network Camera Series

The device interface

Tools

- **Check:** Check for errors on the SD card. This only works for the ext4 file system.
- **Repair:** Repair errors in the ext4 file system. To repair an SD card with the VFAT file system, eject the SD card, insert it in a computer and perform a disk repair.
- **Format:** Format the SD card, for example when you need to change the file system or quickly erase all data. VFAT and ext4 are the two available file system options. The recommended format is ext4, due to its resilience against data loss if the card is ejected or if there is an abrupt power loss. However, you need a third-party ext4 driver or application to access the file system from Windows®.
- **Encrypt:** Use this tool to format the SD card and enable encryption. **Encrypt** deletes all data stored on the SD card. After using **Encrypt** data that's stored on the SD card is protected using encryption.
- **Decrypt:** Use this tool to format the SD card without encryption. **Decrypt** deletes all data stored on the SD card. After using **Decrypt** data that's stored on the SD card is not protected using encryption.
- **Change password:** Change the password required to encrypt the SD card.

Click **Use tool** to activate the selected tool.

Wear trigger: Set a value for the SD card wear level at which you want to trigger an action. The wear level ranges from 0–200%. A new SD card that has never been used has a wear level of 0%. A wear level of 100% indicates that the SD card is close to its expected lifetime. When the wear-level reaches 200% there is a high risk of the SD card malfunctioning. We recommend setting the wear trigger between 80–90%. This gives you time to download any recordings as well as replace the SD card in time before it potentially wears out. The wear trigger allows you to set up an event and get a notification when the wear level reaches your set value.

Stream profiles



Click  to create and save groups of video stream settings. You can use the settings in different situations, for example in continuous recording or when you use action rules to record.

ONVIF

ONVIF users

ONVIF (Open Network Video Interface Forum) is a global interface standard that makes it easier for end-users, integrators, consultants, and manufacturers to take advantage of the possibilities offered by network video technology. ONVIF enables interoperability between different vendor products, increased flexibility, reduced cost and future-proof systems.



Add user: Click to add a new ONVIF user.

Username: Enter a unique username.

New password: Enter a password for the user. Passwords must be 1 to 64 characters long. Only ASCII printable characters (code 32 to 126) are allowed in the password, for example letters, numbers, punctuation, and some symbols.

Repeat password: Enter the same password again

Role:

- **Administrator:** Has full access to all settings. Administrators can also add, update, and remove other users.
- **Operator:** Has access to all settings except:
 - All **System** settings.
 - Adding apps.
- **Media user:** Allows access to the video stream only.



The context menu contains:

Update user: Edit the user's properties.

AXIS M30 Network Camera Series

The device interface

Delete user: Delete the user. You can't delete the root user.

By creating an ONVIF user, you automatically enable ONVIF communication. Use the username and password for all ONVIF communication with the device. For more information see the Axis Developer Community at axis.com.

ONVIF media profiles

An ONVIF media profile consists of a set of configurations that you can use to change media stream settings.



Add media profile: Click to add a new ONVIF media profile.

profile_x: Click a profile to edit.

Analytics metadata

Metadata producers

Metadata producers lists the channels used by apps and the metadata they are streaming from the device.

Producer: The app producing the metadata.

Channel: The channel used by the app. Check to enable the metadata stream. Uncheck to disable the stream for compatibility or resources management reasons.

Detectors

Camera tampering

The camera tampering detector generates an alarm when the scene changes, for example because the lens is covered, sprayed or severely put out of focus, and the time in **Trigger after** has passed. The tampering detector only activates when the camera has not moved for at least 10 seconds. During this period the detector sets up a scene model to use as a comparison to detect tampering in current images. For the scene model to be set up properly, make sure that the camera is in focus, the lighting conditions are correct, and the camera doesn't point at a scene that lacks contours, for example a blank wall. Camera tampering can be used as a condition to trigger actions.

Trigger after: Enter the minimum time that the tampering conditions must be active before the alarm triggers. This can help prevent false alarms for known conditions that affect the image.

Trigger on dark images: It is very difficult to generate alarms when the camera lens is sprayed, since it is impossible to distinguish that event from other situations where the image turns dark in a similar way, for example when the lighting conditions change. Turn on this parameter to generate alarms for all cases where the image turns dark. When it's turned off, the device doesn't generate any alarm when the image turns dark.

Audio detection

These settings are available for each audio input.

Sound level: Adjust the sound level to a value from 0–100, where 0 is the most sensitive and 100 the least sensitive. Use the activity indicator as a guide when you set the sound level. When you create events, you can use the sound level as a condition. You can choose to trigger an action if the sound level rises above, falls below or passes the set value.

Video out

HDMI

AXIS M30 Network Camera Series

The device interface

You can connect an external monitor to the device through an HDMI cable.

Single source

A stream from a single camera is displayed on the external monitor.

- **Source:** Select only one camera.
- **Rotate image 180°:** Click to rotate the image.
- **Mirror image:** Click to flip the image.

- **Dynamic overlays**  : Click to overlay.

Quad view

View streams from four separate cameras at the same time on the external monitor.

- **Sources:** Select a different camera from each of the four drop-down lists. The image beside the source shows where the video from that camera will be displayed on the screen.
- **Rotate image 180°:** Click to rotate all images.

Playlist

Single streams from multiple cameras alternate on the external monitor.

- **Rotate image 180°:** Click to rotate the image from all sources.
- **+** : Click to add a camera to the playlist.
- **Source:** Select the desired camera.
- **Duration:** Set how long (in mm:ss) the playlist will stream from this camera in each rotation.
- **Mirror image:** Click to flip the image.
- **Create:** Click to save.

Picture-in-picture

Two streams are displayed on the external monitor at the same time. One stream fills the display and the other is a smaller picture. **Position**, **picture size** and **borders** are customizable.

- **Picture-in-picture**
 - **Source:** Select the camera that will stream as the smaller picture.
 - **Rotate image 180°:** Click to rotate the image.
 - **Mirror image:** Click to flip the image.
 - **Position:** Select where on the screen the picture should appear.
 - **Picture size:** Drag the slider to set the size (% of screen) of the picture.
 - **Border:** Click to toggle borders for the picture on or off.
 -  : Drag the slider to set the thickness for the entire border.
 -  : Drag the slider to set the thickness for the top border.
 -  : Drag the slider to set the thickness for the right border.
 -  : Drag the slider to set the thickness for the bottom border.
 -  : Drag the slider to set the thickness for the left border.
 - **Border color:** Select a border color.
- **Main view**
 - **Source:** Select the camera that will stream on the full display.
 - **Rotate image 180°:** Click to rotate the image.
 - **Mirror image:** Click to flip the image.

Logs

Reports and logs

AXIS M30 Network Camera Series

The device interface

Reports

- **View the device server report:** Click to show information about the product status in a pop-up window. The Access Log is automatically included in the Server Report.
- **Download the device server report:** Click to download the server report. It creates a .zip file that contains a complete server report text file in UTF-8 format, as well as a snapshot of the current live view image. Always include the server report .zip file when you contact support.
- **Download the crash report:** Click to download an archive with detailed information about the server's status. The crash report contains information that is in the server report as well as detailed debug information. This report might contain sensitive information such as network traces. It can take several minutes to generate the report.

Logs

- **View the system log:** Click to show information about system events such as device startup, warnings and critical messages.
- **View the access log:** Click to show all failed attempts to access the device, for example when a wrong login password is used.

Network trace

Important

A network trace file might contain sensitive information, for example certificates or passwords.

A network trace file can help you troubleshoot problems by recording activity on the network. Select the duration of the trace in seconds or minutes, and click **Download**.

Remote system log

Syslog is a standard for message logging. It allows separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Each message is labeled with a facility code, which indicates the software type generating the message, and assigned a severity level.



Server: Click to add a new server.

Host: Enter the hostname or IP address of the server.

Format: Select which syslog message format to use.

- RFC 3164
- RFC 5424

Protocol: Select the protocol and port to use:

- UDP (Default port is 514)
- TCP (Default port is 601)
- TLS (Default port is 6514)

Severity: Select which messages to send when triggered.

CA certificate set: See the current settings or add a certificate.

Plain config

Plain config is for advanced users with experience of Axis device configuration. Most parameters can be set and edited from this page.

AXIS M30 Network Camera Series

The device interface

Maintenance

Restart: Restart the device. This does not affect any of the current settings. Running applications restart automatically.

Restore: Return *most* settings to the factory default values. Afterwards you must reconfigure the device and apps, reinstall any apps that didn't come preinstalled, and recreate any events and PTZ presets.

Important

The only settings saved after restore are:

- Boot protocol (DHCP or static)
- Static IP address
- Default router
- Subnet mask
- 802.1X settings
- O3C settings

Factory default: Return *all* settings to the factory default values. Afterwards you must reset the IP address to make the device accessible.

Note

All Axis device firmware is digitally signed to ensure that you only install verified firmware on your device. This further increases the overall minimum cybersecurity level of Axis devices. For more information, see the white paper "Signed firmware, secure boot, and security of private keys" at axis.com.

Firmware upgrade: Upgrade to a new firmware version. New firmware releases can contain improved functionality, bug fixes, and completely new features. We recommend you to always use the latest release. To download the latest release, go to axis.com/support.

When you upgrade, you can choose between three options:

- **Standard upgrade:** Upgrade to the new firmware version.
- **Factory default:** Upgrade and return all settings to the factory default values. When you choose this option, you can't revert to the previous firmware version after the upgrade.
- **Autorollback:** Upgrade and confirm the upgrade within the set time. If you don't confirm, the device reverts to the previous firmware version.

Firmware rollback: Revert to the previously installed firmware version.

AXIS M30 Network Camera Series

[Learn more](#)

[Learn more](#)

View area

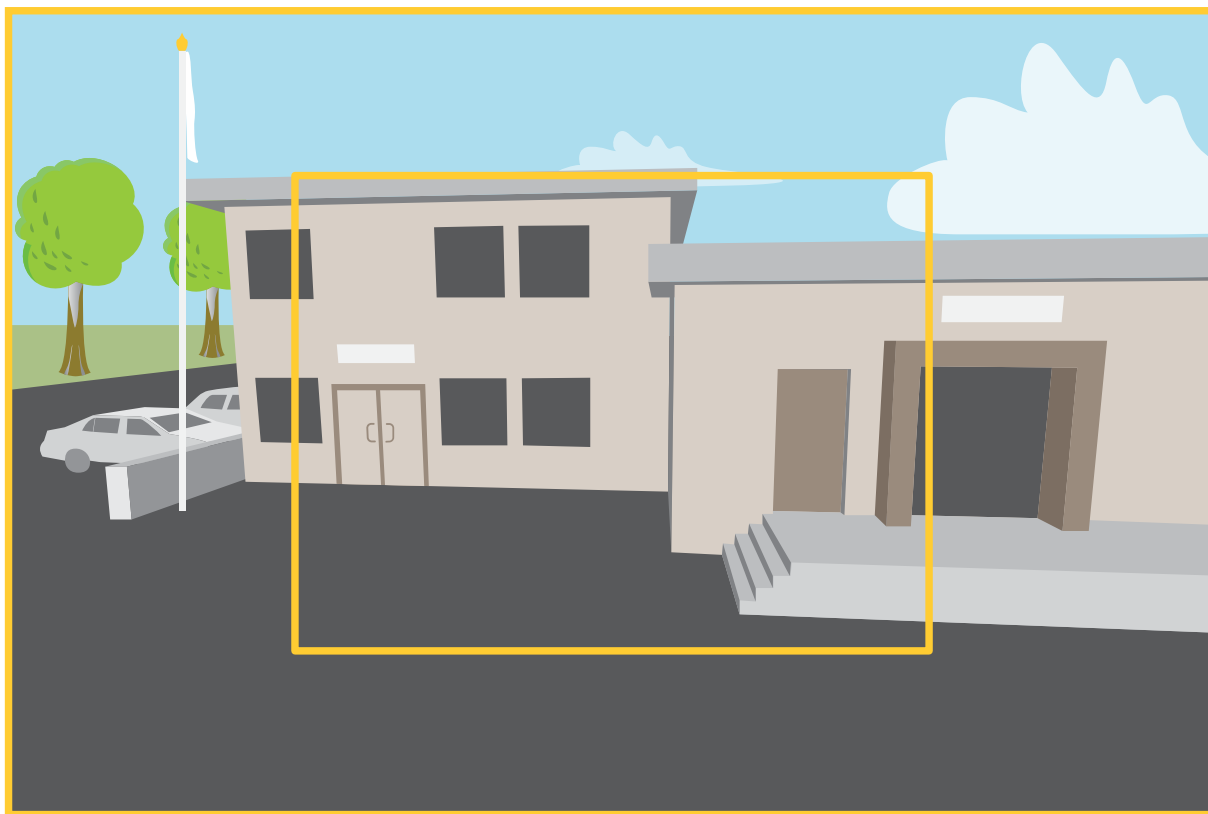
A view area is a cropped part of the full view. You can stream and store view areas instead of the full view to minimize bandwidth and storage needs. If you enable PTZ for a view area, you can pan, tilt and zoom within it. By using view areas you can remove parts of the full view, for example, the sky.

When you set up a view area, we recommend you to set the video stream resolution to the same size as or smaller than the view area size. If you set the video stream resolution larger than the view area size it implies digitally scaled up video after sensor capture, which requires more bandwidth without adding image information.

Capture modes

A capture mode is a preset configuration that defines how the camera captures images. The capture mode setting can affect the camera's field of view and aspect ratio. The shutter speed can also be affected, which in turn affects the light sensitivity.

The lower resolution capture mode might be sampled from the original resolution, or it might be cropped out from the original, in which case the field of view could also be affected.



The image shows how the field of view and aspect ratio can change between two different capture modes.

What capture mode to choose depends on the requirements for the frame rate and resolution of the specific surveillance setup. For specifications about available capture modes, see the product's datasheet at axis.com.

AXIS M30 Network Camera Series

Learn more

Privacy masks

A privacy mask is a user-defined area that prevents users from viewing a part of the monitored area. In the video stream, privacy masks appear as blocks of solid color.

You'll see the privacy mask on all snapshots, recorded video, and live streams.

You can use the VAPIX® application programming interface (API) to hide the privacy masks.

Important

If you use multiple privacy masks it may affect the product's performance.

You can create several privacy masks. The maximum number of masks depends on the complexity of all the masks combined. The more anchor points in each mask, the fewer masks you can create. Each mask can have 3 to 10 anchor points.

Overlays

Overlays are superimposed over the video stream. They are used to provide extra information during recordings, such as a timestamp, or during product installation and configuration. You can add either text or an image.

Streaming and storage

Video compression formats

Decide which compression method to use based on your viewing requirements, and on the properties of your network. The available options are:

Motion JPEG

Note

To ensure support for the Opus audio codec, the Motion JPEG stream is always sent over RTP.

Motion JPEG, or MJPEG, is a digital video sequence that is made up of a series of individual JPEG images. These images are then displayed and updated at a rate sufficient to create a stream that shows constantly updated motion. For the viewer to perceive motion video the rate must be at least 16 image frames per second. Full motion video is perceived at 30 (NTSC) or 25 (PAL) frames per second.

