Recommended cybersecurity policies for deploying and managing a Milestone and Axis system

Mitigate cybersecurity risks by focusing on day-to-day operations

Version 2.0
October 2024

Contents

1. Lack of policies and procedures is the root cause of failure

A one-size-fits-all, all-in-one feature that could make any security system and site 100% cybersecure does not exist. There is no quick fix for ensuring 100% cybersecure deployments and day-to-day operations. But there are many ways to mitigate risks. And the foundation for securing deployments and day-to-day operations is having well-defined policies in place in your organization and following clear procedures day after day.

Network security failures occur in many organizations because the company has not established clear policies, rules and procedures that govern the usage of and access rights for their own employees. IBM's 2014 Cyber security Intelligence Index concluded that more than 95% of all successful breaches could be attributed to human mistakes, poorly configured systems and poorly maintained systems. More than 10 years later, this remains true.

A recommended approach is to work according to well-defined IT protection standards, such as ISO 27001, NIST or similar. While this may seem burdensome for smaller organizations, having even minimal policy and processes in place is far better than having none at all.

2. The purpose of this document

This document recommends the cybersecurity policies that installers, integrators and end customers should focus on to mitigate security risks when deploying and managing a system involving Milestone XProtect Video Management Software (VMS) and Axis devices.

3. Important prerequisites

Employing the following three prerequisites is important to effectively implement cybersecurity policies and procedures for a Milestone-Axis system.

3.1: Follow user’s manuals and hardening guides

It is assumed that the recommendations and procedures defined and described in the Milestone and Axis manuals and hardening guides are understood and followed.

3.2: Map various user roles for system privileges

This document refers to several common user roles that interact with a Milestone-Axis system. Please map these user roles to match your own user and role classifications. An individual user may have multiple roles, depending on the organization.

- **System installer**: Installs, sets up, repairs, upgrades, and downgrades systems
- **IT and network administrator**: Configures and maintains the IT and network infrastructure
- **Surveillance system administrator**: Defines and manages the video system to secure its usage, performance, and user privileges
- **Surveillance system maintainer**: Monitors, adjusts, and troubleshoots components to secure system performance on behalf of the surveillance system administrator
- **Users**: Use Milestone XProtect VMS clients to access live and recorded media and are typically responsible for an organization’s physical protection.

3.3: Use AXIS Optimizer for Milestone XProtect

AXIS Optimizer is a constantly growing suite of plugins and integrations that optimizes the performance and usage of a Milestone and Axis system. Available for free as a one-time installer, its capabilities are used throughout the entire system lifecycle of designing, installing, configuring, operating, and upgrading the system in Milestone XProtect. It streamlines dozens of workflows for all system users, including offering several ways to efficiently apply security controls.

These will be highlighted in relevant parts of this document. In addition, other security control examples include:

- **Optimizer privileges control**: administrator roles can configure which AXIS Optimizer capabilities an operator has access to through its built-in role settings
- **Device assistant:** administrator roles gain direct, easy access to all settings for Axis devices within the Milestone XProtect Management Client. There is no need or time wasted on managing IP addresses, passwords, or additional logins to adjust device settings and configure applications installed on your devices.
- **Operator controls:** administrator roles and approved operators gain access to an Axis device's specific features directly from Smart Client.

4. Milestone and Axis system security policies

4.1 Physical protection policy

Servers, devices, network equipment and cables are physical objects that can be interfered with, sabotaged, or stolen. XProtect VMS servers and important network gear (routers, switches, etc.) should be placed in locked areas. Cameras should be mounted in hard-to-reach places and feature vandal-resistant models or casings.

Attention should be made to protect the cables in walls or conduits, as these mitigate risks of tampering and sabotage - especially for devices installed outdoors.

Recommended policies and procedures

Define an individual or organization that is responsible for visually auditing the physical protection for the XProtect VMS servers, all cameras, speakers, intercoms, and other devices as well as cabling at defined intervals. It is essential to maintain an accurate inventory of all servers and devices, including their location.

4.2 Account policies

Account policies are about outlining who gets access to what and how to ensure the system and its functions are accessed only by authorized people. Administrator-level rights are sometimes granted to normal users for the sake of convenience. In many organizations, no one really knows who is responsible for reviewing security measures, in order to ensure best practices are being followed.

Recommended policies and procedures

We recommend that organizations use the principle of least privileged accounts. This means that user access privileges are limited to only the resources needed to perform their specific work tasks.

4.3 Windows server account policy

A common, but not recommended, practice seen when deploying the Milestone XProtect VMS on one or more Microsoft Windows servers is configuring the Windows servers to only be part of a workgroup and not a Microsoft Active Directory (AD) domain. With Windows servers running in a workgroup, each server has a separate administrator account for which the password must be shared with everyone who needs to manage the servers' hardware, the Windows configuration or apply Windows updates. Over time, the risk is that the password will be shared widely within the organization, providing unauthorized individuals with administrator privileges to the Windows servers. Furthermore, when employees in the organization change roles or leaves the organization, it is not possible to disable their access to the Windows servers as the account is shared with other people.

Recommended policies and procedures

It is recommended that the Microsoft Windows servers hosting the Milestone XProtect VMS are joined to a Microsoft AD domain. This will allow central control of who in the organization have administrator permissions for the servers. It also eliminates the need to share passwords, as each individual user has his or her own AD account and password. Furthermore, it allows the organization to change or disable users' permissions to the Windows servers centrally from the Microsoft AD.

