

AXIS Secure Remote Access

Remote access made easy, secure and available

AXIS Camera Station 5

AXIS Camera Station Pro

AXIS Companion 3.5 (Classic)



Table of contents

1. Introduction: The challenge with remote access	3
2. Axis solution to remote access	3
21 Easy to setup	3
22 Secure communication	3
23 Availability and geolocation of services	3
3. Using remote access with AXIS Companion	4
31 System setup	4
32 Establish connection	5
33 Fallback to relayed communication	5
34 Secure communication	5
35 Data limitations	5
36 Scheduled End of Service	5
4. Using remote access with AXIS Camera Station	5
41 AXIS Camera Station System setup	6
42 Establish connection	6
43 Fallback to relayed communication	6
44 Secure communication	7
45 Data limitations	7
5. Benefits for installation and use	7
6. Conclusion	7

1. Introduction: The challenge with remote access

An easy, secure and reliable way to access cameras remotely is a priority for many users of surveillance systems. However, connecting to remote cameras can be a challenge, especially when the cameras are located behind routers or firewalls. To give the user an easy and secure way of accessing cameras remotely, Axis has developed the AXIS Secure Remote Access technology.

This white paper describes AXIS Secure Remote Access and gives examples of the technology when used in AXIS Companion and AXIS Camera Station.

2. Axis solution to remote access

AXIS Secure Remote Access makes it possible for a smartphone or PC client to access Axis network cameras when the client and the cameras are located on different local networks. Using external mediator servers, the client and the camera can find each other and establish a secure peer-to-peer connection. As a fallback the communication is automatically relayed through the mediator servers, when direct communication cannot be established.

2.1 Easy to setup

AXIS Secure Remote Access significantly simplifies the installation of remote access to surveillance systems. It is automatically configured during installation and removes the need of manual port-forwarding or router configuration.

2.2 Secure communication

Secure communication is in the core of AXIS Secure Remote Access. It uses multiple levels of authentication to establish an encrypted communication between a client and the cameras in the surveillance system.

2.3 Availability and geolocation of services

To keep the response time to a minimum, and reduce latency, AXIS Secure Remote Access is supported by multiple mediator servers set up around the world: in Sweden, for European and Middle East regions; in the United States, for Americas; In Australia, for Asia and Oceania. The redundant environment also secures the availability of the system.

Communication with the servers is based on their host names, due to the IP addresses are subject to change in time. For the most up-to-date list of host names used, please visit: [AXIS Camera Station 5 - Troubleshooting guide](#).

3. Using remote access with AXIS Companion

With AXIS Companion software, Axis cameras are turned into a surveillance solution that needs a PC only at installation and operating the system is conveniently done by using a mobile viewing app on a smartphone or tablet. AXIS Secure Remote Access is included in AXIS Companion from version 3.

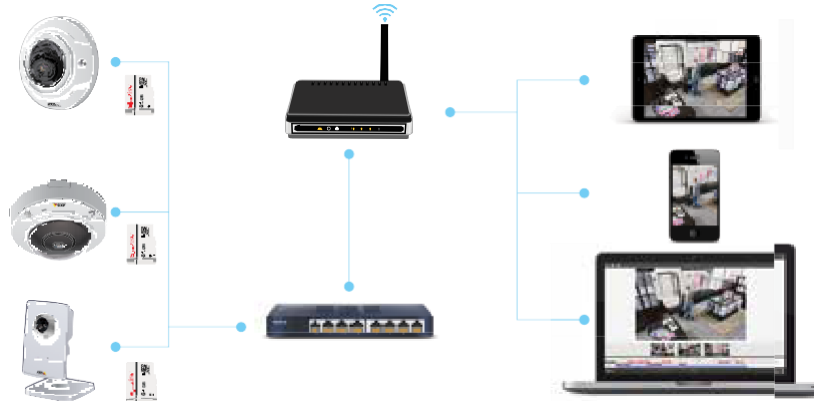


Figure 1: Illustration of an AXIS Companion system with three cameras, storage on SD cards, PoE switch, router and clients.

