AXIS COMMUNICATIONS

Cybersecurity

SECURING BETTER CYBER PROTECTION TOGETHER

TABLE OF CONTENTS

Mitigating the risk of cyber incidents

Protecting network products and software services from cyberthreats is key to securing the data and systems on your network. A compromised system can mean the loss of confidentiality and integrity of your data, or data or access can be unavailable when you need it.

As part of being a responsible cybersecurity partner, we've put together some considerations and guidelines to help you procure, as well as secure, IP-based physical security products. We want to make it easier for you to put safeguards in place, so you can use Axis offerings in the most secure way possible.

Apart from the following pages, you can learn more about cybersecurity, and how we can secure better cyber protection together at www.axis.com/cybersecurity

A shared responsibility

Cybersecurity is about products, people, technology, and ongoing processes. And it's clear that we all need to join forces to ensure that every link of the cyber-security chain is as strong as possible. Cybersecurity is a shared responsibility that requires the following stakeholders – including end customers – to work together.

Device manufacturers

This is where cybersecurity starts. Manufacturers should apply cybersecurity best practices in design, development, production, as well as software maintenance, to minimize the risk of flaws throughout a product lifecycle. Careful control of their own supply chain is important. Products should have built-in features that allow various security controls to be implemented. There should be tools for efficient device configuration and management that support a customer's security processes or policies. And there should be channels for informing partners and customers about newly discovered vulnerabilities.

Distributors

For distributors who do not directly touch the products they handle, cybersecurity becomes relatively simple. However, value-add distributors need to consider the same aspects as integrators and installers, especially when they buy equipment from a manufacturer and relabel it under another (or their own) brand. Transparency is key. The origin of the equipment must be clear.

Consultants, integrators, and installers

They can help end customers identify, design, and implement security controls and ensure that physical security devices are not a liability on a customer's network. This may involve developing a strategy for such things as passwords, remote access management, and maintenance of software and connected devices. It may include ensuring that installed equipment is patched with the latest updates and that the system is scanned for viruses. The challenges of using OEM/ODM equipment – where cybersecurity responsibilities often are unclear – should also be a part of the overall discussion about cybersecurity.

End customers

As each organization has specific and unique cybersecurity needs, there is no universal cybersecurity configuration. Instead, it's important to have a set of information security policies in place to define the scope of security required. Removing default accounts, establishing unique – strong – passwords that are stored safely and changed regularly, assigning differentiated permissions, and always installing patches and updates are just a few steps that should be taken.

Researchers

They often discover device vulnerabilities. If the vulnerability is not intentional, the researcher typically informs the manufacturer and gives the company a chance to fix it before publishing it. However, if a critical vulnerability has an intentional character, they often approach the public to raise awareness among users.

What cybersecurity can learn from physical security

For most people, it's easy to understand physical security risks. An unlocked door increases the risk of unauthorized people entering. Valuable goods that are visible could be easily taken. Mistakes and accidents may cause harm to people, property, and things. Physical security and cybersecurity are tackled in generally the same way.

Whether you are responsible for your organization's physical security or cybersecurity, you need to apply the same principles:

> Identify and classify your assets and resources (what to protect)

> Identify plausible threats (who and what to protect it from)

> Identify plausible vulnerabilities that threats may exploit (the likelihood)

> Identify the expected cost if bad things happen (the consequences). Risk is often defined as the probability of a threat multiplied by the harmful result. Once you have determined this, you must ask yourself what you are willing to do to prevent a negative impact.

What is cybersecurity?
Cybersecurity is the protection of computer systems and services from cyberthreats. Cybersecurity practices include processes for preventing damage and restoring computers, electronic communications systems and services, wire and electronic communications, and stored information to ensure their confidentiality, integrity, availability, safety, authenticity, and nonrepudiation.

What threats should you look out for?

The key elements to protect in an IT (information technology) or OT (operational technology) system are confidentiality, integrity, availability, and safety. Anything that negatively impacts any of them is a cybersecurity incident.

Let's now have a look at the most common threats to cybersecurity and the vulnerabilities they exploit. The four most common cyberthreats for IP-based physical security systems are:

1. **Unintentional human naivety and error**
2. **Deliberate misuse of the system**
3. **Physical tampering and sabotage**
4. **Exploitation of software vulnerabilities**

1 Unintentional human naivety and error

No matter how great the technology you use to protect your network, the human element remains a major factor in security breaches.

Types of human error that open the door to cyberattack include:

> **Social engineering**
When a user is tricked by psychological manipulation into making security mistakes or giving away sensitive information. Phishing and scareware are examples of social engineering.

> **Password misuse**
Including failing to use strong passwords or failing to protect and/or update passwords appropriately.

> **Mismanagement of critical components**
Losing or misplacing something that allows access to the system. Access cards, phones, laptops, and documentation are some examples.

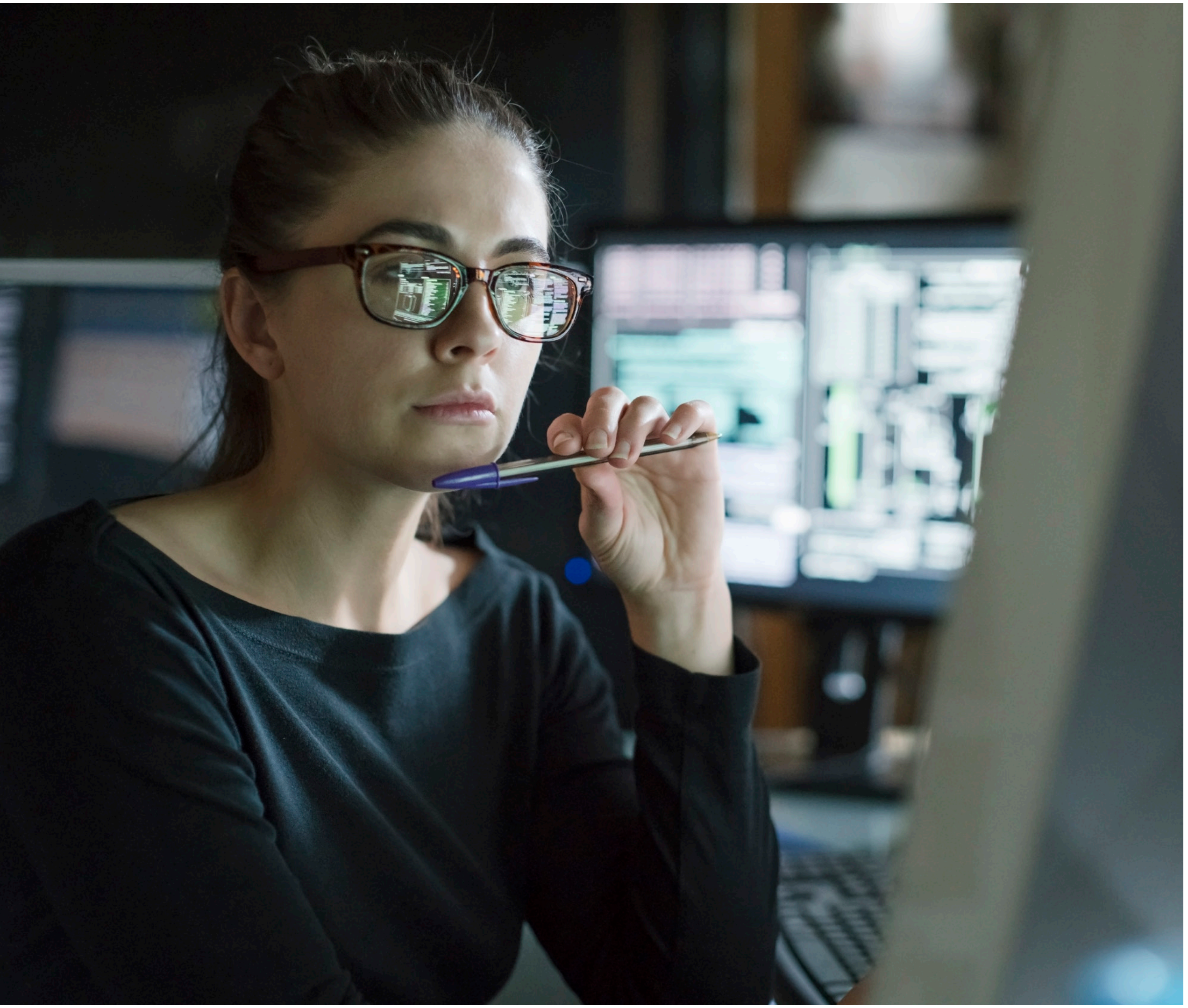
> **Poor system management**
Failure to install system updates and security patches.