If it is not feasible to join the Windows servers to a Microsoft AD, it is recommended that for every single Windows server, a dedicated administrator account is created per user that needs administrator access to the Windows servers. This will limit the risk of passwords being shared, and it allows users to have their Windows server permissions changed or removed.

4.4 XProtect administrator account policy

Milestone XProtect VMS is delivered and installed without a predefined administrator account and password. Because of this, the administrator group account on the Windows server running the XProtect VMS' management server, is added to the XProtect VMS' built-in administrator group during the initial XProtect VMS installation.

This allows the Windows server's administrator account on the Windows server to be used to login to the XProtect VMS for initial configuration.

Recommended policies and procedures

The Windows server administrator account can initially be used to login to the XProtect VMS. However, after the XProtect VMS software has been installed on the Windows servers, it is recommended to separate permissions and responsibilities between the Microsoft AD or Windows server administrators and the VMS administrators.

Separation of permissions and responsibilities are achieved by:

1. Adding a user (that will become the VMS administrator) to the VMS' built-in administrator role. This user can either be a regular Microsoft AD user or group, a Windows server user or group from the Windows server running XProtect VMS management server, or a native VMS Basic user
2. Remove the Windows server administrator user — added during the initial installation of the XProtect VMS — from the VMS' built-in administrator role.

When this is done, the Microsoft AD and/or Windows server administrators cannot login to the Milestone XProtect VMS - not even locally on the Windows servers running the XProtect VMS. Likewise, the VMS administrators do not need to have administrator privileges in the Microsoft AD or on the Windows servers.

4.5 XProtect user account policy

Users are assigned to roles in the XProtect VMS, which in turn determines the specific permissions each user has in the system, such as which specific devices they can access and what they are allowed to do with them, such as managing settings, viewing live or recorded video, export evidence, etc.

If multiple users share a single user account, there is a risk that the password is shared with other employees in the organization, or even external system integrators. Furthermore, when employees in the organization change roles or leaves the organization, it is not possible to disable their access to the VMS as the account is shared with other people.

In addition, if users share the same account, it will make it practically impossible to audit who has performed which actions in the VMS, or who has viewed live or recorded media or exported media from the VMS.

Recommended policies and procedures

For larger organizations, it is recommended that the Microsoft Windows servers hosting the Milestone XProtect VMS are joined to a Microsoft AD domain or that an external Identity Provider (IDP), for instance Microsoft Entra ID or okta, are integrated in the XProtect VMS.

By using Microsoft AD or an external IDP, their central user management functionality provides the organization with centralized control over their user accounts, including policies for password complexity, password rotation, brute force protection, multi-factor authentication etc. These policies also apply to users accessing the XProtect VMS.

Furthermore, it is recommended to use Microsoft AD's or the external IDP's grouping or "claims" functionality as this will allow the organization to centrally control which users can access the XProtect VMS, and which role(s) they have in the XProtect VMS.

Providing access to the XProtect VMS for specific users is then just a matter of adding the users to the right Microsoft AD group(s) or setting the right IDP claim(s). The XProtect VMS administrator does not need to also add the users to the XProtect VMS and VMS roles. Similar, removing access for users, is just a matter of removing the user from the AD group, or removing their claims.

For smaller installations where the Windows servers are not joined to a domain or don't have an integration with an external IDP, it is recommended to create native VMS Basic users for each user in the VMS. Using native XProtect VMS users still provides a set of basic security functionality such as password complexity policy, brute force protection, password management, and ability to disable/enable user accounts.

4.6 Axis device account and password policy

Authentication and privilege control is an important part of protecting network resources. Implementing device account and password policies helps reduce the risk of accidental or deliberate misuse over a longer time period. A key part is to reduce the risk of compromised passwords. Strong passwords are important. However, device passwords can spread within an organization. When they do, you lose control over who may access them.

The accounts in Axis devices are primarily service accounts used for machine-to-machine communication such as with Milestone XProtect VMS. A common, but not recommended, strategy is for all devices to have the same password. And another practice seen in older systems is the use of the default root password, even though it introduces additional risks that need to be mitigated.

Another common mistake is that devices are added to the system with a single account shared by multiple roles. Two months later, when someone needs to use a browser to adjust something, the device's administrator-privileged account's password is disclosed. Within months, most people in the organization will know the password for all devices.

Recommended policies and procedures

During daily operations, Axis devices should only be allowed to interact with Milestone XProtect's recording/signaling server or device administration and management tools. System users should not be allowed to access Axis devices directly. Axis devices should have at least two accounts: one for device administrators and one for the Milestone XProtect VMS' recording/signaling server. Note that the account that the Milestone XProtect VMS recording server will use must have administrator privileges. Temporary access, for example for a surveillance system maintainer using a web browser, should be managed using temporary accounts.

Since AXIS OS 9, Axis devices do not support default passwords. In addition, AXIS Optimizer can be used to ease the task of managing multiple accounts and passwords for Axis devices used by Milestone XProtect VMS. It lets you create an XProtect VMS service account and unique 16-character passwords for each device. This eliminates usage of root accounts and passwords, and it provides efficient, automated batch process for managing accounts or passwords for Axis devices.

4.7 Axis device inventory and management policy

A fundamental aspect of ensuring the security of an enterprise network is maintaining a complete inventory of the devices on it. When creating or reviewing an overall security policy, it is important to have knowledge and clear documentation about each device and not just critical assets. That is because any single overlooked device can be a means of entry for attackers. You can't protect devices which you overlook or are not fully aware of.

