AXIS OS Forensics Guide

Introduction

The purpose of this guide is to help you conduct a forensic analysis and cleanup of an Axis network device in the event of a cyberattack on its associated network.

Specifically, we cover how to detect whether the device has been compromised, how to collect evidence, and how to restore the device to a clean and secure state.

This guide applies to all AXIS OS-based products running AXIS OS LTS or active track software.

The forensic process

In simplified terms, the forensic process consists of three steps:

1. Detection
2. Evidence collection
3. Cleanup

Detection

The first step is to detect any signs that an Axis network device has been affected by a cyberattack. Such signs are commonly referred to as indicators of compromise (IoC). Consult the table below for the most common IoCs related to Axis devices.

For information about how to detect IoCs, see .

Note

We recommend that you subscribe to *Axis security notification service* to receive information about newly discovered vulnerabilities in Axis products, solutions, and services.

Indicator of compromise (IoC)	Example
Changes in network access	An Axis device typically accessed only through the web interface is suddenly accessed via SSH from an unknown IP address.
Unknown network traffic to or from the device	The device starts sending large amounts of data to an external server not previously authorized for video storage.
Unknown file transfers to or from the device	Video recordings are being streamed to an external IP address without the knowledge of the system administrator.
Changes in device configuration	Sudden changes in the device configuration.
Changes in device accounts	New administrator accounts are created on the device with unknown usernames and passwords.
Loss of video and audio	The device stops sending video and audio streams to the video management system (VMS) it's connected to.
Unknown software or applications installed	The device shows signs of running unauthorized software not provided by Axis.

Evidence collection

If you have detected one or several IoCs on an Axis device, the next step is to collect evidence about the device's current status. Avoid making any modifications to the device, such as turning it off or installing additional tools. Tampering with the device could destroy evidence.

For information on how to collect evidence about the device's status, see .

Cleanup

The final step in the forensic process is to restore the device to a secure state. For Axis devices, the most efficient way to do this is to perform a factory default.

- For **devices without signed OS and secure boot**, you should download the latest supported AXIS OS version from axis.com and install it on the device after you perform a factory default. Make sure to monitor the device for some time afterwards before you reintroduce it into the operational system.
- For **devices with signed OS and secure boot**, a factory default returns them to a guaranteed non-compromised state.

Consult your device's user manual for instructions about how to perform a factory default.

You can find more information about signed OS and secure boot at *axis.com/solutions/edge-vault*.

Investigative tools

Web interface

Use the web interface of your Axis device to review the device configuration whenever possible. Consult your device's user manual for instructions about how to open the device's web interface.

Server report

Visit the web interface to view the device server report. Server reports contain current and historical data about health monitoring, system information, configuration details, and log files.

You can also download a .zip file of the server report. This file contains all the data related to your device configuration and should be used as your primary resource for forensic investigation.

AXIS OS version	Web interface navigation path
< 7.10	Setup > System Options > Support > Logs & Reports > Download Server Report
≥ 7.10	Settings > System > Maintenance > Download Server Report
≥ 10.9	System > Logs > Download the device server report

AXIS Server Report Viewer

AXIS Server Report Viewer is a web-based, graphical user interface designed to facilitate the upload and visualization of server report data. Developed by Axis, this tool is the most efficient way to analyze server report data. To use AXIS Server Report Viewer, visit *axisserverreportviewer.axis.com/about* and log in with your MyAxis account.

Checklists

If you suspect your Axis device may have been compromised, use the investigative tools to go through each of the checklists in this section. If you detect any indicators of compromise, proceed to collect evidence and clean the device.

Verify software integrity and certificates

Verify software integrity in legacy Axis devices

- Analyze network traffic and login attempts to identify unauthorized network activity.
- Consider a factory reset as a last resort to clean the configuration, but be aware it might not remove all traces of malware.

You don't need to verify software integrity for devices with signed OS and secure boot, as these features prevent compromised software installation. For more information about signed OS and secure boot, see *axis.com/solutions/edge-vault*.

Verify certificates

1. Confirm the validity and integrity of certificates used for services like HTTPS, MQTT, IEEE802.1x, and remote syslog.
2. Verify that the correct client-server and CA certificates are uploaded on the Axis device. Note that several authorized and well-known CA certificates are pre-loaded on the Axis device.
3. Specifically inspect user-uploaded client-server and CA certificates and verify the accuracy of certificate details such as:
   - common name
   - country
   - key encryption
   - time validation

Verify user access configuration

Verify integrity of user accounts

1. Use the web interface to check whether it's still possible to log in with the configured user accounts and associated passwords.
2. Verify that each user account still belongs to the correct access group.
3. Verify that no new accounts have been added.
4. Verify that **Allow anonymous viewers** is turned off.

