AXIS OS Forensics Guide

Introduction

AXIS OS Forensic Guide

for Axis edge devices

Axis Communications strives to apply cybersecurity best practices in the design, development, and testing of our devices to minimize the risk of flaws that could be exploited in an attack. However, securing a network, its devices, and the services it supports requires active participation by the entire vendor supply chain, as well as the end-user organization. A secure environment depends on its users, processes, and technology. The purpose of this guide is to support you in managing security incidents in your network, devices, and services.

From an IT/network perspective, the Axis device is a network endpoint like any other, such as laptop and desktop computers, or mobile devices. Unlike a laptop computer, however, a network device does not have users visiting potentially harmful websites or opening malicious e-mail attachments. Nevertheless, a network camera is a device with an interface that may expose risks to the system it is connected to.

The guide provides technical advice for anyone conducting forensic analysis of Axis devices in the event of a cybersecurity attack on the surrounding network and IT infrastructure where the Axis device is installed. It establishes a baseline of forensic checklists and inspection techniques that will help you understand if the Axis device was compromised during the cause of a cybersecurity attack.

The guide includes references to modifying device settings within the web interface of the Axis device as per the following format:

AXIS OS version	Web interface configuration path
< 7.10	Setup > System Options > Security > IEEE 802.1x
≥ 7.10	Settings > System > Security
≥ 10.9	System > Security

To provide feedback on AXIS OS Forensic guide, contact *Axis support helpdesk* or your local Axis sales representative.

Scope

The forensic checklists and inspection instructions outlined in this guide are written for, and can be applied to, all AXIS OS-based products that are running an AXIS OS LTS or active track software. Legacy products running 4.xx and 5.xx software are also in scope.

The operating system for Axis edge devices.

Security notifications

We recommend that you subscribe to *Axis security notification service* to receive information about newly discovered vulnerabilities in Axis products, solutions, and services as well as how to keep your Axis devices secure.

Indicators of compromise (IoC)

Indicator of compromise is a concept in the IT forensic industry and is used as an important measurement to understand if, and how likely, a network device could be compromised in the event of a cybersecurity attack. The list of IoCs that follows is most relevant in the context of how Axis devices are operated and used. While it is important to forensically investigate Axis devices, it is just as important to investigate a security incident from a system level point of view since the underlying network and IT infrastructure in the system may be compromised first (through e.g., botnet or ransomware), before the security incident reaches network edge devices such as Axis devices.

Changes in network access

Changes in network access patterns, such as accessing the Axis device via protocols that would usually be disabled during normal operation (e.g., FTP, SSH, or others), would indicate malicious attempts to compromise the Axis device.

Unknown network traffic from/to the device

Unusual or unauthorized network traffic patterns sent from/to the Axis device would indicate that the Axis device is compromised or of there being attempts to compromise it.

Unknown file transfer from/to the device

Unknown file transfers from/to the Axis device (e.g., video or audio streams) sent from/to unknown network hosts would indicate unauthorized utilization of data.

Changes in device configuration

Sudden changes in the Axis device configuration, such as disabling secure protocols and system features, or enabling insecure protocols or features that are by default not enabled during normal operation, may indicate a malicious attempt to render the Axis device inoperative towards e.g., video management systems and other infrastructure network connections.

Changes in device accounts

Sudden changes in the Axis device user account configuration, such as changing the password of existing accounts, removing accounts, or even creating new accounts, indicate a malicious attempt to render the Axis device inoperative, or an attempt to establish permanent access from unauthorized network hosts.

Loss of video and audio

Changes in streaming-related communication protocols or ports (RTSP, RTP, SIP, etc.) indicate an attempt to compromise the Axis device and disconnect it from the intentional system which usually receives the device's video and audio streaming data.

Unknown software/applications installed

The upload or usage of non-Axis authorized software binaries or add-on applications would indicate a malicious attempt to compromise the Axis device e.g., by installing additional malware or functionality that would benefit the adversary.

Quickstart guide

Follow the quickstart guide to learn about collecting evidence from the Axis device, which investigative tools to use to gather information, and how to perform a cleanup after collecting the evidence.

Evidence collection

In the beginning of the forensic investigation it is important to only verify the current status of the device. Do not in any way tamper with, change or modify the device, since this might lead to evidence being destroyed. Examples of such changes/modifications are to turn off the device, to install tools, etc.

After investigating if your Axis device is affected by an intrusion, evidence must be collected. Until the collection has taken place, no cleanup of the device, such as removing unknown users and/or applications, should be performed.

Cleanup

The fastest and most efficient way to clean up a compromised Axis device is to perform a factory default. A factory default performed on an Axis device with support for signed firmware and secure boot will forensically clean the device and revert it back to a guaranteed non-compromised state. More information about signed firmware and secure boot can be found *here*.

For Axis devices without support for signed firmware and secure boot, a factory default is also recommended. However, it cannot be guaranteed that the device is completely free from malware after the factory default. Due to this, it is recommended to forensically monitor the factory defaulted Axis device for a short period of time afterwards, and if no indications of compromise are found, integrate it back into the operational system.

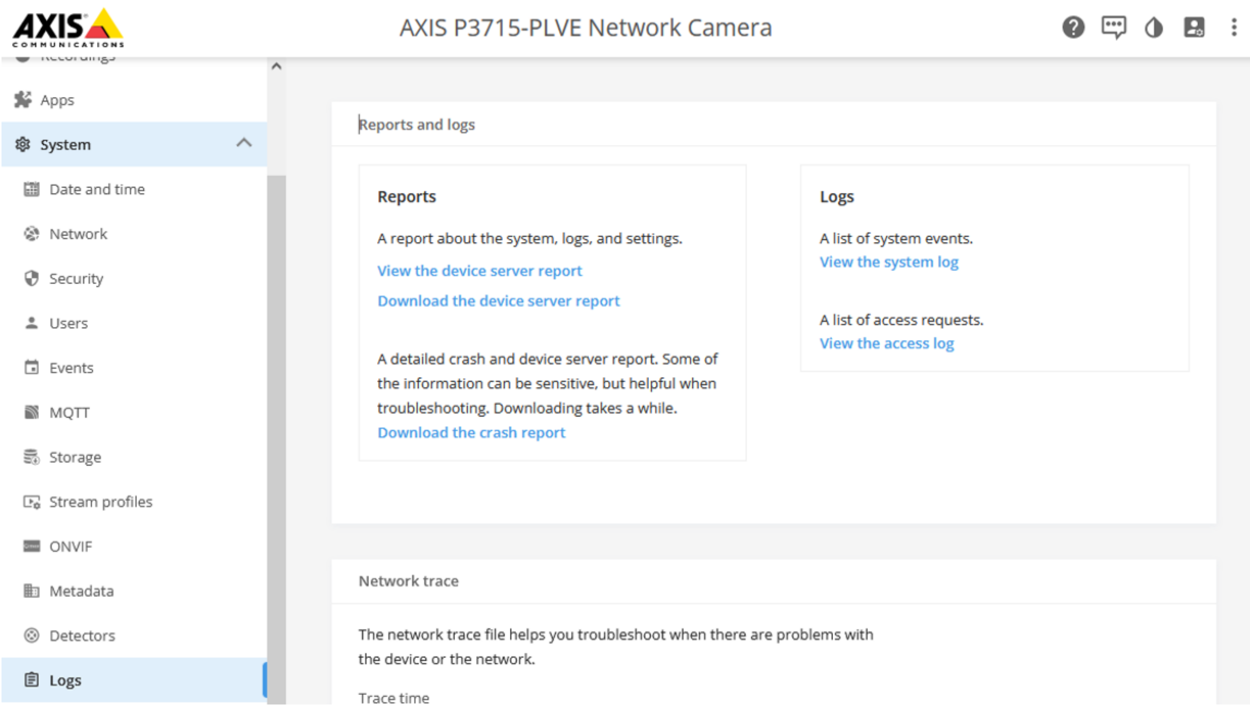
Investigative tools

Web interface

The web interface of the Axis device offers the possibility to quickly review the device configuration and should be used when possible.