Device inventory represents an essential step in securing an enterprise network. AXIS Device Manager or AXIS Device Manager Extend helps you as it:

- Lets you easily access a current, complete inventory of your network devices when working with audits and incident responders
- Provides a complete list of your devices, sorted by total number, type, model numbers, etc.
- Gives you status of each device on your network

Recommended policies and procedures

We recommend using AXIS Device Manager or AXIS Device Manager Extend as the primary application for managing Axis devices. AXIS Optimizer's integration to AXIS Device Manager Extend provides an easy way to gain a complete inventory of all Axis devices for one or multiple sites connected to a Milestone XProtect VMS. Admin roles can connect all Axis devices in the Milestone XProtect VMS to the AXIS Device Manager Extend online software application. This smart tool allows admin roles to identify, list, and sort all devices on all sites, review device warranty information, perform device software upgrades on multiple devices simultaneously, and apply security policies to harden the system.

AXIS Device Manager Extend lets you verify that all devices are running the latest AXIS OS version and deploy the desired version in minutes. You get automated checks for new device software with recommended upgrades, and you can install new OS versions across multiple sites and locations all at once.

Use AXIS Device Manager Extend when someone in a maintainer role needs to use a web browser to access devices for troubleshooting or maintenance. Select the devices and create a new account, preferably with operator privileges, that the maintainer may use. Once the task is complete, use AXIS Device Manager Extend to remove the temporary account.

4.8 Define a maintenance schedule process policy

As any other IT or security system containing physical and software components, video surveillance systems and their components also need to be properly maintained to provide high uptime and operational reliability. This requires a planned, periodic, or corrective maintenance approach. Most organizations follow the planned maintenance of video systems at regular intervals; these are typically performed by or with the support of system integrators.

In day-to-operations, the larger the system and the more devices connected to it, the more time and effort is required for admin roles to manage the system. They often need to travel to a site to resolve simple tasks — like upgrading a local Smart Client — if the system is isolated or at remote locations.

Recommended policies and procedures

For customers with larger installations or customers where the video surveillance installation is a critical element of their operation, it is highly recommended to test out all updates in a “sandbox” (a test environment separated from the production environment). This especially applies to the operating system updates for the Microsoft Windows servers running the Milestone XProtect VMS servers, as these updates are delivered outside Axis’ and Milestone’s control and knowledge.

Furthermore, it is recommended to let the Microsoft Windows servers download the updates automatically, but only apply the updates manually once testing has been done in the sandbox environment.

Finally, it is highly recommended to document your maintenance procedures and interval to ensure that existing and future colleagues understand your processes.

AXIS Optimizer can be used by administrators to remotely roll out updates to the AXIS Optimizer plug-ins installed in XProtect Smart clients. When rolling out updates, no operator interaction is required: when a local XProtect Smart Client operator restarts a client machine, the Axis Optimizer plug-in is automatically updated. This ensures client software stays up to date and is upgraded in a tightly controlled manner, both of which are important security controls.

4.9 Monitor system operation

In many installations, it can be difficult to regularly check that every part of the surveillance system is working as intended. This is especially true of larger installations with hundreds of cameras and Milestone XProtect VMS servers installed across multiple Windows servers. However, monitoring system operations can be a challenge even for smaller systems as they often are not accessed regularly by users.

Recommended policies and procedures

It is recommended to configure the Milestone XProtect VMS to send notifications, trigger alarms, or to use the system monitor feature to monitor the XProtect VMS and Axis camera performance and operation.
Notifications to recipients and systems outside of the XProtect VMS can be emails, SNMP traps or integration of webhooks. Notifications to users of the XProtect VMS clients can be XProtect VMS alarms. Permissions for alarms can be configured so the VMS administrators do not see the operational alarms, and the security operators are not disturbed by technical alarms.

The recommended events to use for triggering notifications or alarms, are the error and ‘OK’ events in these categories:

- Devices
- XProtect VMS servers
- Media database
- Storage system (disk)
- System monitor performance events (‘OK’, warning and critical events)

Alternatively, the XProtect VMS administrators and operators can use the system monitor feature to monitor the real-time status of the XProtect VMS and Axis camera operation and performance.

For larger installations where the operation of the XProtect VMS is critical, the Microsoft Windows servers, network equipment, storage systems etc. as well as the XProtect VMS software itself can be integrated into the Microsoft System Center, which among many other features, offers management, monitoring and notification functions.

Note: Not all features and events listed above are supported in all Milestone XProtect VMS products. Consult the XProtect product comparison chart for an overview of the features supported in each Milestone XProtect product.

For Axis devices, it is recommended to configure the devices to stream their log messages to a centralized SIEM or network monitoring application where logs can be stored and analyzed to meet individual policies. It makes audits easier and prevents log messages from being deleted in the Axis device, either intentionally/maliciously or unintentionally.

Depending on company policies, it can also provide extended retention time of device logs. Furthermore, Axis devices support SNMP device monitoring for more individual technical insights. Please refer to the AXIS OS Hardening Guide for more information.

4.11 XProtect and device software update policy

Leaving a system unpatched for a longer period will increase the risk of an adversary exploiting newly found vulnerabilities, possibly compromising components in the surveillance system – be it Microsoft Windows, Milestone XProtect VMS or Axis network products.

Ensuring that all software across the surveillance system is updated to the latest versions will, in most cases, ensure that your surveillance system is protected against recently found vulnerabilities since the latest versions will include patches for known vulnerabilities that attackers may try to exploit.

Recommended policies and procedures

Milestone aims to deliver three XProtect VMS software releases per year. Each release will address issues and vulnerabilities found in previous releases. It is, therefore, important to update the XProtect VMS software regularly. Updating the XProtect software to a new release requires active Milestone Care™ coverage of your purchased XProtect Product.

