WHITE PAPER

# Axis Cloud Connect

May 2025

# Summary

Axis Cloud Connect provides an efficient way to use Axis devices, manage video surveillance, and boost business performance. It is an open hybrid cloud platform that, together with Axis devices, enables connected services, such as video operation, user and access management, and device management. It's designed to provide secure, flexible, and scalable security solutions.

As a hybrid platform, it allows data processing both on-premise and in the cloud, therefore, using the cloud in the most optimized way regardless of the system setup.

# Table of Contents

# 1 Introduction

Cloud computing has evolved rapidly and is now utilized by most organizations. It allows users to access and utilize computing resources such as servers and databases over the internet rather than depending on local resources. Cloud computing offers many benefits and access to a wide range of services such as artificial intelligence, storage, analytics, etc. Rather than storing data and applications on personal computers or servers, cloud computing allows users to store and process their data remotely.

Axis Cloud Connect is a cloud-based platform that uses cloud computing to provide secure remote access to Axis devices. Users can configure, monitor, and manage their devices from anywhere in the world and at any time. Cloud Connect allows developers to access VAPIX® remotely.

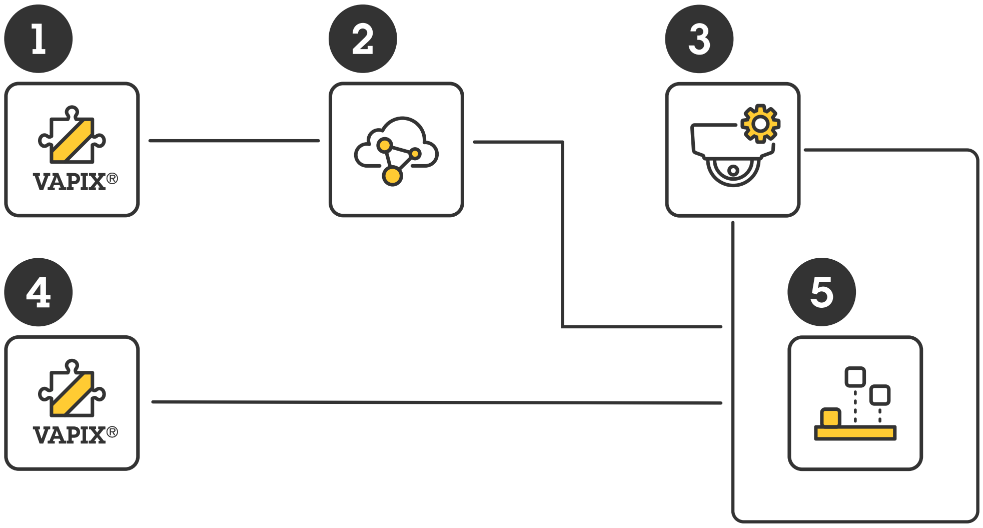


Figure 1.1 *Secure and remote access to VAPIX®.*

1 *VAPIX® cloud*
2 *Axis Cloud Connect*
3 *Device*
4 *VAPIX® on-premise*
5 *ACAP SDK*

Cloud Connect provides a cloud based API set that supports both cloud and device features from one cloud based entry point. It uses a distributed architecture, where data is split into smaller chunks and stored across multiple cloud servers across the world. This approach provides high durability, availability, and performance, allowing you to access your data quickly and efficiently. You can use cloud servers to store and retrieve video, audio, and metadata from a surveillance system. The data in these servers are classified into system and user data. System data is automatically stored in a region Axis chooses, depending on the location of the devices.

While there are important considerations related to security, privacy, and compliance with cloud-based solutions, Axis addresses these concerns and enhances trust for all users. We have evaluated and implemented good security measures by employing robust encryption methods, secure authentication protocols, and regular software updates.

Axis is ISO 27001 certified from October 2022 to date, as a commitment to fulfilling cybersecurity standards in our products and Work Order Workflow (WoW). Axis also has SOC 2 Type 1 attestation for Axis Cloud Connect.