Server report

You can download a so called server report from your Axis device. The report includes actual, and to some extent historical, information about health-monitoring, general system and configuration information, as well as valuable log files.



Reports and logs

Reports

A report about the system, logs, and settings.

View the device server report

Download the device server report

A detailed crash and device server report. Some of the information can be sensitive, but helpful when troubleshooting. Downloading takes a while.

Download the crash report

Logs

A list of system events.

View the system log

A list of access requests.

View the access log

Network trace

The network trace file helps you troubleshoot when there are problems with the device or the network.

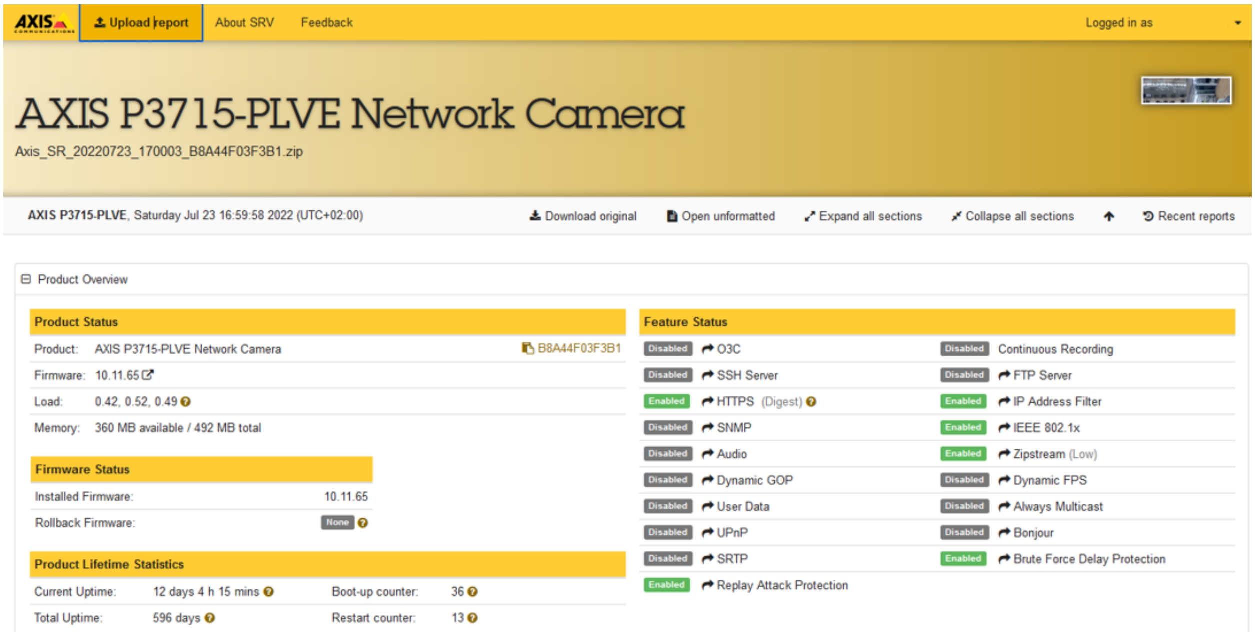
Trace time

The server report, including the configuration of the device web interface, can be downloaded as a .zip file. The file is used as the main resource upon forensic inspection of the Axis device.

AXIS OS version	Web interface download instructions
< 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 that makes it possible to upload and visualize the data of the server report. The tool is developed by Axis and greatly enhances the speed and efficiency of analyzing the data in the server report. You can access AXIS Server Report Viewer after logging in to *www.axis.com* with your MyAxis account.



AXIS P3715-PLVE Network Camera

Axis_SR_20220723_170003_B8A44F03F3B1.zip

AXIS P3715-PLVE, Saturday Jul 23 16:59:58 2022 (UTC+02:00)

Product Status

Product:	AXIS P3715-PLVE Network Camera	B8A44F03F3B1
Firmware:	10.11.65	
Load:	0.42, 0.52, 0.49	
Memory:	360 MB available / 492 MB total	

Firmware Status

Installed Firmware:	10.11.65
Rollback Firmware:	None

Product Lifetime Statistics

Current Uptime:	12 days 4 h 15 mins	Boot-up counter:	36
Total Uptime:	596 days	Restart counter:	13

Feature Status

Disabled	O3C	Disabled	Continuous Recording
Disabled	SSH Server	Disabled	FTP Server
Enabled	HTTPS (Digest)	Enabled	IP Address Filter
Disabled	SNMP	Enabled	IEEE 802.1x
Disabled	Audio	Enabled	Zipstream (Low)
Disabled	Dynamic GOP	Disabled	Dynamic FPS
Disabled	User Data	Disabled	Always Multicast
Disabled	UPnP	Disabled	Bonjour
Disabled	SRTP	Enabled	Brute Force Delay Protection
Enabled	Replay Attack Protection		

Checklists

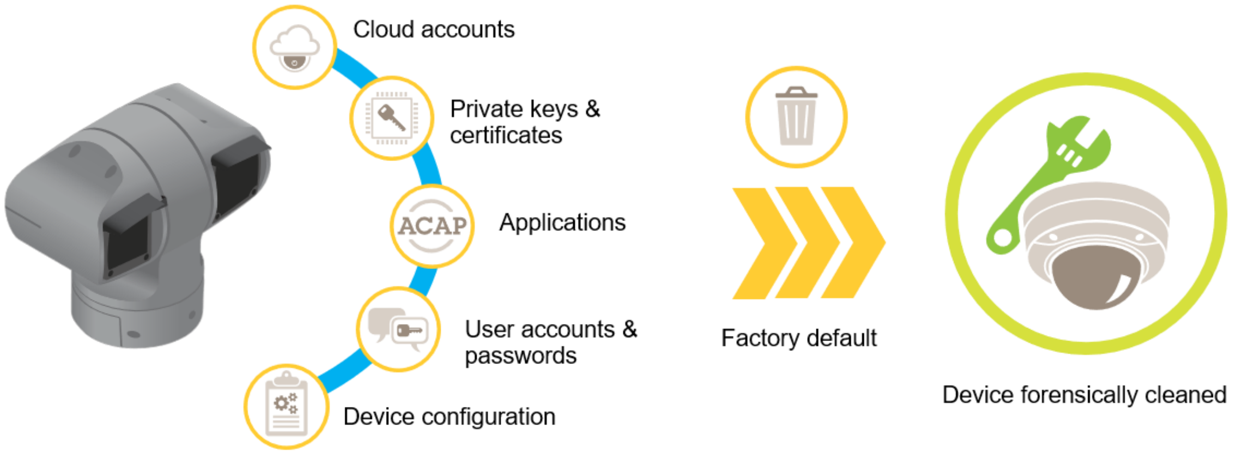
Security and integrity

Software integrity

When checking the software integrity, it is important to understand the differences between modern Axis devices supporting signed firmware and secure boot vs. legacy Axis devices lacking these security measures.

Axis devices with signed firmware and secure boot
The authenticity and integrity of Axis software and the capability of Axis devices to detect compromised software is ensured by the features signed firmware and secure boot. Signed firmware means that an integrity check of the software is performed during the software upgrade process. If the device detects that the software integrity is compromised, the upgrade will be rejected.

The secure boot feature on the other hand ensures that the Axis device will only accept Axis-authorized software to run on the device during the boot-up process. If the software integrity check fails during boot-up, the Axis device will not start up. Secure boot also guarantees that the factory defaulted state of the Axis device is forensically clean and in a non-compromised state.


Cloud accounts
Private keys & certificates
ACAP
Applications
User accounts & passwords
Device configuration
Factory default
Device forensically cleaned

Axis devices without signed firmware and secure boot
For Axis devices that do not support signed firmware and secure boot, it is recommended to closely observe the network and login access activity of the Axis device to understand if it is exposed to unauthorized network activity.