> **Unsuccessful improvements**
Individuals trying to fix something, which results in reduced system performance.

Vulnerabilities and human error

Some of the most common vulnerabilities caused by human error are a lack of cyber awareness and a lack of policies and long-term processes for managing risk. To mitigate the threat of human error, everyone in an organization must be educated about cybersecurity best practices. You should also limit access to networked devices to a few trusted individuals via your video management system (VMS) or device manager.

2 Deliberate misuse of the system



Another all-too-common cyberthreat is the deliberate misuse of a system by people with legitimate access to it.

Types of intentional misuse include:

Manipulation of system services and resources

Stealing data

Causing deliberate harm to the system

Vulnerabilities and intentional misuse

It's important to implement policies and long-term processes to help manage vulnerabilities and mitigate the threat of intentional misuse of the system. Proper vetting of individuals with permissions that allow them access to sensitive data is important, as is limiting the number of individuals with such permissions.

Software used for managing networked physical security devices, such as cameras, should use an administrator account with its own credentials. This account should be unique and not shared. Site operators should then have individual accounts in the management software. And no individuals should have direct access to the physical security devices. If there are reasons for allowing direct access, this access should be temporary.

3 Physical tampering or sabotage

Physical protection is very important from a cybersecurity perspective:

- Physically exposed gear may be tampered with.
- Physically exposed gear may be stolen.
- Physically exposed cables may be disconnected, redirected, or cut.

Vulnerabilities and physical threats

Common vulnerabilities include network gear such as servers and switches that are not placed in locked areas, cameras that are easily reached and not shielded by protective housing, and cables that are not protected by walls or conduits. Networked devices may also expose other assets on the same network.

Be aware of the negative impact

Video, audio and access control systems do not process financial transactions or hold customer data. This means an attack on such systems may be hard to monetize and thus have limited value to organized cybercriminals. But a compromised system may become a threat to other systems. So estimating costs is hard. Unfortunately, in many cases, organizations learn the hard way. Protection is like quality, you get what you pay for. And if you buy cheap, it may end up costing you much more in the long run if the suppliers haven't taken into consideration cybersecurity throughout a product lifecycle.

4 Exploitation of software vulnerabilities

```
od = modifier_ob.
t mirror object to mirror
mirror_mod.mirror_object
operation == "MIRROR_X":
mirror_mod.use_x = True
mirror_mod.use_y = False
mirror_mod.use_z = False
_operation == "MIRROR_Y":
mirror_mod.use_x = False
mirror_mod.use_y = True
mirror_mod.use_z = False
_operation == "MIRROR_Z":
mirror_mod.use_x = False
mirror_mod.use_y = False
mirror_mod.use_z = True

selection at the end -add
_ob.select= 1
ier_ob.select=1
ntext.scene.objects.active
("Selected" + str(modifier
irror_ob.select = 0
bpy.context.selected_obj
data.objects[one.name].se

int("please select exactly

-- OPERATOR CLASSES ----

types.Operator):
X mirror to the selected
ject.mirror_mirror_x"
ror X"
```

In software development, there are risks, most commonly bugs or coding errors, that may lead to security vulnerabilities that could be exploited in an attack. The greater the number of software vulnerabilities present in a product, the higher the risk of exposure to attacks. Before a product is released, the manufacturer should ideally have a software development model that includes processes and tools that minimize the risk of vulnerabilities throughout all stages of software development.

Though it's rare in the industry to have software releases that are completely error-free, bugs and other improper implementations that pose security risks should be identified, fixed, and communicated to customers by the product manufacturer. Therefore, the manufacturer needs to be transparent in their communication of newly discovered software vulnerabilities and offer a solution to customers in a timely manner. It's also important that the customer continually implements software updates containing security patches and bug fixes as they are made available by the product manufacturer.

What considerations should end customers undertake to mitigate risks?

For starters, when procuring physical security products with cybersecurity in mind, there are several things to consider.

First, examine the cybersecurity approach of your physical security suppliers – do they have a company policy governing cybersecurity in which they continually identify and evaluate their assets and perform risk assessments related to those assets? It's also important that you understand how your suppliers work with their supply chain. In addition, are their products designed and manufactured with built-in cybersecurity features and support?

What measures do they offer to support cybersecurity throughout the lifecycle of a network product? And what if you experience an attack on your system? Are there guidelines from your suppliers to help you respond to a cybersecurity incident involving their products?

These are just some of the questions to consider. We'll look into more details in the following pages.

What do you need to know about your surveillance supplier – and your supplier's suppliers?

Security threats are always present. New threats arise, and their nature might change at any point in time. Oftentimes, organizations focus solely on how their suppliers assess and counter these risks. But what about the supplier's supplier? How do suppliers control and maintain their entire supply chain and ensure all products have a safe journey from component level to finished product?

Is your supplier focused on minimizing security risks?

> Do they control the entire supply chain from the component level to the finished product?

> Do they have a software development model that makes security considerations an integral part?

> Do they design and manufacture products with built-in protection?

> Do they share knowledge and tools for putting safeguards in place?

> Do they provide speedy response and free upgrades in case of newly discovered software vulnerabilities?

Supply chain partners

Supply chain security begins with choosing the right supply chain partners through a rigorous evaluation process. The evaluation process should include an analysis of each company's quality and sustainability management process. As a minimum, it should be certified by a third party according to ISO 9001 or IATF 16949.

Evaluating sub-suppliers

Your supplier should be evaluating its sub-suppliers' processes for risk management, as well as their production facilities and processes. There should be site visits and follow-up onsite audits to assess if the facilities meet the requirements and standards set for approved vendor qualification. As part of the evaluation of a potential new supply chain partner, an in-depth analysis of the sub-suppliers' financial position and ownership structure should be conducted.

Strategic sub-suppliers

When it comes to suppliers of critical components and manufacturing partners, relationships with these parties tend to be particularly close and long-term. They are strategic sub-suppliers, with whom your supplier drives joint projects and development, sets targets, and makes long-term mutual commitments and plans. All critical components in your supplier's products should be procured directly from strategic sub-suppliers and stored in-house. Non-critical components can be procured by manufacturing partners, but only from suppliers on an approved vendor list.

How secure is your supplier's production?

- Do they define and monitor the manufacturing processes?
- Are they developing and producing critical production equipment?
- Does your supplier provide a system for testing components, modules, and products during production, along with software, testing computers, and other IT hardware infrastructure?
- Does your supplier gather production data 24/7 to enable real-time data analysis, assess any potential security risks, and implement mitigation plans?