The Motion JPEG stream uses considerable amounts of bandwidth, but provides excellent image quality and access to every image contained in the stream.

H.264 or MPEG-4 Part 10/AVC

Note

H.264 is a licensed technology. The Axis product includes one H.264 viewing client license. To install additional unlicensed copies of the client is prohibited. To purchase additional licenses, contact your Axis reseller.

H.264 can, without compromising image quality, reduce the size of a digital video file by more than 80% compared to the Motion JPEG format and by as much as 50% compared to older MPEG formats. This means that less network bandwidth and storage space are required for a video file. Or seen another way, higher video quality can be achieved for a given bitrate.

H.265 or MPEG-H Part 2/HEVC

H.265 can, without compromising image quality, reduce the size of a digital video file by more than 25% compared to H.264.

Note

- H.265 is licensed technology. The Axis product includes one H.265 viewing client license. Installing additional unlicensed copies of the client is prohibited. To purchase additional licenses, contact your Axis reseller.
- Most web browsers don't support H.265 decoding and because of this the camera doesn't support it in its web interface. Instead you can use a video management system or application supporting H.265 decoding.

AXIS M30 Network Camera Series

Learn more

How do Image, Stream, and Stream profile settings relate to each other?

The **Image** tab contains camera settings that affect all video streams from the product. If you change something in this tab, it immediately affects all video streams and recordings.

The **Stream** tab contains settings for video streams. You get these settings if you request a video stream from the product and don't specify for example resolution, or frame rate. When you change the settings in the **Stream** tab, it doesn't affect ongoing streams, but it will take effect when you start a new stream.

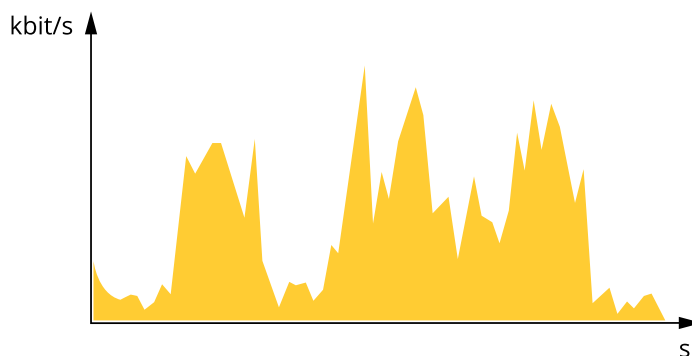
The **Stream profiles** settings override the settings from the **Stream** tab. If you request a stream with a specific stream profile, the stream contains the settings of that profile. If you request a stream without specifying a stream profile, or request a stream profile that doesn't exist in the product, the stream contains the settings from the **Stream** tab.

Bitrate control

Bitrate control helps you to manage the bandwidth consumption of your video stream.

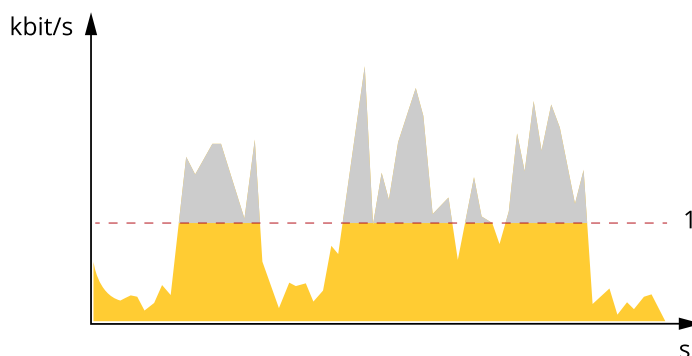
Variable bitrate (VBR)

Variable bitrate allows the bandwidth consumption to vary depending on the level of activity in the scene. The more activity, the more bandwidth you need. With variable bitrate you are guaranteed constant image quality, but you need to make sure you have storage margins.



Maximum bitrate (MBR)

Maximum bitrate lets you set a target bitrate to handle bitrate limitations in your system. You might see a decline in image quality or frame rate as the instantaneous bitrate is kept below the specified target bitrate. You can choose to prioritize either image quality or frame rate. We recommend that you configure the target bitrate to a higher value than the expected bitrate. This gives you a margin in case there is a high level of activity in the scene.



1 Target bitrate

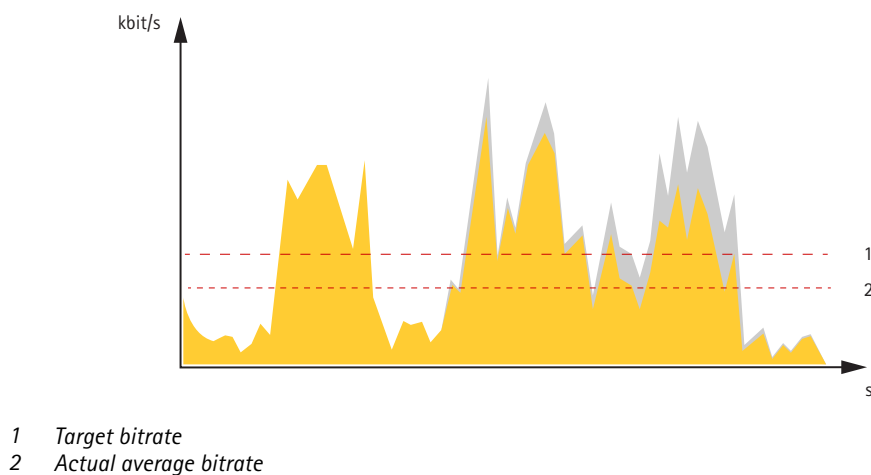
AXIS M30 Network Camera Series

Learn more

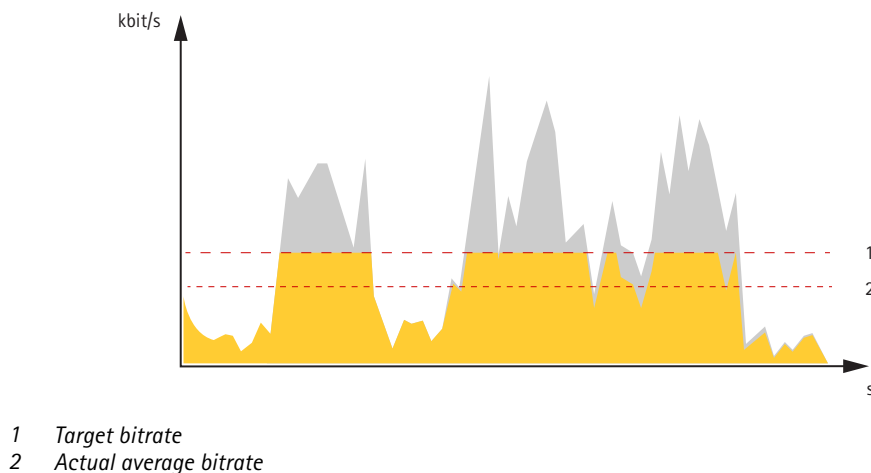
Average bitrate (ABR)

With average bitrate, the bitrate is automatically adjusted over a longer period of time. This is so you can meet the specified target and provide the best video quality based on your available storage. Bitrate is higher in scenes with a lot of activity, compared to static scenes. You are more likely to get better image quality when in scenes with a lot of activity if you use the average bitrate option. You can define the total storage required to store the video stream for a specified amount of time (retention time) when image quality is adjusted to meet the specified target bitrate. Specify the average bitrate settings in one of the following ways:

- To calculate the estimated storage need, set the target bitrate and the retention time.
- To calculate the average bitrate, based on available storage and required retention time, use the target bitrate calculator.



You can also turn on maximum bitrate and specify a target bitrate within the average bitrate option.



Applications

With applications you can get more out of your Axis device. AXIS Camera Application Platform (ACAP) is an open platform that makes it possible for third parties to develop analytics and other applications for Axis devices. Applications can be preinstalled on the device, available for download for free, or for a license fee. To find out more about available applications, downloads, trials and licenses, go to axis.com/acap.

To find the user manuals for Axis applications, go to help.axis.com.

AXIS M30 Network Camera Series

Learn more

Note

- Several applications can run at the same time but some applications might not be compatible with each other. Certain combinations of applications might require too much processing power or memory resources when run in parallel. Verify that the applications work together before deployment.



To watch this video, go to the web version of this document.

help.axis.com/?&pid=49386§ion=about-applications

How to download and install an application



To watch this video, go to the web version of this document.

help.axis.com/?&pid=49386§ion=about-applications

How to activate an application licence code on a device

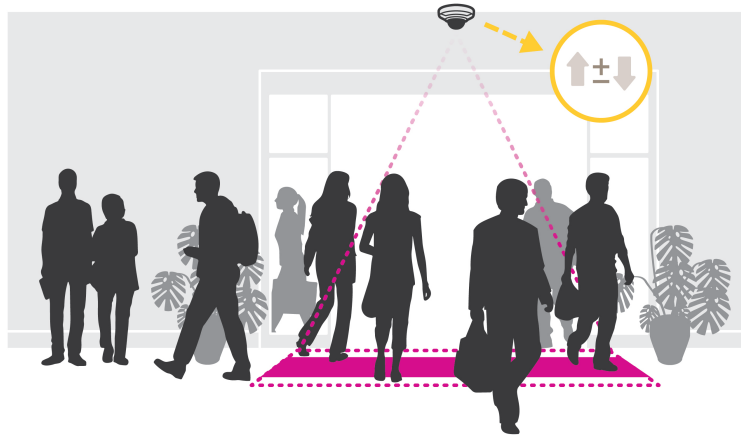
AXIS People Counter

AXIS People Counter is an analytic application that you can install on a network camera. You can use the application to count how many people pass through an entrance, in what direction they pass, and if more than one person passes during a predefined interval. You can also use it to estimate how many people are currently occupying an area, and the average visiting time.

The application runs embedded in the camera which means you don't need a dedicated computer to run the application. AXIS People Counter is suitable for any indoor environment, like stores, libraries, or gyms.

AXIS M30 Network Camera Series

Learn more



How does estimating occupancy work?

You can use the application to estimate occupancy in areas with one or several entrances and exits. Each entrance and exit needs to be equipped with a network camera with AXIS People Counter installed. If there are several cameras, they communicate with each other over the network in a primary and secondary concept. The primary camera continuously fetches data from the secondary cameras and presents the data in the live view. Every fifteen minutes, the primary camera sends the statistical data to AXIS Store Data Manager. Consequently, the reports generated from AXIS Store Data Manager can present the data in a minimum of 15 minutes time interval.

AXIS M30 Network Camera Series

Cleaning recommendations

Cleaning recommendations

NOTICE

Never use harsh detergent, for example gasoline, benzene, or acetone.

1. Use a can of compressed air to remove any dust or loose dirt from the device.
2. If necessary, clean the lens with a soft cloth dampened with lukewarm water.

Note

Avoid cleaning in direct sunlight or at elevated temperatures, as this may cause stains when the water droplets dry.

AXIS M30 Network Camera Series

Troubleshooting

Troubleshooting

Reset to factory default settings

Important

Reset to factory default should be used with caution. A reset to factory default resets all settings, including the IP address, to the factory default values.

To reset the product to the factory default settings:

1. Disconnect power from the product.
2. Press and hold the control button while reconnecting power. See *Product overview on page 57*.
3. Keep the control button pressed for 15–30 seconds until the status LED indicator flashes amber.
4. Release the control button. The process is complete when the status LED indicator turns green. The product has been reset to the factory default settings. If no DHCP server is available on the network, the default IP address is 192.168.0.90.
5. Use the installation and management software tools to assign an IP address, set the password, and access the device.

The installation and management software tools are available from the support pages on axis.com/support.

You can also reset parameters to factory default through the device's webpage. Go to **Maintenance > Factory default** and click **Default**.

Firmware options

Axis offers product firmware management according to either the active track or the long-term support (LTS) tracks. Being on the active track means continuously getting access to all the latest product features, while the LTS tracks provide a fixed platform with periodic releases focused mainly on bug fixes and security updates.

Using firmware from the active track is recommended if you want to access the newest features, or if you use Axis end-to-end system offerings. The LTS tracks are recommended if you use third-party integrations, which are not continuously validated against the latest active track. With LTS, the products can maintain cybersecurity without introducing any significant functional changes or affecting any existing integrations. For more detailed information about Axis product firmware strategy, go to axis.com/support/firmware.

Check the current firmware version

Firmware is the software that determines the functionality of network devices. When you troubleshoot a problem, we recommend you to start by checking the current firmware version. The latest firmware version might contain a correction that fixes your particular problem.

To check the current firmware:

1. Go to the device interface > **Status**.
2. See the firmware version under **Device info**.

Upgrade the firmware

Important

Preconfigured and customized settings are saved when you upgrade the firmware (provided that the features are available in the new firmware) although this is not guaranteed by Axis Communications AB.

Important

Make sure the device remains connected to the power source throughout the upgrade process.

AXIS M30 Network Camera Series

Troubleshooting

Note

When you upgrade the device with the latest firmware in the active track, the product receives the latest functionality available. Always read the upgrade instructions and release notes available with each new release before you upgrade the firmware. To find the latest firmware and the release notes, go to axis.com/support/firmware.

1. Download the firmware file to your computer, available free of charge at axis.com/support/firmware.
2. Log in to the device as an administrator.
3. Go to **Maintenance > Firmware upgrade** and click **Upgrade**.

When the upgrade has finished, the product restarts automatically.

You can use AXIS Device Manager to upgrade multiple devices at the same time. Find out more at axis.com/products/axis-device-manager.

Technical issues, clues, and solutions

If you can't find what you're looking for here, try the troubleshooting section at axis.com/support.

Problems upgrading the firmware

Firmware upgrade failure	If the firmware upgrade fails, the device reloads the previous firmware. The most common reason is that the wrong firmware file has been uploaded. Check that the name of the firmware file corresponds to your device and try again.
Problems after firmware upgrade	If you experience problems after a firmware upgrade, roll back to the previously installed version from the Maintenance page.

Problems setting the IP address

The device is located on a different subnet	If the IP address intended for the device and the IP address of the computer used to access the device are located on different subnets, you cannot set the IP address. Contact your network administrator to obtain an IP address.
The IP address is being used by another device	Disconnect the Axis device from the network. Run the ping command (in a Command/DOS window, type <code>ping</code> and the IP address of the device): • If you receive: <code>Reply from <IP address>: bytes=32; time=10...</code> this means that the IP address may already be in use by another device on the network. Obtain a new IP address from the network administrator and reinstall the device. • If you receive: <code>Request timed out</code>, this means that the IP address is available for use with the Axis device. Check all cabling and reinstall the device.
Possible IP address conflict with another device on the same subnet	The static IP address in the Axis device is used before the DHCP server sets a dynamic address. This means that if the same default static IP address is also used by another device, there may be problems accessing the device.

