

HOW TO

How to handle breaking changes when upgrading devices to AXIS OS 13

October 16, 2026

Rev. 1.3

© Axis Communications AB

Contents

Introduction	3
ACAPs	3
Unsigned applications removed	3
ACAP manifest compatibility declaration	3
Prepare 32-bit platforms for 2038	4
Axhttp will be removed	4
Restricted ACAP application device access	4
Failover	4
Fallback	4
ACAP package.conf removed	5
Compressing firmware meta data using ZSTD	5
HTTPS only	6
Password Complexity Enforcement	9
Legacy parameters are removed from management	10
Remove time params in param.cgi	11
UPnP and mDNS service removed from management	11
"Camera tampering" detector removed	12
AXIS Guard Suite (Motion, Fence & Loitering) removed	12
Video rotation parameters removed	12
Strict Security Mode (SSM) – Customer Information	13
Adding devices with SSM enabled	14
Manually Trusting a device in AXIS Camera Station Pro	15

Introduction

AXIS Camera Station Pro 6.16 / AXIS Camera Station 5.59 or lower versions can experience breaking changes when installing AXIS OS 13 on connected devices.

In this document you get information about what the changes are and what impact they have on the installation.

ACAPs

Unsigned applications removed

Starting from AXIS OS 13.0, the option to allow unsigned applications has been removed and only signed ACAP applications are allowed. This is to increase trust in ACAP applications and comply with international regulations and best practices for secure software delivery.

If an unsigned ACAP application is installed on the device, it must be removed or replaced with a signed version before upgrading to AXIS OS 13. This replacement must be done while the device is still running AXIS OS 12.

All ACAP applications that are installed in AXIS OS 13 must be signed, otherwise the ACAP installation will fail.

Please contact AXIS support for more information if you have any problems with your ACAPs.

ACAP manifest compatibility declaration

In AXIS OS 12.x, we're introducing an optional field in the application manifest that specifies the AXIS OS major versions the application supports. To adapt to this change, ACAP developers must include compatibility information in the ACAP manifest. This field will become mandatory in AXIS OS 13 and only ACAP with this explicit compatibility information will be supported on OS 13.

Note that package.conf doesn't support this feature. As a result, an ACAP application with only a package.conf file (and no manifest) won't meet the AXIS OS 13 requirements.

Impact: An ACAP application can only be installed or upgraded if it declares compatibility with the current AXIS OS version. Likewise, an upgrade will only proceed if all installed applications are compatible with the target AXIS OS version.

AXIS OS also checks application compatibility at boot. If any application lacks a valid compatibility declaration, the upgrade will be refused or rolled back. This safeguard ensures system stability, especially when upgrading from older AXIS OS versions that don't support compatibility checks.

Prepare 32-bit platforms for 2038

To allow 32-bit AXIS OS products to operate past 03:14:07 UTC on 19 January 2038, AXIS OS will switch to use 64-bit `time_t` and the 64-bit time APIs in `glibc` and the Linux kernel.

This will require any ACAPs to be recompiled for 32-bit platforms.

Axhttp will be removed

The `axhttp` C lib will be removed from firmware. Any ACAPs that utilize the `transferCGI`, used by `axhttp` C lib needs to be updated to use either `FastCGI` or reverse proxy solution instead.

Restricted ACAP application device access

Limitations will be put on applications regarding their access to the device.

- The application will only be able to run as a "dynamic" user specifically created for the application, or as the user "sdk". All other users will now be disallowed. (The "sdk" user will eventually be removed, and only dynamic users will be supported.)
- The application process can only make itself a member of a small subset of groups on the device. These are the groups needed to be able to use the officially supported APIs.
- The application can only get access to a small subset of D-Bus APIs, namely those that are needed to use the official APIs.

Only ACAP applications that are signed and use the application **manifest schema v.2** can be used.

If applications not using manifest schema v.2 are installed in an earlier version of AXIS OS, upgrading to AXIS OS 13 will be blocked.

Failover

Failover = The recording is stored on the SD card if the AXIS Camera Station server loses connection to the camera.

- This feature will work the same way even after upgrading to AXIS OS 13.

Fallback

Fallback = The recordings are stored to an S30 if the AXIS Camera Station server loses connection. The cameras are connected to the S30.