The best way for your supplier to assure sub-supplier compliance with specified requirements is to conduct regular onsite audits, yearly or bi-yearly. These audits should cover a range of important aspects such as process compliance, quality control, and traceability records. It should also include reviews of physical in-plant handling, inventory handling, and production equipment.

Quarterly business reviews are a good way of following up on performance against expectations. For strategic sub-suppliers, it's recommended that these reviews be conducted at the top management level.

Physical security

Every site within the supply chain, from the component supplier to the distribution center, must meet high requirements for facility security. For instance, they must ensure entrances and exits are continuously guarded, and access controls and visitor registration should be logged and stored. Additionally, they should use scanning equipment to detect undesirable objects or materials. And transportation should only be arranged through recognized, well-known forwarders who maintain rigorous security regulations and controls. It's also recommended that incoming and outgoing goods are frequently surveilled and documented using cameras.

Zero-trust networks

Networks are increasingly vulnerable. Exponential growth in connected devices creates network endpoints that are open to attacks. Cyberattacks have grown not only more numerous, but also more sophisticated. As a result, the concept of "zero trust" has emerged.

Trust nobody and nothing in the network

As the name suggests, the default position in a zero-trust network is that no entity connecting to and within the network – whether human or machine – can be trusted. This is regardless of where these entities are, and how they're connecting. Rather, the overriding philosophy of zero-trust networks is, "Never trust, always verify."

Stick to the minimum access required

This demands that the identity of any entity accessing or within the network is verified multiple times in different ways, depending on the behavior and the sensitivity of the specific data being accessed. In essence, entities are granted the minimum level of access required to complete their task.

Zero-trust networks and architectures

As customers become more knowledgeable about the need to strengthen cybersecurity, they are implementing zero-trust networks and architectures, including HTTPS and the more sophisticated IEEE 802.1X standard, which can automatically allow authenticated devices into the network or block unauthenticated ones. It becomes essential for network device manufacturers to meet such requirements by including technologies or interfaces that support such networks.

The default position in a zero-trust network is that no entity connecting to and within the network can be trusted.

Enter the policy engine…

At the heart of every zero-trust network is a policy engine: software that lets an organization create, monitor, and enforce rules about how data and network resources can be accessed. Policy engines use a combination of network analytics and programmed rules to grant role-based permission based on several factors.

Yea or nay to every request

Put simply, the policy engine compares every request for network access to policy, and informs the enforcer whether the request will be permitted or not. In a zero-trust network, the policy engine defines and enforces data security and access policies across hosting models, locations, users, and devices.

Defining and applying rules

For a policy engine to work, organizations must carefully define rules and policies within key security controls such as next-generation firewalls (NGFWs), email and cloud security gateways, and data loss prevention (DLP) software. Together, these controls combine to enforce network micro-segmentations beyond hosting models and locations.

How can data and network resources be accessed?

Policy engines let you:

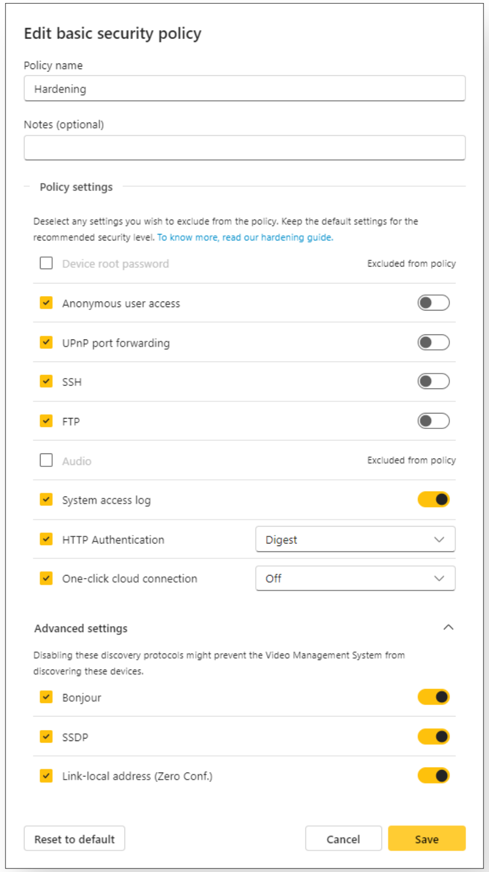
> Create rules

> Monitor rules

> Enforce rules

Policy engines today and tomorrow

At present, it may be necessary to set policies in each solution's management console, but increasingly integrated consoles can automatically define and update policies across products. Identity and Access Management (IAM), multifactor authentication, push notifications, file permissions, encryption, and security orchestration all play a role in the design of zero-trust network architectures.



Edit basic security policy

Policy name: Hardening

Notes (optional):

Policy settings

Deselect any settings you wish to exclude from the policy. Keep the default settings for the recommended security level. To know more, read our hardening guide.

- □ Device root password — Excluded from policy
- ☑ Anonymous user access — ○
- ☑ UPnP port forwarding — ○
- ☑ SSH — ○
- ☑ FTP — ○
- □ Audio — Excluded from policy
- ☑ System access log — ●
- ☑ HTTP Authentication — Digest
- ☑ One-click cloud connection — Off

Advanced settings

Disabling these discovery protocols might prevent the Video Management System from discovering these devices.

- ☑ Bonjour — ●
- ☑ SSDP — ●
- ☑ Link-local address (Zero Conf.) — ●

Setting a policy engine.

Why it's critical to implement effective lifecycle management

Keeping pace with threats

Effective lifecycle management can help organizations keep their business secure and better prepare for the future. It requires knowing where risks lie and keeping up to date on areas that might be exploited. This is especially important for security systems, because if a network surveillance camera goes down, the consequences could be serious.

Networked devices need updating

All networked devices – from network cameras to VMS – need to be updated and patched to prevent attackers from exploiting known vulnerabilities and undermining existing protections.

Manufacturers regularly release updates and security patches for device software that address vulnerabilities, fix bugs, and resolve other performance issues to help ensure a stable and secure system. However, organizations often fail to update the firmware or operating system that the hardware runs on. This is usually because they lack a full overview of all the devices on their network. And even with an overview, it can be cumbersome and time-consuming to update all the devices.

Neglecting to update device software can leave devices vulnerable to cyberattacks and can result in anything from loss of operation to large fines from regulators for non-compliance.

As the saying goes, a network is only as secure as the devices connected to it, so it's important to effectively manage the lifecycle of networked physical assets.

One device – two lifetimes

There are two types of lifecycles associated with software-based devices:

1) The device's functional lifetime – or how long a device can realistically operate and function. For instance, a network camera typically has a functional lifetime of 10-15 years.

2) The device's economic lifecycle – or how long until the device starts costing more to maintain than adopting new technology? While an IP camera might function for 15 years, its actual lifespan will be shorter due to rapid changes in the cybersecurity landscape.