A factory default can be used as a last resort to clean the configuration, but it cannot be guaranteed that these Axis devices will be completely clean from possible malware even after a factory default.

Verify certificates

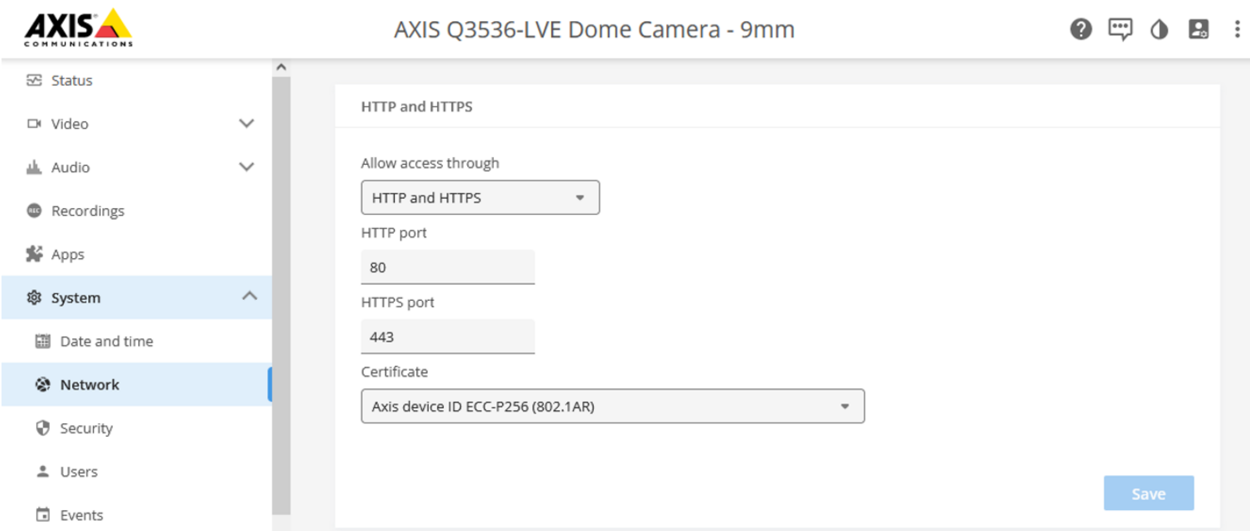
Cryptographic material, like certificates, is used in Axis devices to ensure secure and authorized communication from/to the device itself. It is important to check if the certificate configuration has been altered.

Checklist

1. Verify that the correct certificate is configured in the Axis device. Examples of sections that require certificate configuration are HTTP and HTTPS, remote syslog, MQTT, IEEE 802.1x, etc.

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 uploaded client-server and CA certificates that are user-uploaded and verify if certificate details such as *common name*, *country*, *key encryption*, and *time validation* is still accurate.



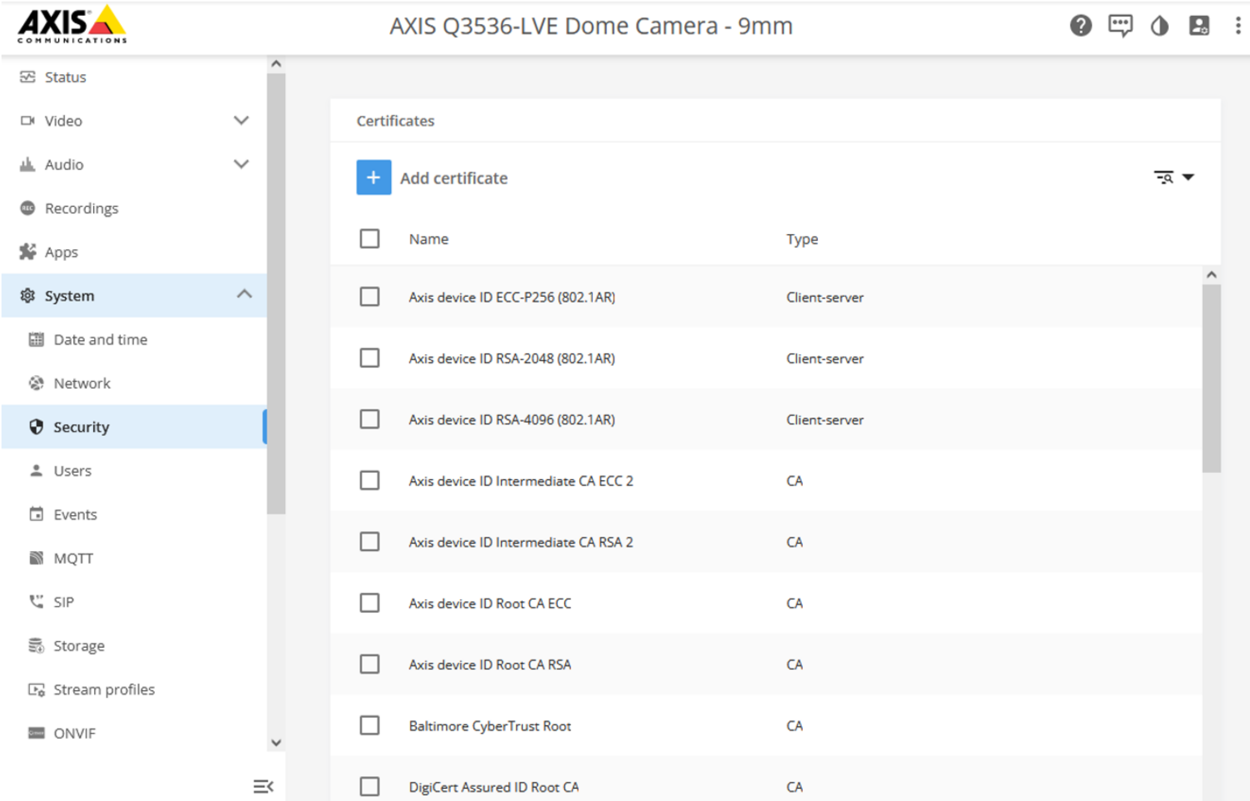
HTTP and HTTPS

Allow access through: HTTP and HTTPS

HTTP port: 80

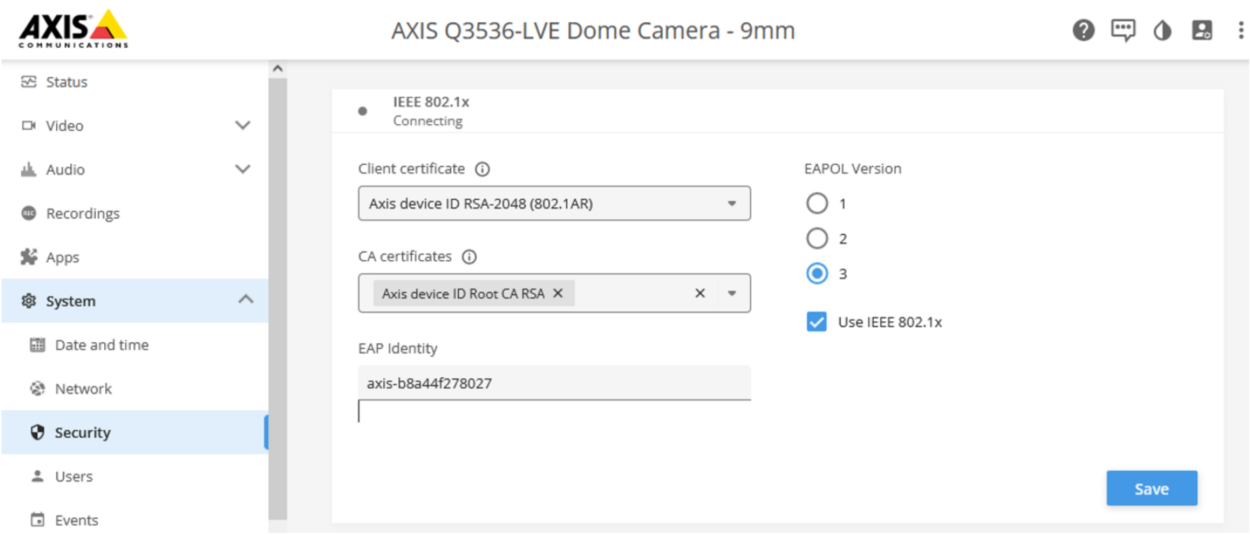
HTTPS port: 443

Certificate: Axis device ID ECC-P256 (802.1AR)