- From AXIS Camera Station Pro version 6.18 the "fallback" feature will be renamed to "failover".
- If you upgrade your **recorder** to AXIS OS 13, you need to upgrade your server to AXIS Station Pro version 6.18 for fallback/failover to work. It's the recorders firmware that counts.
- On servers with lower AXIS Camera Station Pro version than 6.18, fallback/failover will work as before if your **recorder** has AXIS OS 12 or lower versions installed. It will **not** be possible to upgrade to AXIS OS 13 at all. It's the recorders firmware that counts.

Loopback interfaces removed

Loopback interfaces are used by various internal clients to access Vapix inside AxisOS. In AXIS OS 13 the ways of accessing VAPIX APIs are unified. When upgrading to AXIS OS 13 these hosts are still supported:

Vhost	Unique trait
127.0.0.12	Vapix service accounts, +h2c
127.0.0.1	only basic auth, +h2c
127.0.0.4	Client Credential Grant auth (if configured)

ACAP package.conf removed

Package.conf and Manifest.json are part of an ACAP application and its configuration and needed for ACAP application installation on Axis devices.

From AXIS OS 13.0, all ACAP applications must contain a **manifest.json** file that describes their configuration. The old way of using a package.conf file will not be supported.

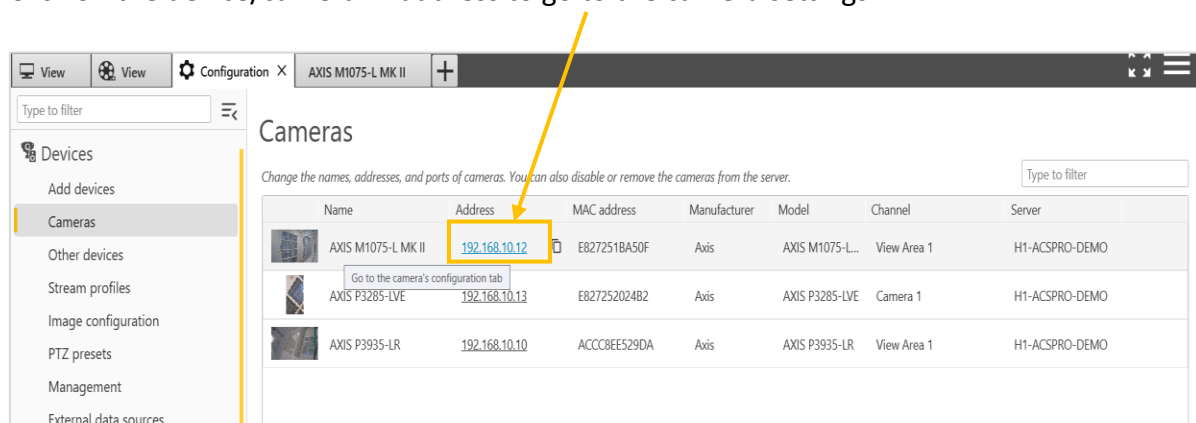
If an ACAP application without a manifest.json file has been installed on the device, it needs to be removed or replaced before upgrading to AXIS OS 13.

Compressing firmware meta data using ZSTD

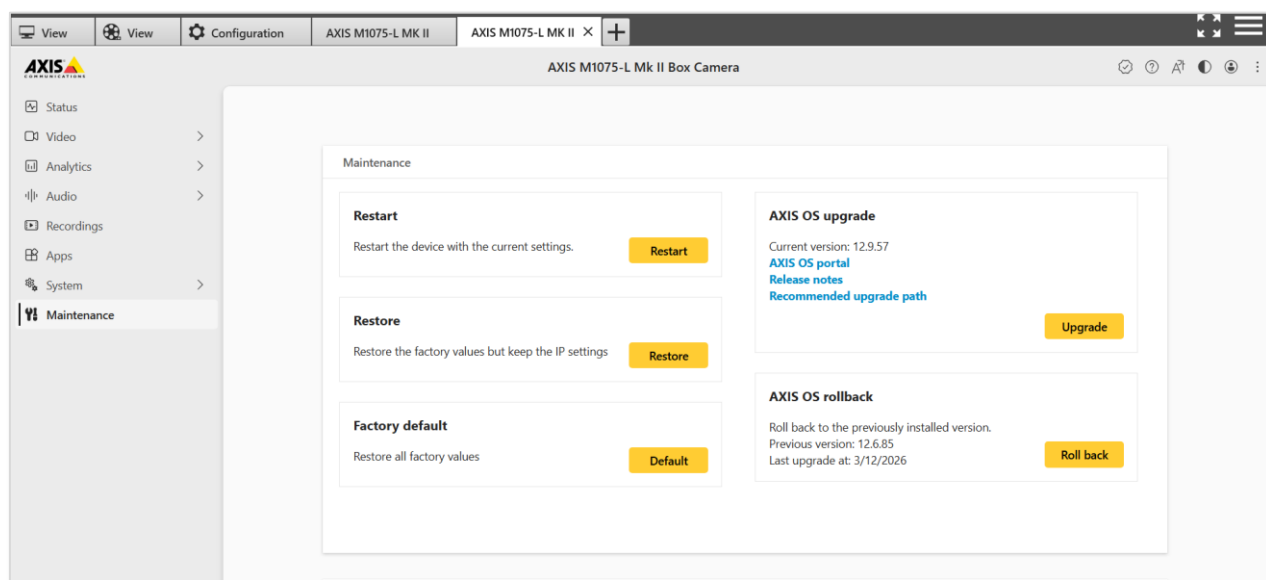
Devices with AXIS OS 13 use ZSTD instead of GZIP as firmware meta data compression. Metadata that is compressed with ZSTD will not be able to be analyzed in older AXIS Camera Station Pro/5 versions. This means that the feature for upgrading these devices within AXIS Camera Station Pro/5 will stop working.