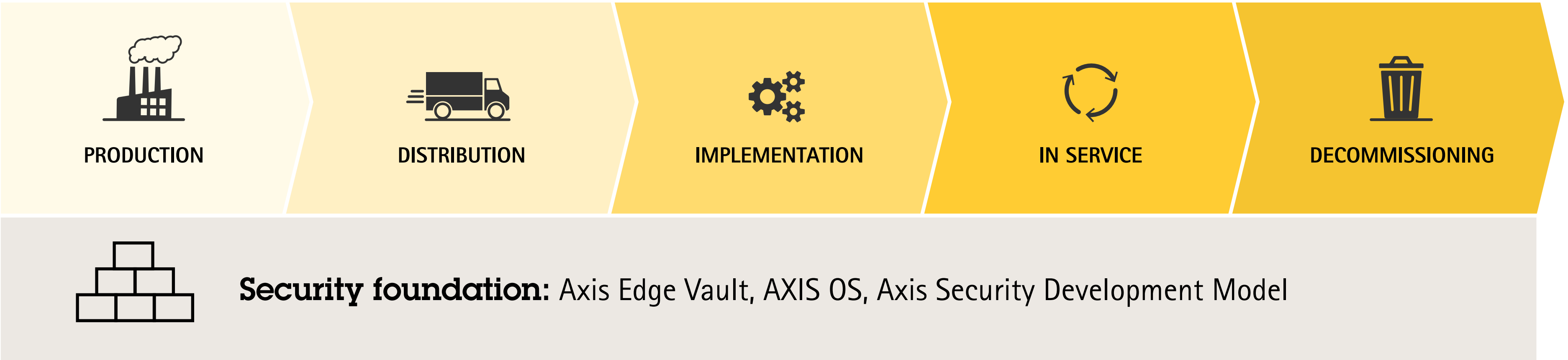
Proactively manage your assets

Lifecycle management is the effective management of both the functional and economic lifecycle of physical assets. Organizations need a clear overview of all the devices deployed on the network to ensure they're safe from threats.

Axis cybersecurity approach

Axis is committed to supporting high levels of cybersecurity. We work continuously to improve our offerings and cybersecurity processes. We believe in the importance of being transparent about how we secure our operations and our supply chain, how we handle software development that reduces the risks of vulnerabilities, how we manage newly discovered vulnerabilities, and how we build security into our products and support cybersecurity throughout their lifecycle.

The following pages detail the measures we take as our security foundation, as well as what we do and provide throughout the various phases of a product lifecycle – from production to implementation, in service, and decommissioning – to mitigate risks and help you to secure Axis products.



PRODUCTION

DISTRIBUTION

IMPLEMENTATION

IN SERVICE

DECOMMISSIONING

Security foundation: Axis Edge Vault, AXIS OS, Axis Security Development Model

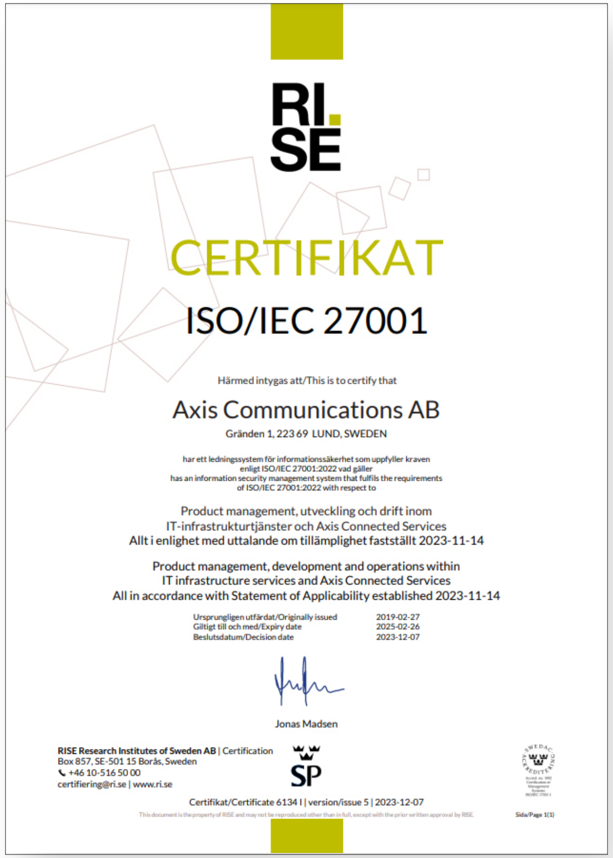
Security foundation

A structured and systematic approach to internal security

At Axis, we promote a collaborative approach to security where all employees help drive the continuous improvement of our internal security. Our ISO 27001-certified Information Security Management System (ISMS) is the foundation of our cybersecurity framework. As part of the ISMS, we've implemented cybersecurity controls to ensure we follow best practices when managing our IT infrastructure and development platform for software, as well as for connected services.

By following a structured and systematic approach, we protect the confidentiality, integrity, and availability of our assets. Axis also complies with a variety of regulatory requirements, and strategically selected frameworks and standards, including the cybersecurity standard ETSI EN 303 645 for the AXIS OS portfolio of devices. But we don't rely solely on regulations and certifications; numerous certifications do not necessarily mean better cybersecurity.

Learn more about Axis compliance



RI.
SE

CERTIFIKAT

ISO/IEC 27001

Härmed intygas att/This is to certify that

Axis Communications AB

Gränden 1, 223 69 LUND, SWEDEN

har ett ledningssystem för informationssäkerhet som uppfyller kraven
enligt ISO/IEC 27001:2022 vad gäller
has an information security management system that fulfils the requirements
of ISO/IEC 27001:2022 with respect to

Product management, utveckling och drift inom
IT-infrastrukturtjänster och Axis Connected Services
Allt i enlighet med uttalande om tillämplighet fastställt 2023-11-14

Product management, development and operations within
IT infrastructure services and Axis Connected Services
All in accordance with Statement of Applicability established 2023-11-14

Ursprungligen utfärdat/Originally issued	2019-02-27
Giltigt till och med/Expiry date	2025-02-26
Beslutsdatum/Decision date	2023-12-07

Jonas Madsen

RISE Research Institutes of Sweden AB | Certification
Box 857, SE-501 15 Borås, Sweden
☎ +46 10-516 50 00
certifiering@ri.se | www.ri.se

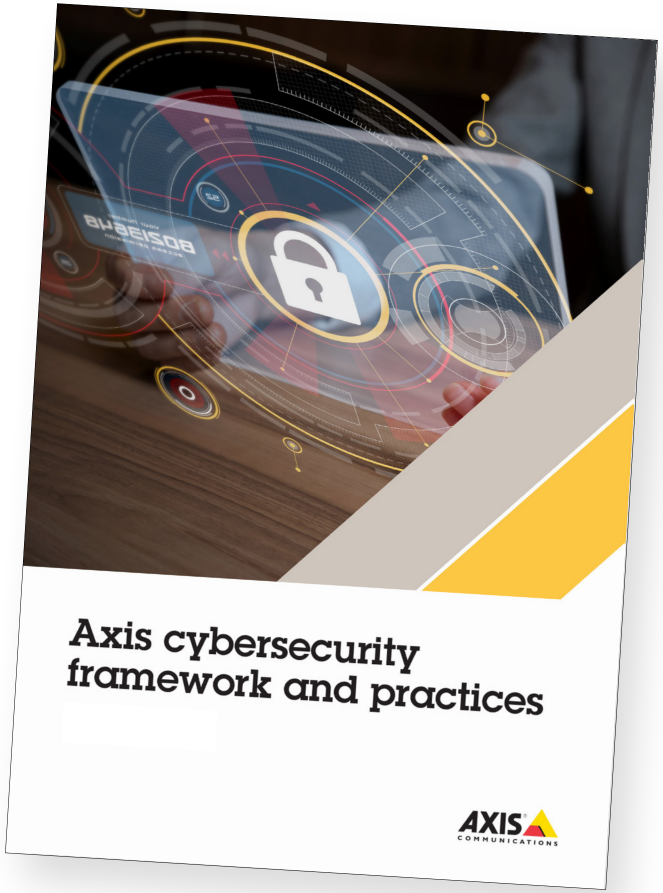
SP

SWEDAC ACKREDITERING

Certifikat/Certificate 6134 I | version/issue 5 | 2023-12-07

This document is the property of RISE and may not be reproduced other than in full, except with the prior written approval by RISE.