Certificates

	Name	Type
□	Axis device ID ECC-P256 (802.1AR)	Client-server
□	Axis device ID RSA-2048 (802.1AR)	Client-server
□	Axis device ID RSA-4096 (802.1AR)	Client-server
□	Axis device ID Intermediate CA ECC 2	CA
□	Axis device ID Intermediate CA RSA 2	CA
□	Axis device ID Root CA ECC	CA
□	Axis device ID Root CA RSA	CA
□	Baltimore CyberTrust Root	CA
□	DigiCert Assured ID Root CA	CA



AXIS Q3536-LVE Dome Camera - 9mm

● IEEE 802.1x
Connecting

Client certificate: Axis device ID RSA-2048 (802.1AR)

CA certificates: Axis device ID Root CA RSA

EAP Identity: axis-b8a44f278027

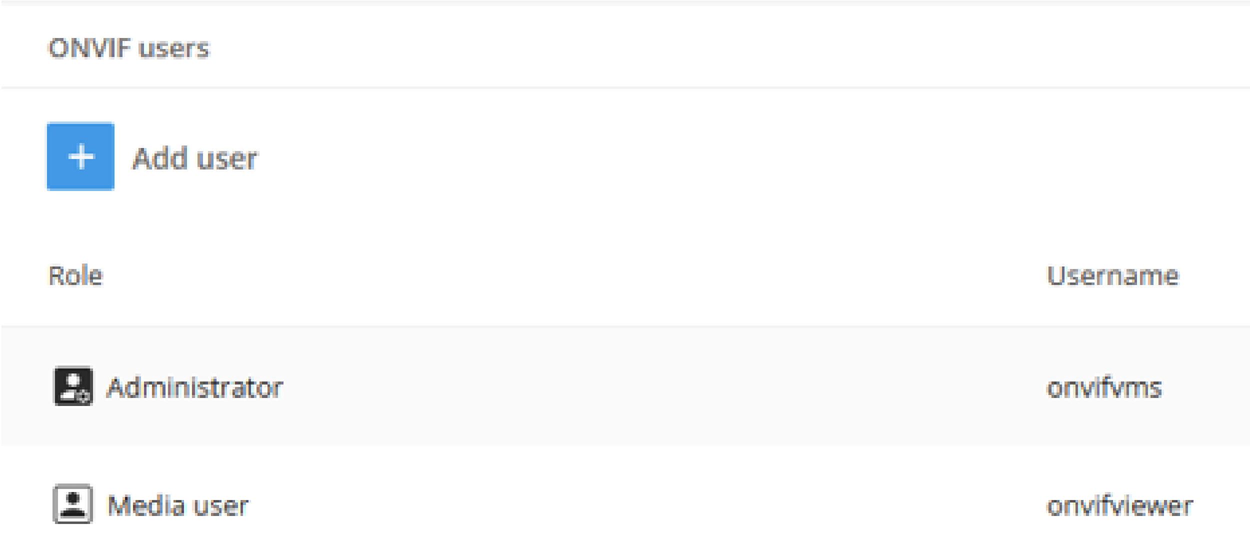
EAPOL Version: ○ 1 ○ 2 ● 3

☑ Use IEEE 802.1x

User access

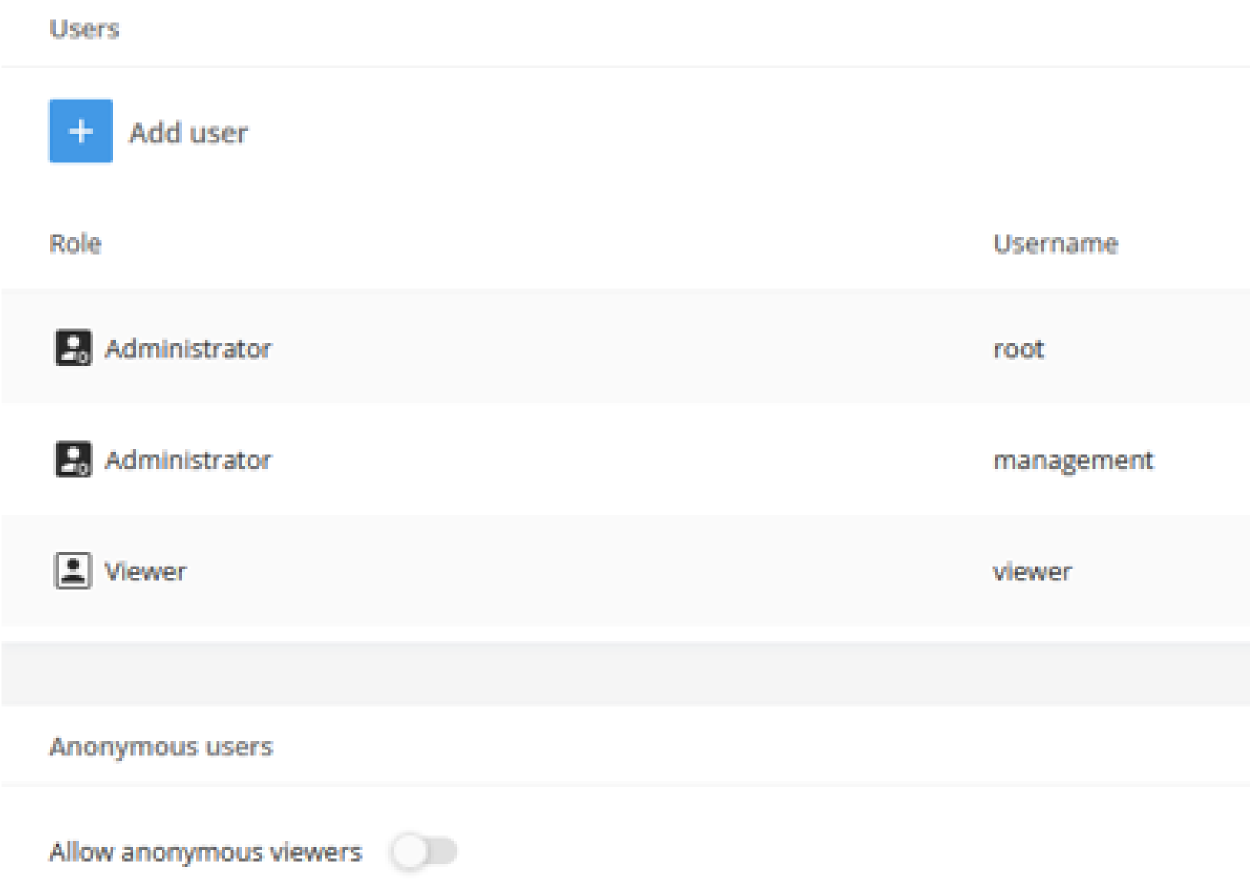
Verify integrity of user accounts

It is recommended to verify the integrity of existing user accounts by checking if they are in fact still existing, if they belong to the desired access group, as well as checking if the password is still matching. Axis devices have separate user configuration interfaces for VAPIX and ONVIF users.



ONVIF users

Role	Username
Administrator	onvifvms
Media user	onvifviewer



Users

+ Add user

Role	Username
Administrator	root
Administrator	management
Viewer	viewer

Anonymous users

Allow anonymous viewers ○

Checklist

1. Use the web interface of the Axis device to verify that it is possible to log in with the configured user accounts and password.
2. Verify that the user accounts are configured with the correct access group.
3. Verify that no new accounts have been added.
4. Verify that "Allow anonymous viewers" is disabled.