To upgrade devices with AXIS OS 13 you need to do that camera by camera within the device's configuration page.

1. Click on the device/camera IP-address to go to the camera settings.



2. Choose “Maintenance” to where to upgrade AXIS OS in the camera settings.



HTTPS only

For better cyber security devices with AXIS OS 13 only communicate through HTTPS by default.

AXIS Camera Station Pro trusts HTTPS certificates that are signed by either:

1. A Certificate Authority that's in the Windows certificate store.
2. The AXIS Camera Station Pro Certificate Authority.
3. The Axis Device ID Certificate Authority.

In AXIS OS 13, network connections to the device from factory (or factory defaulted) will only be allowed using secure HTTPS/443 connections. In AXIS OS 12 and earlier, the device would allow both HTTPS/443 secure as well as HTTP/80 insecure connections.

NOTE: Even with a secure HTTPS connection, your browser might still show a warning due to issues validating the certificate. This is expected behavior, as IoT device certificates aren't compatible with most browsers.

As HTTP is disabled, it still is possible to enable HTTP if there is a need to do so. Follow these steps:

1. Disable the validation of the certificate. "Configuration => Security => Certificates". And toggle off the "Validate device certificate" toggle.

Devices

HTTPS

Validate device certificate  

Validate device address  

IEEE 802.1X 

EAPOL version:

EAP identity:

Custom:

IEEE 802.1X authentication CA certificate:

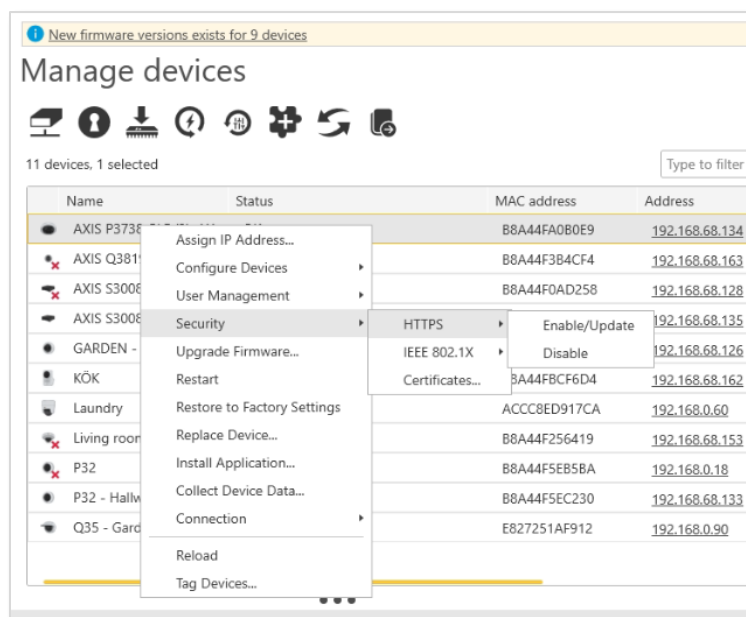


Client certificates will be signed by AXIS Camera Station Pro Certificate Authority and have the following property.