Note

Axis devices have separate user configuration interfaces for VAPIX and ONVIF users.

Check for user account changes

- **If you use remote syslog**: Check the central monitoring system for user management configuration changes. For recommendations on how to configure remote syslog, see *AXIS OS Hardening Guide*.
- **If you don't use remote syslog**: Download a server report and review logs using . Note that Axis devices may apply log rotation where old log files are deleted after some time.

In AXIS OS 10.9 and later, user configuration changes are saved in the system log, which means they can be sent to a remote syslog server. In AXIS OS, VAPIX, and ONVIF, user accounts are separated into their own management interfaces and access rights. Consult the table below for what log messages to expect in the event of user management configuration changes.

API interface	Use case	Log message
VAPIX	Add user	`VAPIX user andre from IP-address 10.197.240.104 created VAPIX user benjamin with role Administrator`
VAPIX	Change access group	`VAPIX user susanna from IP-address 10.197.240.104 changed VAPIX user linda role from Administrator to Operator`
VAPIX	Change password	`VAPIX user root from IP-address 10.197.240.104 changed VAPIX user thomas password`
VAPIX	Delete user	`VAPIX user root from IP-address 10.197.240.104 deleted VAPIX user sebastian with role Operator`
ONVIF	Add user	`VAPIX user root from IP-address 10.197.240.104 created ONVIF user andre with role Administrator`
ONVIF	Change access group	`ONVIF user andre from IP-address 10.197.240.104 changed ONVIF user susanna role from Administrator to Operator`
ONVIF	Change password	`ONVIF user thomas from IP-address 10.197.240.104 changed ONVIF user andre password`
ONVIF	Delete user	`ONVIF user pernilla from IP-address 10.197.240.104 deleted ONVIF user sebastian with role Operator`

Identify failed login attempts

Note

Failed login attempts from network hosts are generally logged in the device's system log. We recommend that you enable enhanced logging via the access log, as described in *AXIS OS Hardening Guide*.

- Check which access protocols, such as HTTP(S) and RTSP, are enabled on the device.
- Check whether there are any unauthorized user accounts in the Axis device's web interface. If you find any, remove them and update authorized users' passwords.
- Trace any dubious IP addresses or user accounts across the network to determine their origin.

- Review both successful and unsuccessful login attempt logs in the **Combined Logs** section of AXIS Server Report Viewer or a central monitoring system. For examples of successful and unsuccessful login attempts, see the sample log messages below.

SSH	
Successful	`[ INFO ] sshd[17583]: Accepted password for root from 10.197.252.38 port 41988 ssh2`
Unsuccessful	`[ INFO ] sshd[17727]: Failed password for root from 10.197.252.38 port 41994 ssh2`

After 5 failed attempts	`[ ERR ] sshd[17727]: error: maximum authentication attempts exceeded for root from 10.197.252.38 port 41994 ssh2 [preauth]`
	`[ INFO ] sshd[17727]: Disconnecting authenticating user root 10.197.252.38 port 41994: Too many authentication failures [preauth]`

FTP	

Successful	`[ INFO ] vftpd[18263]: Accepted request from 172.27.0.3 50333`
	`[ INFO ] vftpd[18263]: User root logged in.`

Unsuccessful	`[ INFO ] vftpd[18163]: Accepted request from 172.27.0.3 64936`
	`[ INFO ] vftpd[18163]: Incorrect username/password. User access from 172.27.0.3 denied.`
	`[ INFO ] vftpd[18163]: Client 172.27.0.3 disconnected.`

RTSP protocol	
Successful	`[ NOTICE ] monolith: RTSP UNKNOWN session h4fIznyTZNy16tLt created from 172.25.155.83`
Unsuccessful	`[ WARNING ] monolith: Rtsp login failed from 172.25.155.83`

HTTP(S) protocol	
Successful[1]	`[ NOTICE ] httpd[22254]: root from 10.197.240.111 /axis-cgi/admin/accesslog.cgi GET 200`
Unsuccessful[2]	`[ NOTICE ] httpd[21459]: root from 10.197.240.111 failed to access /axis-cgi/usergroup.cgi.Password mismatch`

[1] *Requires that Access log has been enabled through **Plain Config** > **System**.*