# 2 What is Axis Cloud Connect?

Cloud Connect is an open hybrid cloud platform that enables connected services for efficient device management, video and data delivery. These services are managed by Axis and leverage AXIS OS and our know-how in analytics, image usability, and cybersecurity.

With this cloud platform, we and our partners can rapidly develop cloud-based solutions while tailoring solutions to customers' needs. Using Cloud Connect for your cloud based solution means that you can access your Axis device remotely anywhere, anytime, and on any device through web browsers or mobile applications. Storing your video in the cloud supports storage efficiency, accessibility, and remote management of your device fleet.

Cloud Connect extends the open VAPIX® API set with services such as remote interaction with Axis devices while maintaining convenience and safeguarding the system's cybersecurity. It makes AXIS OS better and more relevant in a modern world where cameras are consumed as a service and cybersecurity threats and concerns are ever increasing.

The cloud platform offers separate customer tenancy through organizations, device fleet management, and user access and authentication. Managing a device fleet includes AXIS OS updates, AXIS OS device configuration, media streaming, and media storage.

Organizations are the fundamental building blocks of this cloud solution. An organization defines a specific customer's tenancy in the cloud. For each organization, there are licenses for utilizing services and managing users' access and resource groups. A resource group consists of a fleet of devices that are grouped together.

Each organization has a device fleet. It is a list of all devices that you add through an onboarding process.

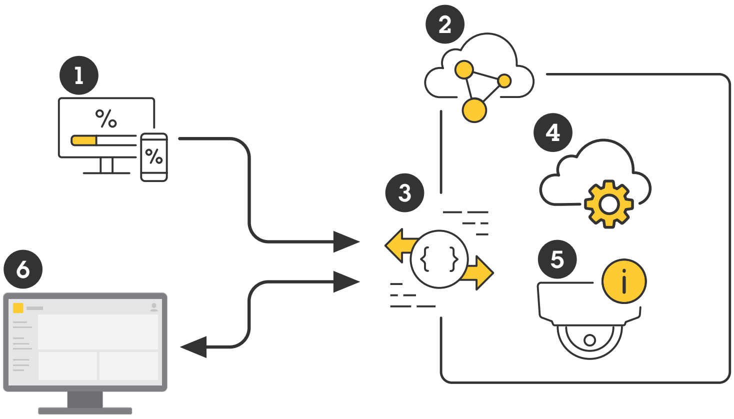


Figure 2.1 *After onboarding, your devices become part of the organization's device fleet. You can view information about the devices and also access the device through the application and solution in Cloud Connect.*

1 *AXIS Installer*
2 *Axis Cloud Connect*
3 *Axis Cloud Connect API*
4 *Axis managed services*
5 *Device info (such as warranty, end of life, and end of support.)*
6 *Device fleet management*

# 3 Traditional on-premise to cloud-based solution

The shift to cloud-based solutions is transforming industries worldwide as more organizations consider moving their operations from a traditional on-premise system to a cloud-based infrastructure or adding cloud capabilities to their current system.

Traditional on-premise requires that all hardware and software be located and managed in-house by the organization. You can't host it in the cloud or access it remotely. A cloud-based solution offers a more flexible and scalable system where you can remotely manage your system and store data through a web-based interface. With a cloud-based solution, you can easily scale your cloud resources down or up to meet your organization's changing needs. You can access your data from anywhere and on any web browser or applicable mobile application. Cloud providers handle software updates and maintenance for your organization while protecting your data with cybersecurity measures.

Axis Cloud Connect is a hybrid cloud platform that offers a powerful solution for organizations looking to maximize their cloud presence while maintaining control and security over their most valuable assets.

With a hybrid cloud platform, you can process data both on-premise and in the cloud. It is cost-effective, and provides better flexibility by allowing data and applications to move between these two solutions. It provides two cloud services; private and public.

Private and public cloud services mainly differ in their security features and access controls. Private cloud service offers more customized and restrictive access controls and additional security measures such as encryption and firewalls, to protect highly sensitive or regulated data. In contrast, public cloud services often provide standardized security features and access controls. Specific organizations and governments may specifically require private cloud services when handling extremely sensitive data.