Common name:

2. Go to "Configuration tab => Add device page" and refresh the page.
3. Add your device.
4. Go to "Configuration tab => Devices => Management".
5. Right click on your selected device.

6. Enable or disable HTTPS.



7. Enable "Validate device certificate" again. (See first step.)

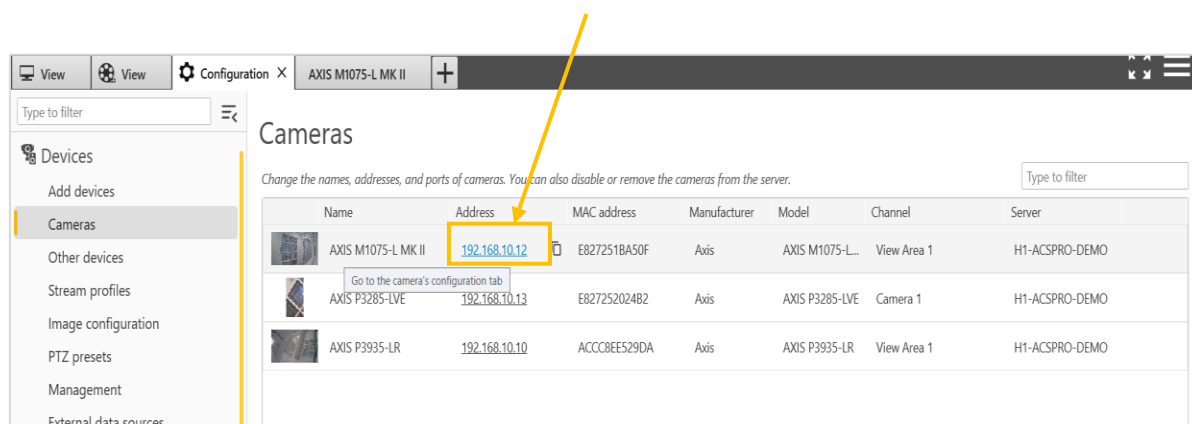
Password Complexity Enforcement

When creating a password for a device in AXIS Camera Station Pro (Configuration tab => Devices => Add device), the password complexity in AXIS Camera Station Pro and the device/camera are no longer the same.

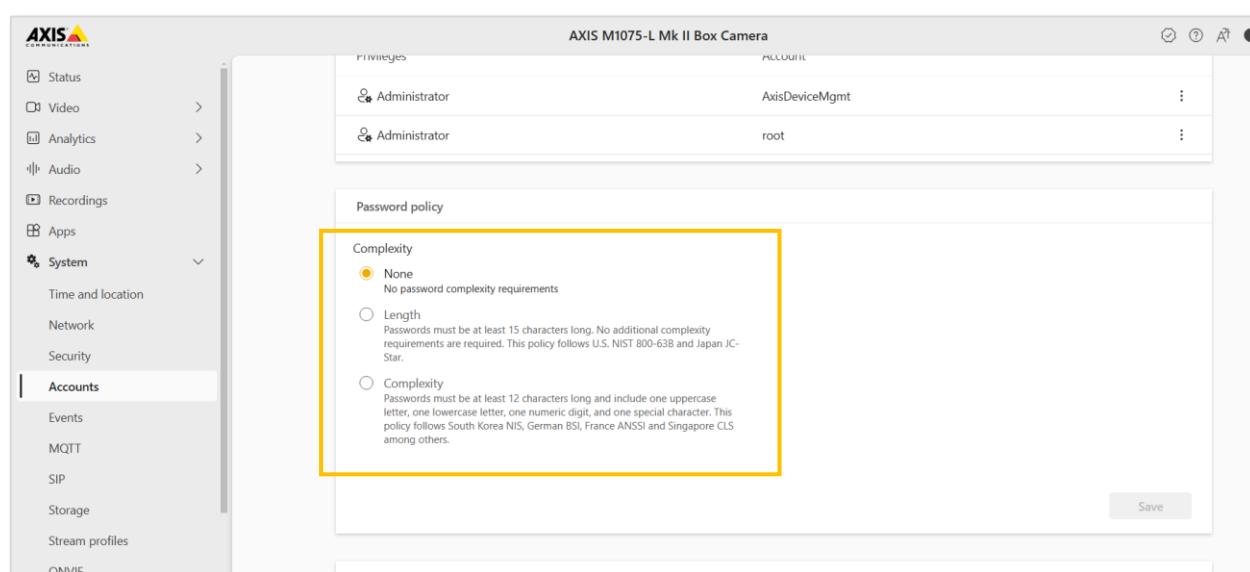
If you create a password in AXIS Camera Station Pro that the camera's password complexity cannot handle, you will only get a general error message that it is the wrong password. This can make it difficult to understand what the problem really is.