Verify account changes

From AXIS OS 10.9 and onwards, user configuration related changes are logged in the system log, which means they can be sent to a remote syslog server. In AXIS OS, VAPIX and ONVIF, users are separated by having their own management interfaces and access rights. The following table illustrates what log messages to expect when certain changes to the user management configuration have been made:

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`

Checklist

1. If AXIS OS Hardening Guide is applied and the *Extended hardening > Remote syslog* procedure is followed, the Axis device sends its log messages to a central monitoring system where you can search for and review the logs.

2. Alternatively, download a server report from the Axis device and review the logs using *AXIS Server Report Viewer*. Note that Axis devices may apply log rotation where old log files are deleted after some time.

Identify failed login attempts

Failed login attempts from network hosts are generally logged in the system log of the Axis device. It is recommended to enable further enhanced logging via the access log, as described in *AXIS OS Hardening Guide*. Login attempts can be reviewed using AXIS Server Report Viewer and the **Combined Logs** section. If the Axis device is configured to stream its logs to a central monitoring system, this can also be used to review the logs.

Checklist

1. Consider which access protocols are enabled on the Axis device. Common examples are HTTP(S) and RTSP.

2. Look up the sample log messages listed below for successful and unsuccessful login attempts and review them in AXIS Server Report Viewer or in the central monitoring system.

3. Follow up IP addresses and/or users that seem suspicious and track them throughout the network to understand the source these requests are made from.

4. Check if there are unknown user accounts configured in the web interface of the Axis device and delete them. It is also recommended to change the password of authorized/known user accounts.

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

Requires the **Access Log parameter to be enabled from **Plain Config > System**.*
***Only login attempts using the correct username will be logged. This log message is only available from AXIS OS 10.4 and onwards.*

PreventDosAttack***

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.`

****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.*

Network access

Verify open network ports and protocols

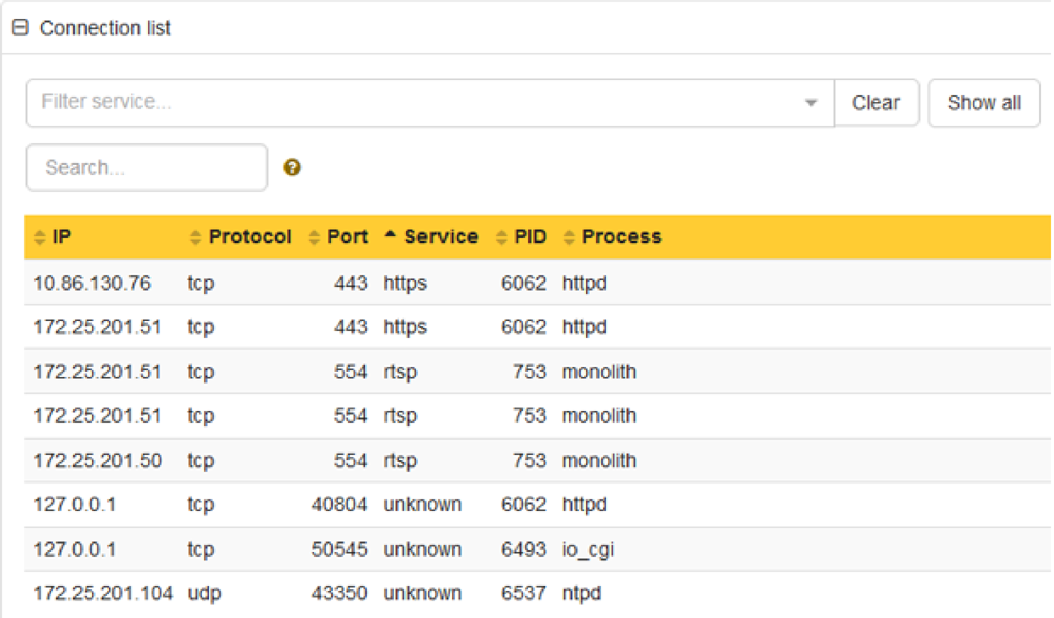
Some enabled services and functionality in Axis devices require certain network protocols and corresponding ports to be opened by the Axis device. It is recommended to check if changes in the configuration of enabled network protocols have been made.

Checklist

1. Learn more about the commonly used network protocols and ports of the Axis device. Note that some are enabled by default, and that some are configuration dependent. Read more *here*.

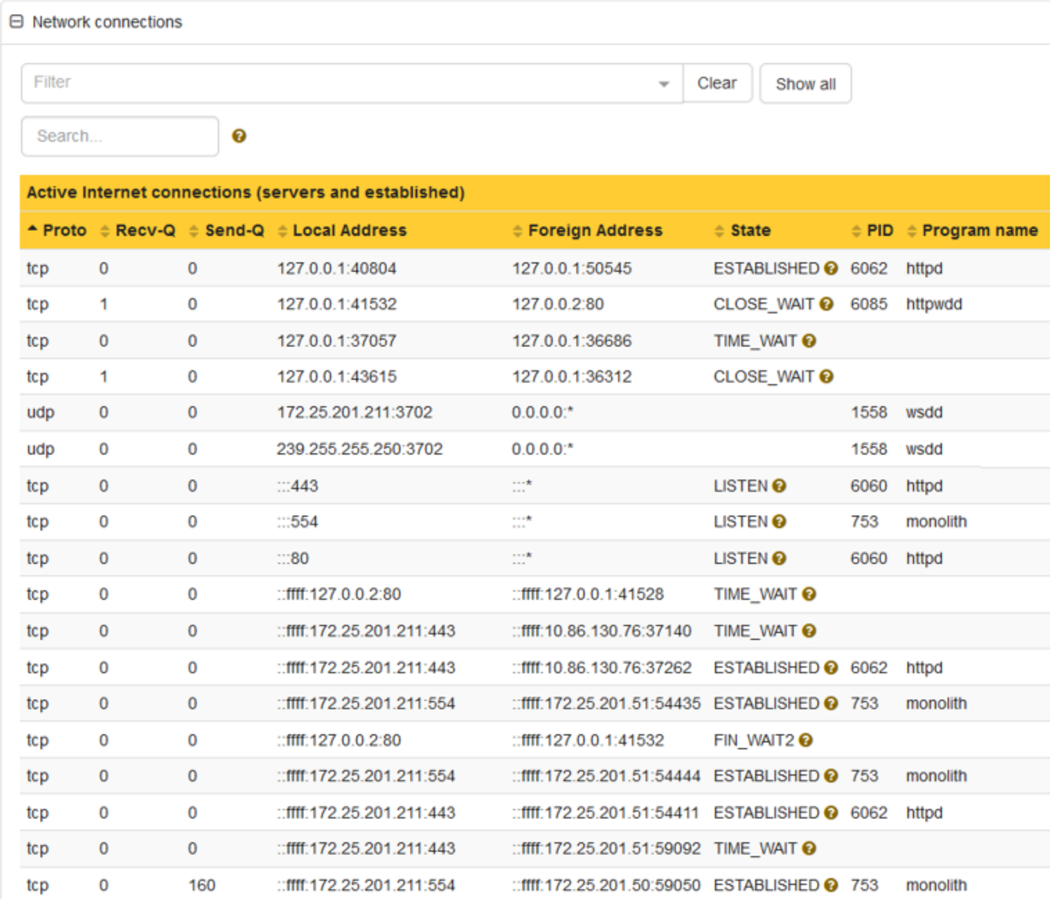
2. Download a server report from the Axis device and use AXIS Server Report Viewer to analyze the currently enabled network protocols and open ports. Review the following two telemetric sections within the report:

   - The list in the **Connection list** section is a simple list that outlines all current active network connections from the Axis device to other network hosts.