In case the XProtect VMS installation is not covered by Milestone Care, or it is not desired or feasible to update the VMS installation right away to address a found issue, it is possible to install so-called 'hotfixes' that address one or more specific issues. Milestone's XProtect Hotfixes web page can be monitored to check for new hotfixes, or alternatively, it is possible to subscribe to newly released hotfixes.

Axis provides device software updates regularly to address, among other things, newly discovered security vulnerabilities in its products. Axis offers two main alternatives for keeping the AXIS OS of devices up to date: the active track and the long-term support (LTS) track. The active track provides access to the latest state-of-the-art features and functionalities, as well as bug fixes and security patches.

AXIS OS versions on the long-term support track maximize stability by providing only bug fixes and security patches since the focus is on maintaining a well-integrated, third-party system. If XProtect is compatible with one AXIS OS version on the LTS track, it will also be compatible with newer releases on that track.

It is standard procedure for new AXIS OS versions to undergo compatibility testing with Milestone XProtect VMS prior to being released.

Axis also provides device management tools to make it easier for customers to keep Axis device software up to date. Through AXIS Optimizer, AXIS Device Manager Extend online software tool lets you see if new AXIS OS versions are available for the Axis devices connected to your network. This enables efficient deployment and maintenance of software upgrades for all Axis products.

AXIS Optimizer also supports an auto-upgrade service to keep the AXIS Optimizer plug-in in the XProtect Smart Clients updated with the latest versions and capabilities.

For both Axis devices and the Milestone XProtect VMS software, it is important to define a policy that describes how often software should be checked and if new versions or hotfixes have been released – including who are responsible for this task.

Axis also provides a security notification service that anyone may subscribe to.

4.12 Internet exposure policy for handling remote access

Device and services exposed to the internet increase the risk of external adversaries probing or exploiting known vulnerabilities. Axis devices that are exposed to the Internet (for instance, by small organizations that need remote video access) can become easy victims if weak passwords are used or a new critical vulnerability is discovered.

Similarly, exposing all XProtect VMS servers and services to the internet through the use of port forwarding may expose the Windows Servers, and through them, possibly the internal network and other servers to hacking from the internet.

Recommended policies and procedures

Never expose a device's IP address/port in a way that makes it accessible directly from the internet. See AXIS OS Hardening Guide. Similarly, do not expose all the XProtect VMS servers directly to the internet.

If it is desired to provide access to the XProtect VMS from the internet, the Mobile Server can provide access for the XProtect Mobile Client or the XProtect Web client. The XProtect Mobile server is designed for being exposed to the internet, and doing so will only expose a single endpoint on the XProtect Mobile Server, and thus not all the XProtect VMS servers.

When configuring the XProtect Mobile server for access from the internet, the XProtect VMS certificates guide must be followed, and it is, furthermore, recommended to install the XProtect Mobile server in a DMZ for increased cybersecurity protection.

Secondly, it is recommended to enable the XProtect VMS mobile server's two-step verification feature. With two-step verification enabled, the XProtect VMS mobile server will send an email with a validation code to the user, which must be entered to complete the login. Alternatively, use an external Identity Provider (IDP) for user management and authentication in the XProtect VMS. By using an external IDP for user authentication, multi-factor authentication can be provided as well as and other security features provided by the external IDP.

If it is desired to use the XProtect Smart Client or the XProtect Management Client to access the XProtect VMS remotely, a VPN must be configured to provide secure access to the XProtect VMS from remote locations or computers. Similarly, as for the XProtect Mobile server, an external IDP can be used to provide multi-factor authentication for the XProtect Smart Client and XProtect Management Client users.

4.13 Milestone-Axis system supports HTTPS

Communication between all XProtect VMS servers and clients support HTTPS. HTTPS provides secure authentication and bidirectional encryption of all communication, including user credentials, configuration, and media data. This prevents eavesdropping and tampering of the communication.

Recommended policies and procedures

It is recommended to configure the Axis device for HTTPS only as described in the AXIS OS Hardening Guide.

It is recommended to follow the XProtect VMS certificate guide and configure the XProtect VMS with certificates for all XProtect VMS servers to ensure all communication between XProtect VMS servers and clients is encrypted using HTTPS.

To simplify creation, distribution, trust of certificates, and renewal of certificates used by the XProtect VMS servers, it is recommended that the Microsoft Windows servers hosting the Milestone XProtect VMS are joined to a Microsoft AD domain configured with Microsoft Certificate Services, which then provides PKI functionality for the servers in the AD – simplifying the certificate handling process.

4.14 Milestone-Axis system supports SRTP/RTSPS for secure video streaming

Axis devices support secure video streaming over RTP, also referred to as SRTP/RTSPS. SRTP/RTSPS uses a secure end-to-end encrypted transportation method to make sure that only authorized clients receive the video stream from the Axis device. Using SRTP/RTSPS has certain advantages over RTP/RTSP tunneled HTTPS video streaming in terms of lower latency, lower data-throughput and multicast-capable network setups where distributed video streaming is required.

Recommended policies and procedures

Follow the AXIS OS Hardening Guide for instructions on how to configure RTSPS/SRTP.

4.15 Local network exposure policy

Reducing local network exposure can mitigate a number of risks. There are many ways to reduce the network exposure, including physical network segmentation (separate network switches and cables), virtual LAN (VLAN) and IP filtering/firewall. Axis devices support firewall techniques such as IP address filtering that only responds to requests from whitelisted IP addresses.