Sida/Page 1(1)



Axis cybersecurity framework and practices

Security foundation

Protecting product integrity and reducing the risk of vulnerabilities in software

Moving from internal security to product security, the following measures form the security foundation for Axis hardware and software, and reflect our guiding principle of transparency.

Axis Edge Vault cybersecurity platform

Built into Axis devices, this hardware-based platform includes features that safeguard the integrity of Axis devices, so you can securely boot them, integrate them, and ensure sensitive data, like cryptographic keys, are protected from unauthorized access.

Read more about Axis Edge Vault

Axis Security Development Model (ASDM)

ASDM is the development methodology applied at Axis to reduce the risk of releasing products with software vulnerabilities. It ensures that security considerations are an integral part of software development and cover areas such as risk assessments, threat modeling, analysis of code, penetration testing, bug bounty program, and vulnerability scanning and management. By promptly detecting and resolving issues at every stage of development, ASDM helps reduce security-related risks for our customers.

Read more about ASDM

Security foundation

AXIS OS

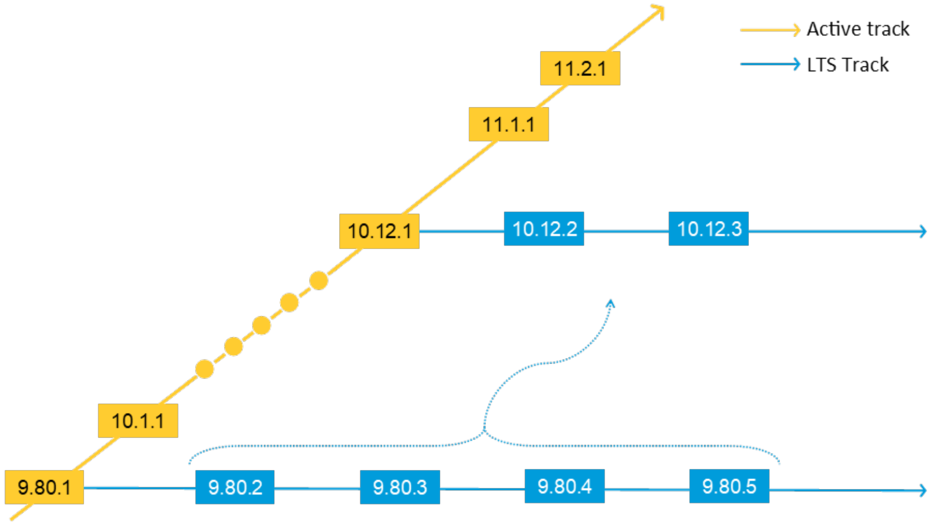
AXIS OS is our Linux-based operating system for edge devices. Built around openness, transparency, and cybersecurity, this powerful operating system features different OS tracks for Axis devices, allowing Axis to quickly release software security features and patches across a great number of products. It's designed to help you mitigate risks and keep your Axis products and services up to date and protected. The end-of-support date for many products are shown on the Axis website, enabling you to plan for the decommissioning and replacement of the products in a timely manner.

Read more about AXIS OS

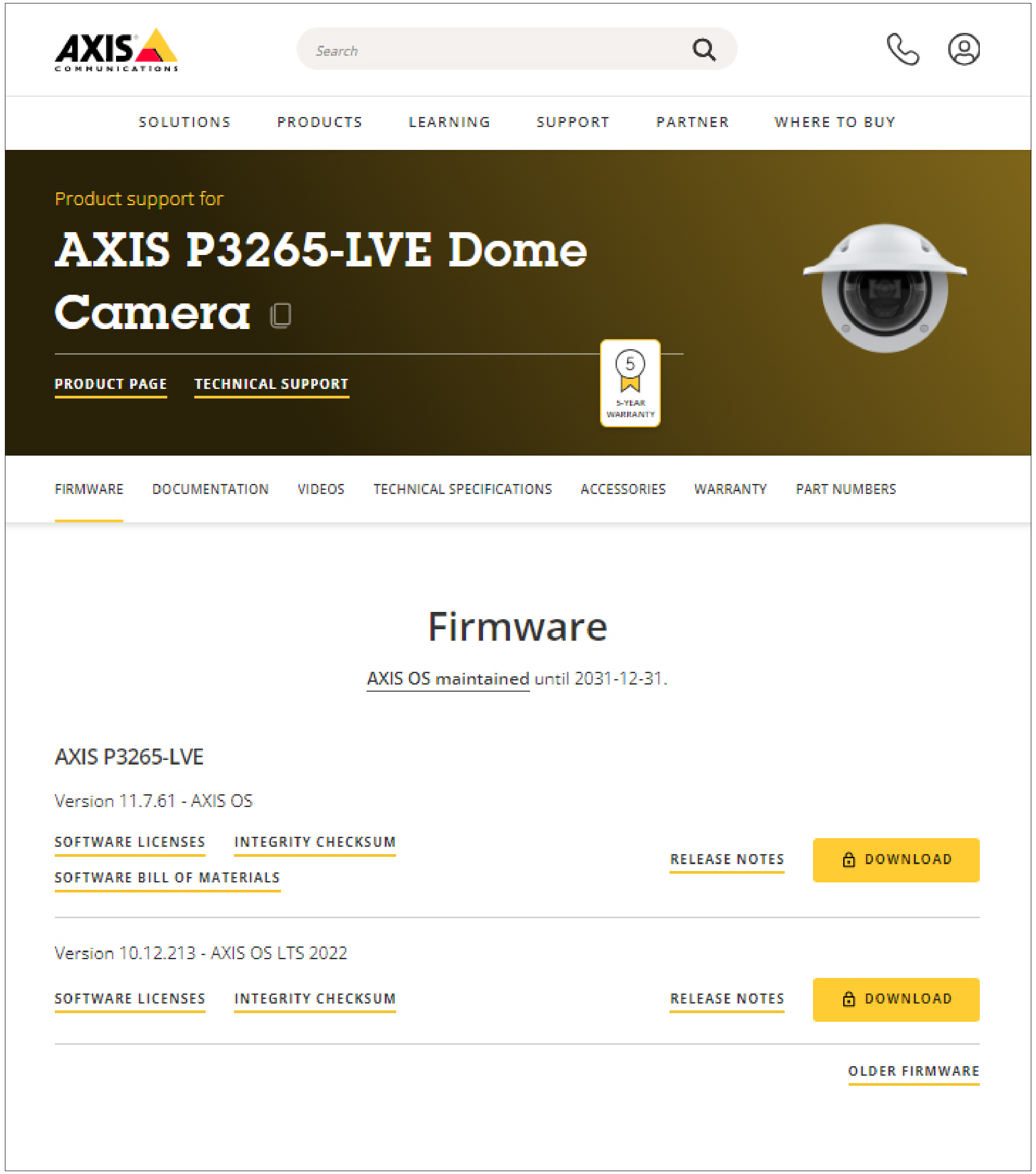
Software bill of materials (SBOM)

Additionally, we publish a software bill of materials (SBOM) for AXIS OS with an added focus on cybersecurity and improved transparency for customers, security researchers, and authorities. The SBOM provides an extensive, detailed list of the components used to construct the operating system for Axis devices. It offers insight into the cybersecurity best practices applied by suppliers and includes valuable information for third parties who specialize in vulnerability assessment, threat analysis, and remediation plans.

Read more about the software bill of materials



AXIS OS tracks.



Product support for

AXIS P3265-LVE Dome Camera

PRODUCT PAGE | TECHNICAL SUPPORT

FIRMWARE | DOCUMENTATION | VIDEOS | TECHNICAL SPECIFICATIONS | ACCESSORIES | WARRANTY | PART NUMBERS

Firmware

AXIS OS maintained until 2031-12-31.

