WHITE PAPER

Device lifecycle management in the cloud

Efficient device management and system administration

April 2025

AXIS COMMUNICATIONS

Table of Contents

1 Introduction

Effective device lifecycle management is crucial for organizations seeking to optimize the performance, security, and longevity of their network devices. By leveraging cloud-based device management software you can streamline the deployment, maintenance, and decommissioning of devices, ultimately reducing costs and improving operational efficiency.

This white paper presents an overview of Axis portfolio of cloud-based device management software, highlighting the software products AXIS Device Manager Edge and AXIS Device Manager Extend with their key components and benefits. We also explore typical system setups, demonstrating how our solutions can simplify device lifecycle management and support business success.

2 Background

In today's networked world, IP-based devices are the backbone of modern surveillance and security systems. As the number and complexity of these devices continue to grow, effective device management becomes essential to ensuring system reliability, security, and optimal performance. Cloud-based device management offers a powerful solution, enabling organizations to streamline their operations, enhance scalability, and reduce costs. With cloud-based device management, organizations can gain real-time visibility into their device fleet, automate routine tasks, and make sure that their devices are always up to date and protected.

3 The benefits of device lifecycle management in the cloud

Effectively managing your devices is critical to ensuring the reliability, security, and efficiency of your video surveillance system. Cloud-based device lifecycle management offers a range of benefits that can help you optimize your system's performance, reduce downtime, and improve overall productivity.

3.1 Remote and instant overview and control

With secure remote access, cloud-based device management software enables you to instantly access a comprehensive overview of your system, including device status, software versions, and application updates. It also lets you control all devices from remote, enabling you to oversee and manage your system from anywhere, at any time – without compromising security.

3.2 Device software management

Managing device software upgrades via the cloud enables IT administrators to efficiently verify that all devices are running the latest device software version and deploy the desired version in minutes. You get automated checks for new device software and recommended upgrades, and you can install upgrades for your entire organization across multiple sites and locations all at the same time.

3.3 Cybersecurity management

By setting basic security policies and applying them across your entire network you can make sure that all devices comply with current security policies and practices to maintain cybersecurity control. Monitoring discontinuation dates and device warranty dates also helps you plan maintenance and avoid unexpected costs.

3.4 User management

Cloud-based device lifecycle management simplifies user management by providing a single interface for managing user roles, permissions, and access controls.

3.5 Application management

Cloud-based device lifecycle management enables you to easily view and manage the application inventories, for instance to see which applications and versions are running and easily apply new ones. For example, you can start hundreds of applications at once. There is policy support for a selection of Axis applications. This means you can schedule and automatically install, update, and reinstall the supported applications whenever suitable (night, morning, evening, afternoon, or as soon as possible).

4 Cloud-based device management software from Axis

At Axis Communications, we offer a range of device management solutions, including both on-premises and cloud-based options, to give you the freedom to choose the approach that best suits your specific needs and infrastructure. Our cloud-based software products, AXIS Device Manager Edge and AXIS Device Manager Extend, complement our established on-premises device management software, AXIS Device Manager, allowing customers to choose the approach that best fits their specific requirements and infrastructure. AXIS Device Manager Edge and AXIS Device Manager Extend require an internet connection.

4.1 AXIS Device Manager Edge

AXIS Device Manager Edge provides a site-by-site overview, allowing users to remotely monitor device connectivity status and perform simple management tasks. It offers an instant status overview of all devices in the system, enabling automatic upgrades and secure remote access. This allows for easy application and maintenance of safeguards throughout a device's lifecycle.

4.2 AXIS Device Manager Extend

AXIS Device Manager Extend aggregates data sites allowing you to manage thousands of Axis devices and remote sites and perform maintenance tasks at scale, regardless of physical location. It identifies network performance issues, such as connectivity failures or unstable devices, and helps with maintenance and proactive planning by showing product warranty and discontinuation dates for the individual devices in the system. Important events are automatically stored in the system log. This includes items such as user activity, device status, and network status.

5 Device management with edge hosts and clients

Our cloud-based products, AXIS Device Manager Edge and AXIS Device Manager Extend, consist of two main components: edge hosts and clients.

The **edge host** enables discovery and management of devices in a local network. It is a light-weight service that runs on a machine on the same network as the devices. It typically runs on the machine that also runs the VMS, but it can also run on a dedicated machine or a virtual machine on a server. The edge host facilitates device-to-cloud communication, ensuring data security. It acts as the gateway of the local network to the cloud so that the system administrator can manage firewall settings and other traffic rules for one machine.

You can run multiple edge hosts if you have multiple sites or segmentation in your network. One edge host is limited to handling 1000 devices. For larger systems the administrator must install more edge hosts.