Recommended policies and procedures

Milestone XProtect VMS support recording servers with dual network adaptors. One adaptor can be used to access a segmented “camera” network with Axis devices and the other can be connected to the “client/corporate” network to serve the XProtect Clients. The XProtect VMS recording server will, with this configuration, act as a bridge and firewall to the device network, preventing XProtect Clients and other users or equipment on the “client/corporate” network from accessing devices directly. This reduces risks of adversaries interfering with cameras and recording media streams. If the XProtect VMS servers and devices are placed on the same network, it is recommended to configure the device firewall and whitelist the Windows servers hosting the XProtect VMS, AXIS Device Manager Extend and any additional maintenance clients.

4.16 Network security and infrastructure policy

Data that is transferred over networks should always be encrypted.

Recommended policies and procedures

It is recommended to use managed switches for the network and enable network access control mechanisms such as IEEE 802.1X combined with layer-2 network encryption provided by IEEE 802.1AE MACsec. IEEE 802.1AE MACsec adds additional network encryption on layer-2 networks on top of already secure protocols such as HTTPS and SRTP/RTSPS but provides baseline network encryption for network protocols that natively have no encryption method (for example, DHCP, NTP).

The network traffic between the XProtect VMS clients and XProtect VMS server(s) should use encryption. The traffic between XProtect recording server(s) and Axis devices should be encrypted depending on the infrastructure.
This can be done by using, for instance, HTTPS for general communication and SRTP/RTSPS for encrypted video streaming specifically.

Axis devices come with a self-signed certificate or IEEE 802.1AR-compliant device ID, and HTTPS enabled by default. Modern Axis devices also support IEEE 802.1X, IEEE 802.1AR and IEEE 802.1AE, which are enabled by default. These supports enable automated and secure onboarding and authentication of Axis devices to an IEEE 802.1X network, as well as automatic encryption of data communications between Axis devices and MACsec-enabled Ethernet switches.

4.17 FIPS 140 compliance

Recommended policies and procedures

The FIPS 140 standard specifies the security requirements of hardware and software modules needed to ensure the confidentiality and integrity of data. The Federal Information Processing Standards (FIPS) are issued by the National Institute of Standards & Technology (NIST), and many U.S. and Canadian federal entities and contractors need to ensure the products they use in their systems comply with such standards.

Milestone XProtect VMS is FIPS 140-2 conformant and can thus be configured for operation in installations where FIPS 140-2 are required. Information about how to configure the Windows servers and XProtect VMS to run in FIPS 140-2 conformant mode can be found in the XProtect VMS hardening guide's FIPS 140-2 compliance section.

Axis devices comply with FIPS 140 either through a dedicated hardware cryptographic computing module that is built into the product or through a software module for Axis network products running AXIS OS 12 or later. Please refer to product datasheets for detailed information.

4.18 Secure key storage

Recommended policies and procedures

It is recommended to run the XProtect VMS servers on computers with TPM 2.0 enabled. TPM (Trusted Platform Module) is a hardware-based cryptographic computing module that effectively protects sensitive information such as private cryptographic keys and other cryptographic material against tampering and extraction.

Axis devices are shipped with built-in support for secure key storage through the Axis Edge Vault platform. Axis Edge Vault relies on a strong foundation of cryptographic computing modules (secure element and TPM) and system-on-chip security (TEE) to protect sensitive information such as the Axis device ID and customer-loaded cryptographic information from unauthorized access. For more detailed information, please refer to product datasheets at axis.com/solutions/edge-vault.

4.19 Media storage encryption

Similar to protecting network communication against hacking or eavesdropping by using encryption, the recorded and stored media (video, audio, metadata) should also be protected against unauthorized access and tampering. This applies to both media stored in the Axis devices' edge storage (SD cards), and media stored in the XProtect VMS recording server's media database.

Recommended policies and procedures

It is recommended to enable and configure media storage encryption for both the Axis devices' edge storage and the XProtect VMS recording server's media database.

Information on how to enable and configure edge storage encryption in the Axis devices can be found in the AXIS OS Hardening Guide here. For the XProtect VMS, information on how to enable encryption for the media database can be found in the XProtect VMS hardening guide.

Note: Media database encryption is not available in all XProtect VMS products. Consult the XProtect product comparison chart to see which Milestone XProtect products support media database encryption.

4.20 Audit and monitoring

In case of incidents such as cameras being vandalized or stolen, there a risk that log files are lost.

Recommended policies and procedures

It is recommended to send and store log files and other notifications from Axis cameras in a centralized logging facility such as a remote syslog server or a more sophisticated and feature-rich monitoring management system.

By doing so, you can ensure that no log files are lost during incidents, and furthermore, logs can be stored for a longer or desired length of time. It also enables network monitoring management systems to generate alarms and notifications.

For the Milestone XProtect VMS servers, it is recommended to follow the previously mentioned recommendation to place the servers in a secure and locked location. This protects the XProtect VMS servers and the audit log messages stored in the Microsoft SQL server used by the XProtect VMS from direct exposure to being stolen or vandalized. If it is important for the organization to protect the XProtect VMS audit logs against every imaginable incident, like for instance a fire in the server room, it is recommended to regularly backup the XProtect VMS' Microsoft SQL database to a remote location that will not be affected by any incidents on the site of the surveillance system installation.