To mitigate this problem and facilitate this process, it is recommended to remove the password complexity requirement directly in the camera's settings or closely look at what complexity rules for the password that is set in the camera(s).

1. Click on the device/camera IP-address to go to the camera settings.



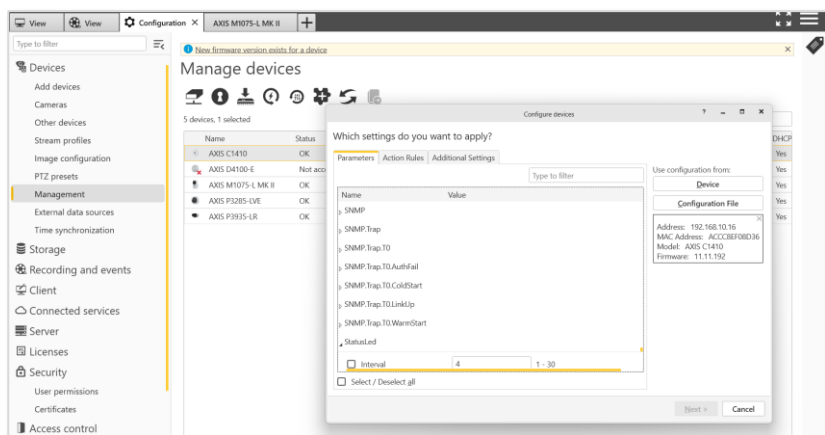
2. Choose "Accounts" in the menu and then "None" as password complexity for the device/camera. Or choose one of the length or complexity password rules. Click "Save".



Legacy parameters are removed from management

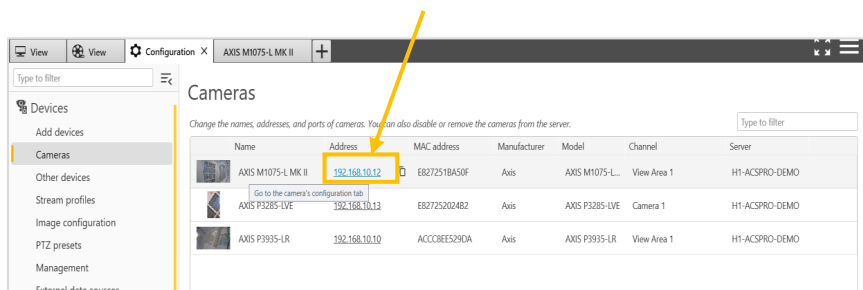
Some of the parameters that have been able to manage in AXIS Camera Station Pro (Configuration tab => Devices => Management) will be removed.

This applies to param.cgi parameters for SNMP, HTTP authentication and streaming related parameters.

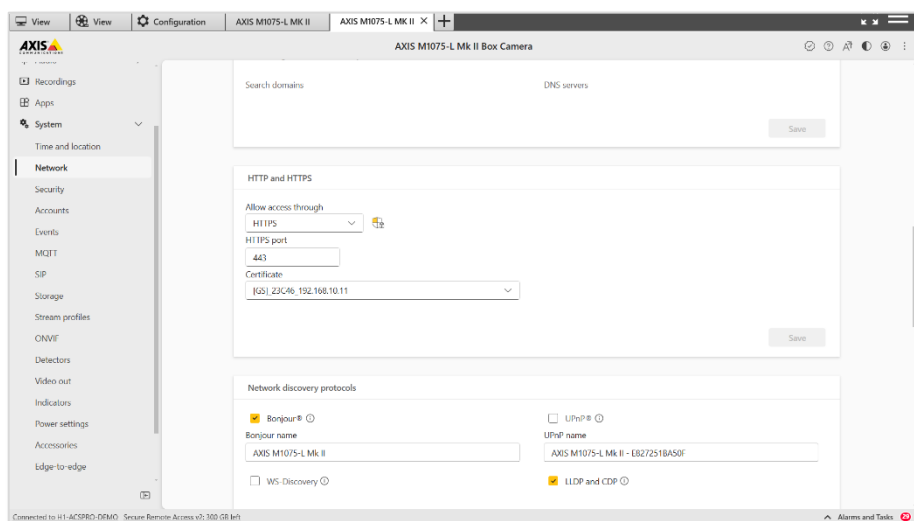


These parameters can still be found in the devices/cameras settings. Configure through the device/camera settings but the parameters can only be managed camera by camera.