The **client** provides the user interface. As the primary interface for interactions with the system, there are two variants of the client that cater to different needs:

- **Desktop application.** This client can be installed on any hardware running Windows 10 or a later Windows version. The desktop application is primarily used during installation of the system, like local device discovery and installation of edge hosts. But it also gives access to more advanced capabilities not available in the web client.
- **Web client in My Systems portal.** This client allows access to the system from any web browser on any operating system. It provides you with instant access without having to install a client on the local machine.

In the web client you can perform core management tasks such as upgrading the device software and see connection and health information.

You can run the edge host and client on the same machine in smaller installations or distributed over several machines in larger installations. We currently support Windows 10 and later Windows versions as operating system for both desktop application and edge host.

6 Typical system setups

The minimum requirement for being able to establish a WebRTC connection is to allow a TCP connection to the STUN/TURN server. In situations with bandwidth fluctuations you might get a smoother video experience by also allowing a UDP connection to the STUN/TURN server.

To establish a true peer-to-peer connection with minimum latency, UDP ports 49152-65535 need to be allowed to any IP address and at least one of the peers must have its NAT configured to use endpoint-independent mapping as described in RFC4787.

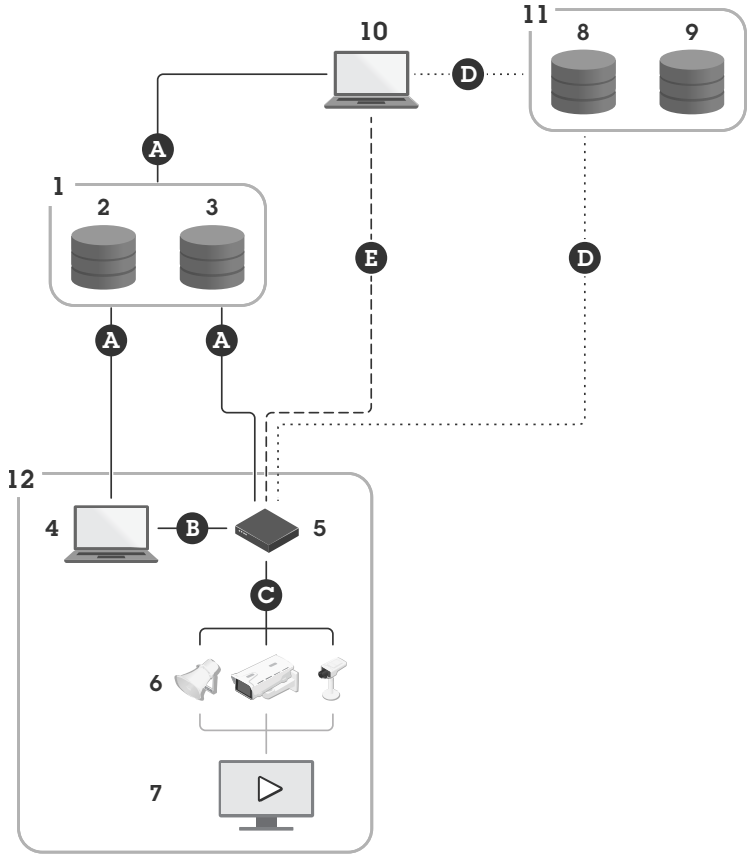
Table 6.1 *Guide to the connections in the system setup graphs in the following sections.*

Connection	URL and IP	Port	Protocol	Comment
A	prod.adm.connect.axis.com (52.224.128.152 or 40.127.155.231)	443	HTTPS	Required.
B	HTTP discovery (from client to edge hosts)	37080	HTTP	Needed to provision the site. Optional after provision.
	Data transfer (between client and edge host)	37443	HTTPS	
	Multicast discovery (from client to edge hosts)	6801	UDP	
	Multicast discovery (from edge hosts to client)	6801	UDP	
C	Data transfer (between edge host and devices)	80 / custom port, 443	HTTP, HTTPS	Required.
	Unicast discovery	1900	SSDP, Bonjour	
	Multicast discovery	1900, 5353	Multicast	
	HTTP discovery	80, 443	HTTP/ HTTPS	
D	signaling.prod.webrtc.connect.axis.com	443	HTTPS	Based on WebRTC standard. Optional and set to off by default.
	*.turn.prod.webrtc.connect.axis.com	443, 5349	HTTPS, DTLS (UDP and TCP)	
E	Peer to peer (P2P)	49152-65535	DTLS (UDP and TCP)	

Note that the information in this table is subject to periodic changes. Check the frequently asked questions on *faq.axis.com* for the latest version.

6.1 Single site

In this single-site setup, the connections A and C are mandatory. The client and edge host have a direct connection to each other (via connection B) and connect to a service platform (via A) for updated device software and other support information. After the system is provisioned, the connection (B) between the edge host and the local client can be replaced with remote access between the edge host and a remote client (via D or E).