The device can't be accessed from a browser

Can't log in	When HTTPS is enabled, ensure that the correct protocol (HTTP or HTTPS) is used when attempting to log in. You may need to manually type <code>http</code> or <code>https</code> in the browser's address field. If the password for the user <code>root</code> is lost, the device must be reset to the factory default settings. See <i>Reset to factory default settings</i> on page 53.
--------------	---

AXIS M30 Network Camera Series

Troubleshooting

The IP address has been changed by DHCP	IP addresses obtained from a DHCP server are dynamic and may change. If the IP address has been changed, use AXIS IP Utility or AXIS Device Manager to locate the device on the network. Identify the device using its model or serial number, or by the DNS name (if the name has been configured). If required, a static IP address can be assigned manually. For instructions, go to axis.com/support .
Certificate error when using IEEE 802.1X	For authentication to work properly, the date and time settings in the Axis device must be synchronized with an NTP server. Go to System > Date and time .

The device is accessible locally but not externally

To access the device externally, we recommend you to use one of the following applications for Windows®:

- AXIS Companion: free of charge, ideal for small systems with basic surveillance needs.
- AXIS Camera Station: 30-day trial version free of charge, ideal for small to mid-size systems.

For instructions and download, go to axis.com/vms.

Problems with streaming

Multicast H.264 only accessible by local clients	Check if your router supports multicasting, or if you need to configure the router settings between the client and the device. You might need to increase the TTL (Time To Live) value.
No multicast H.264 displayed in the client	Check with your network administrator that the multicast addresses used by the Axis device are valid for your network. Check with your network administrator to see if there is a firewall that prevents viewing.
Poor rendering of H.264 images	Ensure that your graphics card uses the latest driver. You can usually download the latest drivers from the manufacturer's website.
Color saturation is different in H.264 and Motion JPEG	Modify the settings for your graphics adapter. Go to the adapter's documentation for more information.
Lower frame rate than expected	• See <i>Performance considerations</i> on page 56. • Reduce the number of applications running on the client computer. • Limit the number of simultaneous viewers. • Check with the network administrator that there is enough bandwidth available. • Lower the image resolution. • Log in to the device's webpage and set a capture mode that prioritizes frame rate. If you change the capture mode to prioritize frame rate it might lower the maximum resolution, depending on the device used and capture modes available. • The maximum frames per second is dependent on the utility frequency (60/50 Hz) of the Axis device.
Can't select H.265 encoding in live view	Web browsers don't support H.265 decoding. Use a video management system or application that supports H.265 decoding.

Problems retrieving additional video streams

- 'Video Error' displayed in AXIS Companion, or
- 'Stream: Error. Something went wrong. Maybe there are too many viewers.' in Chrome/Firefox, or
- '503 service unavailable' error in Quick Time, or
- 'Camera not available' displayed in AXIS Camera Station, or
- 'Error reading video stream' message in browser when using the Java applet

This camera is designed to deliver up to four different streams. If a fifth unique stream is requested, the camera can't provide it, and an error message is displayed. The error message depends on the way the stream is requested. The streams are used on a first come, first served basis. Examples of instances that use a stream are:

- Live viewing in a web browser or other application
- While recording - continuous or motion triggered recording
- An event that uses images on the camera, for example an event that sends an e-mail with an image every hour
- An installed and running application, such as AXIS Video Motion Detection, will always consume a video stream, whether it is used or not. A stopped application does not consume a video stream.

AXIS M30 Network Camera Series

Troubleshooting

The camera can deliver more than four simultaneous streams provided the configuration of any additional stream is identical to any of the first four streams. Identical configuration implies exactly the same resolution, frame rate, compression, video format, rotation etc. For more information see the white paper "Max number of unique video stream configurations", available at axis.com.

Performance considerations

When setting up your system, it is important to consider how various settings and situations affect the performance. Some factors affect the amount of bandwidth (the bitrate) required, others can affect the frame rate, and some affect both. If the load on the CPU reaches its maximum, this also affects the frame rate.

The following factors are the most important to consider:

- High image resolution or lower compression levels result in images containing more data which in turn affects the bandwidth.
- Rotating the image in the GUI can increase the product's CPU load.
- Access by large numbers of Motion JPEG or unicast H.264 clients affects the bandwidth.
- Access by large numbers of Motion JPEG or unicast H.265 clients affects the bandwidth.
- Simultaneous viewing of different streams (resolution, compression) by different clients affects both frame rate and bandwidth.

Use identical streams wherever possible to maintain a high frame rate. Stream profiles can be used to ensure that streams are identical.

- Accessing Motion JPEG and H.264 video streams simultaneously affects both frame rate and bandwidth.
- Accessing Motion JPEG and H.265 video streams simultaneously affects both frame rate and bandwidth.
- Heavy usage of event settings affects the product's CPU load which in turn affects the frame rate.
- Using HTTPS may reduce frame rate, in particular if streaming Motion JPEG.
- Heavy network utilization due to poor infrastructure affects the bandwidth.
- Viewing on poorly performing client computers lowers perceived performance and affects frame rate.
- Running multiple AXIS Camera Application Platform (ACAP) applications simultaneously may affect the frame rate and the general performance.

Contact support

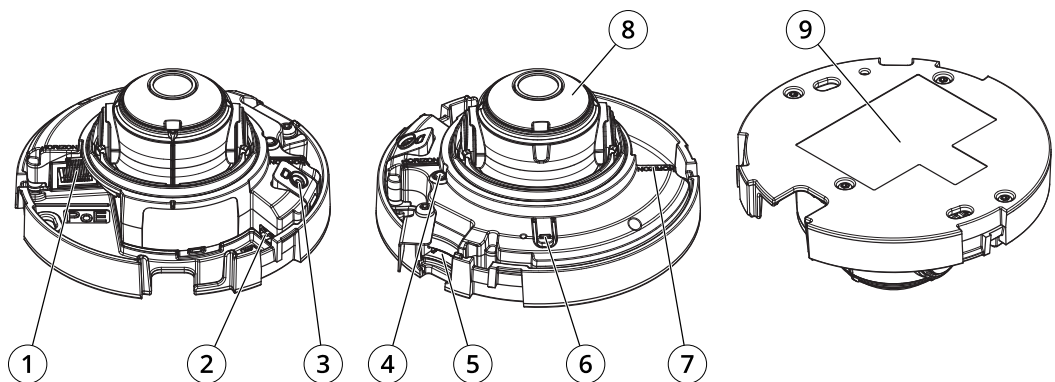
Contact support at axis.com/support.

AXIS M30 Network Camera Series

Specifications

Specifications

Product overview



- 1 Network connector (PoE)
- 2 HDMI connector (Micro)
- 3 Microphone (AXIS M3075-V)
- 4 Status LED indicator
- 5 SD card slot
- 6 Control button
- 7 Leveling mark
- 8 Focus ring
- 9 Part number (P/N) & Serial number (S/N)

LED indicators

Note

The Status LED can be configured to flash while an event is active.

Status LED	Indication
Unlit	Connection and normal operation.
Green	Shows steady green for 10 seconds for normal operation after startup completed.
Amber	Steady during startup. Flashes during firmware upgrade or reset to factory default.
Amber/Red	Flashes amber/red if network connection is unavailable or lost.
Red	Firmware upgrade failure.

SD card slot

NOTICE

- Risk of damage to SD card. Do not use sharp tools, metal objects, or excessive force when inserting or removing the SD card. Use your fingers to insert and remove the card.
- Risk of data loss and corrupted recordings. Unmount the SD card from the product's webpage before removal. Do not remove the SD card while the product is running.

This product supports microSD/microSDHC/microSDXC cards.

AXIS M30 Network Camera Series

Specifications

For SD card recommendations, see *axis.com*.



microSD, microSDHC, and microSDXC Logos are trademarks of SD-3C LLC. microSD, microSDHC, microSDXC are trademarks or registered trademarks of SD-3C, LLC in the United States, other countries or both.

Buttons

Control button

The control button is used for:

- Resetting the product to factory default settings. See *Reset to factory default settings on page 53*.
- Connecting to an AXIS Video Hosting System service. To connect, press and hold the button for about 3 seconds until the status LED flashes green.

Connectors

HDMI connector

Use the microHDMI™ connector to connect a display or public view monitor.

Network connector

RJ45 Ethernet connector with Power over Ethernet (PoE).

AXIS M32 Dome Camera Series

AXIS M3215-LVE Dome Camera

AXIS M3216-LVE Dome Camera

Table of Contents

Installation	4
Preview mode	4
Get started.....	5
Find the device on the network.....	5
Browser support.....	5
Open the device's web interface.....	5
Create an administrator account.....	5
Secure passwords.....	6
Make sure that no one has tampered with the device software	6
Web interface overview	6
Configure your device.....	7
Adjust the image.....	7
Level the camera	7
Select exposure mode	7
Benefit from IR light in low-light conditions by using night mode	7
Optimize IR illumination.....	8
Reduce noise in low-light conditions.....	8
Reduce motion blur in low-light conditions.....	8
Maximize the details in an image	9
Handle scenes with strong backlight.....	9
Compensate for barrel distortion.....	10
Monitor long and narrow areas.....	10
Verify the pixel resolution.....	10
Hide parts of the image with privacy masks.....	11
Show an image overlay	11
Show a text overlay.....	11
Straighten a skewed image.....	11
View and record video	12
Reduce bandwidth and storage	12
View a live video stream on a monitor	12
Set up network storage	13
Record and watch video	13
Set up rules for events	13
Trigger an action	13
Record video when the camera detects an object.....	14
Show a text overlay in the video stream when the device detects an object	14
Record video when a PIR detector senses motion	15
Provide visual indication of an ongoing event.....	16
Record video when the camera detects loud noises	17
Detect tampering with input signal	17
Trigger a notification when the enclosure is opened.....	18
Trigger a notification when the camera lens is tampered	18
Audio.....	19
Add audio to your recording	19
Add audio capability to your product using portcast.....	19
Connect to a network speaker.....	20
Connect to a strobe siren	20
The web interface	21
Learn more.....	22
Privacy masks	22
Overlays	22
Streaming and storage.....	23
Video compression formats.....	23

How do Image, Stream, and Stream profile settings relate to each other?	23
Bitrate control.....	24
Edge-to-edge technology.....	25
Speaker pairing	25
Network pairing	25
Analytics and apps	26
AXIS Object Analytics.....	26
Metadata visualization.....	26
AXIS Image Health Analytics.....	26
Specifications.....	27
Product overview	27
.....	27
LED indicators.....	27
SD card slot.....	29
Buttons.....	29
Control button	29
Connectors.....	29
Network connector	29
Audio connector.....	30
I/O connector.....	32
Troubleshooting.....	35
Reset to factory default settings	35
AXIS OS options.....	36
Check the current AXIS OS version	37
Upgrade AXIS OS.....	37
Technical problems and possible solutions	37
The image is blurry	40
Performance considerations	41
Contact support.....	42
Cybersecurity	43
Vulnerability management	43
Security notifications.....	43
Secure product lifecycle.....	43

Installation

For instructions on how to install the product, see the installation guide on the product's support page on *axis.com*.

Preview mode

Preview mode is ideal for installers when fine tuning the camera view during the installation. No login is required to access the camera view in preview mode. It is available only in factory defaulted state for a limited time from powering up the device.



To watch this video, go to the web version of this document.

This video demonstrates how to use preview mode.

Get started

Find the device on the network

To find Axis devices on the network and assign them IP addresses in Windows®, use AXIS IP Utility or AXIS Device Manager. Both applications are free and can be downloaded from axis.com/support.

For more information about how to find and assign IP addresses, go to *How to assign an IP address and access your device*.

Browser support

You can use the device with the following browsers:

	Chrome™	Edge™	Firefox®	Safari®
Windows®	✓	✓	*	*
macOS®	✓	✓	*	*
Linux®	✓	✓	*	*
Other operating systems	*	*	*	*

✓: Recommended

*: Supported with limitations

Open the device's web interface

1. Open a browser and type the IP address or host name of the Axis device.
If you don't know the IP address, use AXIS IP Utility or AXIS Device Manager to find the device on the network.
2. Type the username and password. If you access the device for the first time, you must create an administrator account. See *Create an administrator account*, on page 5.

For descriptions of all features and settings in the web interface of devices with AXIS OS, see *AXIS OS web interface help*.

Create an administrator account

The first time you log in to your device, you must create an administrator account.

1. Enter a username.
2. Enter a password. See *Secure passwords*, on page 6.
3. Re-enter the password.
4. Accept the license agreement.
5. Click **Add account**.

Important

The device has no default account. If you lose the password for your administrator account, you must reset the device. See *Reset to factory default settings*, on page 35.

Secure passwords

Important

Use HTTPS (which is enabled by default) to set your password or other sensitive configurations over the network. HTTPS enables secure and encrypted network connections, thereby protecting sensitive data, such as passwords.

The device password is the primary protection for your data and services. Axis devices do not impose a password policy as they may be used in various types of installations.

To protect your data we strongly recommend that you:

- Use a password with at least 8 characters, preferably created by a password generator.
- Don't expose the password.
- Change the password at a recurring interval, at least once a year.

Make sure that no one has tampered with the device software

To make sure that the device has its original AXIS OS, or to take full control of the device after a security attack:

1. Reset to factory default settings. See *Reset to factory default settings, on page 35*.
After the reset, secure boot guarantees the state of the device.
2. Configure and install the device.

Web interface overview

This video gives you an overview of the device's web interface.



Axis device web interface

Configure your device

Adjust the image

This section includes instructions about configuring your device. If you want to learn more about how certain features work, go to *Learn more, on page 22*.

Level the camera

To adjust the view in relation to a reference area or an object, use the level grid in combination with a mechanical adjustment of the camera.

1. Go to **Video > Image >** and click .
2. Click  to show the level grid.
3. Adjust the camera mechanically until the position of the reference area or the object is aligned with the level grid.

Select exposure mode

To improve image quality for specific surveillance scenes, use exposure modes. Exposure modes lets you control aperture, shutter speed, and gain. Go to **Video > Image > Exposure** and select between the following exposure modes:

- For most use cases, select **Automatic** exposure.
- For fast moving objects that require a fast or fixed shutter, select **Automatic aperture**.
- To maintain a longer depth of field or focus range, select **Automatic shutter**.
- For environments with certain artificial lighting, for example fluorescent lighting, select **Flicker-free**. Select the same frequency as the power line frequency.
- For environments with certain artificial light and bright light, for example outdoors with fluorescent lighting at night and sun during daytime, select **Flicker-reduced**. Select the same frequency as the power line frequency.
- If you need full control of all parameters, select **Manual**. This is mostly useful for scenes with little change in lighting.
- To lock the current exposure settings, select **Hold current**.

Benefit from IR light in low-light conditions by using night mode

Your camera uses visible light to deliver color images during the day. But as the visible light diminishes, color images become less bright and clear. If you switch to night mode when this happens, the camera uses both visible and near-infrared light to deliver bright and detailed black-and-white images instead. You can set the camera to switch to night mode automatically.

1. Go to **Video > Image > Day-night mode**, and make sure that the **IR-cut filter** is set to **Auto**.
2. To set at what light level you want the camera to switch to night mode, move the **Threshold** slider toward **Bright** or **Dark**.
3. To use the built-in IR light when the camera is in night mode, turn on **Allow illumination** and **Synchronize illumination**.
4. If you use an accessory IR illuminator, turn on **Allow illumination** and **Synchronize illumination** to use IR light when the camera is in night mode.