3.1 System setup

To use AXIS Secure Remote Access in AXIS Companion, the user must have a MyAxis account. The MyAxis account organizes the user's sites and cameras and makes them accessible from different clients.

For AXIS Secure Remote Access to work, an initial one-time setup is required while the AXIS Companion PC client and the camera are located on the same network. The one-time setup is conducted using a setup wizard, guiding the installer through all necessary steps. The firmware version of the camera is automatically updated during the wizard, and system configuration is performed.



Figure 2: System set-up when client and camera located on the same network.

Once the initial setup is complete, the camera is accessible remote from any client device using the specific MyAxis account and the camera and/or site credentials.

3.2 Establish connection

To be accessible remote, the camera keeps an open connection to its nearest mediator server. When the client wants to contact the camera, it uses the mediator servers to find out how and where to contact the camera. The client and the camera establish a connection via the mediator server, verify each other's identities and establish a secure, direct, peer-to-peer communication.

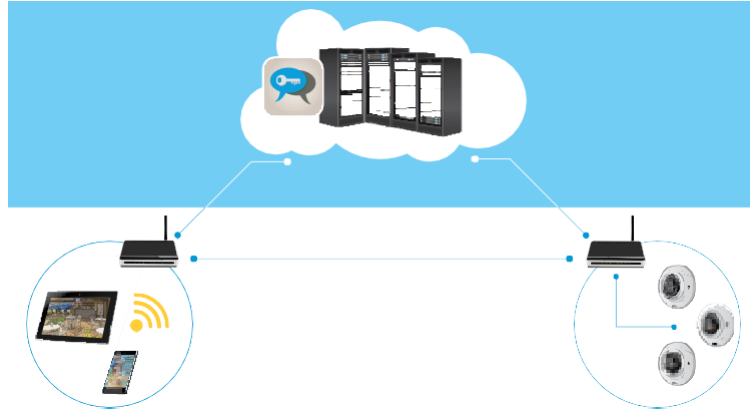


Figure 3: Secure, peer-to-peer communication between a client and a camera located on different networks.

3.3 Fallback to relayed communication

In some scenarios, for example, complex network configurations, it is not possible to set up a peer-to-peer connection. For maximal availability, AXIS Secure Remote Access has a fallback option to relay the communication through the mediator servers. This is seamlessly handled by the system.

3.4 Secure communication

The data transferred via Axis mediator servers and over peer-to-peer connection is end-to-end encrypted which means that the data communicated only can be decrypted by the client and server. All data is encrypted with AES 256 (256 bit) end-to-end encryption using 2048-bit certificates and TLS 1.2 - an encryption method also used in the banking sector to secure money transactions.

3.5 Data limitations

AXIS Secure Remote Access is provided as a free-of-charge service for AXIS Companion 3.5 users. While not limited by the amount of data allowance, AXIS Companion 3.5 is in control of the streams and their quality: the video stream will be reduced in quality after 5 minutes from stream activation and will be automatically closed if there are no active operations done on the client for 15 minutes.

3.6 Scheduled End of Service

AXIS Companion 3.5 has been announced to reach End of Support, therefore AXIS Secure Remote Access will also reach End of Service = this is planned to happen on **December 31st 2024**. After this date, there will be no remote access solution available for AXIS Companion 3.5 (Classic). All users are recommended to upgrade to AXIS Camera Station Edge where the new Secure Remote Access solution is available.

4. Using remote access with AXIS Camera Station

AXIS Camera Station software is the ideal solution to meet the needs for active and efficient surveillance of retail shops, hotels, schools and manufacturing sites. It is designed to perfectly match Axis' wide range of network video products and product features to optimize system reliability.