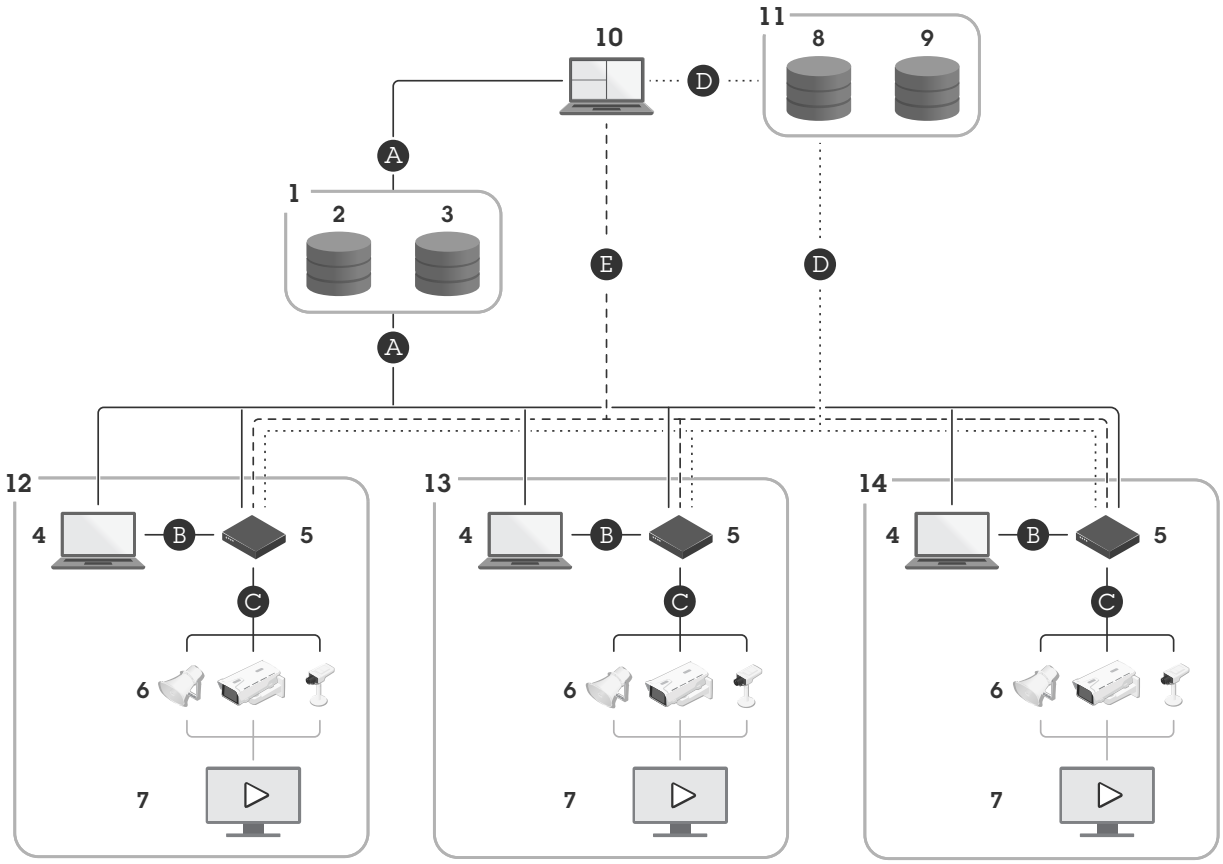
Typical setup for single-site operations with local and remote access using AXIS Device Manager Edge.

1 *Axis servers*
2 *Identity and access management (My Axis)*
3 *Organization data*
4 *Local client (with internet connection)*
5 *Edge host (with internet connection)*
6 *Devices*
7 *VMS (video management software)*
8 *TURN (traversal using relays around NAT)*
9 *Signaling*
10 *Remote client*
11 *Remote access WebRTC servers*
12 *Site*

6.2 Multiple sites using local and remote access

For efficient remote, multiple-site management a remote client will communicate with each edge host to manage the organization's separate sites.

In this multisite setup, the connections A and C are mandatory. After the system is provisioned, the connections (B) between the edge hosts and local clients can be replaced with remote access between the edge hosts and the remote client (via D or E).



Typical setup for multisite operations with local and remote access using AXIS Device Manager Extend.

1 *Axis servers*
2 *Identity and access management (My Axis)*
3 *Organization data*
4 *Local client (with internet connection)*
5 *Edge host (with internet connection)*
6 *Devices*
7 *VMS (video management software)*
8 *TURN (traversal using relays around NAT)*
9 *Signaling*
10 *Remote client*
11 *Remote access WebRTC servers*
12 *Site 1*
13 *Site 2*
14 *Site 3*

About Axis Communications

Axis enables a smarter and safer world by creating solutions for improving security and business performance. As a network technology company and industry leader, Axis offers solutions in video surveillance, access control, intercom, and audio systems. They are enhanced by intelligent analytics applications and supported by high-quality training.

Axis has around 4,000 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