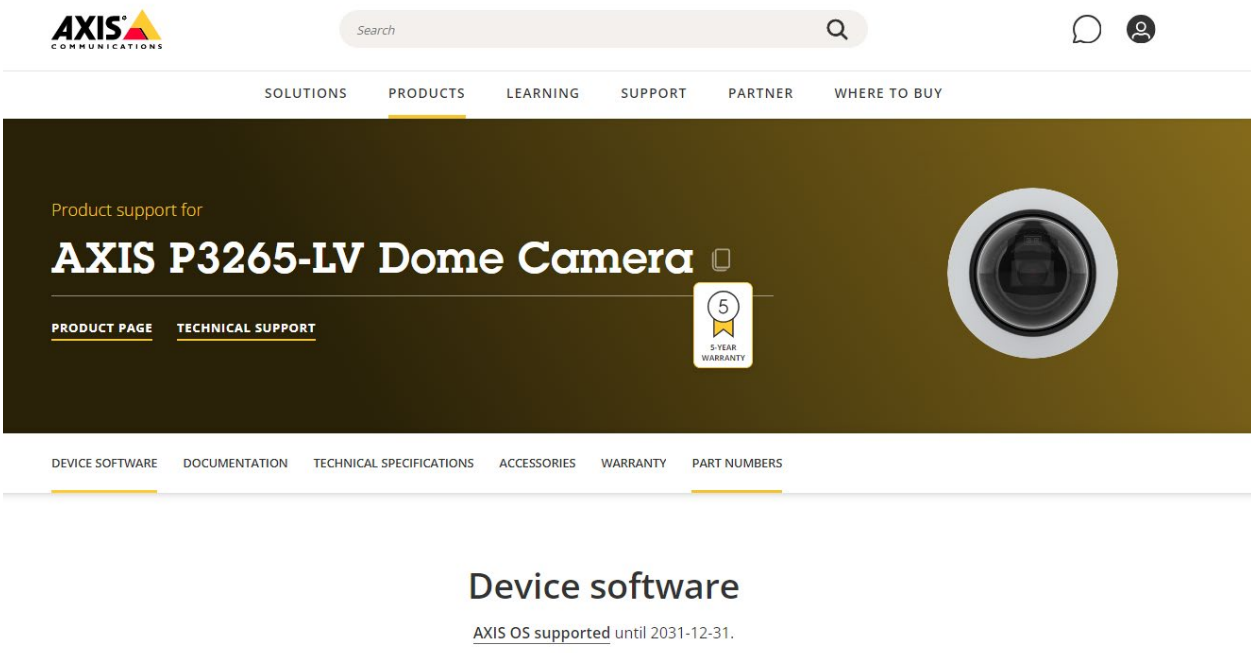
By default, the XProtect VMS logs critical user and administrator activities in the XProtect VMS audit log. Logged activities include log in, configuration changes to the XProtect VMS, and export of recorded video. However, users' regular operation activities, such as viewing live video from a camera, controlling a PTZ camera, or playing back recorded video, are not logged.

In some cases, there is a wish to audit log all user activities. This can be enabled by checking the '*Enable user access logging*' setting for the audit log. When this is enabled, all user actions in the VMS will be audit logged.

Important: If there are many active users in the XProtect VMS, the CPU and storage system load on the Windows server running the Microsoft SQL database may increase considerably, requiring a more powerful computer and a faster storage system for the Microsoft SQL database.

4.21 Axis device lifecycle and software support

Upon product launch, the support period for Axis products is outlined on the corresponding product page on axis.com. For instance, AXIS P3265 products will receive software support up until the end of 2031 as seen below.



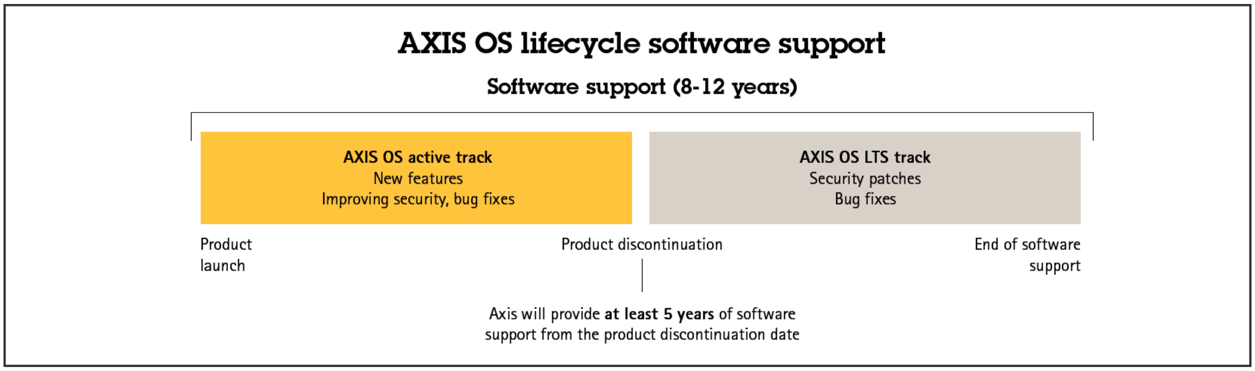
Product support for

AXIS P3265-LV Dome Camera

Device software

AXIS OS supported until 2031-12-31.

When an Axis product is in service, the security of the device should be maintained by implementing the latest available device software (AXIS OS). As mentioned in section 4.11, the AXIS OS lifecycle support consists of two main tracks: active and long-term support (LTS). When a new product is launched, only the active track is available, where updates of AXIS OS include new features, as well as patches and bug fixes. Within two years after a product launch, an LTS track is introduced, providing OS updates with only patches and bug fixes to maintain compatibility with other system components. Customers can then choose between OS updates on either the active or the LTS track. When a device is discontinued, the active track is also discontinued and only the LTS track is supported for a minimum of 5 years. Most devices have software support for 8 to 12 years.