Note

If you set the switch to night mode to occur when it's brighter, the image remains sharper as there is less low-light noise. If you set the switch to occur when it's darker, the image colors are maintained for longer, but there is more image blur due to low-light noise.

Optimize IR illumination

Depending on the installation environment and the conditions around the camera, for example external light sources in the scene, you can sometimes improve the image quality if you manually adjust the intensity of the LEDs. If you have problems with reflections from the LEDs, you can try to reduce the intensity.

1. Go to **Video > Image > Day-night mode**.
2. Turn on **Allow illumination**.
3. Click  in the live view and select **Manual**.
4. Adjust the intensity.

You can also reduce the reflections by changing the illumination angle.

1. Go to **Video > Image > Day-night mode**.
2. Turn off **Automatic illumination angle**.
3. Adjust the illumination angle slider.

Reduce noise in low-light conditions

To reduce noise in low-light conditions, you can adjust one or more of the following settings:

- Adjust the trade-off between noise and motion blur. Go to **Video > Image > Exposure** and move the **Blur-noise trade-off** slider toward **Low noise**.
- Set the exposure mode to automatic.

Note

A high max shutter value can result in motion blur.

- To slow down the shutter speed, set max shutter to the highest possible value.

Note

When you reduce the max gain, the image can become darker.

- Set the max gain to a lower value.
- If there is an **Aperture** slider, move it towards **Open**.
- Reduce sharpness in the image, under **Video > Image > Appearance**.

If the above settings do not improve the image sufficiently, change to a lens with a lower f-value.

Reduce motion blur in low-light conditions

To reduce motion blur in low-light conditions, adjust one or more of the following settings in **Video > Image > Exposure**:

- Set **Exposure mode** to **Automatic** and turn on **Motion-adaptive exposure**.

Note

When you increase the gain, image noise also increases.

- Set **Max shutter** to a shorter time, and **Max gain** to a higher value.

Note

When you open the aperture, the depth of field gets shallower.

- Move the **Aperture** slider toward **Open**.

If you still have problems with motion blur:

- Increase the light level in the scene.
- Mount the camera so that objects move toward it or away from it rather than sideways.

Note

If you use a lens with a larger aperture, the depth of field gets shallower.

- Change to a lens with a larger aperture.

Maximize the details in an image

Important

If you maximize the details in an image, the bitrate will probably increase and you might get a reduced frame rate.

- Make sure to select the capture mode that has the highest resolution.
- Go to **Video > Stream > General** and set the compression as low as possible.
- Below the live view image, click  and in **Video format**, select MJPEG.
- Go to **Video > Stream > Zipstream** and select **Off**.

Handle scenes with strong backlight

Dynamic range is the difference in light levels in an image. In some cases the difference between the darkest and the brightest areas can be significant. The result is often an image where either the dark or the bright areas are visible. Wide dynamic range (WDR) makes both dark and bright areas of the image visible.



Image without WDR.



Image with WDR.

Note

- WDR can cause artifacts in the image.
 - WDR may not be available for all capture modes.
1. Go to **Video > Image > Wide dynamic range**.
 2. Turn on WDR.
 3. Use the **Local contrast** slider to adjust the amount of WDR.
 4. Use the **Tone mapping** slider to adjust the amount of WDR.
 5. To set the amount of WDR, select Low, Medium or High from the **WDR level** list.
 6. If you still have problems, go to **Exposure** and adjust the **Exposure zone** to cover the area of interest.

Find out more about WDR and how to use it at axis.com/web-articles/wdr.

Compensate for barrel distortion

Barrel distortion is a phenomenon where straight lines appear increasingly bent closer to the edges of the frame. A wide field of view often creates barrel distortion in an image. Barrel distortion correction compensates for this distortion.

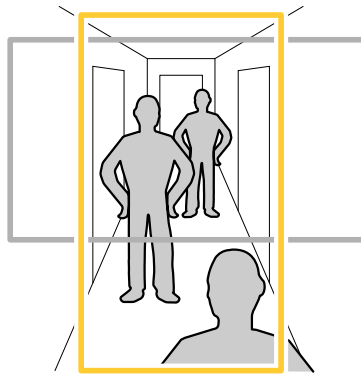
Note

Barrel distortion correction affects the image resolution and field of view.

1. Go to **Video > Installation > Image correction**.
2. Turn on **Barrel distortion correction (BDC)**.

Monitor long and narrow areas

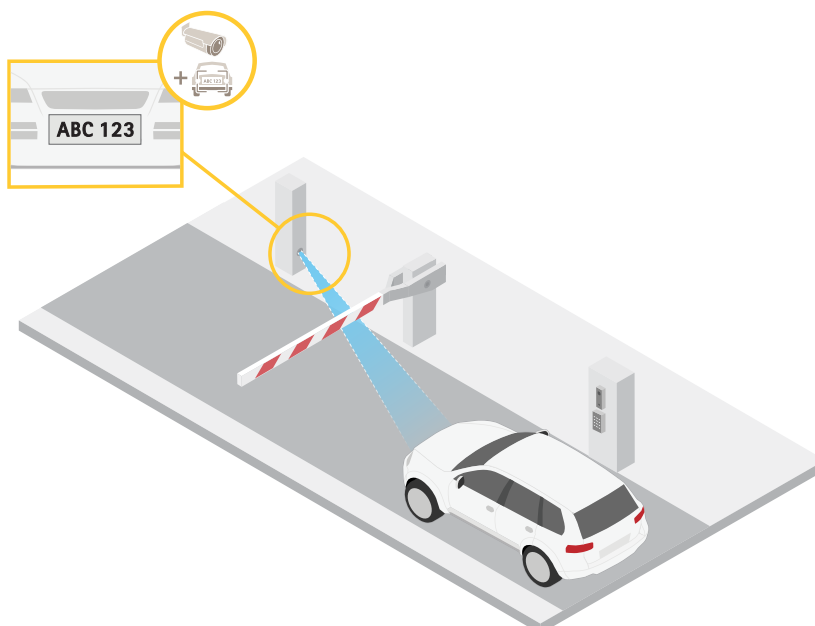
Use corridor format to better utilize the full field of view in a long and narrow area, for example a staircase, hallway, road, or tunnel.



1. Depending on your device, turn the camera or the 3-axis lens in the camera 90° or 270°.
2. If the device doesn't have automatic rotation of the view, go to **Video > Installation**.
3. Rotate the view 90° or 270°.

Verify the pixel resolution

To verify that a defined part of the image contains enough pixels to, for example, recognize license plates, you can use the pixel counter.



1. Go to **Video > Image**.
2. Click .
3. Click  for **Pixel counter**.
4. In the camera's live view, adjust the size and position of the rectangle around the area of interest, for example where you expect license plates to appear.
5. You can see the number of pixels for each of the rectangle's sides, and decide if the values are enough for your needs.

Hide parts of the image with privacy masks

You can create one or several privacy masks to hide parts of the image.

1. Go to **Video > Privacy masks**.
2. Click .
3. Click the new mask and type a name.
4. Adjust the size and placement of the privacy mask according to your needs.
5. To change the color for all privacy masks, click **Privacy masks** and select a color.

See also *Privacy masks*, on page 22

Show an image overlay

You can add an image as an overlay in the video stream.

1. Go to **Video > Overlays**.
2. Click **Manage images**.
3. Upload or drag and drop an image.
4. Click **Upload**.
5. Select **Image** from the drop-down list and click .
6. Select the image and a position. You can also drag the overlay image in the live view to change the position.

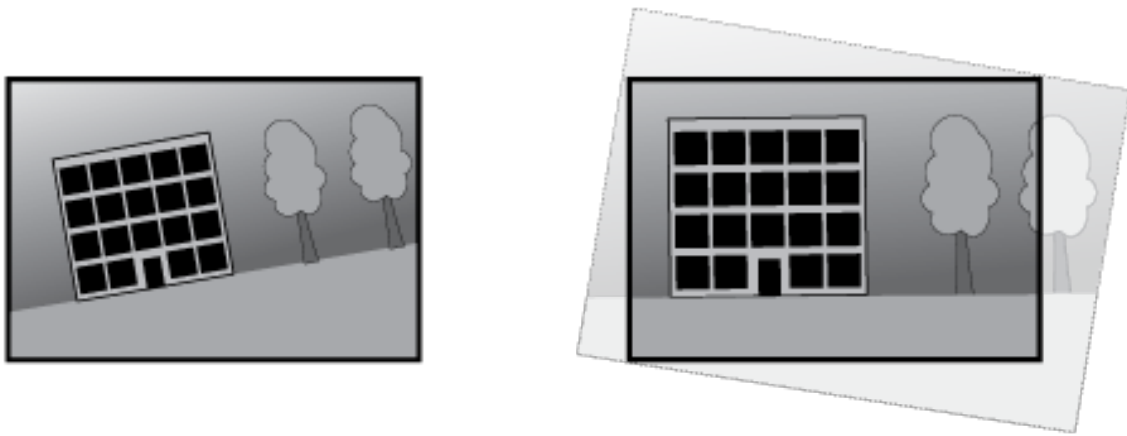
Show a text overlay

You can add a text field as an overlay in the video stream. This is useful for example when you want to display the date, time or a company name in the video stream.

1. Go to **Video > Overlays**.
2. Select **Text** and click .
3. Type the text you want to display, or select modifiers to show for example the current date.
4. Select a position. You can also click-and-drag the overlay in the live view to change the position.

Straighten a skewed image

You can straighten a skewed image by rotating and cropping it digitally. Due to the cropping, a part of the original image is lost. The functionality is useful during installation.



The illustration shows before and after an image has been straightened.

1. Go to **Video > Installation > Image correction**.
2. Turn on **Straighten image**.
3. Use the controls to adjust the image.

View and record video

This section includes instructions about configuring your device. To learn more about how streaming and storage works, go to *Streaming and storage*, on page 23.

Reduce bandwidth and storage

Important

Reducing the bandwidth can lead to loss of detail in the image.

1. Go to **Video > Stream**.
2. Click  in the live view.
3. Select **Video format AV1** if your device supports it. Otherwise select **H.264**.
4. Go to **Video > Stream > General** and increase **Compression**.
5. Go to **Video > Stream > Zipstream** and do one or more of the following:

Note

The **Zipstream** settings are used for all video encodings except MJPEG.

- Select the **Zipstream Strength** that you want to use.
- Turn on **Optimize for storage**. This can only be used if the video management software supports B-frames.
- Turn on **Dynamic FPS**.
- Turn on **Dynamic GOP** and set a high **Upper limit GOP length** value.

Note

Most web browsers don't support H.265 decoding and because of this the device doesn't support it in its web interface. Instead you can use a video management system or application that supports H.265 decoding.

View a live video stream on a monitor

Your camera can transmit a live video stream to a monitor even without a network connection. Connect the camera and the monitor using the RCA connectors. Use the monitor for surveillance purposes or for public viewing, for example in a store.

Your camera can transmit a live video stream to an HDMI monitor even without a network connection. Use the monitor for surveillance purposes or for public viewing, for example in a store.

1. Connect an external monitor using the HDMI connector.
2. Go to **System > Video out** and turn on **HDMI**.
3. Select a **Source**. Rotate the image if needed.

Important

To view the video stream via the HDMI connector, make sure to select a capture mode that supports HDMI.

Set up network storage

To store recordings on the network, you need to set up your network storage.

1. Go to **System > Storage**.
2. Click  **Add network storage** under **Network storage**.
3. Type the IP address of the host server.
4. Type the name of the shared location on the host server under **Network share**.
5. Type the username and password.
6. Select the SMB version or leave it on **Auto**.
7. Select **Add share without testing** if you experience temporary connection issues, or if the share is not yet configured.
8. Click **Add**.

Record and watch video

Record video directly from the camera

1. Go to **Video > Stream**.
2. To start a recording, click .

If you haven't set up any storage, click  and . For instructions on how to set up network storage, see *Set up network storage, on page 13*

3. To stop recording, click  again.

Watch video

1. Go to **Recordings**.
2. Click  for your recording in the list.

Set up rules for events

You can create rules to make your device perform an action when certain events occur. A rule consists of conditions and actions. The conditions can be used to trigger the actions. For example, the device can start a recording or send an email when it detects motion, or show an overlay text while the device is recording.

To learn more, see *Get started with rules for events*.

Trigger an action

1. Go to **System > Events** and add a rule. The rule defines when the device will perform certain actions. You can set up rules as scheduled, recurring, or manually triggered.
2. Enter a **Name**.

3. Select the **Condition** that must be met to trigger the action. If you specify more than one condition for the rule, all of the conditions must be met to trigger the action.
4. Select which **Action** to perform when the conditions are met.

Note

- If you change the definition of a stream profile that is used in a rule, you need to restart all the rules that use that stream profile.

Record video when the camera detects an object

This example explains how to set up the camera to start recording to the SD card when the camera detects an object. The recording will include five seconds before detection and one minute after detection ends.

Before you start:

- Make sure you have an SD card installed.

Make sure that AXIS Object Analytics is running:

Make sure that AXIS Video Motion Detection is running:

1. Go to **Apps > AXIS Object Analytics**.
2. Go to **Apps > AXIS Video Motion Detection**.
3. Start the application if it is not already running.
4. Make sure you have set up the application according to your needs.

Create a rule:

1. Go to **System > Events** and add a rule.
2. Type a name for the rule.
3. In the list of conditions, under **Application**, select **Object Analytics**.
4. In the list of conditions, under **Application**, select **VMD4**.
5. In the list of actions, under **Recordings**, select **Record video while the rule is active**.
6. In the list of storage options, select **SD_DISK**.
7. Select a camera and a stream profile.
8. Set the prebuffer time to 5 seconds.
9. Set the postbuffer time to 1 minute.
10. Click **Save**.

Show a text overlay in the video stream when the device detects an object

This example explains how to display the text "Motion detected" when the device detects an object.

Make sure that AXIS Object Analytics is running:

Make sure that AXIS Video Motion Detection is running:

1. Go to **Apps > AXIS Object Analytics**.
2. Go to **Apps > AXIS Video Motion Detection**.
3. Start the application if it is not already running.
4. Make sure you have set up the application according to your needs.

Add the overlay text:

1. Go to **Video > Overlays**.
2. Under **Overlays**, select **Text** and click **+**.
3. Enter #D in the text field.
4. Choose text size and appearance.

- To position the text overlay, click  and select an option.

Create a rule:

- Go to **System > Events** and add a rule.
- Type a name for the rule.
- In the list of conditions, under **Application**, select **Object Analytics**.
- In the list of conditions, under **Application**, select **VMD4**.
- In the list of actions, under **Overlay text**, select **Use overlay text**.
- Select a video channel.
- In **Text**, type "Motion detected".
- Set the duration.
- Click **Save**.

Note

If you update the overlay text it will be automatically updated on all video streams dynamically.