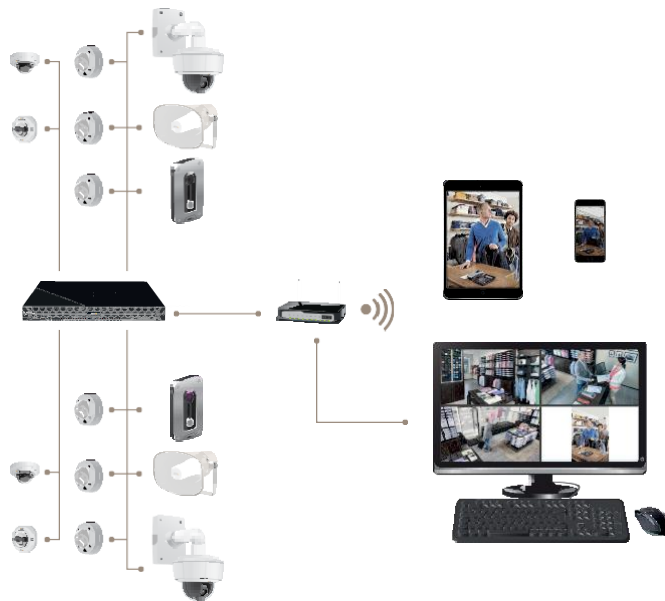


Figure 4: Illustration of an installation with AXIS Camera Station on a system running on AXIS S2016 with integrated PoE switch, 16 devices, and operator clients.

4.1 AXIS Camera Station System setup

To use AXIS Secure Remote Access in AXIS Camera Station, all users must have a joint MyAxis account. The AXIS Camera Station server and the viewing client need Internet access. Install AXIS Camera Station and cameras on the local network and enable AXIS Secure Remote Access in the server configuration.

4.2 Establish connection

To be accessible remotely, the server maintains an open connection to its nearest mediator server. When a client wants to contact the server and cameras, it uses the mediator servers to find out how and where to contact the server. The client and the server establish a connection via the mediator server, verify each other's identities and establish a secure, direct, peer-to-peer communication.



Figure 5: Secure, peer-to-peer communication between a client and a server located on different networks and fallback to relayed communication.

4.3 Fallback to relayed communication

In some scenarios, for example complex network configurations, it is not possible to set up a peer-to-peer connection. For maximal availability, AXIS Secure Remote Access has a fallback option to relay the communication through the mediator servers. This is seamlessly handled by the system.

4.4 Secure communication

The data transferred via Axis mediator servers and over peer-to-peer connection is end-to-end encrypted which means that the data communicated only can be decrypted by the client and server. All data is encrypted with AES 256 (256 bit) end-to-end encryption using 2048-bit certificates and TLS 1.2 - an encryption method also used in the banking sector to secure money transactions.

4.5 Data limitations

If the peer-to-peer connection is used in communication between AXIS Camera Station server and clients (PC, mobile), there is quota on the data exchanged. If the communication is done using relay services (mediator servers), there is a limit of 300 GB.

5. Benefits for installation and use

AXIS Secure Remote Access has benefits for both system installation and use.

- 1) AXIS Secure Remote Access makes setup of remote access easy. It eliminates the need of manual port-forwarding or router configuration.
- 2) AXIS Secure Remote Access makes communication between the client and camera(s) secure. The system has multiple levels of authentication, and all transferred data is encrypted.

AXIS Secure Remote Access can be used on most Axis network cameras and encoders.

6. Conclusion

With AXIS Secure Remote Access technology, Axis provides a solution to the problem of connecting remotely to cameras behind firewalls without the need of manual router configuration. An easy, secure and reliable way to remotely access the surveillance system.

About Axis Communications

Axis offers intelligent security solutions that enable a smarter, safer world. As the market leader in network video, Axis is driving the industry by continually launching innovative network products based on an open platform – delivering high value to customers through a global partner network. Axis has long-term relationships with partners and provides them with knowledge and ground-breaking network products in existing and new markets.

For more information about Axis, please visit our website www.axis.com.