IP	Protocol	Port	Service	PID	Process
10.86.130.76	tcp	443	https	6062	httpd
172.25.201.51	tcp	443	https	6062	httpd
172.25.201.51	tcp	554	rtsp	753	monolith
172.25.201.51	tcp	554	rtsp	753	monolith
172.25.201.50	tcp	554	rtsp	753	monolith
127.0.0.1	tcp	40804	unknown	6062	httpd
127.0.0.1	tcp	50545	unknown	6493	io_cgi
172.25.201.104	udp	43350	unknown	6537	ntpd

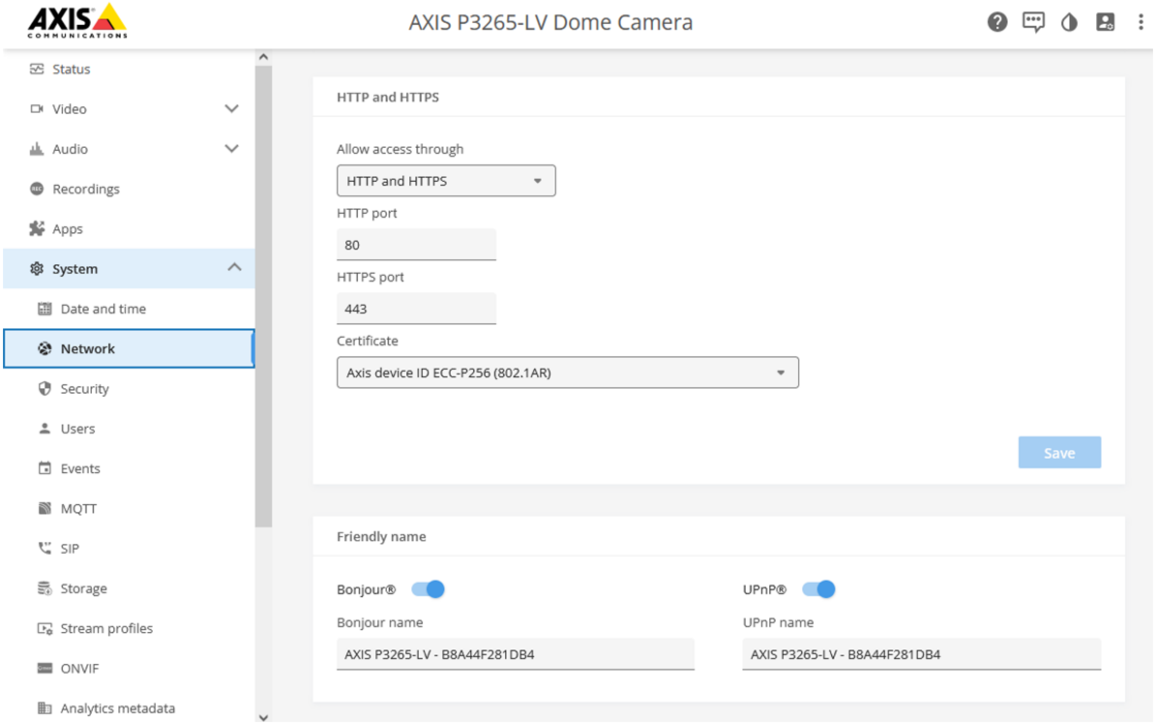
   - The list in the **Network connections** section is a more sophisticated list that includes more information about source and destination ports, IP addresses of the current, ongoing, and to some extent previous network connections, as well as which open ports the Axis device is listening to. Consider the authorized/known IP addresses that are supposed to access Axis device and use as a starting point to understand if there are other IP addresses that currently access the Axis device. Go to *Verify authorized network access on page 15* for information on how to verify the authenticity.



Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID	Program name
tcp	0	0	127.0.0.1:40804	127.0.0.1:50545	ESTABLISHED	6062	httpd
tcp	1	0	127.0.0.1:41532	127.0.0.2:80	CLOSE_WAIT	6085	httpwdd
tcp	0	0	127.0.0.1:37057	127.0.0.1:36686	TIME_WAIT		
tcp	1	0	127.0.0.1:43615	127.0.0.1:36312	CLOSE_WAIT		
udp	0	0	172.25.201.211:3702	0.0.0.0:*		1558	wsdd
udp	0	0	239.255.255.250:3702	0.0.0.0:*		1558	wsdd
tcp	0	0	:::443	:::*	LISTEN	6060	httpd
tcp	0	0	:::554	:::*	LISTEN	753	monolith
tcp	0	0	:::80	:::*	LISTEN	6060	httpd
tcp	0	0	::ffff:127.0.0.2:80	::ffff:127.0.0.1:41528	TIME_WAIT		
tcp	0	0	::ffff:172.25.201.211:443	::ffff:10.86.130.76:37140	TIME_WAIT		
tcp	0	0	::ffff:172.25.201.211:443	::ffff:10.86.130.76:37262	ESTABLISHED	6062	httpd
tcp	0	0	::ffff:172.25.201.211:554	::ffff:172.25.201.51:54435	ESTABLISHED	753	monolith
tcp	0	0	::ffff:127.0.0.2:80	::ffff:127.0.0.1:41532	FIN_WAIT2		
tcp	0	0	::ffff:172.25.201.211:554	::ffff:172.25.201.51:54444	ESTABLISHED	753	monolith
tcp	0	0	::ffff:172.25.201.211:443	::ffff:172.25.201.51:54411	ESTABLISHED	6062	httpd
tcp	0	0	::ffff:172.25.201.211:443	::ffff:172.25.201.51:59092	TIME_WAIT		
tcp	0	160	::ffff:172.25.201.211:554	::ffff:172.25.201.50:59050	ESTABLISHED	753	monolith

3. Vital port configurations can also be obtained from the web interface of the Axis device, such as HTTP (80) and HTTPS (443), as well as UPnP (49152) and Bonjour (5353).



AXIS P3265-LV Dome Camera

HTTP and HTTPS

Allow access through: HTTP and HTTPS

HTTP port: 80

HTTPS port: 443

Certificate: Axis device ID ECC-P256 (802.1AR)