AXIS P3265-LVE

Version 11.7.61 - AXIS OS

SOFTWARE LICENSES | INTEGRITY CHECKSUM | SOFTWARE BILL OF MATERIALS | RELEASE NOTES | DOWNLOAD

Version 10.12.213 - AXIS OS LTS 2022

SOFTWARE LICENSES | INTEGRITY CHECKSUM | RELEASE NOTES | DOWNLOAD

OLDER FIRMWARE

Managing newly discovered vulnerabilities

As a member of the Common Vulnerabilities and Exposures (CVE) Numbering Authority (CNA), Axis publishes and notifies stakeholders about vulnerabilities so our customers can take appropriate and timely action. Working with external researchers, Axis discloses vulnerabilities and exposures in a transparent, responsible, and coordinated process. Axis provides patches to affected devices, software, or services and publishes all the necessary information on the **Axis website** and through the publicly available CVE Program vulnerability database. In addition, we provide a security notification service so you can sign up and receive information about vulnerabilities and other security-related matters. Axis stresses the importance of keeping the operating system of installed products up to date to ensure that the latest security patches are incorporated.

Read more about the Axis Vulnerability Management Policy

Bug bounty program

We run a bug bounty program as part of our transparent vulnerability management strategy. This program is conducted in collaboration with Bugcrowd, the leader in crowdsourced cybersecurity. We are committed to building professional relationships with external security researchers and ethical hackers. As part of the program, researchers who discover vulnerabilities with AXIS OS-based products are eligible to receive a "bounty" cash reward. Axis will then transparently disclose externally such vulnerabilities and others that are found, and provide patches to affected products.

Reducing the risk of compromised hardware and software components

Supply chain security

Just like all products, physical security products must function as designed and intended, with maintained integrity. This can be achieved if the product's hardware and operating system are successfully protected from unauthorized change or manipulation during the product's journey through the supply chain.

Quality controls

Together with our suppliers and manufacturing partners, Axis applies a multitude of quality controls to maintain and protect the integrity of our products. Components are always sourced from a supplier on the Approved Vendor List, according to the bill of materials in the Axis specification. The supplier may not make any changes to the specification, work instructions, or quality inspection documents, without permission from Axis. Any approved changes must be documented and logged.

Traceability

A material handling process always ensures the status of materials, revealing any deviations that could compromise quality. Suppliers and manufacturing partners are required to maintain a traceability system to ensure the traceability of produced batches from incoming material to the finished component. During production, the physical component undergoes multiple tests, verifying conformance and highlighting any deviations.

Detect counterfeit components

An Automatic Optical Inspection (AOI) contributes to verifying that there are no counterfeit components mounted. At Axis, we develop and produce our critical production equipment, as well as the system for testing the components, modules, and products at different stages during production. This process limits the risk of tampering. As an additional security control, all test data is shared with Axis 24/7 so unauthorized modifications are immediately identified.

Read more about
Axis supply chain security

Countering threats during distribution

The built-in cybersecurity features in Axis devices, together with making a factory default on the devices, offer protection from unauthorized software modifications during shipment. The features that are supported by Axis Edge Vault (detailed on the next page) safeguard sensitive information in the devices and ensure the devices run only a genuine Axis operating system.

Understanding supply chain security is necessary when you are doing vendor risk assessments to determine if the vendor has measures in place that mitigate risks posed to your organization.

Built-in cybersecurity features

Axis devices come with built-in security features that enable you to securely boot them, onboard them, and be sure that sensitive information is protected.

Axis Edge Vault cybersecurity platform
Our hardware-based cybersecurity platform provides a solid foundation to ensure your Axis device is a trusted and reliable part of your network. Axis Edge Vault includes features* such as:

> **Secure keystore**, which involves cryptographic computing modules for the secure storage of cryptographic keys, safeguarding the device's identity and other sensitive information from unauthorized access – even in the event the device is compromised. The cryptographic computing modules can be a Trusted Execution Environment that is built into the Axis system-on-chip (SoC). It can also be a secure element or a Trusted Platform Module, which are separate chips on the motherboard. Axis devices are built using one or any combination of these three modules.

> **Signed firmware** and **secure boot**, which ensure the device only downloads and runs a genuine Axis operating system (AXIS OS).

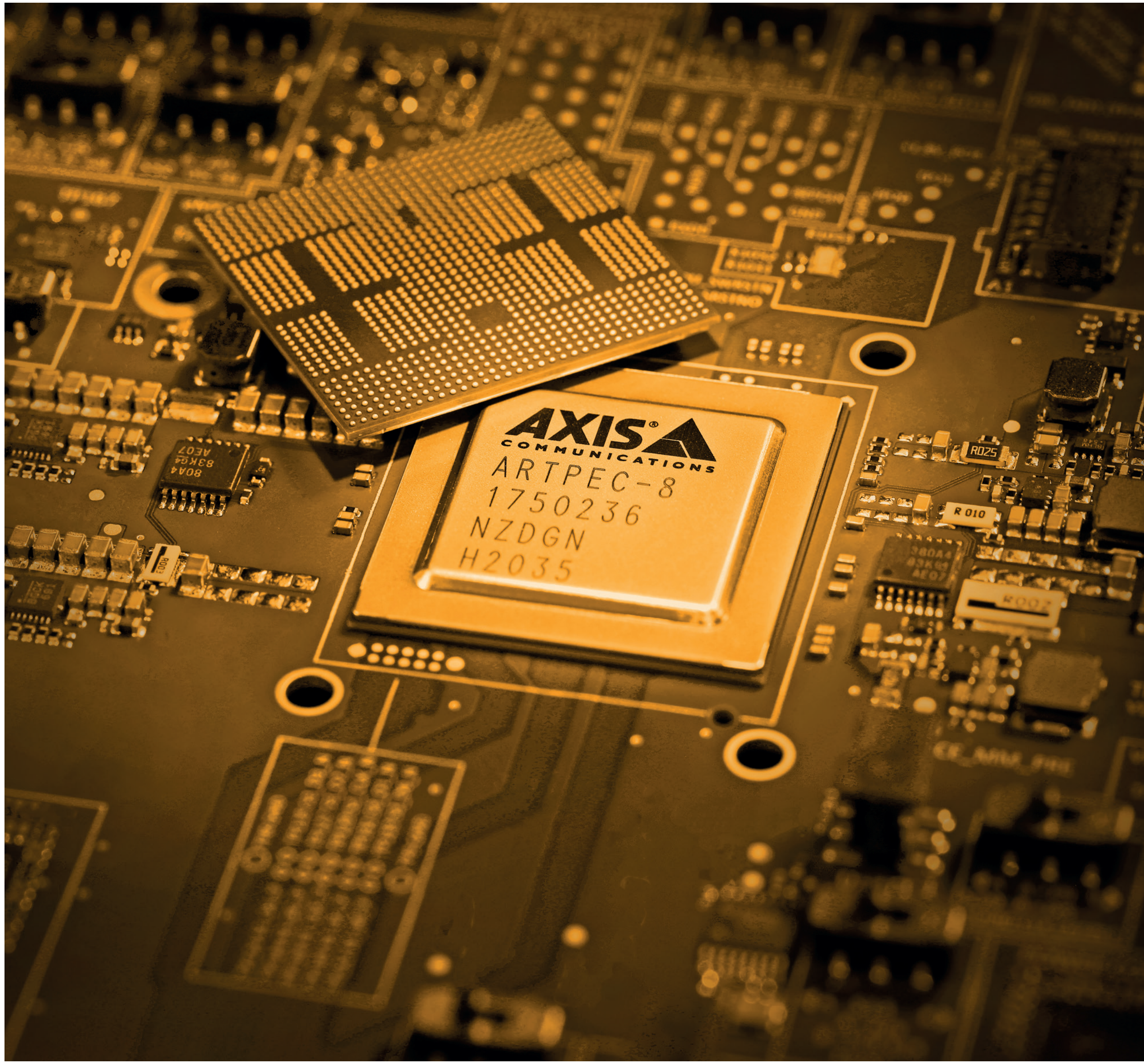
> **Axis device ID**, which is IEEE 802.1AR compliant, for secure device identification and onboarding on a network.