Record video when a PIR detector senses motion

This example explains how to connect a PIR detector (normally closed) to the device, and to start recording video when the detector senses motion.

Required hardware

- 3-wire cable (ground, power, I/O)
- PIR detector, normally closed

NOTICE

Disconnect the device from power before connecting the wires. Reconnect to power after all connections are done.

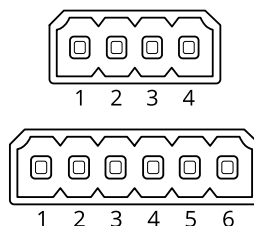
Connect the wires to the device's I/O connector

Note

For information on the I/O connector, see *Connectors, on page 29*.

- Connect the ground wire to pin 1 (GND/-).
- Connect the power wire to pin 2 (12V DC output).
- Connect the I/O wire to pin 3 (I/O input).

Connect the wires to the PIR detector's I/O connector



- Connect the other end of the ground wire to pin 1 (GND/-).
- Connect the other end of the power wire to pin 2 (DC input/+).
- Connect the other end of the I/O wire to pin 3 (I/O output).

Configure the I/O port in the device web interface

- Go to **System > Accessories > I/O ports**.
- Click  to set the direction to input for port 1.

3. Give the input module a descriptive name, for example "PIR detector".
4. If you want to trigger an event whenever the PIR detector senses motion, click  to set the normal state to circuit closed.

Create a rule

1. Go to **System > Events** and add a rule.
2. Type a name for the rule.
3. In the list of conditions, select **PIR detector**.
4. In the list of actions, under **Recordings**, select **Record video while the rule is active**.
5. In the list of storage options, select **SD_DISK**.
6. Select a camera and a stream profile.
7. Set the prebuffer time to 5 seconds.
8. Set the postbuffer time to 1 minute.
9. Click **Save**.

Provide visual indication of an ongoing event

You have the option to connect the AXIS I/O Indication LED to your network camera. This LED can be configured to turn on whenever certain events occur in the camera. For example, to let people know that video recording is in progress.

Required hardware

- AXIS I/O Indication LED
- An Axis network video camera

Note

AXIS I/O Indication LED should be connected to an output port.

Note

For instructions on how to connect the AXIS I/O Indication LED, see the installation guide provided with the product.

The following example shows how to configure a rule that turns on the AXIS I/O Indication LED to indicate that camera is recording.

1. Go to **System > Accessories > I/O ports**.
2. For the port that you connected the AXIS I/O Indication LED to, click  to set the direction to **Output**, and click  to set the normal state to **Circuit open**.
Make sure that the port you connected the AXIS I/O Indication LED to is set to **Output**. Set the normal state to **Circuit open**.
3. Go to **System > Events**.
4. Create a new rule.
5. Select the **Condition** that must be met to trigger the camera to start recording. It can, for example, be a time schedule or motion detection.
6. In the list of actions, select **Record video**. Select a storage space. Select a stream profile or create a new. Also set the **Prebuffer** and **Postbuffer** as required.
7. Save the rule.
8. Create a second rule and select the same **Condition** as in the first rule.
9. In the list of actions, select **Toggle I/O while the rule is active**, and then select the port the AXIS I/O Indication LED is connected to. Set the state to **Active**.

10. Save the rule.

Other scenarios where AXIS I/O Indication LED can be used are for example:

- Configure the LED to turn on when the camera starts, to indicate the presence of the camera. Select **System ready** as a condition.
- Configure the LED to turn on when live stream is active to indicate that a person or a program is accessing a stream from the camera. Select **Live stream accessed** as a condition.

Record video when the camera detects loud noises

This example explains how to set up the camera to start recording to the SD card five seconds before it detects loud noise and to stop two minutes after.

Note

The following instructions require that a microphone is connected to audio-in.

Turn on audio:

1. Set up the stream profile to include audio, see *Add audio to your recording, on page 19*.

Turn on audio detection:

1. Go to **System > Detectors > Audio detection**.
2. Adjust the sound level according to your needs.

Create a rule:

1. Go to **System > Events** and add a rule.
2. Type a name for the rule.
3. In the list of conditions, under **Audio**, select **Audio Detection**.
4. In the list of actions, under **Recordings**, select **Record video**.
5. In the list of storage options, select **SD_DISK**.
6. Select the stream profile where audio has been turned on.
7. Set the prebuffer time to 5 seconds.
8. Set the postbuffer time to 2 minutes.
9. Click **Save**.

Detect tampering with input signal

This example explains how to send an email when the input signal is cut or short-circuited. For more information about the I/O connector, see *page 32*.

1. Go to **System > Accessories > I/O ports** and turn on **Supervised**.
2. Go to **System > Accessories > I/O ports** and turn on **Supervised** for the relevant port.

Add an email recipient:

1. Go to **System > Events > Recipients** and add a recipient.
2. Type a name for the recipient.
3. Select **Email** as the notification type.
4. Type the recipient's email address.
5. Type the email address that you want the camera to send notifications from.
6. Provide the login details for the sending email account, along with the SMTP hostname and port number.
7. To test your email setup, click **Test**.
8. Click **Save**.

Create a rule:

1. Go to **System > Events > Rules** and add a rule.
2. Type a name for the rule.
3. In the list of conditions, under **I/O**, select **Supervised input tampering is active**.
4. Select the relevant port.
5. In the list of actions, under **Notifications**, select **Send notification to email** and then select the recipient from the list.
6. Type a subject line and message for the email.
7. Click **Save**.

Trigger a notification when the enclosure is opened

This example explains how to set up an email notification when the housing or casing of the device is opened.

Add an email recipient:

1. Go to **System > Events > Recipients** and click **Add recipient**.
2. Type a name for the recipient.
3. Select **Email** as the notification type.
4. Type the recipient's email address.
5. Type the email address that you want the camera to send notifications from.
6. Provide the login details for the sending email account, along with the SMTP hostname and port number.
7. To test your email setup, click **Test**.
8. Click **Save**.

Create a rule:

9. Go to **System > Events > Rules** and click **Add a rule**.
10. Type a name for the rule.
11. In the list of conditions, select **Casing open**.
12. In the list of actions, select **Send notification to email**.
13. Select a recipient from the list.
14. Type a subject line and message for the email.
15. Click **Save**.

Trigger a notification when the camera lens is tampered

This example explains how to set up an email notification when the camera lens gets either spray painted, covered, or blurred.

Activate the tampering detection:

1. Go to **System > Detectors > Camera tampering**.
2. Set a value for **Trigger delay**. The value indicates the time that must pass before an email is sent.
3. Turn on **Trigger on dark images** to detect if the lens is sprayed, covered, or rendered severely out of focus.

Add an email recipient:

4. Go to **System > Events > Recipients** and add a recipient.
5. Type a name for the recipient.
6. Select **Email** as the notification type.
7. Type the recipient's email address.

8. Type the email address that you want the camera to send notifications from.
9. Provide the login details for the sending email account, along with the SMTP hostname and port number.
10. To test your email setup, click **Test**.
11. Click **Save**.

Create a rule:

12. Go to **System > Events > Rules** and add a rule.
13. Type a name for the rule.
14. In the list of conditions, under **Video**, select **Tampering**.
15. In the list of actions, under **Notifications**, select **Send notification to email** and then select the recipient from the list.
16. Type a subject line and message for the email.
17. Click **Save**.

Audio

Add audio to your recording

Note

To connect the audio device, this product requires a multicable.

Turn on audio:

1. Go to **Video > Stream > Audio** and include audio.
2. If the device has more than one input source, select the correct one in **Source**.
3. Go to **Audio > Device settings** and turn on the correct input source.

Edit the stream profile that is used for the recording:

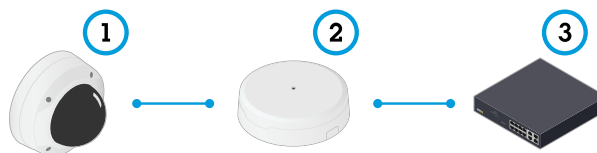
4. Go to **System > Stream profiles** and select the stream profile.
5. Select **Include audio** and turn it on.
6. Click **Save**.

Add audio capability to your product using portcast

With portcast technology, you can add audio capability to your product. It allows audio and I/O communication digitally over the network cable between the camera and the interface.

To add audio capability to your Axis network video device, connect the portcast compatible Axis audio device and I/O Interface between your device and the PoE switch which provides power.

1. Connect the Axis network video device (1) and the Axis portcast device (2) with a PoE cable.
2. Connect the Axis portcast device (2) and the PoE switch (3) with a PoE cable.



- 1 Axis network video device
- 2 Axis portcast device
- 3 Switch

Once the devices are connected, an audio tab becomes visible in the settings for your Axis network video device. Go to the audio tab and turn on **Allow audio**.

See your Axis portcast device's user manual for more information.

Connect to a network speaker

Network speaker pairing allows you to use a compatible Axis network speaker as if it is connected directly to the camera. Once paired, the speaker acts as an audio out device where you can play audio clips and transmit sound through the camera.

Important

For this feature to work with a video management software (VMS), you must first pair the camera with the network speaker, then add the camera to your VMS.

Pair camera with network speaker

1. Go to **System > Edge-to-edge > Pairing**.
2. Click  **Add** and select the pairing type **Audio** from the drop-down list.
3. Select **Speaker pairing**.
4. Type the network speaker's IP address, username and password.
5. Click **Connect**. A confirmation message appears.

Connect to a strobe siren

Network pairing allows you to pair a camera with a compatible Axis device with light and siren functionality. Once paired, the camera can configure and maintain both devices.

Pair the camera with a strobe siren:

1. Go to **System > Edge-to-edge > Pairing**.
2. Click  **Add** and select the pairing type **Network pairing** from the drop-down list.
3. Type the IP address, username and password of the strobe siren.
4. Click **Connect**. A confirmation message appears.

To find devices directly on the network, click **Discover devices**.

Note

- The list shows all Axis devices that are found, not only devices that can be paired.
- An info icon is shown for devices that have already been paired. Hover over the icon to get information about pairings that are already active.
- Make sure the paired devices run the same AXIS OS version.

Important

- It's only possible to discover devices where Bonjour is enabled. To enable Bonjour for a device, open its web interface and go to **System > Network > Network discovery protocols**.

The web interface

To read about all the features and settings available in the web interface of devices with AXIS OS, go to *AXIS OS web interface help*.

Learn more

Privacy masks

A privacy mask is a user-defined area that prevents users from viewing a part of the monitored area. In the video stream, privacy masks appear as blocks of solid color.

A privacy mask is a user-defined area that prevents users from viewing a part of the monitored area. In the video stream, privacy masks appear as blocks of solid color or blurred image elements.

A privacy mask is a user-defined area that covers a part of the monitored area. In the video stream, privacy masks appear either as blocks of solid color or with a mosaic pattern.

A privacy mask is a user-defined area that covers part of the monitored area. In the video stream, privacy masks can appear as blocks of solid color, mosaic patterns, or in chameleon mode, which dynamically adapts to the scene to enhance privacy protection.

The privacy mask is relative to the pan, tilt, and zoom coordinates, so regardless of where you point the camera, the privacy mask covers the same place or object.

You'll see the privacy mask on all snapshots, recorded video, and live streams.

You can use the VAPIX® application programming interface (API) to hide the privacy masks.

Important

If you use multiple privacy masks it may affect the product's performance.

You can create several privacy masks. Each mask can have 3 to 10 anchor points.

Important

Set the zoom and focus before you create a privacy mask.

Note

You can't add privacy masks to the quad stream, but it will show all privacy masks configured on the individual channels.

Note

Privacy masks may appear warped in some view modes.

Overlays

Note

Overlays are not included in the video stream when using SIP calls.

Note

Image and text overlay will not be displayed on video stream over HDMI .

Note

Image and text overlay will not be displayed on video stream over SDI.

Overlays are superimposed over the video stream. They are used to provide extra information during recordings, such as a timestamp, or during product installation and configuration. You can add either text or an image.

The video streaming indicator is another type of overlay. It shows you that the live view video stream is live.

Note

Overlays are included in all video streams except SIP calls when the connection is over PoE class 3.

Streaming and storage

Video compression formats

Decide which compression method to use based on your viewing requirements, and on the properties of your network. The available options are:

Motion JPEG

Note

To ensure support for the Opus audio codec, the Motion JPEG stream is always sent over RTP.

Motion JPEG, or MJPEG, is a digital video sequence that is made up of a series of individual JPEG images. These images are then displayed and updated at a rate sufficient to create a stream that shows constantly updated motion. For the viewer to perceive motion video the rate must be at least 16 image frames per second. Full motion video is perceived at 30 (NTSC) or 25 (PAL) frames per second.

The Motion JPEG stream uses considerable amounts of bandwidth, but provides excellent image quality and access to every image contained in the stream.

H.264 or MPEG-4 Part 10/AVC

Note

H.264 is a licensed technology. The Axis product includes one H.264 viewing client license. To install additional unlicensed copies of the client is prohibited. To purchase additional licenses, contact your Axis reseller.

H.264 can, without compromising image quality, reduce the size of a digital video file by more than 80% compared to the Motion JPEG format and by as much as 50% compared to older MPEG formats. This means that less network bandwidth and storage space are required for a video file. Or seen another way, higher video quality can be achieved for a given bitrate.

H.265 or MPEG-H Part 2/HEVC

H.265 can, without compromising image quality, reduce the size of a digital video file by more than 25% compared to H.264.

Note

- H.265 is licensed technology. The Axis product includes one H.265 viewing client license. Installing additional unlicensed copies of the client is prohibited. To purchase additional licenses, contact your Axis reseller.
- Most web browsers don't support H.265 decoding and because of this the camera doesn't support it in its web interface. Instead you can use a video management system or application supporting H.265 decoding.

AV1

AV1 (AOMedia Video 1) is a license -free video coding format optimized for streaming media. AV1 enables high-quality video streaming even in bandwidth-constrained environments. By reducing a video's bitrate, AV1 preserves video quality while minimizing data usage.

AV1 supports all major browsers, computer operating systems and mobile platforms.

Note

AV1 requires more processing power for encoding and decoding compared to some other codecs.

How do Image, Stream, and Stream profile settings relate to each other?

The **Image** tab contains camera settings that affect all video streams from the product. If you change something in this tab, it immediately affects all video streams and recordings.

The **Stream** tab contains settings for video streams. You get these settings if you request a video stream from the product and don't specify for example resolution, or frame rate. When you change the settings in the **Stream** tab, it doesn't affect ongoing streams, but it will take effect when you start a new stream.

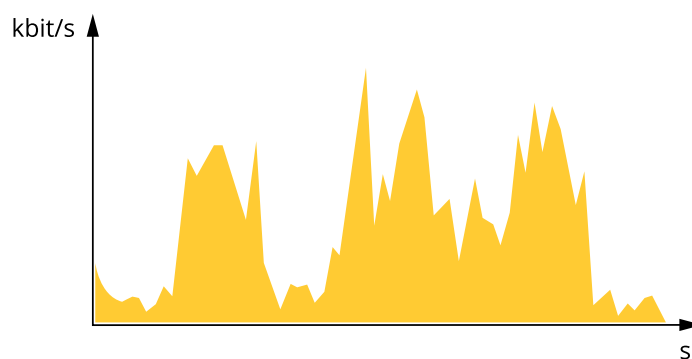
The **Stream profiles** settings override the settings from the **Stream** tab. If you request a stream with a specific stream profile, the stream contains the settings of that profile. If you request a stream without specifying a stream profile, or request a stream profile that doesn't exist in the product, the stream contains the settings from the **Stream** tab.