1. Click on the device/camera IP-address to go to the camera settings.



2. Choose “System” => “Network” to find the different parameters in the camera settings.



Remove time params in param.cgi

The legacy parameters **root.Time.POSIXTimeZone** and **root.Time.DST.Enabled** will be removed. The change takes effect on upgrade to AXIS OS 13.

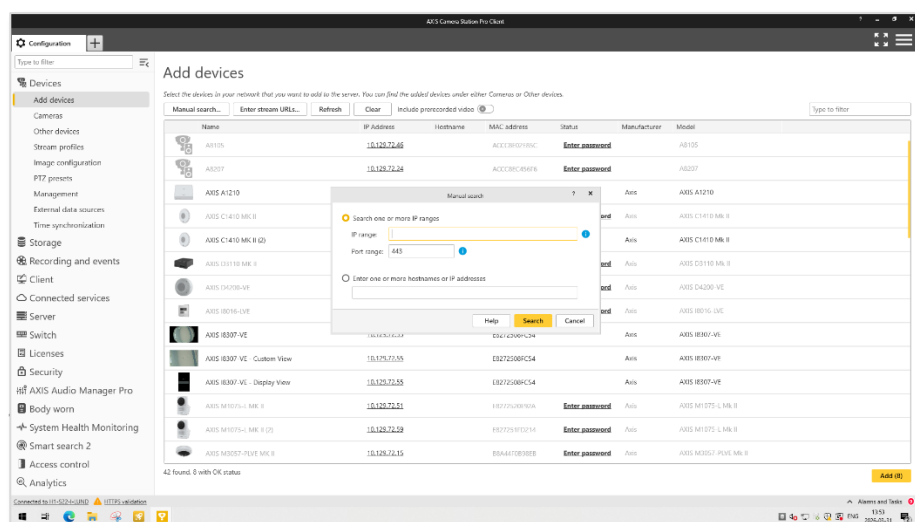
Use instead the [Time API v2](#). For more information about the VAPIX and param.cgi: [Deprecating time parameters](#).

UPnP and mDNS service removed from management

UPnP is now removed from AXIS Camera Station Pro management. However, it is still possible to find cameras/devices via Bonjour, but less information is displayed than before.

To mitigate this, it is recommended to upgrade to AXIS Camera Station Pro 6.3 or AXIS Camera Station 5.57 or later versions.

You can also manually search for your device. But then you need to have the IP addresses that you want to search for. (Configuration tab => Devices => Add devices)



"Camera tampering" detector removed

Events that trigger when a camera is tampered with will stop working. These events/action rules are set up with triggers that listen to removed events.

Use instead AXIS Image Health Analytics: [AXIS Image Health Analytics | Axis Communications](#)

AXIS Guard Suite (Motion, Fence & Loitering) removed

The AXIS Guard Suite ACAPs are removed and triggers that are set up with this will stop working.