Cybersecurity is very important to Axis, and Axis Cloud Connect is no exception. We developed Cloud Connect with Axis Security Development Model, which ensures cybersecurity is front and center in everything the solution offers. It employs robust encryption methods, secure authentication protocols, and regular software updates to safeguard against potential threats.

# 4 How does Axis Cloud Connect work?

In cloud computing, the multi-tenancy and tenant separation approach optimizes the platform for efficiency, scalability, and flexibility. This approach categorizes users separately within the cloud system and stores their data separately in each user's tenancy and enhances data privacy.

Cloud Connect makes it easy to access cloud services and control your devices remotely. We protect our APIs with strong security measures, including authentication and authorization for every single call. This ensures that only authorized users and applications can access your devices. With our APIs, you can securely integrate our services into your applications and solutions.

## 4.1 Integration of partner solutions with Axis Cloud Connect

With Cloud Connect, Axis development partners can integrate applications and solutions into their system and utilize the cloud system capabilities in several applications to meet their customers' specific needs. We provide an efficient and coherent set of tools and applications to support system integrators and owners throughout the system's lifecycle. These tools include AXIS Site Designer, AXIS Installer, AXIS License Manager, Axis device management software, and Axis video management software.

An end customer is represented as an organization in the system. After you create your organization, you can integrate devices into the Cloud Connect infrastructure at different levels of integration.

- **Light device integration**: With this type of integration, you register the device as a logical entity in Cloud Connect. The system only provides integrated devices' static information such as serial number, device model, warranty, end of support, recommended AXIS OS version, etc.

- **Deep device integration**: Here, you take the integration further by enabling a device-to-cloud connection through one-click device onboarding or local discovery onboarding. Your device becomes available for remote configuration, direct communication and data exchange with the cloud platform. The system provides relevant and dynamic information about the onboarded devices such as devices' onboarding status, current AXIS OS version, connection status, etc. It also supports AXIS OS update.

  During the onboarding process, you set a device profile which determines the system composition and managed services your device should configure.

  - **One-click device onboarding:** To add devices to the system, you click the device's control button, scan the QR code on an Axis device, or enter a serial number and owner authentication key code in AXIS Installer app. After this, the device becomes part of the Cloud Connect device inventory and allows you to use Cloud Connect services.
  - **Local discovery onboarding:** The device-to-cloud connection is routed through an AXIS Device Manager Extend that is connected to your organization. You need to install EdgeHost on your AXIS Device Manager Extend before you can find and onboard Axis devices that are on the same local network that the EdgeHost is installed on.

After integrating your device into the cloud system, you select a management mode for the device. This mode determines several functions including how the system should configure your device and update its software: AXIS OS and ACAP applications. In Cloud Connect, devices can operate on any of these management modes:

- **Managed mode:** In this mode, Axis manages your devices' system composition, including how to use credentials for certificate-based authentication, local users limit, access rights, and software updates. Though managed by Axis, you can access the devices locally through an on-premise VMS. A device in managed mode automatically switches to connected mode when it doesn't have AXIS OS active track or the latest long-term support (LTS). Other scenarios that can cause this switch include uploading ACAP applications that are not part of the system composition that your device profile defines, and accessing a device's local administrator account, which implies that changes to the system composition is possible outside Axis management.

  To update the system composition in this mode, you can choose to let Axis decide when to do the update or set a time window for when Axis can do it. Having the option to set a time window depends on the organization's offering.

  There are four different ways the devices in managed mode can interact with the cloud system: through VAPIX® calls over EdgeLink, asynchronous device configuration with Task Manager, Remote Axis Device Assistant (ADA), and WebRTC video and data channels.
- **Connected mode:** It is the same onboarding process for devices in managed mode and connected mode, but they have different device profiles. The device owner, also known as the user, decides, updates, and manages the system composition using Cloud Connect API or AXIS Device Manager. The device owner has local administrator access to the device and is responsible for the device account credentials. Some features such as WebRTC video and data channels are not available.
- **Standalone mode:** A device is in standalone mode when it's been registered in Cloud Connect but hasn't been onboarded to the system. For example, an Axis device is in standalone mode if you have registered it in Cloud Connect but due to no internet connection, it only works in an on-premise VMS system. You need to onboard the device into Cloud Connect to change the management mode to either connected or managed.