Bitrate control

Bitrate control helps you to manage the bandwidth consumption of your video stream.

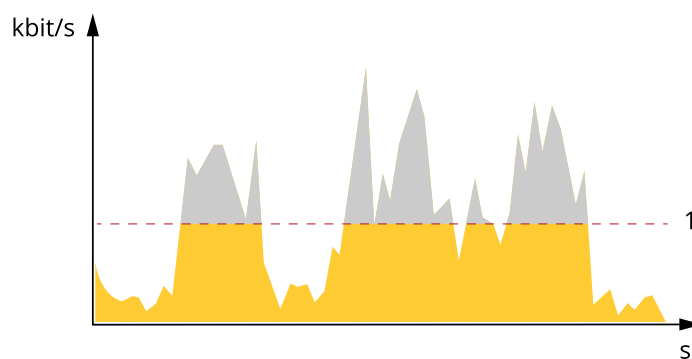
Variable bitrate (VBR)

Variable bitrate allows the bandwidth consumption to vary depending on the level of activity in the scene. The more activity, the more bandwidth you need. With variable bitrate you are guaranteed constant image quality, but you need to make sure you have storage margins.



Maximum bitrate (MBR)

Maximum bitrate lets you set a target bitrate to handle bitrate limitations in your system. You might see a decline in image quality or frame rate as the instantaneous bitrate is kept below the specified target bitrate. You can choose to prioritize either image quality or frame rate. We recommend that you configure the target bitrate to a higher value than the expected bitrate. This gives you a margin in case there is a high level of activity in the scene.



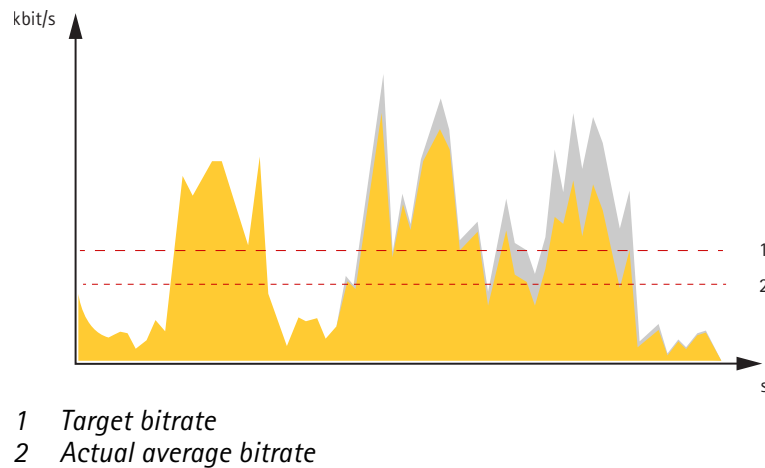
1 Target bitrate

Average bitrate (ABR)

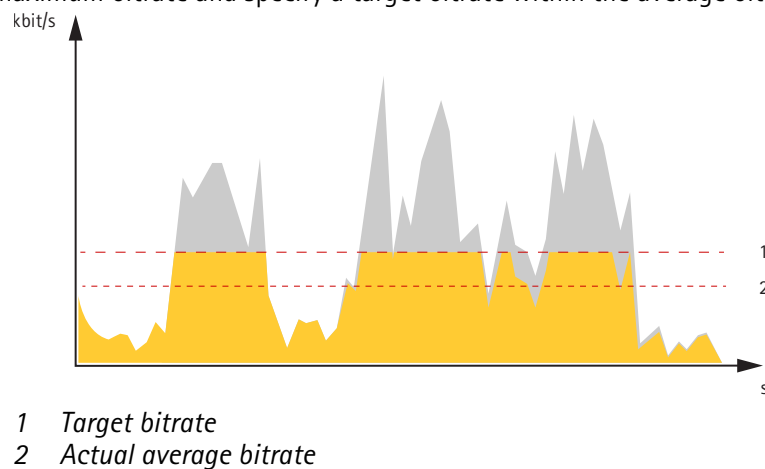
With average bitrate, the bitrate is automatically adjusted over a longer period of time. This is so you can meet the specified target and provide the best video quality based on your available storage. Bitrate is higher in scenes with a lot of activity, compared to static scenes. You are more likely to get better image quality when in scenes with a lot of activity if you use the average bitrate option. You can define the total storage required to store the video stream for a specified amount of time (retention time) when image quality is adjusted to meet the specified target bitrate. Specify the average bitrate settings in one of the following ways:

- To calculate the estimated storage need, set the target bitrate and the retention time.

- To calculate the average bitrate, based on available storage and required retention time, use the target bitrate calculator.



You can also turn on maximum bitrate and specify a target bitrate within the average bitrate option.



Edge-to-edge technology

Edge-to-edge is a technology that makes IP devices communicate directly with each other. It offers smart pairing functionality between, for example, Axis cameras and Axis audio or radar products.

Note

Make sure the paired devices run the same AXIS OS version.

For more information, see the white paper "Edge-to-edge technology" at whitepapers.axis.com/edge-to-edge-technology.

Speaker pairing

Edge-to-edge speaker pairing allows you to use a compatible Axis network speaker as if it's part of your camera. Once paired, the speaker's features are integrated in the camera's web interface and the network speaker acts as an audio out device where you can play audio clips and transmit sound through the camera.

The camera will identify itself to the VMS as a camera with integrated audio output and redirect any played audio to the speaker.

Network pairing

With edge-to-edge network pairing, you can connect your camera to a compatible Axis device with light and siren or illuminator light functionality and benefit from its integrated features.

Analytics and apps

With analytics and apps you can get more out of your Axis device. AXIS Camera Application Platform (ACAP) is an open platform that makes it possible for third parties to develop analytics and other apps for Axis devices. Apps can be preinstalled on the device, available for download for free, or for a license fee.

To find the user manuals for Axis analytics and apps, go to *help.axis.com*.

Note

- We recommended running one app at a time.
- Several apps can run at the same time but some apps might not be compatible with each other. Certain combinations of apps might require too much processing power or memory resources when run in parallel. Verify that the apps work together before deployment.
- Avoid running apps when the built-in motion detection is active.
- Apps are supported on channel 1.

AXIS Object Analytics

AXIS Object Analytics is an analytic application that comes preinstalled on the camera. It detects objects that move in the scene and classifies them as, for example, humans or vehicles. You can set up the application to send alarms for different types of objects. To find out more about how the application works, see *AXIS Object Analytics user manual*.

Metadata visualization

Analytics metadata is available for moving objects in the scene. Supported object classes are visualized in the video stream through a bounding box surrounding the object, along with information about the object type and confidence level of the classification. To learn more about how to configure and consume analytics metadata, see *AXIS Scene Metadata integration guide*.

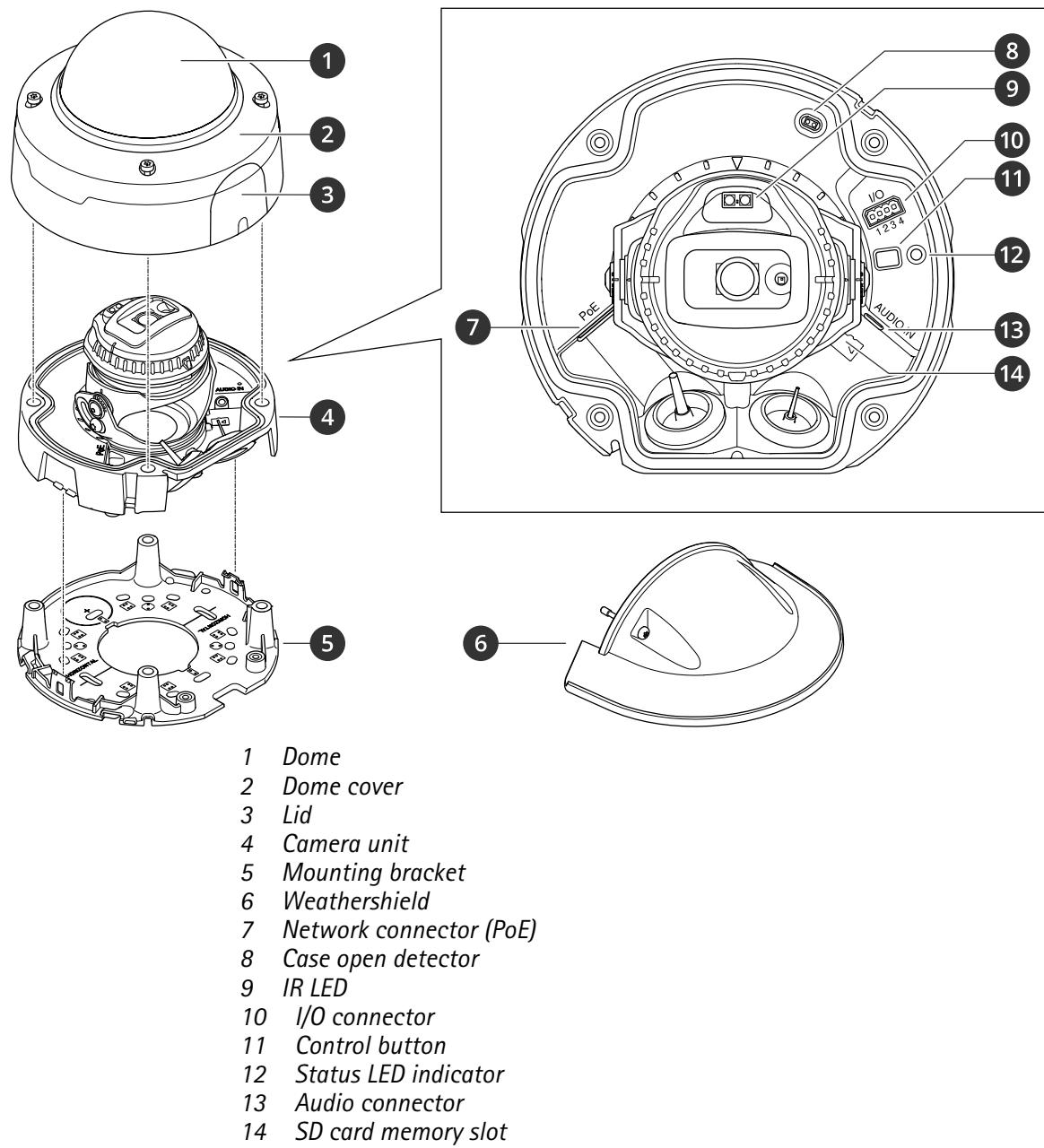
AXIS Image Health Analytics

AXIS Image Health Analytics is an AI-based application that can be used to detect image degradations or tampering attempts. The application analyzes and learns the behavior of the scene to detect blurriness or underexposure in the image, or to detect an obstructed or redirected view. You can set up the application to send events for any of these detections, and trigger actions through the camera's event system or third-party software.

To find out more about how the application works, see *AXIS Image Health Analytics user manual*.

Specifications

Product overview



LED indicators

- Note
- The Status LED can be configured to flash while an event is active.
 - The LEDs turn off when you close the casing.

Status LED	Indication
Unlit	Connection and normal operation.
Green	Shows steady green for 10 seconds for normal operation after startup completed. Flashes green during wireless network pairing. Steady green for normal operation.

	Flashes before startup if the temperature is below -20 °C and heating is required. The product starts when it reaches operating temperature.
Amber	Steady during startup. Flashes during device software upgrade or reset to factory default. Steady during startup. Flashes when restoring settings.
Amber/Red	Flashes amber/red if network connection is unavailable or lost.
Red	Device software upgrade failure.

Network LED	Indication
Green	Steady for connection to a 100 Mbit/s network. Flashes for network activity. Steady for connection to a 1 Gbit/s network. Flashes for network activity.
Amber	Steady for connection to a 10 Mbit/s network. Flashes for network activity. Steady for connection to a 10/100 Mbit/s network. Flashes for network activity.
Unlit	No network connection.

Power LED	Indication
Green	Normal operation.
Amber	Flashes green/amber during device software upgrade.

Microphone power LED	Indication
Unlit	Phantom power off.
Blue	Phantom power on. Steady when the phantom power is on and the microphone is connected. Flashes when the phantom power is on and the microphone is disconnected.

Wireless LED	Indication
Unlit	Wired mode.
Green	Steady for connection to a wireless network. Flashes for network activity.
Red	Steady for no wireless network connection. Flashes while scanning for wireless networks.
Amber	Steady or flashing during wireless network pairing.

Note

- The tally LED (indication LED) only indicates network transmission. If video or audio is only transmitted through HDMI or SDI the tally LED will be unlit.

Tally LED	Indication
Unlit	Camera idle.
Red	Active network transmission or recording.

SD card slot

NOTICE

- Risk of damage to SD card. Don't use sharp tools, metal objects, or excessive force when inserting or removing the SD card. Use your fingers to insert and remove the card.
- Risk of data loss and corrupted recordings. Unmount the SD card from the device's web interface before removing it. Don't remove the SD card while the product is running.

This device supports SD/SDHC/SDXC cards.

This device supports microSD/microSDHC/microSDXC cards.

For SD card recommendations, see axis.com.

 SD, SDHC, and SDXC Logos are trademarks of SD-3C LLC. SD, SDHC and SDXC are trademarks or registered trademarks of SD-3C, LLC in the United States, other countries or both.

 microSD, microSDHC, and microSDXC Logos are trademarks of SD-3C LLC. microSD, microSDHC, microSDXC are trademarks or registered trademarks of SD-3C, LLC in the United States, other countries or both.

Buttons

Control button

The control button is used for:

- Enabling the Focus Assistant. Press and very quickly release the Control button.
- Resetting the product to factory default settings. See *Reset to factory default settings, on page 35*.
- Ensuring the camera is level. Press the button for not more than two seconds to start the leveling assistant and press again to stop. The status LED and buzzer signal (see) assist leveling of the camera. The camera is level when the buzzer beeps continuously.
- Ensuring the camera is level. Press the button for not more than two seconds to start the leveling assistant and press again to stop. The buzzer signal (see) assist leveling of the camera. The camera is level when the buzzer beeps continuously.
- Connecting to an AXIS Video Hosting System service. To connect, press and hold the button for about 3 seconds until the status LED flashes green.
- Connecting to a one-click cloud connection (O3C) service over the internet. To connect, press and release the button, then wait for the status LED to flash green three times.

Connectors

Network connector

The Axis device is available in two variants with different network connectors:

RJ45 Ethernet connector.

RJ45 Ethernet connector with Power over Ethernet (PoE).

RJ45 Ethernet connector with Power over Ethernet Plus (PoE+).

RJ45 with High Power over Ethernet (High PoE).