> **Encrypted file system**, which protects data in the file system from being extracted or tampered with while the device is not in use, such as during transit from a system integrator to the end customer.

> **Signed video**, which enables users to verify the authenticity of captured video and ensure it hasn't been tampered with.

**Note: Not all device models support all the Axis Edge Vault features. Check the datasheet or the Axis product selector for confirmation of the features supported by the product.*

Learn more about Axis Edge Vault



Default settings

Beyond product security features, Axis devices are delivered with predefined default protection settings.

Credentials and network protocols

The Axis device will not operate until accounts involving a username and password are set. After setting them, access to admin functions and/or video streams is only provided when those credentials are used.

In addition, only a minimum number of network protocols and services are enabled by default in Axis devices, such as HTTP and HTTPS for accessing device interfaces, RTSP and RTP for video and audio streaming, and some protocols like UPnP and Bonjour for the discovery of Axis devices by third-party applications.

Meeting customers' zero-trust networks

Axis has responded to zero-trust requirements by producing products with unique Axis device IDs and support for the HTTPS protocol and the IEEE 802.1X standard, as well as the IEEE 802.1AR for device authentication and IEEE 802.1AE MACsec for automatic data encryption.

HTTPS is enabled by default, allowing passwords for devices to be securely set. It also allows video management software using HTTPS to verify the trusted CA-signed SSL certificate, which is supported by the Axis device ID in newer products.

Support for IEEE 802.1X, IEEE 802.1AR and IEEE 802.1AE – enabled by default in Axis products – allows for automated device onboarding, authentication and end-to-end encryption. This provides IT professionals with standard mechanisms to efficiently and securely integrate Axis devices into a corporate network with support for IEEE 802.1X. Customers using Axis devices in an Aruba network can download the integration guide that outlines the best practice configurations for secure onboarding and management of Axis devices.

Learn more about
Axis solutions for enterprise IT

IMPLEMENTATION

Cybersecurity during implementation

An Axis device is a network endpoint like any other device, such as laptops, desktop computers, or mobile devices. However, unlike a laptop computer, Axis devices don't have users visiting potentially harmful websites, opening malicious email attachments, or installing untrusted applications. Nevertheless, a network video, audio or access control product is a device with an interface that may expose risks to the system it's connected to.

Hardening guides, which are available for Axis products, provide recommendations on how to reduce exposure to cyber risks. The following are some of the basic recommendations. For instance, we recommend that you perform a factory default before configuring a device to ensure that it is free of unwanted software or configuration.

In addition, check to make sure that the device runs on the latest AXIS OS, which would contain the latest security patch and bug fixes for the particular device.

You should set strong passwords, limit direct access to the device's web interface, configure the device to use only HTTPS (which encrypts data traffic between the client and device), and disable unused services and functions to reduce unnecessary risks. It's also important to set the date and time on the device correctly to enable accurate system logs and ensure that digital certificates – which services such as HTTPS and IEEE 802.1X rely on – can be validated and used.

An Axis tool that enables efficient configuration and management of Axis devices locally is AXIS Device Manager. It enables batch processing of installation and security tasks, such as managing device credentials, deploying digital certificates, disabling unused services, and upgrading AXIS OS. See the next page for more information about device management software.

For the full and extended hardening recommendations for AXIS OS-based devices, go to the AXIS OS Hardening Guide. To access hardening guides for Axis video management software and network switches, go to the Cybersecurity resource page. And for information about how Axis devices can integrate seamlessly into enterprise IT infrastructure and networks, see Axis solutions for enterprise IT.

Axis provides tools, documentation, and training to help you mitigate risks and keep your Axis products and services up to date and protected.
Access our cybersecurity resources.

IN SERVICE

Cybersecurity of devices in service

While a device is in operation, one of the most important ways to maintain its cybersecurity is to make sure that its firmware or operating system, AXIS OS, is kept up to date. This will ensure that the device incorporates the latest security patches and bug fixes. The features, signed firmware and secure boot, in Axis devices ensure that only genuine AXIS OS can be installed and operated. AXIS OS versions, which are provided free of charge, are either on the active track or on the long-term support (LTS) tracks. AXIS OS versions on the active track support new features, while those on the LTS tracks do not in order to minimize the risk of compatibility issues. Both tracks, however, include security patches and bug fixes. A way to keep tabs on newly discovered vulnerabilities is to sign up for the Axis Security Notification Service. Published vulnerabilities will have instructions on how affected products should be fixed with new device software.

To make it easier and more efficient to update the operating system for large numbers of devices, Axis offers device management software like AXIS Device Manager and AXIS Device Manager Extend.

How does device management software work?

Device management software can quickly gather a full real-time inventory of all the cameras, encoders, access control, audio, and other devices connected to the network. It scans the entire network, and when a new or updated device is found, it captures all the key information including model number, IP and MAC addresses, device software version, and certificate status.

The full overview

With a highly detailed overview of the entire network ecosystem, it's easier to implement consistent lifecycle management policies and practices across all devices and securely manage all major installation, deployment, configuration, security, and maintenance tasks.

Cybersecurity policies and best practices for device management need to address questions around such things as password strength and how often users need to change their passwords; which unused services should be turned off to reduce the surface area for potential attacks; how frequently devices should be scanned for vulnerabilities; and what procedures are in place for assessing risk levels when a manufacturer posts known exploitations.

Save time and effort

Device management software helps organizations save time and effort when it comes to managing cybersecurity risks. It can be used to:

- Push out system changes, device software updates, and new digital certificates to all appropriate devices simultaneously.
- Easily create or reconfigure security settings and apply them across your entire network to ensure all devices comply with the most current security policies and practices.
- Verify that all devices are running the latest and most secure software version.
- Manage user privilege levels across the network and configure modifications.

Gain real-time insights

Device management tools offer organizations real-time insights into the state of their ecosystem. For instance, you can see which devices need to be updated with the latest software updates and certificates, as well as get information on product discontinuation and end-of-support date so you can plan for when devices need to be replaced.

Device management tools from Axis

Our device management software, AXIS Device Manager and AXIS Device Manager Extend, help you to efficiently manage your Axis devices. AXIS Device Manager and AXIS Device Manager Extend complement each other.

AXIS Device Manager

AXIS Device Manager helps ensure fast and easy installation and configuration of new devices. This on-premise tool supports all major installation, security, and operational tasks, including the installation of software upgrades and applications. It allows you to configure Axis devices with backup and restore settings, and you can view the warranty status. It's also possible to apply cybersecurity controls such as HTTPS and IEEE 802.1X certificates.