These edge devices are classified as 1st and 2nd tier devices. 1st tier devices are AXIS OS devices that host the default Cloud Connect edge services natively, enabling device-to-cloud solution.

2nd tier devices can't host Cloud Connect edge services natively because they have limitations in installing or updating software, technical incompatibilities, or other restrictions. However, you can get a device-to-cloud solution by using an Axis recorder.

### 4.1.1 Application onboarding

In your organization, you need to onboard and activate an application, developed by either Axis or an Axis integration partner. You can onboard applications in any of these processes:

- When you create an organization.
- When you select an existing organization from an application's client.
- When you allow your application's client to access an organization through OAuth.

## 4.2 Software updates and device configuration

Cloud Connect has a device software deploy functionality that allows you to remotely manage and update your device software. This cloud-based functionality retrieves information about available AXIS OS and ACAP and feeds this information to EdgeHosts and DeviceHosts. They check every second hour if there are any new applicable releases.

- **AXIS OS updates:**

  For devices in managed mode, you define the process for their AXIS OS upgrade during the onboarding process. For example, you can choose to target the latest published AXIS OS version, which means that the system will automatically update AXIS OS either immediately or within a specified time window.

  In connected mode, the system recommends all AXIS OS information to the user to choose which version to deploy, upgrade, or downgrade.

The cloud part of the device software deploy system, called the Task Manager Service (TMS), holds the aggregated information of all tasks for an organization. The part of the system that lives on-premise in the EdgeHost and DeviceHost is called the Task Engine. It runs the instructions for the tasks and modifies the devices.

A task is a small bundle of information containing an action or a setting that needs to be done or applied on a device. For example, you can set a task for text overlay configuration or software upgrade for selected devices. TMS creates a task or a collection of tasks, and dispatches them to EdgeHost or DeviceHost, depending on which one manages the device. The task engine does its own local dispatch to assign tasks to runners and the runners execute the task in the corresponding device. Finally, the task engine reports back to the cloud with the results so that they can be displayed back to the user.

Apart from the tasks created by the client, EdgeHost and DeviceHost can also create tasks. An example is when you add a device to an EdgeHost. It happens in a local context and there is no need to involve the cloud. EdgeHost creates the task directly and sends it to the TMS in the cloud. TMS sends information about the actual device that you added to the cloud through the usual channels which is separate from the task. These tasks are also visible to you so you can track progress such as the number of devices successfully added to EdgeHost.

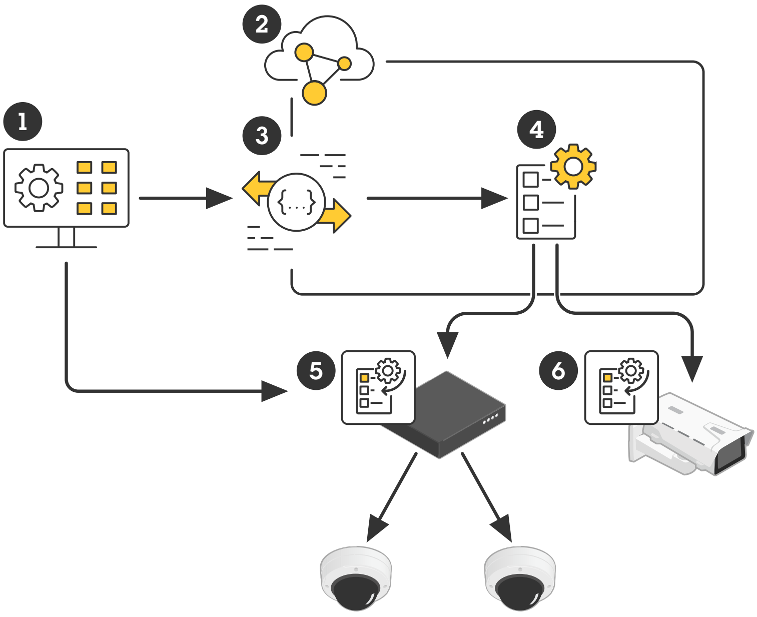


Figure 4.1 *AXIS OS device configuration is done either in a federated asynchronous or federated synchronous way. Axis uses a task manager to send asynchronous device configurations from the cloud to the edge or device host.*