RJ45 Push-pull Connector (IP66) with High Power over Ethernet (High PoE).

RJ45 Ethernet service port.

D-coded M12 connector with Power over Ethernet (PoE).

SFP connector.

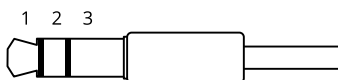
NOTICE

To comply with the IP66-rated design of the camera and maintain the IP66 protection, the supplied RJ45 Push-pull Connector (IP66) shall be used. Alternatively, use the RJ45 IP66-rated cable with premounted connector which is available from your Axis reseller. Don't remove the plastic network connector shield from the camera.

Audio connector

3.5 mm connector

- **Audio in** – 3.5 mm input for a mono microphone, or a line-in mono signal (left channel is used from a stereo signal).
- **Audio in** – 3.5 mm input for a digital microphone, an analog mono microphone, or a line-in mono signal (left channel is used from a stereo signal).
- **Audio in** – 3.5 mm input for two mono microphones, or two line-in mono signals (using the supplied stereo-to-mono adapter).
- **Audio in** – 3.5 mm input for a stereo microphone, or a line-in stereo signal.
- **Audio out** – 3.5 mm output for audio (line level) that can be connected to a public address (PA) system or an active speaker with a built-in amplifier. A stereo connector must be used for audio out.
- **Audio out** – 3.5 mm output for audio (line level) that can be connected to a public address (PA) system or an active speaker with balanced input and a built-in amplifier. A balanced connector must be used for audio out.
- **Audio out** – 3.5 mm output for audio (line level) that can be connected to a public address (PA) system or an active speaker with a built-in amplifier. A pair of headphones can also be attached. A stereo connector must be used for audio out.



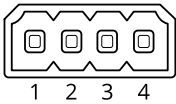
Audio input

1 Tip	2 Ring	3 Sleeve
Unbalanced microphone (with or without electret power) or line-in	Electret power if selected	Ground
Balanced microphone (with or without phantom power) or line-in, "hot" signal	Balanced microphone (with or without phantom power) or line-in, "cold" signal	Ground
Digital signal	Ring power if selected	Ground
Stereo unbalanced microphone (with or without electret power) or line-in, "left"	Stereo unbalanced microphone (with or without electret power) or line-in, "right"	Ground

Audio output

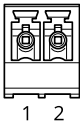
1 Tip	2 Ring	3 Sleeve
Channel 1, unbalanced line, mono	Channel 1, unbalanced line, mono	Ground
Balanced line, "hot" signal	Balanced line, "cold" signal	Ground
Stereo unbalanced line, "left"	Stereo unbalanced line, "right"	Ground
Channel 1, unbalanced line	Channel 2, unbalanced line	Ground

4-pin terminal block for audio input and output.



Function	Pin	Notes
GND	1	Ground
Ring power	2	12 V for external source
Microphone/Line in	3	Microphone (analog or digital) or line in (mono). 5 V microphone bias is available.
Line out	4	Line level audio output (mono). Can be connected to a public address (PA) system or an active speaker with a built-in amplifier.

2-pin terminal block for line out.



Function	Pin	Notes
Line out (+)	1	Line audio out
0 V DC (-)	2	

2-pin terminal block for amplifier out.

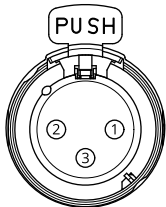
Function	Pin
Amplifier out (+)	1
Amplifier out (-)	2

The internal microphone is used by default; the external microphone is used when connected. You can disable the internal microphone by connecting a plug to the microphone input.

The external microphone is used when connected.

XLR connector

- Left – 3-pin XLR connector for balanced audio input. Use left connector for mono.
- Right – 3-pin XLR connector for balanced audio input.



Pin	1	2	3
Function	Ground	Balanced Microphone Hot (+) In	Balanced Microphone Cold (-) In

I/O connector

Use the I/O connector with external devices in combination with, for example, motion detection, event triggering, and alarm notifications. In addition to the 0 VDC reference point and power (12 V DC output), the I/O connector provides the interface to:

Digital input – For connecting devices that can toggle between an open and closed circuit, for example PIR sensors, door/window contacts, and glass break detectors.

Supervised input – Enables possibility to detect tampering on a digital input.

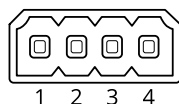
Digital output – For connecting external devices such as relays and LEDs. Connected devices can be activated by the VAPIX® Application Programming Interface, through an event or from the device's web interface.

A digital light sensor – For receiving a value of the ambient light intensity from an external light sensor. This is used to control the device's day and night functionality.

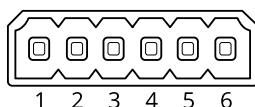
Note

The I/O connector is connected to the housing (fan/heater) on delivery. In case of a fan or heater error, an input signal will be triggered in the camera. Set up an action rule in the camera to configure which action the signal shall trigger.

4-pin terminal block



6-pin terminal block



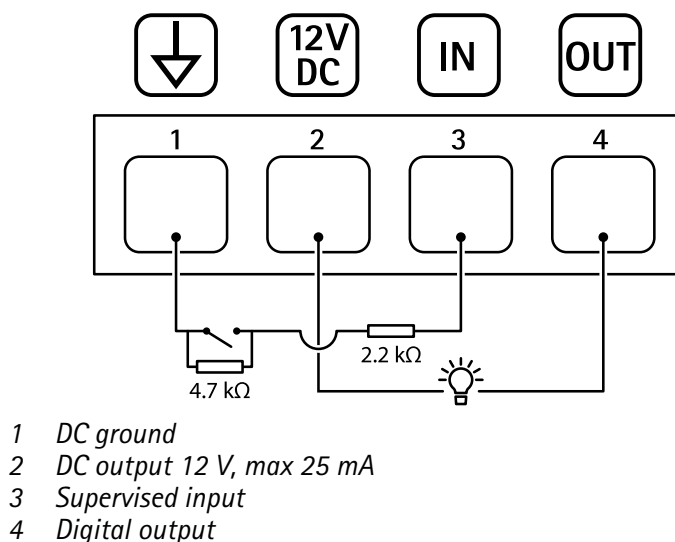
Function	Pin	Notes	Specifications
DC ground	1		0 VDC
DC output	2	 Can be used to power auxiliary equipment. Note: This pin can only be used as power out.	12 VDC Max load = 25 mA
Digital Input or Supervised Input	3	Connect to pin 1 to activate, or leave floating (unconnected) to deactivate. To use supervised input, install end-of-line resistors. See connection diagram for information about how to connect the resistors.	0 to max 30 VDC
Digital Output	4	Internally connected to pin 1 (DC ground) when active, and floating (unconnected) when inactive. If used with an inductive load, e.g., a relay, connect a diode in parallel with the load, to protect against voltage transients.	0 to max 30 VDC, open drain, 100 mA

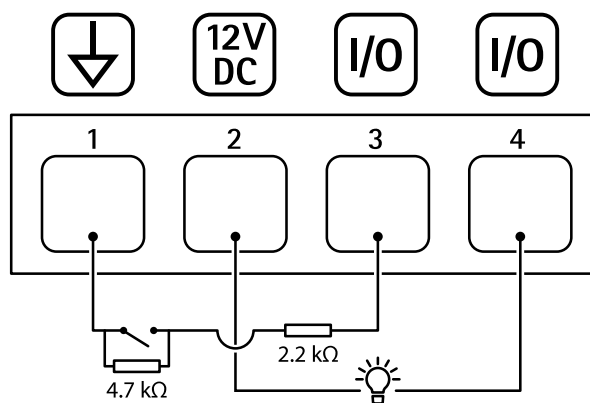
Function	Pin	Notes	Specifications
DC ground	1		0 VDC
DC output	2	 Can be used to power auxiliary equipment.	12 VDC Max load = 50 mA

		Note: This pin can only be used as power out.	
Configurable (Input or Output)	3–4	Digital input or Supervised input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate. To use supervised input, install end-of-line resistors. See connection diagram for information about how to connect the resistors.	0 to max 30 VDC
		Digital output – Internally connected to pin 1 (DC ground) when active, and floating (unconnected) when inactive. If used with an inductive load, e.g., a relay, connect a diode in parallel with the load, to protect against voltage transients.	0 to max 30 VDC, open drain, 100 mA

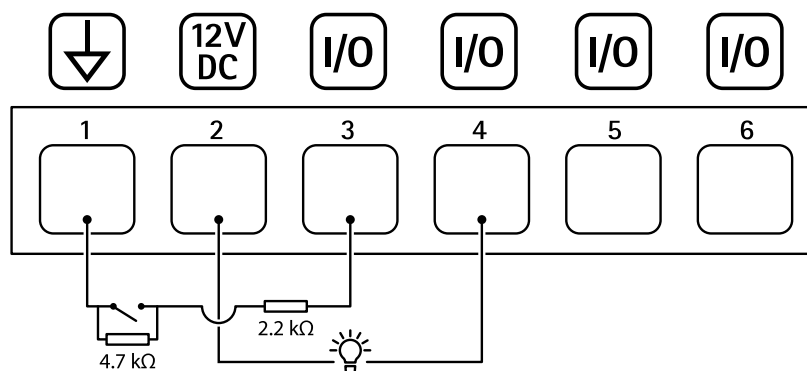
Function	Pin	Notes	Specifications
DC ground	1		0 VDC
DC output	2	 Can be used to power auxiliary equipment. Note: This pin can only be used as power out.	12 VDC Max load = 50 mA
Configurable (Input or Output)	3–6	Digital input or Supervised input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate. To use supervised input, install end-of-line resistors. See connection diagram for information about how to connect the resistors.	0 to max 30 VDC
		Digital output – Internally connected to pin 1 (DC ground) when active, and floating (unconnected) when inactive. If used with an inductive load, e.g., a relay, connect a diode in parallel with the load, to protect against voltage transients.	0 to max 30 VDC, open drain, 100 mA

Example:





- 1 DC ground
- 2 DC output 12 V, max 50 mA
- 3 I/O configured as supervised input
- 4 I/O configured as output



- 1 DC ground
- 2 DC output 12 V, max 50 mA
- 3 I/O configured as supervised input
- 4 I/O configured as output
- 5 Configurable I/O
- 6 Configurable I/O

Troubleshooting

Reset to factory default settings

▲ WARNING

⚠ Possibly hazardous optical radiation is emitted from this product. It can be harmful to the eyes. Don't stare at the operating lamp.

Important

Reset to factory default should be used with caution. A reset to factory default resets all settings, including the IP address, to the factory default values.

Note

For products with multiple IP addresses and AXIS OS 11.11 or earlier, channel 1 will have the address 192.168.0.90, channel 2 will have the address 192.168.0.91 and so on. Products with AXIS OS 12.0 and later will obtain a distinct IP address obtained from the link-local address subnet for each channel (169.254.x.x).

To reset the product to the factory default settings:

1. Disconnect power from the product.
2. Press and hold the control button while reconnecting power. See *Product overview*, on page 27.
3. Keep the control button pressed for 15–30 seconds until the status LED indicator flashes amber.
4. Release the control button. The process is complete when the status LED indicator turns green. If no DHCP server is available on the network, the device IP address will default to one of the following:
 - **Devices with AXIS OS 12.0 and later:** Obtained from the link-local address subnet (169.254.0.0/16)
 - **Devices with AXIS OS 11.11 and earlier:** 192.168.0.90/24
5. Use the installation and management software tools to assign an IP address, set the password, and access the device.
The installation and management software tools are available from the support pages on axis.com/support.
6. Refocus the product.
 1. Press and hold the control button and the restart button at the same time.
 2. Release the restart button but continue to hold down the control button for 15–30 seconds until the status LED indicator flashes amber.
 3. Release the control button. The process is complete when the status LED indicator turns green. If no DHCP server is available on the network, the device IP address will default to one of the following:
 - **Devices with AXIS OS 12.0 and later:** Obtained from the link-local address subnet (169.254.0.0/16)
 - **Devices with AXIS OS 11.11 and earlier:** 192.168.0.90/24
4. Use the installation and management software tools to assign an IP address, set the password and access the video stream.
5. Release the restart button and hold the control button.
6. Keep the control button pressed until the power LED indicator turns green and the 4 status LED indicators turn amber (this may take up to 15 seconds).
7. Keep the control button pressed until the power LED indicator turns green and the 6 status LED indicators turn amber (this may take up to 15 seconds).
8. Release the control button. When the status LED indicators display green (which can take up to 1 minute) the process is complete and the unit has been reset.
9. The process is now complete. If no DHCP server is available on the network, the device IP addresses will default to either of the following:
 - **Devices with AXIS OS 12.0 and later:** Obtained from the link-local address subnet (169.254.x.x)

- **Devices with AXIS OS 11.11 and earlier:** 192.168.0.90 to 192.168.0.93
- 10. The process is now complete. If no DHCP server is available on the network, the device IP addresses will default to either of the following:
 - **Devices with AXIS OS 12.0 and later:** Obtained from the link-local address subnet (169.254.x.x)
 - **Devices with AXIS OS 11.11 and earlier:** 192.168.0.90 to 192.168.0.95
- 11. Use the installation and management software tools to assign the IP addresses, set the password and access the video stream.

Note

To reset a single channel to the original factory default settings, log in to the device's web interface and use the provided button.

1. Press and hold the control button and the power button for 15–30 seconds until the status LED indicator flashes amber. See *Product overview, on page 27*.
2. Release the control button but continue to hold down the power button until the status LED indicator turns green.
3. Release the power button and assemble the product.
4. The process is now complete. The product has been reset to the factory default settings. If no DHCP server is available on the network, the device IP address will default to one of the following:
 - **Devices with AXIS OS 12.0 and later:** Obtained from the link-local address subnet (169.254.0.0/16)
 - **Devices with AXIS OS 11.11 and earlier:** 192.168.0.90/24
5. Using the installation and management software tools to assign an IP address, set the password and access the video stream.
 1. Press and hold the control button and the power button. See *Product overview, on page 27*.
 2. Release the power button but continue to hold down the control button for 15–30 seconds until the status LED indicator flashes amber.
 3. Release the control button.
 4. The process is now complete. The product has been reset to the factory default settings. If no DHCP server is available on the network, the device IP address will default to one of the following:
 - **Devices with AXIS OS 12.0 and later:** Obtained from the link-local address subnet (169.254.0.0/16)
 - **Devices with AXIS OS 11.11 and earlier:** 192.168.0.90/24
 5. Using the installation and management software tools, assign an IP address, set the password and access the video stream.

You can also reset parameters to factory default through the device's web interface. Go to **Maintenance > Factory default** and click **Default**.

AXIS OS options

Axis offers device software management according to either the active track or the long-term support (LTS) tracks. Being on the active track means continuously getting access to all the latest product features, while the LTS tracks provide a fixed platform with periodic releases focused mainly on bug fixes and security updates.

Using AXIS OS from the active track is recommended if you want to access the newest features, or if you use Axis end-to-end system offerings. The LTS tracks are recommended if you use third-party integrations, which are not continuously validated against the latest active track. With LTS, the products can maintain cybersecurity without introducing any significant functional changes or affecting any existing integrations. For more detailed information about Axis device software strategy, go to axis.com/support/device-software.