[2] *Only login attempts with the correct username are logged. These log messages only appear in devices with AXIS 10.4 and later versions.*

PreventDosAttack[3]		
Unsuccessful	AXIS OS 11.5 and lower	`[ WARNING ] httpd[22254]: [evasive20:warn] [pid 22254:tid 1428104112] [client 172.25.201.116:42058] Blacklisting address 172.25.201.116: possible DoS attack.`
Unsuccessful	AXIS OS 11.6 and higher	`[ WARNING ] httpd[22254]: [evasive20:warn] [pid 22254:tid 1428104112] [client 172.25.201.116:42058] Blocklisting address 172.25.201.116: possible DoS attack.`

Network access

Verify open network ports and protocols

- Use AXIS Server Report Viewer to check whether any changes have been made to network protocols and ports.

Note

Familiarize yourself with common network protocols and ports used by the Axis device. Some protocols are pre-configured, while others depend on the device setup. For more information, see *AXIS OS Knowledge base*.

- Use AXIS Server Report Viewer to check whether the device is being accessed or has been accessed by any unknown or unauthorized IP addresses:
  - **Connection list**: Provides a simple overview of current active network connections from the Axis device to other network hosts.
  - **Network connections**: Provides more detailed information about current and previous network connections.

You can also obtain vital port configurations from the web interface of the Axis device, such as HTTP (80) and HTTPS (443), as well as UPnP (49152) and Bonjour (5353).

Verify authorized network access

1. Examine the **Network connections** list in AXIS Server Report Viewer to identify any unfamiliar or unauthorized IP addresses connected to your Axis device.
2. Document and investigate unknown IP addresses to determine their presence and purpose within your network.

Note

- We recommend that you enable IP address filter on your device to restrict access to authorized network hosts only. For more information, see *AXIS OS Hardening Guide*. You can also use your network infrastructure to limit access to only authorized network hosts.

Verify network access control configuration

Review the current network access control settings on your device or your network infrastructure and verify that no changes have occurred.

[3] *Can be enabled through the device web interface. This will only log unsuccessful login attempts and IP addresses that have been blocked due to such attempts.*

Identify failed network access attempts

Use Axis Server Report Viewer to review logs of unsuccessful network access attempts in **Combined Logs** and **Kernel Logs**. In the tables below, you can see examples of how failed network attempts are logged.

IP filtering[4]	

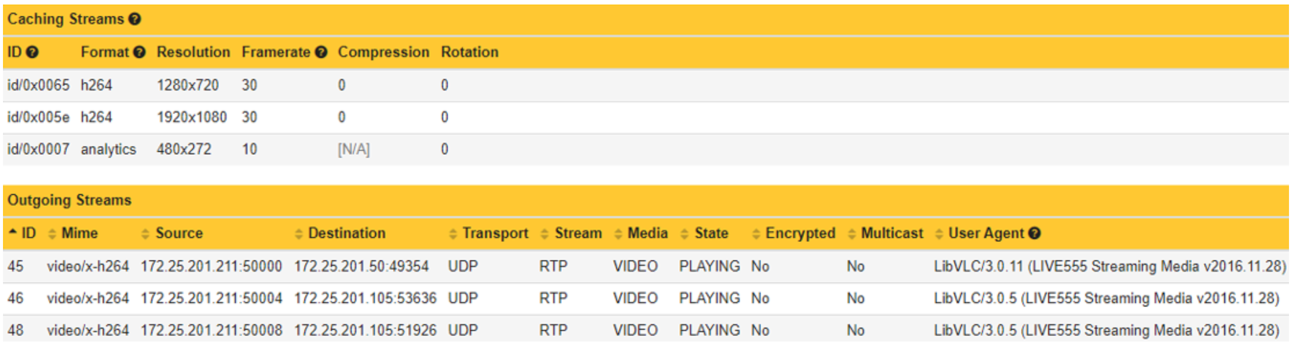
Unsuccessful	`IP_FILTER: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:30:9c:23:e2:48:b5:08:00 SRC=172.25.201.50 DST=172.25.201.255 LEN=78 TOS=0x00 PREC=0x00 TTL=128 ID=60428 PROTO=UDP SPT=137 DPT=137 LEN=58`
	`IP_FILTER: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:30:9c:23:e2:48:b5:08:00 SRC=172.25.201.50 DST=172.25.201.255 LEN=78 TOS=0x00 PREC=0x00 TTL=128 ID=60429 PROTO=UDP SPT=137 DPT=137 LEN=58`