1 *Video Management Software (VMS)*
2 *Axis Cloud Connect*
3 *Axis Cloud Connect API*
4 *Task manager service*
5 *EdgeHost task engine*
6 *DeviceHost task engine*

For federated synchronous device configuration, EdgeLink allows authorized users to make HTTPS requests from anywhere to APIs on the local network through Cloud Connect API. The requests can reach these APIs: VAPIX® on Axis cameras and recorders, AXIS Camera Station Server VMS API, and EdgeHost and DeviceHost GraphQL API.

EdgeLink is a feature of EdgeHost and DeviceHost and it uses the same secure websocket with SignalingServer as WebRTC. It uses the websocket to transfer HTTPS request between Cloud Connect API and the EdgeHost or DeviceHost.

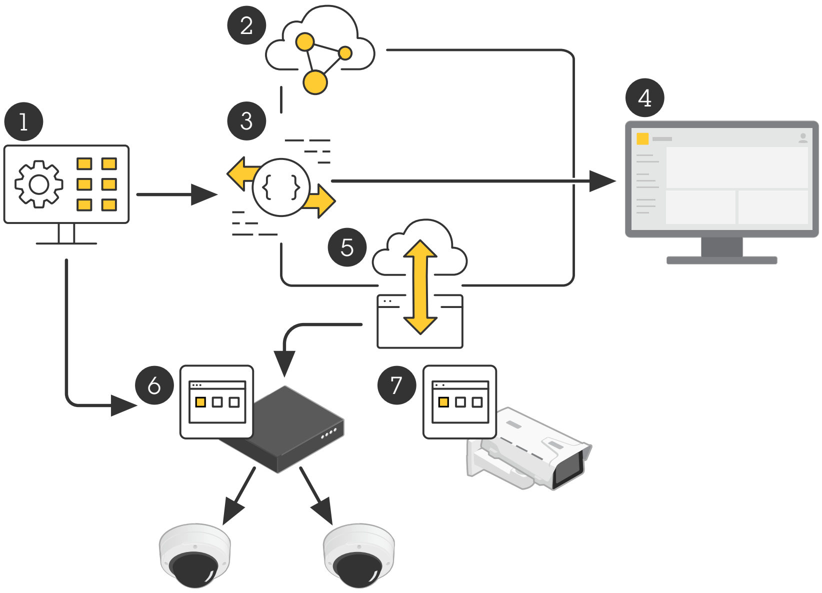


Figure 4.2 *AXIS OS device configuration.*

1 *Video Management Software (VMS)*
2 *Axis Cloud Connect*
3 *Axis Cloud Connect API*
4 *Device fleet management*
5 *EdgeLink*
6 *EdgeHost*
7 *DeviceHost*

# 5 Data privacy, storage, and management

To ensure proper cybersecurity awareness and procedure, Cloud Connect uses both Axis Security Development Model (ASDM) and Information Security Management System (ISMS).

ASDM is a framework that defines the process and tools Axis uses to develop software with security built-in throughout the product's lifecycle, from inception to decommissioning. We mandate ASDM for all software development at Axis and all Axis software included in Axis products and solutions.

ISMS is a systematic approach that helps to identify and manage sensitive company information, ensuring its confidentiality and integrity.

- **Data storage:** Cloud Connect stores data regionally to reduce latency and bring the system closer to the end user. It deploys time-critical use cases, such as signaling service for video stream, in multiple regions. It uses multiple endpoints to store system data either regionally or globally. The system separates data computation from data storage for some services. This means that the database is global, and data processing is done in one or more regions.

  In Cloud Connect, the system categorizes data into system and user data for each organization.