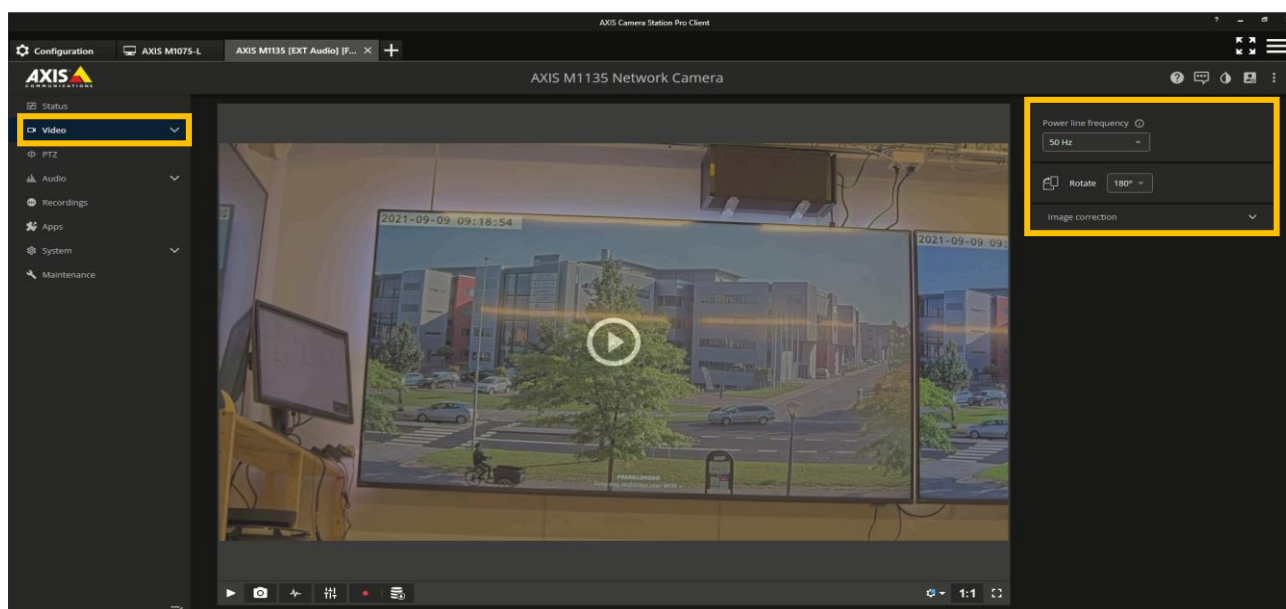
Use instead

- For direct tampering (covering, moving the camera):
 - In modern cameras use the built-in AXIS Video Motion Detection tampering alarm.
- For advanced scenarios (detecting fence violation, trespassing, loitering):
 - Use the pre-installed AXIS Object Analytics.
 - [AXIS Object Analytics | Axis Communications](#)
- Use specialized third-party analytics ACAPs.

Video rotation parameters removed

It will not be possible to configure rotation of a video image through AXIS Camera Station Pro after upgrading to AXIS OS 13.

Use instead the ADA interface of the device to configure image rotation.

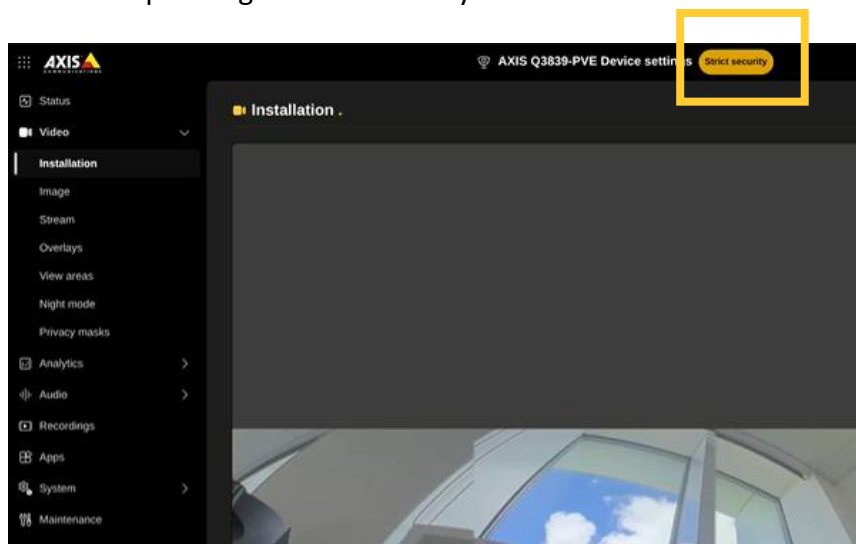


Example on ADA interface for an AXIS M1135 camera.

Strict Security Mode (SSM) – Customer Information

Strict Security Mode (SSM) is a security feature used to enforce a more restrictive security configuration on supported AXIS devices. It is intended for environments with higher security requirements.

In the device web-interface, an information icon next to the product name will indicate whether the device is operating in Strict Security Mode.