Friendly name

Bonjour®: on

Bonjour name: AXIS P3265-LV - B8A44F281DB4

UPnP®: on

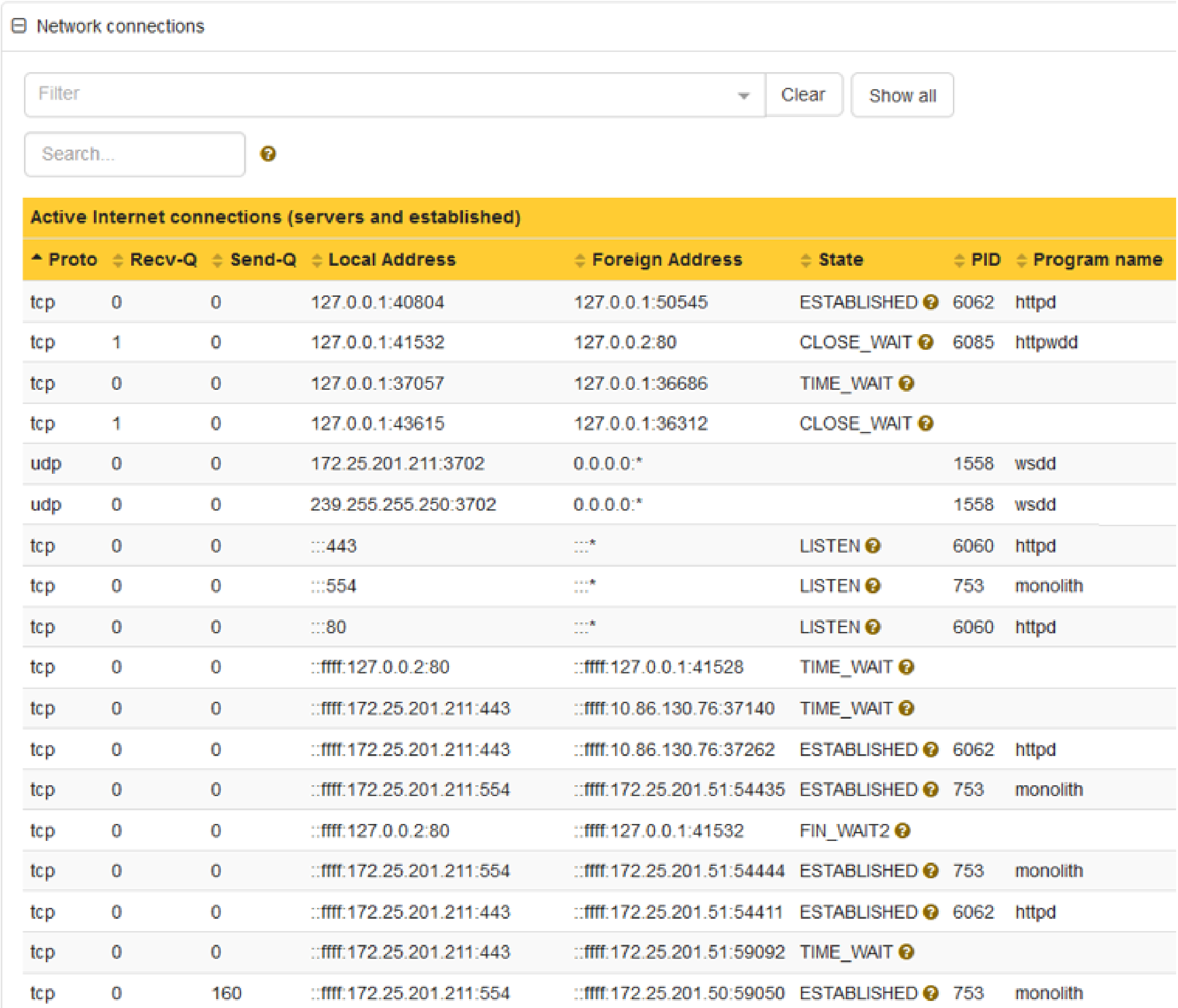
UPnP name: AXIS P3265-LV - B8A44F281DB4

Verify authorized network access

As described in the checklist in *Verify open network ports and protocols on page 13*, the list in the **Network connections** section in AXIS Server Report Viewer includes detailed information about the network ports and connections of the Axis device. It is recommended to review the list and verify the authenticity of the IP addresses that access the Axis device.

Checklist

1. Consider the authorized/known IP addresses that are supposed to access the Axis device.
2. Summarize a list of IP addresses that are unknown and track them throughout the network to understand their purpose.
3. It is recommended to enable network access control on the Axis device according to AXIS OS Hardening Guide or to apply the described techniques on the network infrastructure to allow access to authorized network hosts only.



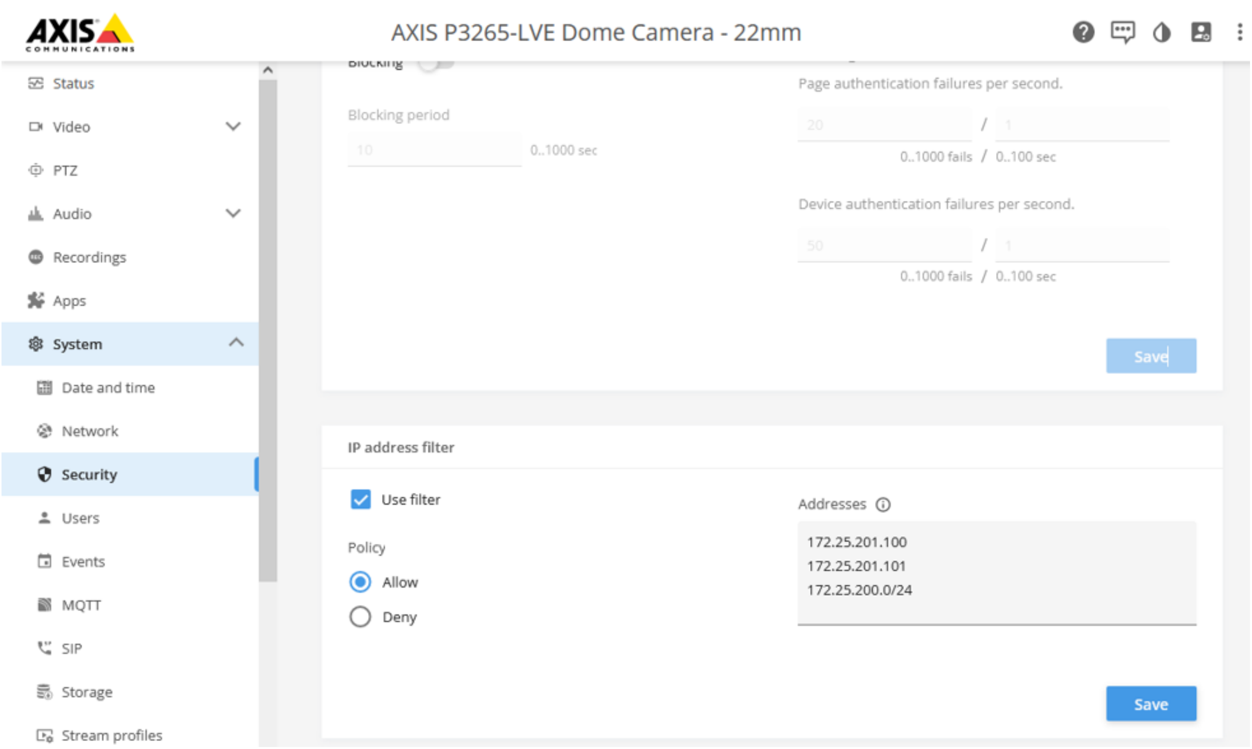
Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID	Program name
tcp	0	0	127.0.0.1:40804	127.0.0.1:50545	ESTABLISHED	6062	httpd
tcp	1	0	127.0.0.1:41532	127.0.0.2:80	CLOSE_WAIT	6085	httpwdd
tcp	0	0	127.0.0.1:37057	127.0.0.1:36686	TIME_WAIT		
tcp	1	0	127.0.0.1:43615	127.0.0.1:36312	CLOSE_WAIT		
udp	0	0	172.25.201.211:3702	0.0.0.0:*		1558	wsdd
udp	0	0	239.255.255.250:3702	0.0.0.0:*		1558	wsdd
tcp	0	0	:::443	:::*	LISTEN	6060	httpd
tcp	0	0	:::554	:::*	LISTEN	753	monolith
tcp	0	0	:::80	:::*	LISTEN	6060	httpd
tcp	0	0	::ffff:127.0.0.2:80	::ffff:127.0.0.1:41528	TIME_WAIT		
tcp	0	0	::ffff:172.25.201.211:443	::ffff:10.86.130.76:37140	TIME_WAIT		
tcp	0	0	::ffff:172.25.201.211:443	::ffff:10.86.130.76:37262	ESTABLISHED	6062	httpd
tcp	0	0	::ffff:172.25.201.211:554	::ffff:172.25.201.51:54435	ESTABLISHED	753	monolith
tcp	0	0	::ffff:127.0.0.2:80	::ffff:127.0.0.1:41532	FIN_WAIT2		
tcp	0	0	::ffff:172.25.201.211:554	::ffff:172.25.201.51:54444	ESTABLISHED	753	monolith
tcp	0	0	::ffff:172.25.201.211:443	::ffff:172.25.201.51:54411	ESTABLISHED	6062	httpd
tcp	0	0	::ffff:172.25.201.211:443	::ffff:172.25.201.51:59092	TIME_WAIT		
tcp	0	160	::ffff:172.25.201.211:554	::ffff:172.25.201.50:59050	ESTABLISHED	753	monolith

Verify network access control configuration

To restrict network access to an Axis device, it is recommended to enable network access control (IP filtering) to ensure that only selected network hosts are allowed to connect. Go to *AXIS OS Hardening Guide* to read more.

In the event of a security incident, it is recommended to check the current configuration of the network access control settings to learn if the configuration has been altered.