AXIS OS lifecycle software support
Software support (8-12 years)
AXIS OS active track
New features
Improving security, bug fixes
AXIS OS LTS track
Security patches
Bug fixes
Product launch
Product discontinuation
End of software support
Axis will provide at least 5 years of software support from the product discontinuation date

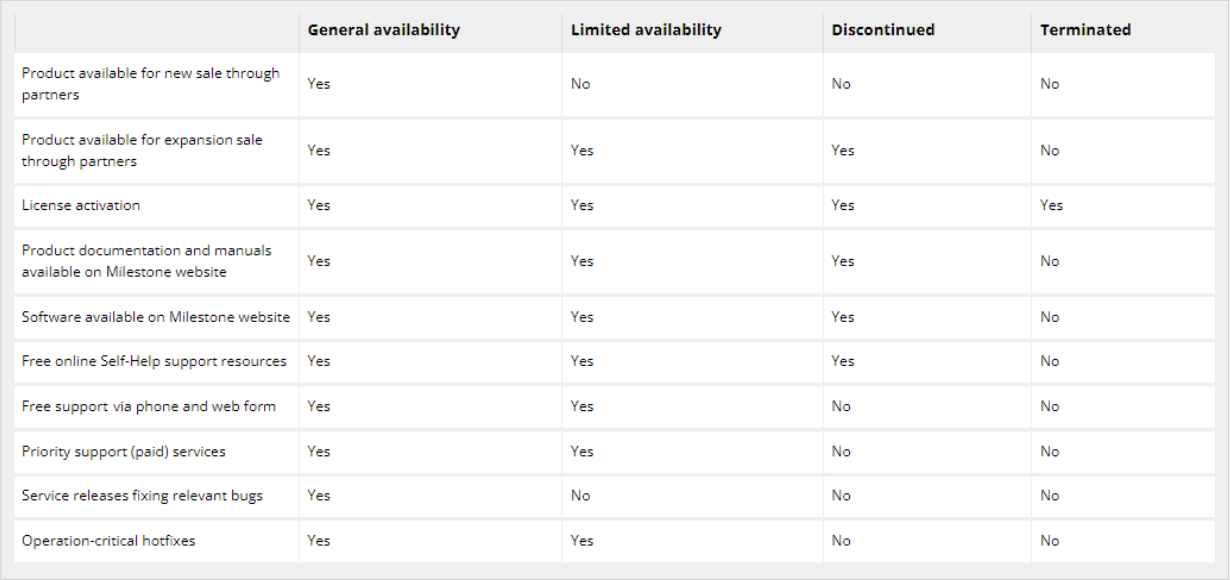
Recommended policies and procedures

Axis recommends that customers sign up for the Axis security notification service, which provides subscribers with timely notifications of security incidents and vulnerabilities.

Axis also recommends that you plan for the decommissioning and replacement of products 18 to 24 months prior to their end-of-software support date. AXIS OS Hardening Guide includes details on how to completely erase customer-specific information before disposal.

4.22 Milestone XProtect product lifecycle and software support

Milestone XProtect products generally follow a three-year lifecycle, during which the product goes through four phases of General availability, Limited availability, Discontinued, and finally Terminated, as can be seen below.



	General availability	Limited availability	Discontinued	Terminated
Product available for new sale through partners	Yes	No	No	No
Product available for expansion sale through partners	Yes	Yes	Yes	No
License activation	Yes	Yes	Yes	Yes
Product documentation and manuals available on Milestone website	Yes	Yes	Yes	No
Software available on Milestone website	Yes	Yes	Yes	No
Free online Self-Help support resources	Yes	Yes	Yes	No
Free support via phone and web form	Yes	Yes	No	No
Priority support (paid) services	Yes	Yes	No	No
Service releases fixing relevant bugs	Yes	No	No	No
Operation-critical hotfixes	Yes	Yes	No	No

Recommended policies and procedures

The exact details and state of current products can be seen on Milestone's Product Lifecycle page.

5. Hardening guides and related resources

5.1 From Milestone

The Milestone XProtect VMS runs on the Microsoft Windows operating system and are therefore at risk of the same attacks by viruses, malware and ransomware as any other IT installation running on Microsoft Windows.

Recommended policies and procedures

To address these risks, the recommendations described in the XProtect VMS hardening guide should be followed - including guidance and recommendations provided from the referenced external resources from, for instance, Microsoft, International Standards Organization (ISO), and United States National Institute of Standards and Technology (NIST).

5.2 From Axis

Recommended policies and procedures

It is recommended to apply hardening on Axis devices as outlined in the AXIS OS Hardening Guide in order to mitigate risks and ensure that Axis devices are operated as securely as possible. Milestone XProtect VMS is tested to work with the hardening applied through the AXIS OS Hardening Guide.

In case of incidents, the AXIS OS Forensic Guide provides instructions for how to forensically analyze Axis devices to ensure compliance and avoid leaving compromised devices in operation.

6. Additional organizational security controls

There are a number of additional security controls we recommend to mitigate cybersecurity risks in day-to-day operations. The following are all based on recommendations from the Center for Internet Security, a non-profit entity that harnesses the power of a global IT community to safeguard private and public organizations against cyber threats.

6.1 Implement a security awareness and training program

Recommended policies and procedures

It is recommended to implement a security awareness training program for your security staff so they can identify different forms of phishing or cybersecurity attacks.