PreventDosAttack[5]		
Unsuccessful	AXIS OS 11.5 and lower	`[ WARNING ] httpd[22254]: [evasive20:warn] [pid 22254:tid 1428104112] [client 172.25.201.116:42058] Blacklisting address 172.25.201.116: possible DoS attack.`
Unsuccessful	AXIS OS 11.6 and higher	`[ WARNING ] httpd[22254]: [evasive20:warn] [pid 22254:tid 1428104112] [client 172.25.201.116:42058] Blocklisting address 172.25.201.116: possible DoS attack.`

Streaming access

Verify clients accessing video and audio streams

The Axis device server report contains a list of video and audio streams delivered to network hosts. **Caching Streams** are the unique encoded video streams of an Axis device. **Outgoing Streams** shows which clients these video streams are delivered to. You can find out more in *AXIS OS Knowledge base*.



Caching Streams

ID	Format	Resolution	Framerate	Compression	Rotation
id/0x0065	h264	1280x720	30	0	0
id/0x005e	h264	1920x1080	30	0	0
id/0x0007	analytics	480x272	10	[N/A]	0

Outgoing Streams

ID	Mime	Source	Destination	Transport	Stream	Media	State	Encrypted	Multicast	User Agent
45	video/x-h264	172.25.201.211:50000	172.25.201.50:49354	UDP	RTP	VIDEO	PLAYING	No	No	LibVLC/3.0.11 (LIVE555 Streaming Media v2016.11.28)
46	video/x-h264	172.25.201.211:50004	172.25.201.105:53636	UDP	RTP	VIDEO	PLAYING	No	No	LibVLC/3.0.5 (LIVE555 Streaming Media v2016.11.28)
48	video/x-h264	172.25.201.211:50008	172.25.201.105:51926	UDP	RTP	VIDEO	PLAYING	No	No	LibVLC/3.0.5 (LIVE555 Streaming Media v2016.11.28)

1. Cross-reference the list of IP addresses that are supposed to access the Axis device with the metrics from the **Outgoing Streams** section.

[4] *IP filtering in Axis devices is a network layer-2 Linux Kernel functionality that blocks network packages depending on the configured rules. No authentication will be performed if an unsuited source IP address is trying to access the Axis device, since the network transmission is blocked right at the layer-2 network while authentication is performed on higher level application layers. Corresponding logs of the IP filtering can be created when the VAPIX parameter is enabled in* ***Plain Config > Network > IP Filtering****.*

[5] *PreventDosAttack can be enabled from* ***Plain Config > System*** *and will only log unsuccessful login attempts and correspondingly log when a source IP address is blocked.*

2. Identify and investigate unknown IP addresses that are accessing video and audio streams. Track them throughout the network to understand their purpose and whether they should have access to this data.

Note

We recommend that you enable network access control on the Axis device according to the AXIS OS Hardening Guide. Alternatively, you can apply the same techniques on the network infrastructure level to allow access to authorized network hosts only.

Identify failed attempts to access video and audio streams

- Review login attempts using the Axis Server Report Viewer, focusing on the **Combined Logs** section, or through a central monitoring system if the Axis device is configured to stream its logs.
- Look for log messages indicating successful and unsuccessful login attempts related to HTTP(S) and RTSP protocols, which are used to deliver video and audio streams.
- Investigate suspicious IP addresses and/or users, tracking them throughout the network to understand the source of these requests.
- Check the Axis device's web interface for unknown user accounts and delete them. Consider changing the passwords of authorized user accounts as an added precaution.

For examples of log messages that indicate successful and unsuccessful login attempts, see the tables below.

RTSP protocol

Successful	`[ NOTICE ] monolith: RTSP UNKNOWN session h4fIznyTZNy16tLt created from 172.25.155.83`
Unsuccessful	`[ WARNING ] monolith: Rtsp login failed from 172.25.155.83`

HTTP(S) protocol

Successful[6]	`[ NOTICE ] httpd[22254]: root from 10.197.240.111 /axis-cgi/admin/accesslog.cgi GET 200`
Unsuccessful[7]	`[ NOTICE ] httpd[21459]: root from 10.197.240.111 failed to access /axis-cgi/usergroup.cgi.Password mismatch`

Applications

Verify installed applications

Both the web interface and the server report of the Axis device can be used to verify installed applications and their current running status. To learn more about secure use of applications on your device, see *AXIS OS Hardening Guide*.

*[6] Requires that **Access log** has been enabled through the device web interface*

[7] Only login attempts using the correct username are logged.