Blocking period: 10 (0..1000 sec)

Page authentication failures per second. 20 / 1 (0..1000 fails / 0..100 sec)

Device authentication failures per second. 50 / 1 (0..1000 fails / 0..100 sec)

IP address filter

☑ Use filter

Policy

● Allow

○ Deny

Addresses

172.25.201.100
172.25.201.101
172.25.200.0/24

Identify failed network access attempts

As outlined in AXIS OS Hardening Guide, network access control can be enabled to restrict the number of network hosts that are allowed to access the Axis device. In addition, further logging of network access attempts can be enabled to learn if undesired network access attempts are made from other network hosts.

Unsuccessful network attempts are logged and can be reviewed using AXIS Server Report Viewer and the sections **Combined Logs** and **Kernel Logs**.

IP filtering*

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`

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*** *in the* ***IP Filtering*** *section.*

PreventDosAttack**

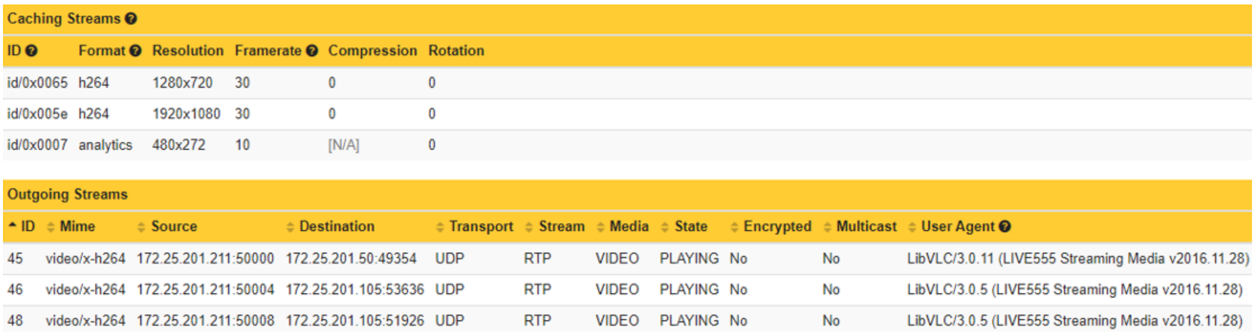
Unsuccessful	AXIS OS 11.5 and lower	`[ WARNING ] httpd[22254]: [evasive20:warn] [pid 22254:tid 1428104112] [client 172.25.201.116:42058] Blacklisting address 172.25.201.116: possible DoS attack.`
Unsuccessful	AXIS OS 11.6 and higher	`[ WARNING ] httpd[22254]: [evasive20:warn] [pid 22254:tid 1428104112]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

***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.*

Streaming access

Verify clients accessing video and audio streams

The server report of the Axis device can be used to learn more about the amount of currently delivered video and audio streams to network hosts. The number of caching streams are the unique encoded video streams of an Axis device, while the **Outgoing Streams** section reflects the currently served clients these video streams are delivered to. More information about video streaming in Axis devices is available *here*.



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)

Checklist

1. Consider the authorized/known IP addresses that are supposed to access the Axis device in your network.
2. Cross-reference the list of authorized IP addresses with the metrics from the **Outgoing Streams** section.
3. Summarize a list of IP addresses that are unknown and track them throughout the network to understand their purpose and if they are supposed to access video and audio data.
4. It is recommended to either enable network access control on the Axis device according to the AXIS OS Hardening Guide, or to 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

Failed login attempts from network hosts are generally logged in the system log of the Axis device. It is recommended to enable further enhanced logging via the access log, as described in *AXIS OS Hardening Guide*. Login attempts can be reviewed using AXIS Server Report Viewer, in the **Combined Logs** section. If the Axis device is configured to stream its logs to a central monitoring system, this can also be used to review the logs.

Checklist

1. Video and audio streams are delivered by the HTTP(S) and/or the RTSP protocol, meaning login attempts related to these protocols are of interest.

2. Look up the sample log messages listed below for successful and unsuccessful login attempts and review them in AXIS Server Report Viewer or in the central monitoring system.

3. Follow up IP addresses and/or users that seem suspicious and track them throughout the network to understand the source these requests are made from.

4. Check if there are unknown user accounts configured in the web interface of the Axis device and delete them. It is also recommended to change the password of authorized/known user accounts.

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

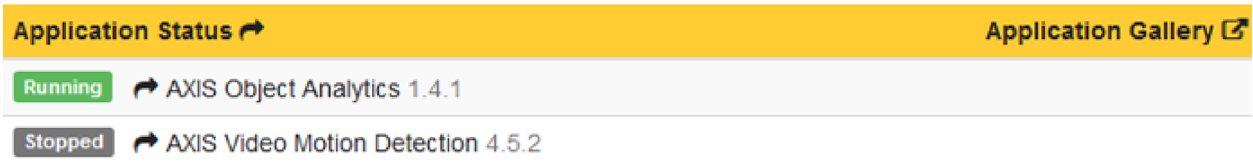
Successful*	`[ NOTICE ] httpd[22254]: root from 10.197.240.111 /axis-cgi/admin/accesslog.cgi GET 200`
Unsuccessful**	`[ NOTICE ] httpd[21459]:  root from 10.197.240.111 failed to access /axis-cgi/usergroup.cgi.Password mismatch`

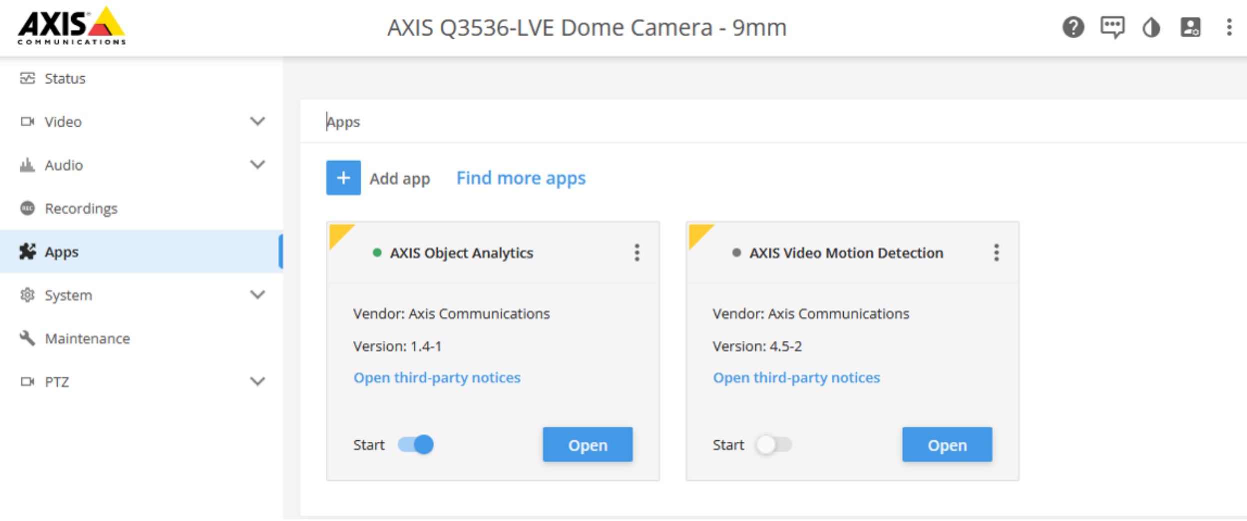
Requires the **Access Log parameter to be enabled from **Plain Config** > **System**.*
***Only login attempts using the correct username will be logged.*

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. Recommendations on how to operate applications are outlined in a dedicated section of *AXIS OS Hardening Guide*.


Application Status
Application Gallery
Running
AXIS Object Analytics 1.4.1
Stopped
AXIS Video Motion Detection 4.5.2



AXIS Q3536-LVE Dome Camera - 9mm

● AXIS Object Analytics

Vendor: Axis Communications

Version: 1.4-1

● AXIS Video Motion Detection

Vendor: Axis Communications

Version: 4.5-2

Ver. M7.2

AXIS OS Forensics Guide

Date: November 2022

Part no.