  - System data: It allows the system to function and includes information about users, organizations, resource groups, devices, subscription notifications, etc. It keeps information about initial device configurations and software updates in the device management and personal identity information in My Axis Identity Provider (IDP) or Axis Cloud Connect IDP for Active Directory (AD) users.
  - User data: This refers to personal and identifiable data that the system collects, stores, and processes when someone logs into the system. It includes email address, name, or IP address, which are regulated by General Data Protection Regulation (GDPR). An example is a video data, video recording, or audit logs containing personal identifiable information (PII) in the cloud storage.
- **Access management:** The person who creates an organization in the cloud system is known as a user and recognized as the owner of the newly formed entity. This user has permission to invite new users through email, assign roles, integrate devices into the system, and delete the organization. The cloud system has three main roles that define the different levels of access and permissions users can get. These roles are administrator, operator, and viewer.
  - Administrators control the entire system; they manage users, devices, licenses, and videos.
  - Operators monitor live video streams, operate integrated devices, and have access to recordings.
  - Viewers only have access to monitor live video streams.

## 5.1 Media streaming and recording

Cloud Connect uses the WebRTC standard to offer live media streaming of video from cameras to web browsers and mobile devices, providing a seamless and secure way to access and view video feeds remotely. Web browsers and a number of open-source libraries support this standard, therefore simplifying partner integration development. It also supports live low-latency streaming of video and two-way audio, peer-to-peer connection between applications and cameras, and mandatory end-to-end encryption. The system automatically adjusts the video bitrate to offer the best possible viewing experience even with constrained and dynamically changing network conditions.

The peer-to-peer connection also allows for low latency PTZ control, playback or export of video recordings that are locally stored in the devices, tunneling of HTTP communication, exposing VAPIX® and ONVIF APIs in the devices, and providing a general remote access solution to devices.

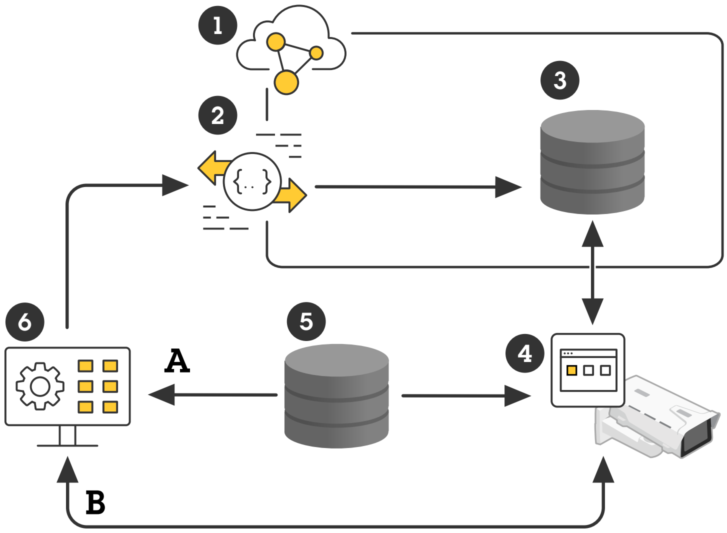


Figure 5.1 *Media streaming*

1 *Axis Cloud Connect*
2 *Axis Cloud Connect API*
3 *Signaling server*
4 *WebRTC Agent*
5 *TURN server*
6 *Video Management Software (VMS)*

*A. Relayed channel*

*B. Peer-to-peer channel*

WebRTC is very flexible and finds the optimal network route between camera and client, through firewalls if needed, and as a fallback through a TURN or relay server in the cloud. TURN servers can either be operated by Axis or by partners themselves, ensuring that media streams never need to pass through Axis servers.

With the Object Store Recording (OSR) functionality, devices can push media and live video directly to a cloud storage endpoint as an HTTP request, which is the most widely permitted way by local firewalls or Network Address Translations (NATs). Otherwise, cloud services cannot directly access cameras to get media streams in an easy way. You can also save recordings to cameras' SD cards, and upload to the cloud when you need a playback or export.