Check the current AXIS OS version

AXIS OS determines the functionality of our devices. When you troubleshoot a problem, we recommend that you to start by checking the current AXIS OS version. The latest version might contain a correction that fixes your particular problem.

To check the current AXIS OS version:

1. Go to the device's web interface > **Status**.
2. Under **Device info**, see the AXIS OS version.

Upgrade AXIS OS

Important

- When you upgrade the device software, your preconfigured and customized settings are saved. Axis Communications AB can't guarantee that the settings are saved, even if the features are available in the new AXIS OS version.
- Starting from AXIS OS 12.6, you must install every LTS version between your device's current version and the target version. For example, if the currently installed device software version is AXIS OS 11.2, you have to install the LTS version AXIS OS 11.11 before you can upgrade the device to AXIS OS 12.6. For more information, see *AXIS OS Lifecycle guide: Upgrade path*.
- Make sure the device remains connected to the power source throughout the upgrade process.
- Make sure the cover is attached during upgrade to avoid installation failure.

Note

- When you upgrade the device with the latest AXIS OS version in the active track, the product receives the latest functionality available. Always read the upgrade instructions and release notes available with each new release before you upgrade. To find the latest AXIS OS version and the release notes, go to axis.com/support/device-software.
1. Download the AXIS OS file to your computer, available free of charge at axis.com/support/device-software.
 2. Log in to the device as an administrator.
 3. Go to **Maintenance > AXIS OS upgrade** and click **Upgrade**.

When the upgrade has finished, the product restarts automatically.

You can use AXIS Device Manager to upgrade multiple devices at the same time. Find out more at axis.com/products/axis-device-manager.

Technical problems and possible solutions

Problems upgrading AXIS OS

AXIS OS upgrade failed

If the upgrade fails, the device reloads the previous version. The most common reason is that the wrong AXIS OS file has been uploaded. Check that the name of the AXIS OS file corresponds to your device and try again.

Problems after AXIS OS upgrade

If you experience problems after the upgrade, roll back to the previously installed version from the **Maintenance** page.

Problems setting the IP address

Can't set the IP address

- If the IP address intended for the device and the IP address of the computer used to access the device are located on different subnets, you can't set the IP address. Contact your network administrator to obtain an IP address.
- The IP address could be in use by another device. To check:
 1. Disconnect the Axis device from the network.
 2. In a Command/DOS window, type `ping` and the IP address of the device.
 3. If you receive: `Reply from <IP address>: bytes=32; time=10...` this means that the IP address might already be in use by another device on the network. Obtain a new IP address from the network administrator and reinstall the device.
 4. If you receive: `Request timed out`, this means that the IP address is available for use with the Axis device. Check all cabling and reinstall the device.
- There could be a possible IP address conflict with another device on the same subnet. The static IP address in the Axis device is used before the DHCP server sets a dynamic address. This means that if the same default static IP address is also used by another device, there could be problems accessing the device.

Problems accessing the device

Can't log in when accessing the device from a browser

When HTTPS is enabled, make sure that you use the correct protocol (HTTP or HTTPS) when you try to log in. You might need to manually type `http` or `https` in the browser's address field.

If you've lost the password for the root account, you must reset the device to the factory default settings. For instructions, see *Reset to factory default settings, on page 35*.

The IP address has been changed by DHCP

IP addresses obtained from a DHCP server are dynamic and could change. If the IP address has been changed, use AXIS IP Utility or AXIS Device Manager to locate the device on the network. Identify the device using its model or serial number, or by the DNS name (if the name has been configured).

If required, you can assign a static IP address manually. For instructions, go to axis.com/support.

Certificate error when using IEEE 802.1X

For authentication to work properly, the date and time settings in the Axis device must be synchronized with an NTP server. Go to **System > Date and time**.

The browser isn't supported

For a list of recommended browsers, see *Browser support, on page 5*.

Can't access the device externally

To access the device externally, we recommend you to use one of the following applications for Windows®:

- AXIS Camera Station Edge: free of charge, ideal for small systems with basic surveillance needs.
- AXIS Camera Station Pro: 90-day trial version free of charge, ideal for small to mid-size systems.

For instructions and download, go to axis.com/vms.

Problems with streaming

Multicast H.264 only accessible by local clients

Check if your router supports multicasting, or if you need to configure the router settings between the client and the device. You might need to increase the TTL (Time To Live) value.

No multicast H.264 displayed in the client

Check with your network administrator that the multicast addresses used by the Axis device are valid for your network.

Check with your network administrator to see if there is a firewall that prevents viewing.

Poor rendering of H.264 images

Ensure that your graphics card uses the latest driver. You can usually download the latest drivers from the manufacturer's website.

Color saturation is different in H.264 and Motion JPEG

Modify the settings for your graphics adapter. Check the adapter's documentation for more information.

Lower frame rate than expected

- See *Performance considerations*, on page 41.
- Reduce the number of applications running on the client computer.
- Limit the number of simultaneous viewers.
- Check with the network administrator that there is enough bandwidth available.
- Lower the image resolution.
- Log in to the device's web interface and set a capture mode that prioritizes frame rate. If you change the capture mode to prioritize frame rate it might lower the maximum resolution, depending on the device used and capture modes available.
- The maximum frames per second is dependent on the utility frequency (60/50 Hz) of the Axis device.

Can't select H.265 encoding in live view

Web browsers don't support H.265 decoding. Use a video management system or application that supports H.265 decoding.

Problems retrieving additional video streams

I get an error message:

- in AXIS Camera Station Edge: 'Video Error', or
- in Chrome/Firefox: 'Stream: Error. Something went wrong. Maybe there are too many viewers.', or
- in Quick Time: '503 service unavailable', or
- AXIS Camera Station 5 or Pro: 'Camera not available', or
- in browser when using the Java applet: 'Error reading video stream'

The reason is that the camera is designed to deliver up to four different streams. If a fifth unique stream is requested, the camera can't provide it, and you get an error message. The error message depends on the way the stream is requested. The streams are used on a first come, first served basis. Examples of instances that use a stream are:

- live viewing in a web browser or other application
- while recording - continuous or motion triggered recording
- an event that uses images on the camera, for example an event that sends an e-mail with an image every hour
- an installed and running application, such as AXIS Object Analytics, always consumes a video stream whether it's used or not. A stopped application doesn't consume a video stream.

The camera can deliver more than four simultaneous streams provided the configuration of any additional stream is identical to any of the first four streams. Identical configuration implies exactly the same resolution, frame rate, compression, video format, rotation etc.

Problems with MQTT

Can't connect over port 8883 with MQTT over SSL

The firewall blocks traffic that uses port 8883 since it's regarded insecure.

In some cases the server/broker might not provide a specific port for MQTT communication. It might still be possible to use MQTT over a port normally used for HTTP/HTTPS traffic.

- If the server/broker supports WebSocket/WebSocket Secure (WS/WSS), typically on port 443, use this protocol instead. Check with the server/broker provider to see if WS/WSS is supported and which port and basepath to use.
- If the server/broker supports ALPN, the use of MQTT can be negotiated over an open port, such as 443. Check with your server/broker provider to see if ALPN is supported and which ALPN protocol and port to use.

Problems with operating the device

Front heater and wiper aren't working

If the front heater or wiper are not turning on, confirm that the top cover is properly fastened to the bottom of the housing unit.

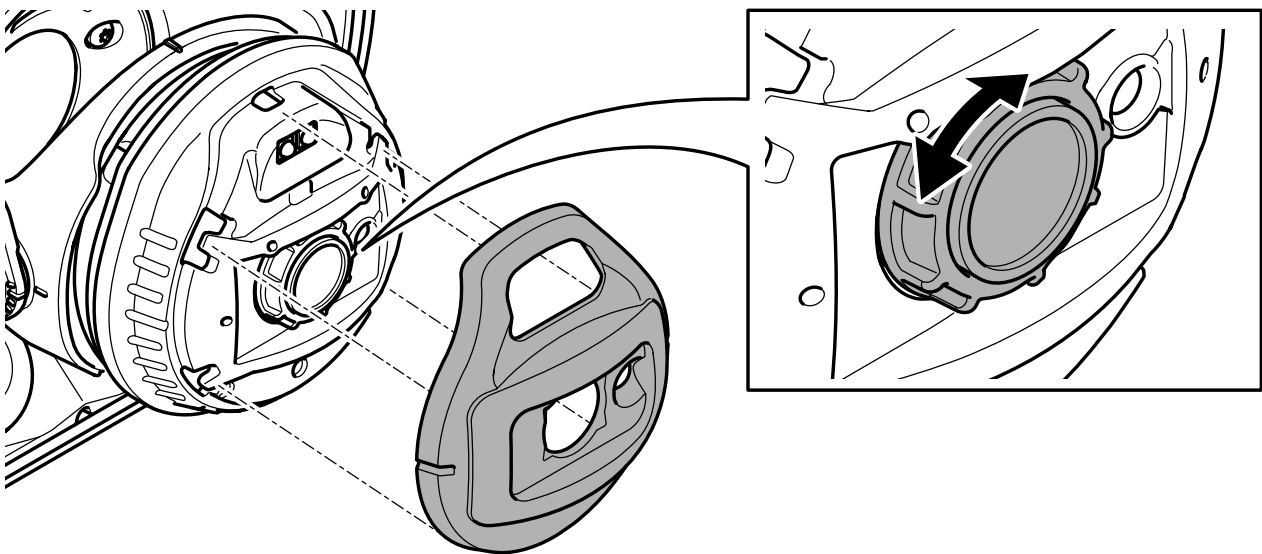
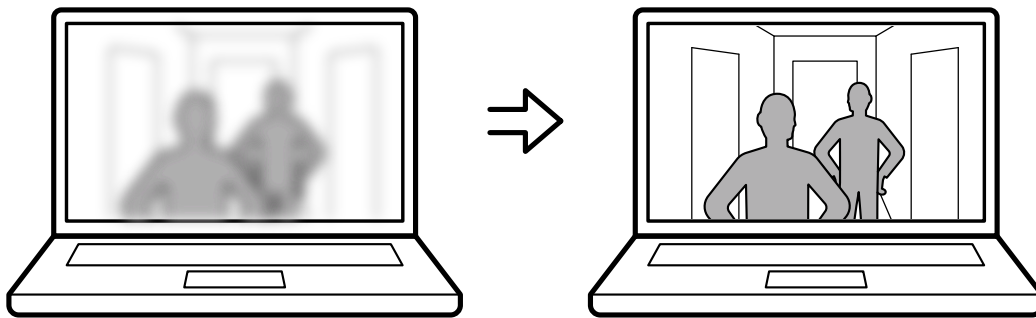
If you can't find what you're looking for here, try the troubleshooting section at axis.com/support.

The image is blurry

The focus is set when the camera is manufactured. But the image can become blurry for different reasons. Try solving the issue in the following order:

1. Clean the dome. See notice below for more information.
2. Clean the lens. See notice below for more information.

3. Turn the focus ring, see image below.
4. Use the focus adjustment tool if you need more precision in turning the focus ring. You can *download the focus adjustment tool* and 3D print it.
5. If the image is still blurry, contact Axis support. See *Contact support, on page 42*.



Set focus using the focus ring.

NOTICE

- Be careful not to scratch, damage or leave fingerprints on the dome or the lens because this can decrease image quality. If possible, keep the protective plastic on the dome until the installation is complete.
- Do not clean a dome or a lens that looks clean to the eye. Excessive cleaning could damage the surface.
- Never polish the dome or the lens.
- For general cleaning of the dome we recommend to use a non-abrasive, solvent-free neutral soap or detergent mixed with pure water and a soft, clean cloth. Rinse well with pure lukewarm water. Dry with a soft, clean cloth to prevent water spotting.
- For general cleaning of the lens we recommend to use a soft, clean cloth.
- Never use harsh detergents, gasoline, benzene, acetone, or similar chemicals.
- Avoid cleaning the dome in direct sunlight or at elevated temperatures.

Performance considerations

When you set up your system, it's important to consider how different settings and situations affect performance. Some factors affect bandwidth (bitrate), others affect frame rate, and some affect both.

The most important factors to consider:

- High image resolution or lower compression levels result in images containing more data which in turn affects the bandwidth.
- Rotating the image in the GUI can increase the product's CPU load.
- Removing or attaching the cover will restart the camera.
- Access by large numbers of Motion JPEG clients or unicast H.264/H.265/AV1 clients affects the bandwidth.
- Simultaneous viewing of different streams (resolution, compression) by different clients affects both frame rate and bandwidth.
Use identical streams wherever possible to maintain a high frame rate. Stream profiles can be used to ensure that streams are identical.
- Accessing video streams with different codecs simultaneously affects both frame rate and bandwidth. For optimal performance, use streams with the same codec.
- Heavy usage of event settings affects the product's CPU load which in turn affects the frame rate.
- Using HTTPS may reduce frame rate, in particular if streaming Motion JPEG.
- Heavy network utilization due to poor infrastructure affects the bandwidth.
- Viewing on poorly performing client computers lowers perceived performance and affects frame rate.
- Running multiple AXIS Camera Application Platform (ACAP) applications simultaneously may affect the frame rate and the general performance.
- Using palettes affects the product's CPU load which in turn affects the frame rate.

Contact support

If you need more help, go to axis.com/support.

Cybersecurity

Cybersecurity supports a successful product lifecycle with minimized risks. You can find in-depth information and documentation about our cybersecurity approach at axis.com/about-axis/cybersecurity. Follow the cybersecurity guidelines below to receive product security notifications from Axis and to configure your product for a secure lifecycle and decommissioning.

At *Axis Trust Center*, you can find information about how Axis implements security compliance, transparency, data protection, and privacy.

Vulnerability management

Axis is a *Common Vulnerability and Exposures (CVE) Numbering Authority (CNA)*. To minimize your risk of exposure, we follow industry standards when identifying and resolving vulnerabilities in our devices, software, and services. Refer to axis.com/vulnerability-management for information about our vulnerability management policy or to report a vulnerability.

Security notifications

Subscribe to Axis security notification emails at axis.com/security-notification-service. We will send you information about vulnerabilities, corresponding security advisories, and other security-related matters for your Axis product.

Secure product lifecycle

Axis minimizes risks throughout the lifetime of our products through secure lifecycle management. Use our hardening guides at help.axis.com to more securely configure and operate your Axis products and to find information about:

Secure first-use – Axis products are pre-configured with high default protection to allow for secure initialization and encrypted communication from the very start.

Intended use and common configuration mistakes – Our guides provide information about the intended usage of Axis products, including common security-relevant misuse and configuration mistakes that should be avoided.

Managing vulnerabilities and supply chain transparency – A Software Bill of Material (SBOM) is published with every software release on axis.com to disclose vulnerabilities and improve supply chain transparency.

Decommissioning and the secure erasure of data – To securely decommission a product when it reaches the end of its lifecycle, reset it to factory default settings. This erases your configurations, stored data, and sensitive information.

T10182262

2026-07 (M22.2)

© 2022 – 2026 Axis Communications AB