Read more about
AXIS Device Manager

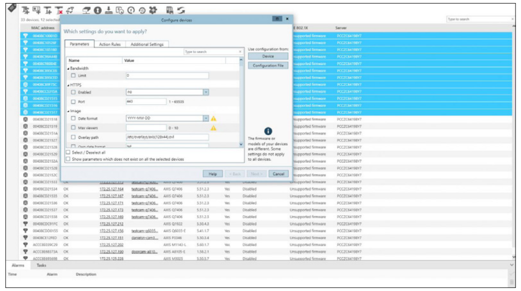
AXIS Device Manager Extend

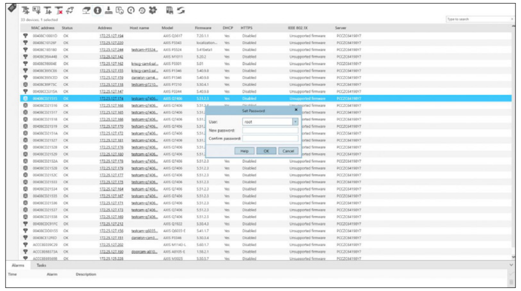
Ideal for multisite operations, AXIS Device Manager Extend helps you remotely manage your assets across all your sites. This easy-to-use application simplifies scaling of crucial maintenance tasks, such as upgrading AXIS OS; defining, applying, and enforcing security policies; and managing applications. Featuring a live dashboard, it speeds up troubleshooting by providing situational awareness of potential issues in the system, such as devices that are offline or out of warranty. Plus, it offers recommendations for device settings to help minimize security threats and mitigate vulnerabilities. Security policies can be defined, applied, and enforced for all Axis devices simultaneously.

Read more about
AXIS Device Manager Extend

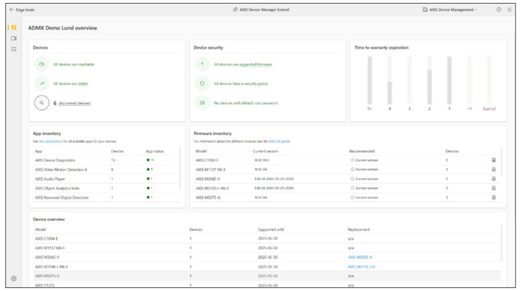
In the event of a security breach

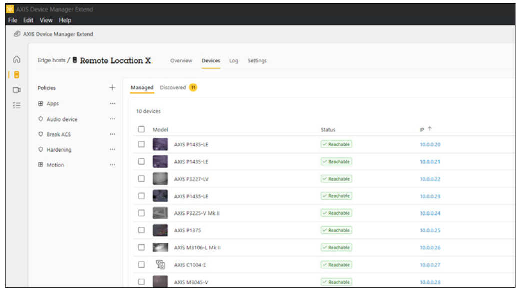
If there is a security breach of your network, Axis provides the AXIS OS Forensic Guide to help you conduct a forensic analysis of your Axis networked devices.





Snapshots of AXIS Device Manager interface.





Snapshots of AXIS Device Manager Extend interface.

DECOMMISSIONING

Planning for decommissioning

Updates and patches are the best way to maintain a product's cybersecurity, but they are not always available when a product becomes too old to be supported. From a cybersecurity perspective, older, unpatched products pose a great risk. Any overlooked device could easily become an entry point for attackers.

It is important to plan for when products should be decommissioned to avoid the risk of running devices that are no longer supported and with potentially unpatched vulnerabilities. Axis shows the end-of-support date for a product's operating system so you can prepare to decommission and replace a device in a timely manner. In addition, AXIS Device Manager Extend allows you to get warranty, product discontinuation and end-of-support information for all devices in the system.

Removing data on a decommissioned device is also important. By performing a factory default, you can quickly erase all configurations and data from the device. Visit the AXIS OS portal for details on decommissioning products.

Compliance

Governments are passing more and more cybersecurity-related laws and regulations that any business operating within their borders must comply with. Likewise, industries and organizations are increasingly mandating conformity to certain standards, including certification of products and services. It is the responsibility of all stakeholders to ensure they comply with laws and regulations, and implement guidelines and specifications relevant to their business processes.

Cybersecurity compliance as a baseline

Cybersecurity compliance means following the standards and regulatory requirements defined by authorities. And, while there is no doubt that standards and certifications are important, this is only part of the story.

There is always a risk that adherence to standards and certifications becomes a "box-ticking" exercise.

Cybersecurity compliance is continuously evolving and what was once "nice to have" is quickly becoming mandatory.

That's why organizations must view standards and certifications as a baseline – a minimum requirement rather than a target. The real goal is for suppliers to deliver products and services that can be operated in the most secure way possible. And to provide customers with guidance and transparency to support the need for continuous cybersecurity maintenance.

Regulations

Cybersecurity regulations aim to force organizations to protect their systems and information and ensure that the products and services they provide have a minimum level of security. Let's look at some of the important regulations and how they apply.

In 2023, the NIS2 Directive came into force, and European Union member states have until October 2024 to transpose the measures into national law. This directive will require all EU companies operating in essential sectors to have a high common level of cybersecurity. Companies can be penalized for derelict cybersecurity, even if this is due to a failure on behalf of one of their suppliers.

So, moving forward, vendor assessments and supply chain security will be even more important. The directive will indirectly impose obligations on manufacturers, importers, and distributors, who will need to ensure they provide a duty of care throughout the lifecycle of their products.

In December 2023, the EU reached a provisional agreement on a new regulation called the Cyber Resilience Act, which defines common cybersecurity standards for hardware and software products with digital elements. It includes products directly or indirectly connected to another device or network, such as IoT devices. The proposed act aims to decrease the number of cybersecurity incidents while increasing transparency and ensuring enhanced data protection. The UK has passed a similar legislation called the UK Product Security and Telecommunications Infrastructure, which comes into effect in April 2024.

Organizations doing business with the U.S. government may also need to comply with standards such as the Cybersecurity Maturity Model Certification, which requires audit certification based on internal management of cybersecurity procedures.

Ensuring cybersecurity requires continuous vigilance and maintenance.

Standards and certifications

Most standards and certifications focus on features, countermeasures, and processes to make sure that security is an integral element. This can be complemented by third-party testing, such as penetration tests and bug bounty programs, for finding software vulnerabilities.

While relying on product certifications can bring a certain peace of mind to customers and governments, it should be noted that certifications have a shelf life of typically one year, after which the product requires recertification. With new technologies and capabilities being constantly developed and released to the market, certifications can lag behind.

Note also that even if standards can help raise the cybersecurity posture, they are no guarantee against cybersecurity incidents. Organizations need to continually review threats and security policies.

Why Axis?

Driving cybersecurity

Cybersecurity is an integral part of Axis. It guides our internal information security system, our supply chain management, the development of our products and services, and our management of software vulnerabilities. We see cybersecurity as a shared and ongoing responsibility where being transparent is key. We aim to enable you to use our offerings in the most secure way possible. It is why our products are designed and manufactured with built-in cybersecurity features and protective default settings, and why we provide hardening guides. We continuously monitor threats and look at ways to improve security. As a CVE Numbering Authority, we respond to newly discovered vulnerabilities by patching and disclosing them so you can take appropriate and timely action. We offer software upgrades to enable you to continue to harden the security of Axis devices after installation. And, with tools like AXIS Device Manager and AXIS Device Manager Extend, we make it easier for you to manage your Axis devices to mitigate cybersecurity risks throughout their lifecycle.

Other reasons for choosing Axis

> **Quality in everything we do:** All our products go through extensive testing to give our customers peace of mind.

> **Innovative technology:** We combine technology and human imagination to enhance both performance and usability. Built on open industry standards, it's flexible, scalable, and easy to integrate.

> **Sustainability at every level:** Axis has an ongoing and recognized commitment to environmentally responsible development with the use of sustainable materials. About 90% of Axis cameras and encoders launched in 2022 were PVC-free.

> **Global presence with local expertise:** Axis has the world's largest installed base of network video products and employees in more than 50 countries. We share insights and experiences and stay up to date on the latest developments.

> **The power of partnerships:** Our commitment to our partners has made Axis the most integrated camera brand on the market.

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.

AXIS® COMMUNICATIONS