Overview when enabled SSM mode:

- HTTPS ONLY
- OpenSSL/Apache version headers disabled
- Firmware downgrades are forbidden
- RTSP/RTP permanently disabled
- Disables “share data with developers” – Google Analytics in ADA
- TLS 1.2 is limited to ECDSA Ciphers Only, so TLS 1.3 is required
- System-wide Brute force protection for ONVIF/HTTPS/SNMP/RTSP/SSH

Important:

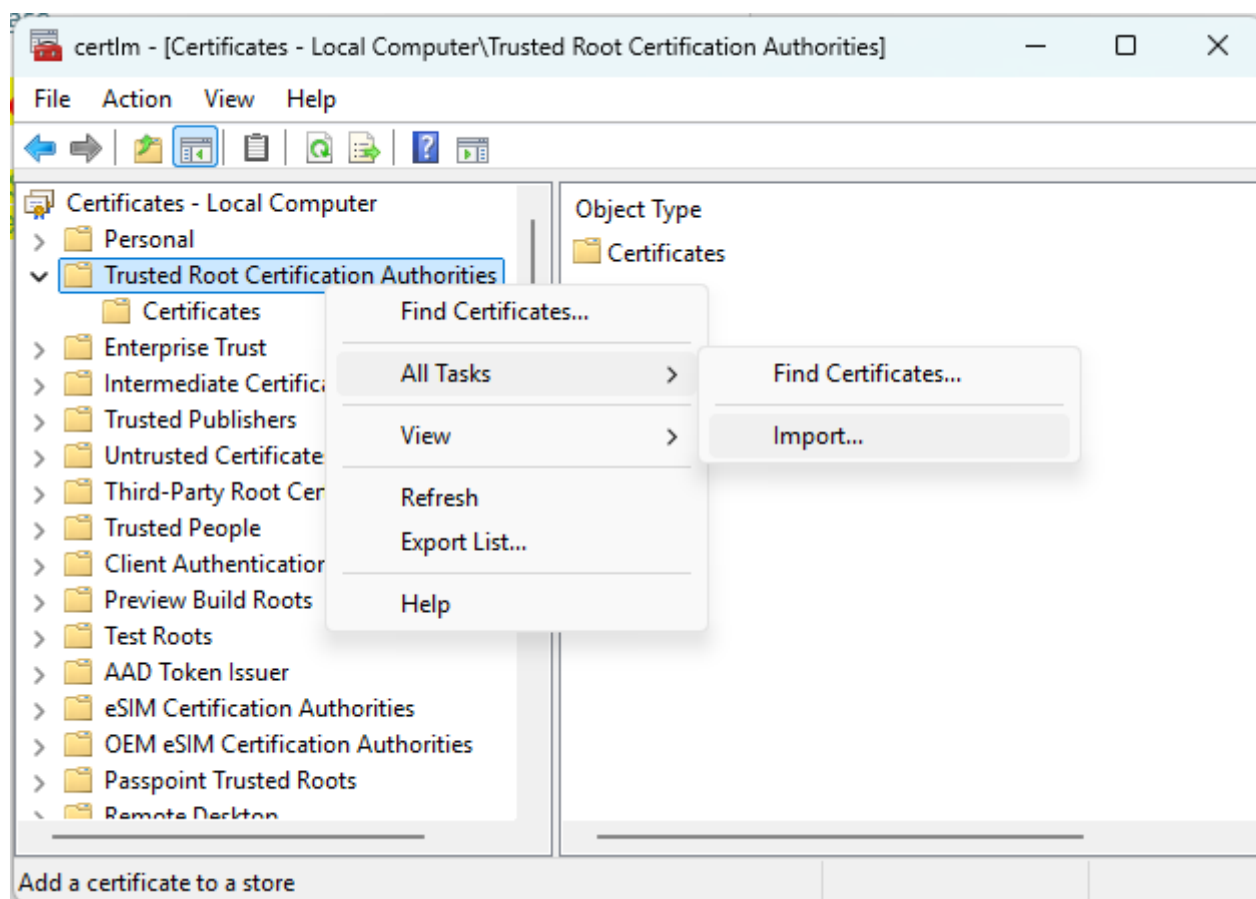
- Once SSM is enable it cannot be disabled unless you ask the Axis support for help.
- SSM can only be enabled before a root-user has been set on the device.
- Devices with SSM enabled will NOT work on ACS Pro running on Windows 10, make sure you are using an operating system supporting TLS 1.3 e.g. Windows 11.

Link to more detailed information: [AXIS OS - Knowledge base](#)

Adding devices with SSM enabled

Devices that have SSM enabled can be added to AXIS Camera Station Pro on a Windows 11 machine by manually trusting the device certificate in AXIS Camera Station Pro or adding the Certificate Authority to the Windows certificate store as a Trusted root certificate.

Adding a Certificate Authority to the Windows local machine certificate store, once added AXIS Camera Station Pro will trust the devices automatically.



Manually Trusting a device in AXIS Camera Station Pro.