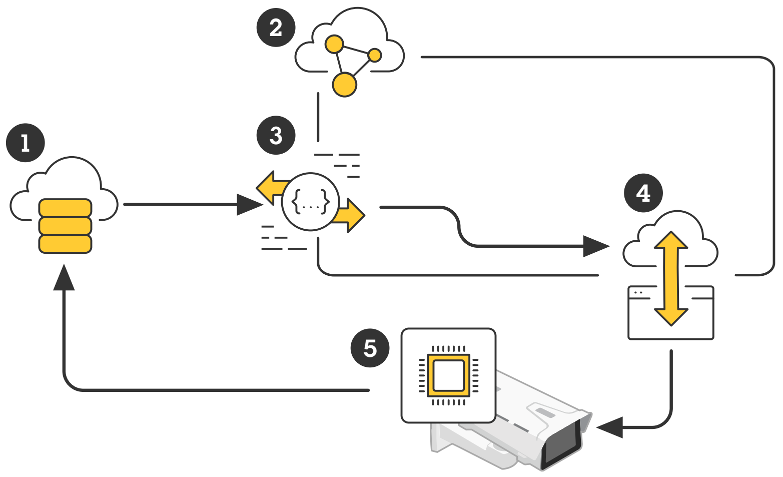


Figure 5.2 *Media recording*

| | |
|---|---|
| *1* | *Client Cloud* |
| *2* | *Axis Cloud Connect* |
| *3* | *Axis Cloud Connect API* |
| *4* | *EdgeLink* |
| *5* | *OSR agent* |

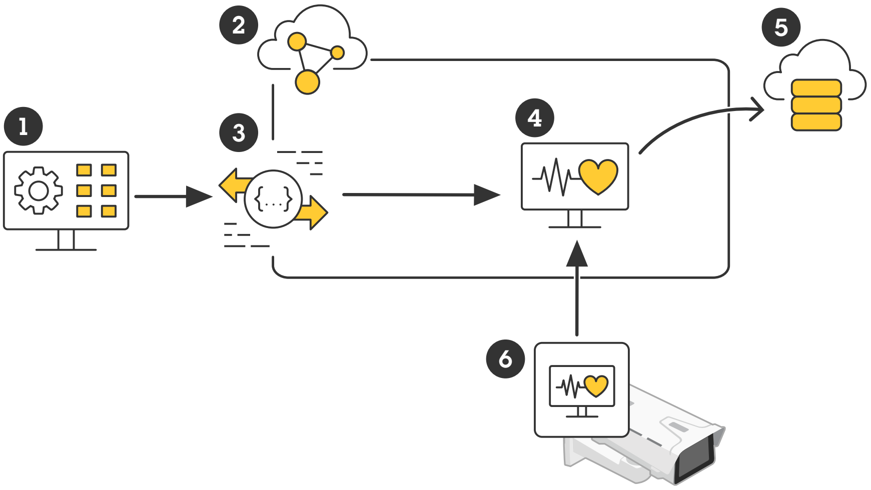
Another feature is that any event occurring in the camera, for example, motion detection can be sent directly to partners' services, enabling systems that handle alarms. You can also upload metadata from analytics in similar ways.

## 5.2 In Device Diagnostics and infrastructure capabilities

- **In Device Diagnostics**

  To improve our products, offer proactive support, and gather telemetry information on how our products are used, In Device Diagnostics (IDD) collects and stores anonymous system data in the cloud. This collection requires user consent. The system data is the base for the service called Device Insights which we use to advise customers about how to fix certain issues like device overload, SD card change, and many more potential issues. We collect anonymous runtime data about logs, metrics, and crashes. IDD can trigger AXIS OS updates as proactive maintenance and live troubleshooting on connected devices.

  Axis monitors the cloud services 24 hours a day, 7 days a week, all year round to ensure quick investigation of alerts and incidents. Axis cloud services updates target zero-outage, which means any potential downtime of the APIs is absolutely minimized



1 *Video Management Software (VMS)*
2 *Axis Cloud Connect*
3 *Axis Cloud Connect API*
4 *In-Device Diagnostics*
5 *Axis*
6 *In-Device Diagnostics Agent*

- **Axis Cloud Connect infrastructure capabilities**
  - **Event bus:** The event bus is a centralized messaging system that enables real-time communication and automation workflows between various devices and applications connected to Cloud Connect. By publishing and subscribing to specific events, devices and applications can exchange information and trigger actions in response to changing conditions.