Milestone offers a ‘Identifying Cybersecurity Threats’ eLearning course which can be used as part of the training program. The course can be found here: https://learn.milestonesys.com/home_securesystems.htm

Axis offers various cybersecurity training courses online.

6.2 Incident response and management

Recommended policies and procedures

Utilize written incident response plans with clearly defined phases of incident handling/management and personnel roles, as well as how to report a security incident to relevant authorities and third parties.

6.3 Penetration tests and self-assessment exercises

Recommended policies and procedures

Use penetration tests to identify and assess vulnerabilities that can be identified in your enterprise as well as perform exercises to assess your current organizational performance levels and improve readiness.

6.4 Vulnerability scanning

Recommended policies and procedures

Scanning devices and software applications for known vulnerabilities using network security scanners is a recommended procedure that should be performed on a regular basis. Axis devices are geared towards optimal communication to reduce false positive alarms but also accurate testing results. Please refer to the AXIS OS Vulnerability Scanner Guide for guidance and instructions on how to manage vulnerability scans, false-positives and remediation plans.

7. Common concerns

The following lists common concerns and ways to manage additional risks. Please refer to the AXIS OS Hardening Guide and Milestone XProtect Hardening Guide for more information.

7.1 Ethernet hijacking of outdoor cameras

A camera that is mounted outdoors exposes risks to the network since an adversary may connect a computer to the Ethernet cable that is connected to the camera. Cameras at risk need to be mounted in a hard-to-reach place, or use vandal-resistant housing. Cables should be protected in walls or with conduits.

Recommended policies and procedures

Option 1: Network segmentation

If an adversary is successful in replacing the camera with his own laptop, he may be able to attack other cameras on the network segment but will not reach other critical network resources.

Option 2: IEEE 802.1X network access control

Referred to as IEEE 802.1X, this standard is designed to prevent unauthorized network devices from accessing the local network. Before a device is allowed access to the network (and its resources), it needs to authenticate itself. There are different authentication methods that can be used, such as MAC address (MAC filtering), user/password, and client certificate (EAP/TLS). Axis cameras support IEEE 802.1X EAP/TLS.

Option 3: Network cable tamper detection

A cable tamper detector is a media converter solution consisting of two modules. The indoor module provides power and Ethernet to the outdoor module that provides the same to the camera. The outdoor module is typically mounted inside the camera housing. The indoor module can detect cable tampering and if the camera becomes disconnected. In the case of tampering or disconnection, it will automatically shut down power and network. The power and network needs to be manually enabled on the indoor module.

Option 4: Additional firewall for outdoor cameras

Adding an additional firewall for outdoor cameras and limiting network access and traffic can help prevent intrusion upon an Ethernet hijack. A recommended solution is to use a PoE switch with a built-in firewall.

7.2 Malware and ransomware

Any network device with a security breach can be infected with malware or ransomware and become potential entry points for hackers to access your network. Attackers usually do not care about the device itself. They care about its interconnectivity and its processing power.

Recommended policies and procedures

Windows servers
Do not run anything other than XProtect VMS server components or third-party integrations on the servers. If the physical server hardware should be utilized for other purposes, it is recommended to use multiple virtual server instances and run the XProtect VMS components in one virtual machine and the third-party non-VMS related software in another virtual machine.

It is recommended that you deploy anti-virus software on all servers and computers that connect to the XProtect VMS. If mobile devices connect to the XProtect VMS, ensure that the devices have the latest operating system and patches (though not directly anti-virus) installed. When you do virus scanning, do not scan recording server directories and subdirectories that contain recording databases. In addition, do not scan for viruses on archive storage directories. Scanning for viruses on these directories can impact system performance. For information about the file types, directories, and subdirectories to exclude from the virus scan, see the section “Virus scanning (explained)” in the XProtect VMS Administrator Guide.

Before integrating an Axis device into a system, users should perform a factory default on the device**.** This action ensures that the device is completely free of unwanted software or configuration since the only software remaining is AXIS OS and its default settings. Axis devices come with the Axis Edge Vault platform, which supports a number of security features such as signed OS, secure boot and an encrypted file system. Signed OS validates that the device operating system is from Axis and ensures that any new AXIS OS to be downloaded and installed on an Axis device is also signed. As a second line of defense, secure boot checks for the signature to ensure the device boots only genuine AXIS OS. If the OS is unauthorized or has been altered, the boot process is aborted and the device stops running. A device’s file system is also encrypted when not in use, for instance, when it is in transit from a system integrator to the end customer to prevent customer-specific configuration and information stored in the file system from being extracted or tampered with.

8. Useful links

Milestone

- Milestone XProtect Hardening Guide
- Milestone XProtect Certificate Guide
- Milestone XProtect GDPR Privacy Guide
- Milestone Cybersecurity
- Milestone Cybersecurity PSIRT
- Milestone Report Vulnerability
- Milestone XProtect VMS system architecture
- Milestone Whitepaper: System architecture guide for IT professionals
- Milestone Whitepaper: XProtect Corporate advanced security management
- Milestone Whitepaper: Ensuring end-to-end protection of media integrity
- Milestone Whitepaper: External Identity Provider
- Milestone Whitepaper: XProtect storage architecture and recommendations

Axis

- Axis Cybersecurity
- Axis Cybersecurity Resources
- AXIS OS Hardening Guide
- AXIS OS Knowledge Base
- AXIS OS Release Notes
- Axis Vulnerability Management
- Axis Cybersecurity Reference Guide