    When a device or application publishes an event to the event bus, it sends a message containing relevant data, such as motion detection, door openings, or temperature changes. This message is then routed to all devices and applications that have subscribed to that specific event type. Subscribed devices and applications receive the notification and take immediate action, such as sending alerts, triggering recordings, or adjusting settings.

    For example, if a camera detects motion, it can publish a 'motion detected' event to the event bus. A nearby speaker, subscribed to this event, can then receive the notification and play a warning message to deter intruders. Similarly, a video management software, also subscribed to the same event, can receive the notification and trigger a recording of the incident.

    The event bus provides a scalable and flexible way for devices and applications to interact with each other, enabling advanced automation scenarios and improving overall system efficiency. By leveraging the event bus, customers can create customized workflows that respond to specific events, enhancing their security, safety, and operational capabilities.
  - **Notifications:** It allows users to receive alerts, device updates and system status. You can customize it to inform you of specific events, such as motion detection, camera tampering, or system errors. Notifications can be in the form of emails, mobile push, or webhooks.
  - **Audit log:** The audit log is an account of events from the event bus that has specific topics with an indication that these topics are meant for auditing. It retains these audit log events and exposes search functionality through an API.

# 6 Glossary

- **Device capability:** It provides a specific feature that enables functionality in applications. The device capability might require functionality in a cloud service, in an on-premise service, in a service running on a device or a combination of these services. A capability provides functionality for different applications and these functionalities are defined in a device profile.
- **DeviceHost:** A Cloud Connect agent responsible for the communication between your device and Cloud Connect backend in a direct device-to-cloud setup.
- **Device inventory:** A device becomes part of the device inventory after onboarding. You can access the inventory through the Cloud Connect API and get both static and dynamic information about the device.
- **Device profile:** A device profile is a pre-configured functionality that defines a device's system composition, settings, and features. It connects to an application and specifies what capabilities to enable on the device, for it to work with the application. When you select a device profile during device onboarding, it configures the device with recommended settings, ensure optimal performance, and reduce manual configuration. If no device profile is set during onboarding, the device uses the organization's default profile.
- **EdgeHost:** A local Cloud Connect device fleet management proxy responsible for routing communication between your device and Cloud Connect backend in a proxied device-to-cloud setup.
- **Logical entity:** A virtual component that provides a specific function or service within the cloud environment.
- **Managed service:** A software service where, apart from selling a physical product, a company takes added responsibility toward a customer by offering services, such as remote system upgrade. A managed service improves product quality and enhances cybersecurity.
- **Owner authentication key:** A key that is provided when buying an Axis device. With it, you can claim ownership of the device when registering it in Cloud Connect.
- **Runners:** Specialized program that performs a specific function on the device, allowing for greater flexibility and customization of the device's behavior.
- **System composition:** A system composition includes AXIS OS, supported AXIS Camera Application Platform (ACAP) applications and configurations.
- **Tenancy:** Refers to the allocation of resources and services within a multi-tenant environment. It's about how multiple customers, also known as tenants, share the same cloud infrastructure, while maintaining their own separate and secure environments.
- **VAPIX®:** An Axis open application programming interface (API) that enables integration of a wide range of solutions and platforms into Axis products. For more information, see *VAPIX library*.
- **WoW:** Stands for Work Order Workflow and refers to the processes and procedures an organization have in place to manage and control changes to their information security management system (ISMS).

T10219144/EN/M1.9/2505

## About Axis Communications

Axis enables a smarter and safer world by improving security, safety, operational efficiency, and business intelligence. As a network technology company and industry leader, Axis offers video surveillance, access control, intercoms, and audio solutions. These are enhanced by intelligent analytics applications and supported by high-quality training.

Axis has around 5,000 dedicated employees in over 50 countries and collaborates with technology and system integration partners worldwide to deliver customer solutions. Axis was founded in 1984, and the headquarters are in Lund, Sweden.